T-AUD
658.5
MAX



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

Auditoría y Control de Gestión

"Administración de Riesgos de Tecnología de Información de una Empresa del Sector Informático"

TESIS DE GRADO

Previa a la obtención del Título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentada por:

Jennifer Dennise Maxitana Cevallos

GUAYAQUIL – ECUADOR

AÑO

2.005

AGRADECIMIENTO

En primer lugar a Dios por que sin Él, esto no hubiera sido posible.

A mis padres, mi hermana Lissette y mi abuela por su amor, apoyo incondicional y constante sacrificio.

A todos mis familiares y amigos (Fabrizzio, Naty, Noé y Vivi) por estar siempre conmigo.

A mi Directora de Tesis por su gran ayuda y colaboración.

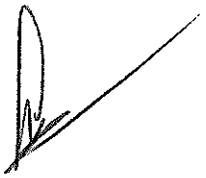
A todos... GRACIAS POR CREER EN MI.

DEDICATORIA

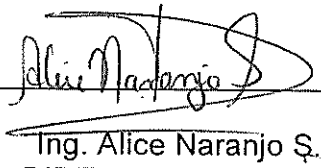
A Marco, Alicia, Lissette, David y Luzmila por ser lo más importante en mi vida.

A mis familiares y amigos por formar parte de la misma.

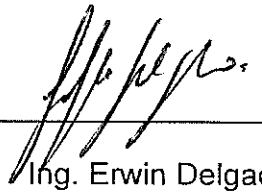
TRIBUNAL DE GRADUACIÓN



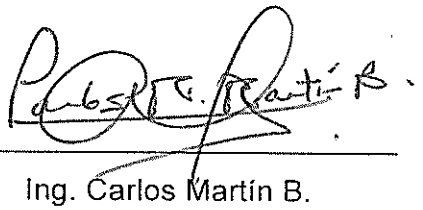
Ing. Félix Ramírez C.
Presidente



Ing. Alice Naranjo S.
DIRECTOR DE TESIS



Ing. Erwin Delgado B.
VOCAL



Ing. Carlos Martín B.
VOCAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado me corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL".



Jennifer Maxitana Cevallos

RESUMEN

La Tecnología de Información (TI) se ha convertido en el corazón de las operaciones de cualquier organización, desde los sistemas transaccionales que ayudan a las operaciones transaccionales diarias hasta las aplicaciones enfocadas a la alta gerencia que contribuyen a definir el rumbo que tiene que seguir una organización, por esta razón es importante preservar una seguridad razonable en la organización.

Una seguridad razonable se consigue con la identificación de los riesgos y la implementación de controles en toda la organización sin dejar a un lado al área de TI.

La Administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Debe juzgar cual puede ser el nivel tolerable, particularmente si se tiene en cuenta el análisis costo-beneficio; esto puede ser una decisión difícil para la Administración. Por esta razón, la Administración debe trabajar en la identificación de los riesgos y en la consiguiente Administración de los mismos.

El presente trabajo muestra una alternativa de administración de riesgos, en una empresa del sector informático, cuyo objetivo principal es satisfacer las necesidades de sus clientes dando garantía de su trabajo. El nombre de este proyecto es: "Administración de Riesgos de Tecnología de Información de una empresa del sector informático" y presenta los principales controles y seguridades que deben implementarse en uno de los departamentos de la empresa como es el caso del departamento de sistemas.

ÍNDICE GENERAL

Pág.

RESUMEN..... VI

INDICE GENERAL..... VII

INDICE DE FIGURAS..... XI

INDICE DE TABLAS..... XIII

INTRODUCCION..... 1

1. ANTECEDENTES..... 2

1.1. La Evolución de la Tecnología de Información..... 2

1.1.1. Importancia de Tecnología de Información..... 4

1.1.2. Los Tipos de Tecnologías..... 6

1.1.2.1. Tecnología Aplicable..... 6

1.1.2.2. Tecnología Necesaria..... 8

1.1.2.3. Tecnología Deseada..... 9

1.1.3. La Necesidad del Control en la Tecnología de Información..... 10

1.1.3.1. El Ambiente de Negocios: Competencia, Cambio y Costos..... 12

1.1.4. La Administración y los Riesgos..... 13

1.1.5. Aparición del Gobierno de la Empresa y el Gobierno

de TI..... 15

2. MARCO TEÓRICO: ADMINISTRACIÓN DE RIESGOS DE TI..... 19

2.1. Fundamentación Teórica..... 19

2.1.1. Riesgos..... 19

2.1.1.1. Concepto..... 19

2.1.1.2. Clasificación de Riesgos..... 20

2.1.1.2.1. Riesgo de Negocio..... 20

2.1.1.2.2. Riesgo Inherente..... 20

2.1.1.2.3. Riesgo de Auditoria..... 20

2.1.1.2.4. Riesgo de Control..... 21

2.1.1.2.5. Riesgo Estratégico..... 21

2.1.1.2.6. Riesgo Operativo..... 21

2.1.1.2.7. Riesgo Financiero..... 22

2.1.1.2.8. Riesgo de Cumplimiento..... 22

2.1.1.2.9. Riesgo de Tecnología..... 22

2.1.1.2.10. Riesgo Profesional..... 23

2.1.1.2. Tipos de Causas de Riesgos..... 23

2.1.2. Riesgos de Tecnología de Información..... 25

2.1.2.1. Concepto..... 25

2.1.2.2. Valoración del Riesgo..... 25

2.1.2.3 Identificación del Riesgo..... 26

2.1.2.4. Análisis del Riesgo..... 27

2.1.2.4.1. Objetivo General del Análisis de Riesgo..... 27

2.1.2.4.2. Objetivos Específicos del Análisis de Riesgo..... 29

2.1.2.5. Matriz de Priorización de los Riesgo..... 30

2.1.2.6. Determinación del Nivel de Riesgo..... 32

2.1.2.7. Manejo del Riesgo..... 33

2.1.2.7.1. Plan de Manejo de Riesgos..... 35

2.1.2.8. Matriz de Riesgos..... 37

2.1.2.8.1.Utilidad del Método Matricial para el análisis de Riesgos..... 37

2.1.2.8.1. Tipos de Matrices de Riesgos..... 37

2.1.2.8.2.1. Matriz de Riesgos Críticos Vs. Escenarios de Riesgo..... 37

2.1.2.8.2.2. Matriz de Riesgos Críticos Vs. Dependencias.... 39

2.1.2.8.2.3. Localización de los Riesgos Críticos en Matriz de Dependencias Vs Escenarios de Riesgo..... 40

2.1.3.- Administración de Riesgos..... 41

2.1.3.1. Definición..... 42

2.1.3.2. Beneficios para la Organización..... 42

2.1.3.3. Beneficios para el Dpto. de Auditoria..... 43

2.1.3.4. Factores a considerar..... 43

2.1.4. Administración de Riesgos de Tecnología de Información..... 44
2.1.4.1. Concepto..... 44
2.1.4.2. Beneficios..... 45
2.1.4.3. Características Generales..... 47
2.1.4.4. Proceso de Administración de Riesgo de T.I..... 47
2.1.4.4.1. Establecimiento de la Metodología de TI..... 48
2.1.4.4.2. Identificación de Riesgos de TI..... 49
2.1.4.4.3. Análisis del Riesgo de TI..... 50
2.1.4.4.4. Evaluación y Priorización de Riesgo de TI..... 51
2.1.4.4.5.Tratamiento de Riesgo de TI (Controles Definitivos)..... 52
2.1.4.4.6. Monitoreo y Revisión..... 54
2.1.4.5. Metodologías de Administración de Riesgos de TI y Seguridad..... 55
2.1.4.5.1. Introducción a las Metodologías..... 55
2.1.4.5.1.1. Los Procedimientos de Control..... 57
2.1.4.5.1.2. Tecnología de Seguridad..... 58
2.1.4.5.1.3. Las Herramientas de Control..... 58
2.1.4.5.2. Metodologías de Evaluación de Sistemas..... 59
2.1.4.5.2.1. Conceptos Fundamentales..... 59
2.1.4.5.2.2. Tipos de Metodologías..... 61

2.1.4.5.2.2.1. Metodologías Cuantitativas..... 62

2.1.4.5.2.2.2. Metodologías Cualitativas..... 64

2.1.4.5.2.3. Metodologías más comunes..... 66

2.1.4.5.2.3.1. Metodologías de Análisis de Riesgo..... 66

2.1.4.5.2.3.1.1. Metodología MAGERIT..... 68

2.1.4.5.2.3.1.2. Metodología MARION..... 72

2.1.4.5.2.3.1.3. Metodología RISCKPAC..... 73

2.1.4.5.2.3.1.4. Metodología CRAMM..... 73

2.1.4.5.2.3.1.5. Metodología PRIMA..... 74

2.1.4.5.2.3.1.6. Metodología DELPHI..... 77

2.1.4.5.3. Metodologías de Auditoría Informática..... 83

2.1.4.5.4. Metodologías de Clasificación de la Información y de Obtención de los Procedimientos de Control.. 84

2.1.4.5.4.1. Clasificación de la Información..... 84

2.1.4.5.4.2. Obtención de los Procedimientos de Control..... 87

2.1.4.5.5. Metodología de Evaluación de Riesgos..... 90

2.2. Definiciones Conceptuales..... 91

3. NORMAS Y/O ESTÁNDARES INTERNACIONALES..... 101

3.1. Ley Sarvanes- Oxley..... 101

3.1.1. SEC. 404: Evaluación de la Gerencia de los Controles

Internos: Regulaciones Requeridas..... 102

3.1.1.2. Evaluación del Control Interno..... 103

3.2. Normas COBIT..... 103

3.2.1. Audiencia: Administración, Usuarios y Auditores..... 104

3.2.1.1. Administración / Gerencia..... 105

3.2.1.2. Usuarios..... 105

3.2.1.3. Auditores..... 105

3.2.2. Principios..... 105

3.2.3. Procesos de TI..... 106

3.2.3.1. Dominios..... 106

3.2.3.2. Procesos..... 106

3.2.3.3. Actividades..... 107

3.2.4. Proceso 9: Análisis de Riesgo..... 107

3.2.4.1. Actividad 1: Evaluación de Riesgos del Negocio:

Objetivo de Control..... 107

3.2.4.2. Actividad 2: Enfoque de Evaluación de Riesgos:

Objetivo de Control..... 108

3.2.4.3. Actividad 3: Identificación de Riesgos: Objetivo de

Control..... 108

3.2.4.4. Actividad 4: Medición de Riesgos: Objetivo de

Control..... 109

3.2.4.5. Actividad 5: Pian de Acción contra Riesgos: Objetivo

de Control..... 109
3.2.4.6. Actividad 6: Aceptación de Riesgos: Objetivo de Control..... 110
3.2.4.7. Actividad 7: Selección de Garantías o Protecciones: Objetivo de Control..... 110
3.2.4.8. Actividad 8: Compromiso con el Análisis de Riesgos: Objetivo de Control..... 111
3.3. COSO Report..... 111
3.3.1. Conceptos Fundamentales..... 113
3.3.2. Componentes..... 114
3.3.3. Controles..... 118
3.3.3.1. Controles generales..... 118
3.3.3.2. Ambientes de control..... 118
3.3.3.3. Controles directos..... 119
3.4. ISO 17999..... 119
3.4.1. Estructura de la Norma ISO 17799:2000..... 120
3.4.1.1. Política de Seguridad de la Información..... 120
3.4.1.2. Organización de la Seguridad..... 120
3.4.1.3. Clasificación y Control de Activos..... 121
3.4.1.4. Seguridad del Personal..... 121
3.4.1.5. Seguridad Física y Ambiental..... 121
3.4.1.6. Gestión de Comunicaciones y Operaciones..... 121

3.4.1.7. Control de Accesos..... 122

3.4.1.8. Desarrollo y mantenimiento de Sistemas..... 122

3.4.1.9. Administración de la Continuidad de los Negocios. 123

3.4.1.10. Cumplimiento..... 123

3.4.2. Beneficios de la Norma..... 123

3.5. S.A.C. (Systems Auditability and Control)..... 124

3.5.1. Definición..... 125

3.5.2. Componentes..... 125

3.5.3. Clasificaciones..... 126

3.5.3.1. Controles Preventivos, Detectivo, Correctivo..... 126

3.5.3.2. Discrecional vs. No Discrecional..... 127

3.5.3.3. Voluntario vs. Mandatorio..... 127

3.5.3.4. Manual vs. Automático..... 128

3.5.3.5. Aplicación vs. General..... 128

3.5.4. Objetivos de Control y Riesgos..... 129

4. ADMINISTRACIÓN DE RIESGOS DE TI DE UNA EMPRESA DEL SECTOR INFORMÁTICO..... 130

4.1. Información Preliminar..... 130

4.1.1. Introducción..... 130

4.1.2. Motivos del Análisis de Riesgo..... 132

4.1.2.1.Ausencia de personal técnico en el tema de

riesgo..... 133
4.1.2.2. Desconocimiento de los Riesgos Informáticos que existen en la organización..... 133
4.1.2.3. Desconocimiento de Metodologías de Administración de Riesgos de TI..... 134
4.1.3. Objetivo General del Análisis de Riesgo..... 135
4.1.3.1. Objetivos Específicos del Análisis de Riesgo..... 135
4.1.3.1.1. Revisar, Evaluar y Actualizar aspectos relacionados tendientes a un control efectivo de de Administración de Riesgo..... 136
4.1.3.1.2. Asegurar una mayor integridad, confidencialidad y confiabilidad de la información..... 137
4.1.3.1.3. Dar a conocer información acerca de los Riesgos Informáticos que existen en la empresa 137
4.1.4. Alcance del Análisis de Riesgo..... 138
4.1.4.1. Evaluar las seguridades físicas del departamento 138
4.1.4.2. Evaluar las seguridades lógicas del departamento 139
4.1.4.3. Definir los controles que deben implantarse..... 139
4.2 Descripción del entorno informático..... 140
4.2.1. Arquitectura informática..... 144
4.2.1.1. Entorno de red..... 144
4.2.1.2. Equipos disponibles..... 144

4.2.1.3. Sistema operativo..... 145
4.2.1.4. Software de sistemas y utilitarios..... 144
4.2.1.4.1. Lenguaje de Programación..... 145
4.2.1.4.2. Sistemas de Aplicación..... 145
4.2.1.4.3. Utilitarios..... 146
4.3. Estrategia de Administración de Riesgos..... 147
4.3.1. Establecer Metodología..... 147
4.3.2.- Identificar Riesgos..... 147
4.3.3. Análisis de Riesgos..... 149
4.3.3.1. Valorar el Riesgo Inherente..... 149
4.3.3.2. Determinar controles existentes..... 150
4.3.3.3. Identificar Nivel de exposición..... 150
4.3.3.4. Método Matricial para el análisis de riesgos..... 151
4.3.3.4.1 Crear la Matriz de Amenazas y Objetos..... 151
4.3.3.4.2. Categorización de Riesgos..... 151
4.3.4. Diseñar los controles definitivos..... 154
4.3.5. Presentar los Resultados..... 154
4.3.5.1. Informe de los Resultados..... 154

5. CONCLUSIONES Y RECOMENDACIONES..... 164

ANEXOS

BIBLIOGRAFÍA

ÍNDICE DE FIGURAS

Pág.

Figura 2.1. Matriz de Priorización de Riesgos..... 30

Figura 2.2. Proceso de Administración de Riesgos de TI..... 48

Figura 2.3. Funcionamiento Esquemático básico de cualquier metodología..... 66

Figura 2.4. Fases de la metodología PRIMA..... 75

Figura 2.5. Lista de Ayuda de la Metodología PRIMA..... 77

Figura 3.1. Principios de COBIT..... 105

Figura 3.2. Niveles de COBIT..... 106

ÍNDICE DE TABLAS

Pág.

Tabla I Etapas de la Identificación del Riesgo..... 27

Tabla II Matriz de Frecuencias de Revisiones de Sistemas..... 31

Tabla III Matriz de Localización de Riesgos Potenciales Críticos en los escenarios de Riesgos..... 38

Tabla IV Matriz de Localización de los Riesgos Críticos en las Dependencias..... 39

Tabla V Mapa de Riesgos Potenciales Críticos..... 41

Tabla VI Comparación entre las Metodologías Cuantitativas y Cualitativas..... 65

Tabla VII Ejemplo de Lista de Control..... 91

INTRODUCCIÓN

En este mundo globalizado y de constantes cambios, las empresas obligadamente requieren ser cada vez más ágiles y se deben adaptar con mayor facilidad a estos cambios.

Actualmente, las organizaciones dependen en su totalidad de tener la información exacta en el momento preciso, las compañías que no son capaces de alcanzar esto, están en peligro de extinción porque con el paso de los años, la información se ha convertido en el arma más potente para la toma decisiones, y es aquí donde radica la prioridad de desarrollar nuevas tecnologías que permitan tener la información requerida y lista para ser uti[illegible]la. Sin embargo, la mayoría de las organizaciones han fallado al no ap[illegible]echar el ambiente existente e implementar ideas innovadoras para mejorar el [illegible]apel que juegan los sistemas de información dentro de sus organizaciones, algunos de estos errores son:

- Resistencia al cambio por parte de la gente
- Deficiencias para reconocer amenazas competitivas rápidamente.
- Robustez de los sistemas de información.

- Escasez de recursos apropiados
- Incertidumbre de cómo o porqué automatizar procesos

Los sistemas y la información que estos guardan debe por consiguiente ser protegida y preservada, para ello es necesario hacer un estudio real de las amenazas y de las formas en que las mismas pueden ser reducidas., por esta razón, el presente trabajo tiene como una de sus metas primordiales el orientar, sobre los aspectos importantes que se deben considerar en la Administración de Riesgos de Tecnología de Información en todas las empresas, narra en especial una aplicación de la administración de riesgos en una empresa del sector informático.

Debido a la trascendencia de los controles y seguridades de los sistemas de procesamiento de información que ameritan ser implementados, este trabajo pretende enfatizar y relevar la importancia y la significación de la Administración de Riesgos en TI, por ello se ha bosquejado una temática amplia y diversa en un lenguaje sencillo que resalta el cómo y qué se debe hacer en la Administración de riesgos de TI .

En el primer capítulo se revisa un poco la historia de la Tecnología de Información (TI) y la situación actual del mercado competitivo, en lo que respecta a la Administración de Riesgos y a la Tecnología de Información.

En la segunda parte se presenta todo el marco conceptual, dejando claro los conceptos y procesos para la iniciación del proyecto.

En el tercer capítulo, se muestra las normas y estándares internacionales sobre los cuales tiene que regirse la elaboración de este trabajo.

En la cuarta parte se lleva a cabo el desarrollo de la Administración de Riesgos, detectándose las falencias durante el análisis y determinando las soluciones respectivas puestas a consideración de la Gerencia de la empresa.

En la quinta y última parte, se muestran las conclusiones y recomendaciones correspondientes.

CAPÍTULO 1

1. ANTECEDENTES.

1.1. La Evolución de Tecnología de Información

La historia recoge cómo un singular sistema que empleaba antorchas sobre torres distantes, permitió en fecha tan lejanas como el siglo 300 AC, la transmisión de los 25 combinaciones correspondientes a cada una de las letras del alfabeto griego, pero no es hasta mediados del pasado siglo 19 que se muestran los reales avances tecnológicos.

El fin de siglo, en particular ha estado marcado por una convergencia tecnológica hasta el momento independiente. Esta convergencia que experimenta la Informática y las Telecomunicaciones.

Como resultado de tal confluencia comienzan a generalizarse conceptos nuevos como: "Tecnología de Información", "Sociedad del Conocimiento" o "Era de la Información".

La Tecnología de Información ha sido conceptualizada como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, sus principales componentes son: el factor humano, los contenidos de la información, el equipamiento, la infraestructura material, el software y los mecanismos de intercambio electrónico de información, los elementos de política y regulaciones y los recursos financieros.

Si analizamos detenidamente estos componentes nos damos cuenta que son los principales protagonistas del desarrollo informático, en una sociedad tanto para su desarrollo como para su aplicación.

Los factores claves han sido:

- La microelectrónica que ha posibilitado el descomunal avance en la potencia y capacidad de cómputo de los ordenadores.
- Los avances en las telecomunicaciones han provocado explosión del uso de las redes de alcances locales y globales.
- El desarrollo acelerado de programas y aplicaciones que se generalizan acercándose más al "gran público" mediante

interfaces de fácil comunicación, agradables con el uso de las técnicas de multimedia.

Estos factores hacen que cada día los costos se reduzcan y por tanto se amplíe el uso de estos medios en otros sectores, no sólo en la academia militar o industrial, sino en el sector empresarial, en la salud, la educación, el ocio y los propios hogares.

La Tecnología de Información se ha convertido en el corazón de las operaciones de cualquier organización, desde los sistemas transaccionales que ayudan a las operaciones diarias hasta las aplicaciones enfocadas a la alta gerencia que contribuyen a definir el rumbo que tiene que seguir una organización. Dentro de las operaciones de una organización, una de las tendencias que está tomando mayor relevancia es la del outsourcing de procesos que están en tu cadena de valor pero que la organización se la encarga a un tercero. Por otro lado las operaciones de una organización tienen que seguir ciertos estándares y lineamientos y a su vez esto puede provocar cambios en la manera de realizar las cosas.

1.1.1. Importancia de Tecnología de Información.- En este mundo globalizado y de constantes cambios, las empresas obligadamente requieren ser cada vez más ágiles y se deben adaptar con mayor facilidad a estos cambios.

Actualmente, las compañías dependen en su totalidad de tener la información exacta en el momento preciso, las empresas que no son capaces de alcanzar esto, están en peligro de extinción porque con el paso de los años la información se ha convertido en el arma más potente para la toma decisiones, y es aquí donde radica la prioridad de desarrollar nuevas tecnología que permitan tener la información requerida y lista para ser utilizada.

Una frase de Sir Francis Bacon dice: "El conocimiento es poder", las empresas que saben manejar la información, tienen el poder de tomar decisiones que las beneficien y es aquí donde la tecnología de información juega un papel fundamental, porque las empresas pueden tener una ventaja competitiva sostenible que les permita estar por encima de sus competidores.

Sin embargo, la mayoría de las organizaciones han fallado al no aprovechar el ambiente existente e implementar ideas innovadoras para mejorar el papel que juegan los sistemas de información dentro de sus organizaciones, algunos de estos errores son:

- Resistencia al cambio por parte de la gente
- Deficiencias para reconocer amenazas competitivas rápidamente.
- Robustez de los sistemas de información.
- Escasez de Recursos apropiados
- Incertidumbre de cómo o porqué automatizar procesos

1.1.2. Los Tipos de Tecnologías.- A continuación se definen los tres tipos de tecnologías vigentes en la actualidad. Estos son:

1.1.2.1. Tecnología Aplicable: La TI[1], como muchas otras tecnologías, han cambiado paulatinamente su papel en las organizaciones:

En los comienzos del desarrollo de la TI[1], ésta se utilizaba para

realizar tareas rutinarias y repetitivas -por ejemplo: impresiones de listas "sábanas" fuera de horario de atención-, las cuales eran muy costosas en tiempo y dinero y eran consideradas como un costo extra en las actividades que las utilizaban.

A medida que transcurrió el tiempo, la tecnología se hizo más permisiva económicamente y empezó a realizar tareas más completas y complejas: libros contables, facturación. etc.

Luego de esto, la TI[1] empieza a integrar todas las actividades de la empresa, tratando de convertirse en una herramienta de soporte para la toma de decisiones y para el logro de objetivos estratégicos. Su costo de obtención sigue disminuyendo y ya no se la considera como un costo inherente a las actividades, sino como una inversión.

---

[1] TI: Tecnología de Información

Hoy en día, las posibilidades que la TI[1] nos da, es la de ser en sí misma la ventaja competitiva del negocio, los costos de obtención han disminuido exponencialmente, y es considerada para la empresa, junto con el SI, como un activo más.

Por lo tanto, la TI[1] juega también un papel importante, no sólo como herramienta de implementación de partes del Sistema de Información (SI), sino por las oportunidades que por sí misma abre a las empresas.

1.1.2.2. Tecnología Necesaria: Según Michael Porter: "De todas las cosas que pueden cambiar las reglas de competencia, el cambio tecnológico está entre las más prominentes." Pero el uso de la tecnología de información no es importante por sí mismo, es importante si trae consigo el logro de una ventaja competitiva. La tecnología de información es importante para la competencia si afecta de manera significativa la ventaja competitiva de la empresa.

[1] TI: Tecnología de Información

Por tanto, la tecnología de información es más o menos necesaria siempre en función de los objetivos estratégicos que persiga el negocio.

1.1.2.3. Tecnología Deseada: La tecnología de información implica cambios, no solo los más obvios como por ejemplo, usar impresoras para realizar una factura, en lugar de confeccionarla a mano.

También hay otros, tales como los provocados por la idiosincrasia que la envuelve por ejemplo, los vendedores de tiendas virtuales han tenido que aprender nuevos métodos de inducción a la compra mediante un canal no utilizado hasta el momento: Internet y el acelerado ritmo de evolución de las tecnologías de información aplicadas.

Y los cambios, hoy en día, pueden verse desde dos puntos de vistas: amenazas del medio que prometen efectos negativos u oportunidades de negocio que implican futuras fortalezas; y dado que actualmente "el cambio es una constante", deberíamos capitalizarlo de la forma que más nos convenga, a pesar de que al principio pareciera natural del ser humano la resistencia a él.

La gente es renuente al cambio, aún cuando pueda muy bien redundar en beneficio propio. Cicerón formuló esta máxima hace más de dos mil años: "No se le pueden conferir beneficios a quien no los quiera". Por consiguiente, si un cambio es algo impuesto a alguien, no se producirá.

1.1.3. La Necesidad de Control en la Tecnología de Información.-

En años recientes, ha sido cada vez más evidente la necesidad de un marco referencial para la seguridad y el control de tecnología de información. Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticalidad emerge de:

- La creciente dependencia de información y de los sistemas que proporcionan dicha información
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información

- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información; y
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, así como para crear nuevas oportunidades y reducir costos.

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa.

Verdaderamente, la información y los sistemas de información son "penetrantes" en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos). Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener una apreciación y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

1.1.3.1. El Ambiente de Negocios: Competencia, Cambio y Costos: La competencia global es ya un hecho. Las organizaciones se reestructuran con el fin de perfeccionar sus operaciones y al mismo tiempo aprovechar los avances en Tecnología de Información para mejorar su posición competitiva.

La reingeniería en los negocios, las reestructuraciones, el outsourcing, el empoderamiento, las organizaciones horizontales y el procesamiento distribuido son cambios que impactan la manera en la que operan tanto los negocios como las entidades gubernamentales. Estos cambios han tenido y continuarán teniendo, profundas implicaciones para la administración y las estructuras de control operacional dentro de las organizaciones en todo el mundo.

La especial atención prestada a la obtención de ventajas competitivas y a la eficiencia en costos implica una dependencia creciente en la tecnología como el componente más importante en la estrategia de la mayoría de las organizaciones. La automatización de las funciones organizacionales, por su naturaleza, dicta la incorporación de mecanismos de control más poderosos en las computadoras y en las redes, tanto para las basadas en hardware como las basadas en

software. Además, las características estructurales fundamentales de estos controles están evolucionando al mismo paso que las tecnologías de computación y las redes.

Dentro del marco referencial de cambios acelerados, si los administradores, los especialistas en sistemas de información y los auditores desean en realidad ser capaces de cumplir con sus tareas en forma efectiva , deberán aumentar y mejorar sus habilidades tan rápidamente como lo demandan la tecnología y el ambiente. Debemos comprender la tecnología de controles involucrada y su naturaleza cambiante si deseamos emitir y ejercer juicios razonables y prudentes al evaluar las prácticas de control que se encuentran en los negocios típicos o en las organizaciones gubernamentales.

1.1.4 La Administración y los Riesgos.- Se debe decidir cual es la inversión razonable en seguridad y en control de Tecnología de Información y cómo lograr un balance entre riesgos e inversiones en el enfoque de control en un ambiente de Tecnología de Información, frecuentemente impredecible. Mientras la seguridad y los controles en los sistemas de información ayudan a administrar los riesgos sin eliminarlos, surge la necesidad de administrar esos riesgos. Puesto

que el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

La Administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Debe juzgar cual puede ser el nivel tolerable, particularmente si se tiene en cuenta el costo-beneficio, esto puede ser una decisión difícil para la Administración. Por esta razón, la Administración necesita un marco de referencia de las prácticas generalmente aceptadas de control y seguridad de Tecnología de información para compararlos contra el ambiente de Tecnología de Información existente y planeado.

Existe una creciente necesidad entre los usuarios de los servicios de Tecnología de Información, de estar protegidos a través de la acreditación y la auditoría de servicios de Tecnología de Información proporcionados internamente o por terceras partes, que aseguren la existencia de controles y seguridades adecuadas. Actualmente, sin embargo, es confusa la implementación de buenos controles de Tecnología de Información en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos

de evaluación, como las evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, COBIT, entre otras. Como resultado, los usuarios necesitan que se establezca una base general como un primer paso.

Frecuentemente, los auditores han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar su opinión acerca de los controles internos frente a la Gerencia.

Sin contar con un marco referencial, la Auditoria se convierte en una tarea demasiado complicada. Incluso, la administración consulta cada vez más a los auditores para que la asesoren en forma proactiva en lo referente a asuntos de seguridad y control de TI[1].

1.1.5. Aparición del Gobierno de la Empresa y del Gobierno de TI[1].- Para lograr el éxito en esta economía de información, el Gobierno de la empresa y el Gobierno de TI[1] no pueden ser consideradas separadamente y en distintas disciplinas.

[1] TI: Tecnología de Información

El gobierno efectivo de la empresa enfoca el conocimiento y la experiencia en forma individual y grupal, donde puede ser más productivo, monitoreado y medido el desempeño así como provisto el aseguramiento para aspectos críticos.

La Tecnología de Información, por mucho tiempo considerada aislada dentro del logro de los objetivos de la empresa debe ahora ser considerada como una parte integral de la estrategia.

El Gobierno de TI[1] provee la estructura que une los procesos de TI[1], los recursos de TI[1] y las estrategias y objetivos de la empresa. El Gobierno de TI[1] integra e institucionaliza de una manera óptima la planeación y organización, la adquisición e implementación, la entrega de servicios y soporte y el monitoreo del desempeño de TI[1].

El Gobierno de TI[1] es integral para el éxito de! Gobierno de la Empresa asegurando una eficiente y efectiva medición para mejorar los procesos de la empresa.

---

[1] TI: Tecnología de Información

El Gobierno de TI[1] le permite a la empresa tomar ventaja total de su información, al maximizar sus beneficios, capitalizar sus oportunidades y ganar ventaja competitiva. Observando en el contexto a la empresa y los procesos del Gobierno de TI[1] con mayor detalle, el gobierno de la empresa, el sistema por el cual las entidades son dirigidas y controladas direcciona y analiza el Gobierno de TI[1].

Al mismo tiempo, TI[1] debería proveer insumos críticos y constituirse en un componente importante de los planes estratégicos. De hecho TI[1] puede influenciar las oportunidades estratégicas de la empresa. Las actividades de la empresa requieren información de las actividades de TI[1] con el fin de satisfacer los objetivos del negocio. Organizaciones exitosas aseguran la interdependencia entre su plan estratégico y sus actividades de TI[1]. TI[1] debe estar alineado y debe permitir a la empresa tomar ventaja total de su información para maximizar sus beneficios, capitalizar oportunidades y ganar ventaja competitiva.

---

[1] TI: Tecnología de Información

Las empresas son gobernadas por buenas (o mejores) prácticas generalmente aceptadas para asegurar que la empresa cumpla sus metas asegurando que lo anterior esté garantizado por ciertos controles. Desde estos objetivos fluye la dirección de la organización, la cual dicta ciertas actividades a la empresa usando sus propios recursos.

Los resultados de las actividades de la empresa son medidos y reportados proporcionando insumos para el mantenimiento y revisión constante de los controles, comenzando el ciclo de nuevo.

También TI[1] es gobernado por buenas prácticas para asegurar que la información de la empresa y sus tecnologías relacionadas apoyan sus objetivos del negocio, estos recursos son utilizados responsablemente y sus riesgos deben ser manejados apropiadamente. Estas prácticas conforman una base para la dirección de las actividades de TI[1] y deben ser tomadas en cuenta en el manejo de riesgo (para obtener seguridad, confiabilidad y cumplimiento) para incrementar la efectividad y eficiencia de las organizaciones.

---

[1] TI: Tecnología de Información

CAPÍTULO 2

2. MARCO TEÓRICO: ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN.

2.1.- Fundamentación Teórica

2.1.1.- Riesgos

2.1.1.1. Conceptos: Se definen tres conceptos de Riesgos a continuación:

Según Fernando Izquierdo Duarte: "El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos".

Según Alberto Cancelado González: "El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas".

Según Martín Vilches Troncoso: "El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio. Es decir es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no-ocurrencia de uno deseado".

2.1.1.2. Clasificación de Riesgos.-

2.1.1.2.1. Riesgo de Negocios: Es el riego de los negocios estratégicos de la empresa y de sus procesos claves. En otras palabras es un riesgo crítico de la empresa.

2.1.1.2.2. Riesgo Inherente: Es la posibilidad de errores o irregularidades en la información financiera, administrativa u operativa, antes de considerar la efectividad de los controles internos diseñados y aplicados por el ente.

2.1.1.2.3. Riesgo de Auditoría: Existe al aplicar los programas de auditoría, cuyos procedimientos no son suficientes para descubrir errores o irregularidades significativas.

2.1.1.2.4. Riesgo de Control: Está asociado con la posibilidad de que los procedimientos de control interno, incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores e irregularidades significativas de manera oportuna.

2.1.1.2.5. Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con el cumplimiento de la misión de la Entidad, la cual busca la vigilancia de la conducta de los servidores públicos, defender el orden jurídico y los derechos fundamentales.

2.1.1.2.6. Riesgo Operativo: Comprende tanto el riesgo en sistemas como operativo provenientes de deficiencias en los sistemas de información, procesos, estructura, que conducen a ineficiencias, oportunidad de corrupción o incumplimiento de los derechos fundamentales.

2.1.1.2.7. Riesgo Financiero: Se relaciona con las exposiciones financieras de la empresa. El manejo del riesgo financiero toca actividades de tesorería, presupuesto, contabilidad y reportes financieros, entre otros.

2.1.1.2.8. Riesgo de Cumplimiento: Se asocia con la capacidad de la empresa para cumplir con los requisitos regulativos, legales, contractuales, de ética pública, democracia y participación, servicio a la comunidad, interacción con el ciudadano, respeto a los derechos, a la individualidad, la equidad y la igualdad.

2.1.1.2.9. Riesgo de Tecnología: Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa y soporten el cumplimiento de la misión.

2.1.1.2.10. Riesgo Profesional: Conjunto de entidades públicas y privadas, normas y procedimientos, destinados a prevenir, proteger y atender a los trabajadores de los efectos, de las enfermedades y los accidentes que puedan ocurrirles con ocasión o como consecuencia del trabajo que desarrollan.

2.1.1.3. Tipos de Causas de Riesgos de TI: Las causas de riesgo más comunes, para efectos del tema, se dividen en:

- Externas e
- Internas.

Las causas de riesgo externas pueden ser de dos clases:

- Naturales y
- Motivadas por el Hombre.

Las causas de riesgo naturales son normalmente las siguientes:

- Inundaciones
- Temblores
- Tornados

- Tormentas Eléctricas
- Huracanes
- Erupciones Volcánicas

Las causas de riesgo originadas por el hombre, son entre otras, las siguientes:

- Incendios
- Explosiones
- Accidentes laborales
- Destrucción intencional
- Sabotaje
- Robo
- Fraude
- Contaminación Ambiental

Las causas internas de riesgo, se generan a partir de las mismas empresas. Son más frecuentes las causas internas de riesgo que las causas externas.

Entre las causas internas de riesgo tenemos básicamente:

- Robo: de materiales, de dinero y de información
- Sabotaje
- Insuficiencia de Dinero
- Destrucción: de datos y de recursos
- Personal No capacitado
- Huelgas
- Fraudes
- Ausencia de seguridades físicas tanto de la empresa como dela información.

2.1.2. Riesgos de Tecnología de Información.-

2.1.2.1. Concepto: El concepto de riesgo de TI puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Es el control el que actúa sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

2.1.2.2. Valoración del Riesgo: La valoración del riesgo consta de tres etapas: La identificación, el análisis y la determinación del nivel

del riesgo. Para cada una de ellas es necesario tener en cuenta la mayor cantidad de datos disponibles y contar con la participación de las personas que ejecutan los procesos y procedimientos para lograr que las acciones determinadas alcancen los niveles de efectividad esperados. Para adelantarlas deben utilizarse las diferentes fuentes de información.

2.1.2.3. Identificación del Riesgo: El proceso de la identificación del riesgo debe ser permanente, integrado al proceso de planeación y responder a las preguntas qué, como y por qué se pueden originar hechos que influyen en la obtención de resultados.

Una manera de realizar la identificación del riesgo es a través de la elaboración de un mapa de riesgos, el cual como herramienta metodológica permite hacer un inventario de los mismos ordenada y sistemáticamente, definiendo en primera instancia los riesgos, posteriormente presentando una descripción de cada uno de ellos y las posibles consecuencias.

TABLA I

ETAPAS DE LA IDENTIFICACIÓN DEL RIESGO

RIESGO.	DESCRIPCIÓN	POSIBLES CONSECUENCIAS
Posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.	Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado	Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros

2.1.2.4. Análisis del Riesgo:

2.1.2.4.1. Objetivo General del Análisis de Riesgo: Su objetivo es establecer una valoración y priorización de los riesgos con base en la

información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

Probabilidad: La posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque éste no se haya presentado nunca.

Para el análisis cualitativo se establece una escala de medida cualitativa en donde se establecen unas categorías a utilizar y la descripción de cada una de ellas, con el fin que cada persona la aplique, por ejemplo:

ALTA: Es muy factible que el hecho se presente

MEDIA: Es factible que el hecho se presente

BAJA: Es poco factible que el hecho se presente

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Ese mismo diseño puede aplicarse para la escala de medida cualitativa de IMPACTO, estableciendo las categorías y la descripción, por ejemplo:

ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la Entidad.

MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.

BAJO: Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

2.1.2.4.2. Objetivos Específicos del Análisis de Riesgo:

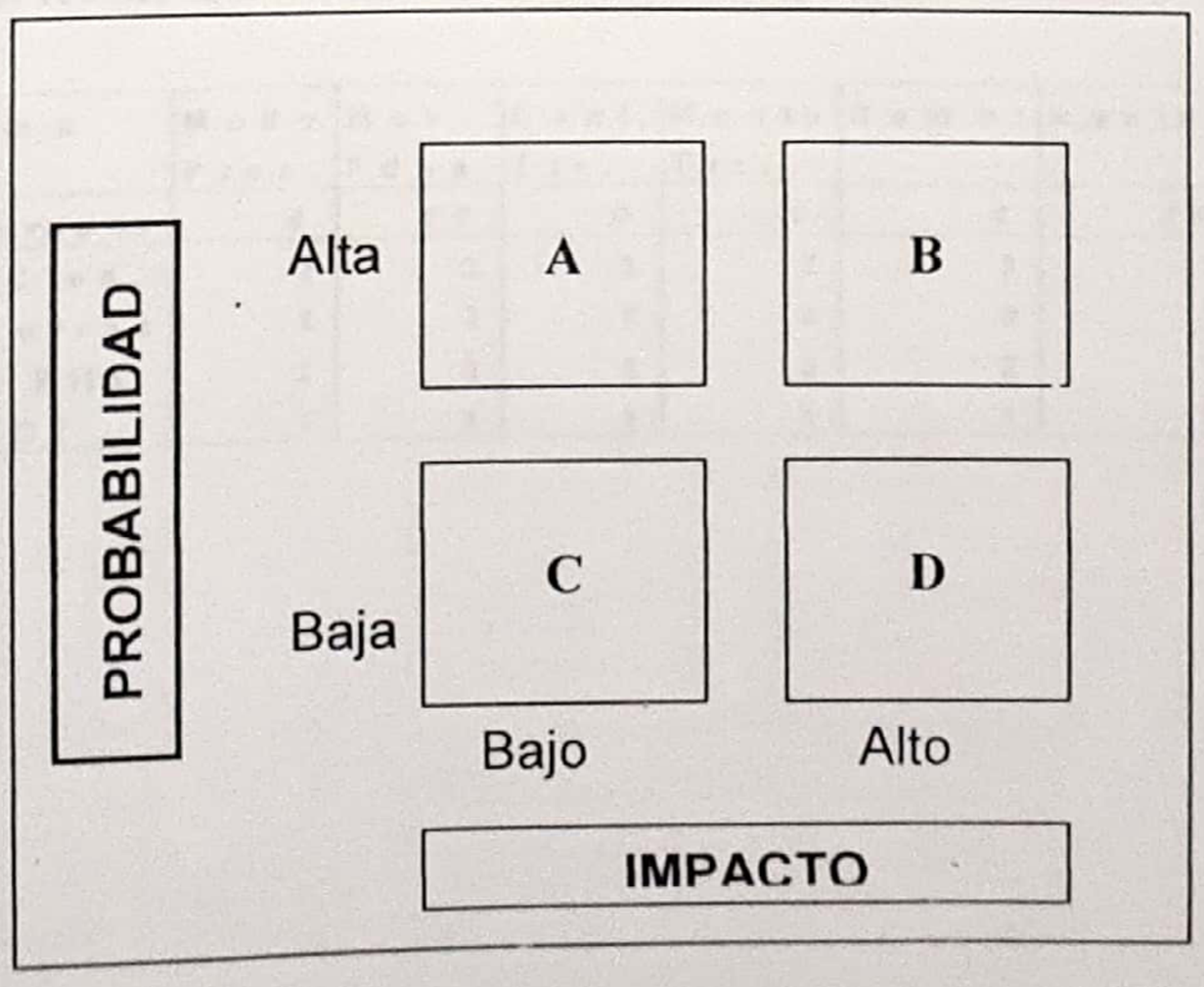
- Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.

- Definir cuáles son los recursos existentes.
- Llevar a cabo un minuciosos análisis de los riesgos y debilidades.
- Identificar, definir y revisar todos los controles de seguridad ya existentes.
- Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados.

2.1.2.5. Matriz de Priorización de los Riesgos: Una vez realizado el análisis de los riesgos con base en los aspectos de probabilidad e impacto, se recomienda utilizar la matriz de priorización que permite determinar cuales riesgos requieren de un tratamiento inmediato.

FIGURA 2.1.

MATRIZ DE PRIORIZACIÓN DE RIESGOS



Cuando se ubican los riesgos en la matriz se define cuales de ellos requieren acciones inmediatas, que en este caso son los del cuadrante B, es decir los de alto impacto y alta probabilidad, respecto a los riesgos que queden ubicados en el cuadrante A y D, se debe seleccionar de acuerdo a la naturaleza del riesgo, ya que estos pueden ser peligrosos para el alcance de los objetivos institucionales por las consecuencias que presentan los ubicados en el cuadrante D o por la constante de su presencia en el caso del cuadrante A.

Podemos citar como ejemplo, una matriz de frecuencia de revisión de sistemas, donde cada índice tiene una ponderación y cada cuenta del sistema es analizada y calificada de acuerdo a la ponderación determinada.

TABLA II

MATRIZ DE FRECUENCIA DE REVISIÓN DE SISTEMAS

Sistema	Modo Proc.	Mov. Fdos.	Cant. Trx.	Monto Trx.	Compl.	Rentab	Irreg.
Ponderador	*4*	*10*	*6*	*8*	*4*	*10*	*10*
Ctas.Ctes.	3	3	3	2	3	3	2
C. Ahorros	3	3	2	2	3	2	2
Plazo Fijo	3	3	2	3	2	1	1
Inf. DGI	1	1	1	1	1	1	1

2.1.2.6. Determinación del Nivel del Riesgo: La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Para adelantar esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser:

ALTO: Cuando el riesgo hace altamente vulnerable a la entidad o dependencia. (Impacto y probabilidad alta versus controles existentes)

MEDIO: Cuando el riesgo presenta una vulnerabilidad media. (Impacto aito - probabilidad baja o Impacto bajo - probabilidad alta versus controles existentes).

BAJO: Cuando el riesgo presenta vulnerabilidad baja.(Impacto y probabilidad baja versus controles existentes).

Lo anterior significa que a pesar que la probabilidad y el impacto son altos confrontado con los controles se puede afirmar que el nivel de riesgo es medio y por lo tanto las acciones que se implementen

entraran a reforzar los controles existentes y a valorar la efectividad de los mismos.

2.1.2.7. Manejo del Riesgo: Cualquier esfuerzo que emprendan las entidades en torno a la valoración del riesgo llega a ser en vano, si no culmina en un adecuado manejo y control de los mismos definiendo acciones factibles y efectivas, tales como la implantación de políticas, estándares, procedimientos y cambios físicos entre otros, que hagan parte de un plan de manejo.

Para el manejo del riesgo se pueden tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

Evitar el riesgo: Es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

Reducir el riesgo: Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

Dispersar y atomizar el riesgo: Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar ejemplo de ello el procedimiento utilizado por la Oficina de Sistemas para la salvaguarda de la información que se genera diariamente en la Entidad.

Transferir el riesgo: Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros; se traslada el riesgo a otra parte o físicamente se traslada a otro lugar. Esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

Asumir el riesgo: Luego que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene. En este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidos cuáles de los anteriores manejos del riesgo se van a concretar, éstos deben evaluarse con relación al beneficio-costo para definir, cuáles son susceptibles de ser aplicados y proceder a elaborar el plan de manejo de riesgo, teniendo en cuenta, el análisis elaborado para cada uno de los riesgos de acuerdo con su impacto, probabilidad y nivel de riesgo.

Posteriormente se definen los responsables de llevar a cabo las acciones especificando el grado de participación de las dependencias en el desarrollo de cada una de ellas. Así mismo, es importante construir indicadores, entendidos como los elementos que permiten determinar de forma práctica el comportamiento de las variables de riesgo, que van a permitir medir el impacto de las acciones.

2.1.2.7.1. Plan de manejo de Riesgos: Para elaborar el plan de manejo de riesgos es necesario tener en cuenta si las acciones

propuestas reducen la materialización del riesgo y hacer una evaluación jurídica, técnica, institucional, financiera y económica, es decir considerar la viabilidad de su adopción. La selección de las acciones más convenientes para la entidad se puede realizar con base en los siguientes factores:

a) el nivel del riesgo

b) el balance entre el costo de la implementación de cada acción contra el beneficio de la misma.

Una vez realizada la selección de las acciones más convenientes se debe proceder a la preparación e implantar del plan, identificando responsabilidades, programas, resultados esperados, medidas para verificar el cumplimiento y las características del monitoreo. El éxito de la adopción y/o ejecución del plan requiere de un sistema gerencial efectivo el cual tenga claro el método que se va a aplicar.

Es importante tener en cuenta que los objetivos están consignados en la planeación anual de la entidad, por tal razón se sugiere incluir el plan de manejo de riesgos dentro de la planeación, con el fin de no solo alcanzar los objetivos sino de definir también las acciones.

2.1.2.8. Matriz de Riesgos:

2.1.2.8.1. Utilidad del Método Matricial para el análisis de Riesgos:

Este método utiliza una matriz para mostrar gráficamente tanto las amenazas a que están expuestos los sistemas computarizados como los objetos que comprenden el sistema.

Dentro de cada celda se muestran los controles que atacan a las amenazas.

2.1.2.8.2. Tipos de Matrices de Riesgo:

2.1.2.8.2.1. Matriz de Riesgos Críticos Vs. Escenarios de Riesgo: En esta se representan los escenarios o puntos del proceso que pueden ser impactados por los riesgos potenciales críticos. Con una "x" se señalan las celdas en donde podría presentarse cada riesgo. Para completar el significado de esta matriz, en hoja separada se describe la forma como podría presentarse cada riesgo en los diferentes escenarios marcado con "x".

TABLA III

MATRIZ DE LOCALIZACIÓN DE RIESGOS POTENCIALES

CRÍTICOS EN LOS ESCENARIOS DE RIESGO

LOCALIZACION DE RIESGOS CRÍTICOS EN LOS ESCENARIOS DE RIESGO

Proceso de Negocio o Sistema : CDTs.

No	Escenario de Riesgo	Fraude	Exceso de Egresos	Sanciones legales	Pérdida Credibilidad
1	Generación y Registro de Transacciones	X		X	
2	Ingreso de los datos al sistema	X			
3	Procesamiento de las transacciones y actualización de la base de datos	X	X	X	X
4	Utilización y control de los resultados por parte de los usuarios del sistema		X		
5	Custodia de títulos valores			X	X
6	Registro contable de las transacciones			X	X

2.1.2.8.2.2. Matriz de Riesgos Críticos Vs. Dependencias. En esta se representan las dependencias que pueden ser impactadas por los riesgos potenciales críticos. Con una "x" se señalan las celdas en donde podría presentarse cada riesgo. Para completar el significado de esta matriz, en hoja separada se describe la forma como podría presentarse cada riesgo en las dependencias marcadas con "x".

TABLA IV

MATRIZ DE LOCALIZACIÓN DE LOS RIESGOS CRÍTICOS EN LAS DEPENDENCIAS

LOCALIZACION DE RIESGOS CRÍTICOS EN LAS DEPENDENCIAS QUE MANEJAN LA INFORMACION

Proceso de Negocio o Sistema : CDTs.

No	*Dependencias*	*Fraude*	*Exceso de Egresos*	*Sanciones legales*	*Pérdida Credibilidad*
1	*Sucursales*	*X*		*X*	
2	*Dpto. de Sistemas*	*X*	*X*	*X*	
3	*Contabilidad*			*X*	
4	*DECEVAL*				*X*

2.1.2.8.2.3. Localización de los Riesgos Críticos en Matriz de Dependencias Vs Escenarios de Riesgo: Es el resultado de combinar las dos matrices anteriores. En las celdas de esta matriz se escriben las identificaciones de los riesgos críticos que corresponidan. Ver figura 5: Localización de riesgos críticos en las Dependencias que intervienen en el proceso o sistema.

Utilizando códigos de identificación alfanuméricos para los riesgos potenciales críticos, dentro de esta matriz se identifican los riesgos que podrían materializarse en cada pareja "escenario – dependencia".

R1: Fraude. **R2:** Sanciones Legales. **R3:** Pérdida de Credibilidad Pública.

TABLA V

MAPA DE RIESGOS POTENCIALES CRÍTICOS.

LOCALIZACION DE RIESGOS CRÍTICOS EN MATRIZ DE ESCENARIOS DE RIESGO – DEPENDENCIAS

Proceso de Negocio o Sistema . CDTs.

No	Escenario de Riesgo	Sucursales	Sistemas	Deceval	Contabilidad
1	Generación de Transacciones	R1, R2			
2	Ingreso de los datos al sistema	R1			
3	Procesamiento de las transacciones y actualización de la base de datos		R1,R2		
4	Utilización y control de los resultados por parte de los usuarios del sistema	R2			
5	Custodia de títulos valores			R1,R3	
6	Registro contable de las transacciones				R2

2.1.3. Administración de Riesgos.- En la economía global, las organizaciones necesitan tomar riesgos para sobrevivir, la mayoría de ellas necesitan incrementar el nivel de riesgos que toman para ser exitosas a largo plazo. Con el significativo incremento en la

competencia, los objetivos y metas agresivos de las corporaciones se están convirtiendo en norma. Para direccionar este cambio, los líderes mundiales están fortaleciendo sustancialmente sus prácticas de administración de riesgos para asegurar que si las iniciativas o el funcionamiento de las unidades de negocio "se descarrilan", esto se identifique rápidamente poder actuar para corregir la situación.

2.1.3.1. Definición: Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.

Es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

2.1.3.2. Beneficios para la Organización:

- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.

- Mejoramiento continuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.

2.1.3.3. Beneficios para el Departamento de Auditoria:

- Soporta el logro de los objetivos de la auditoria.
- Estandarización en el método de trabajo.
- Integración del concepto de control en las políticas organizacionales.
- Mayor efectividad en la planeación general de Auditoria.
- Evaluaciones enfocadas en riesgos.
- Mayor cobertura de la administración de riesgos.
- Auditorias más efectivas y con mayor valor agregado.

2.1.3.4. Factores a considerar: Los principales factores que se deben considerar en la Administración de Riesgos de TI son:

- Seguridades
- Controles: Preventivos, Detectivos y Correctivos
- Objetivos
- Manuales de usuarios
- Políticas

Si no existe una adecuada consideración de los factores antes descritos y si nuestros controles y seguridades fueran errados, nuestros planes organizacionales, financieros, administrativos y de sistemas se verían seriamente afectados, ya que no sólo el área de sistemas será el afectado.

2.1.4.- Administración de Riesgos de TI.-

2.1.4.1. Concepto: La Administración de Riesgos de TI es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales, frente a los riesgos de TI.

Es entonces la administración de riesgos el término asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos de TI de la organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades de mejora.

2.1.4.2. Beneficios: Se pueden mencionar los siguientes beneficios:

A nivel organizacional:

- Alcance o logro de los objetivos organizacionales.
- Énfasis en prioridades de negocio: permite a los directivos enfocar sus recursos en los objetivos primarios. Tomar acción para prevenir y reducir pérdidas, antes que corregir después de los hechos, es una estrategia efectiva de administración del riesgo.
- Fortalecimiento del proceso de planeación.
- Apoyo en la identificación de oportunidades.
- Fortalecimiento de la cultura de autocontrol.

Al proceso de administración:

- Cambio cultural que soporta discusiones abiertas sobre riesgos e información potencialmente peligrosa. La nueva cultura tolera equivocaciones pero no tolera errores escondidos. La nueva cultura también hace énfasis en el aprendizaje de los errores.
- Mejor administración financiera y operacional al asegurar que los riesgos sean adecuadamente considerados en el proceso de toma de decisiones. Una mejor administración operacional generará servicios más efectivos y eficientes. Anticipando los problemas, los directivos tendrán mayor oportunidad de reacción y tomar acciones. La organización será capaz de cumplir con sus promesas de servicio.
- Mayor responsabilidad de los administradores en el corto plazo. A largo plazc, se mejorarán todas las capacidades de los directivos.

2.1.4.3. Características Generales:

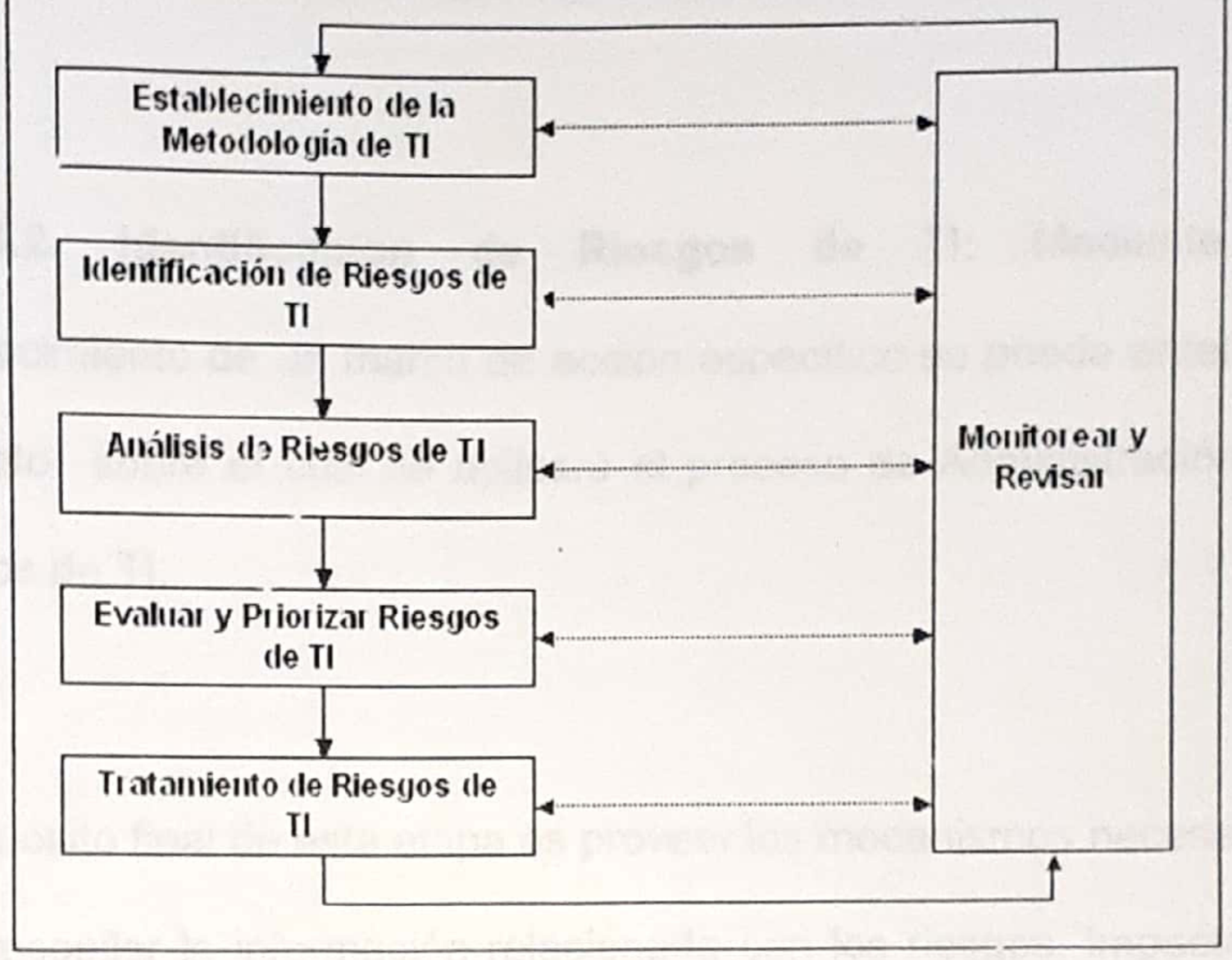
- La Administración de Riesgos debe estar apoyada por la Alta Gerencia de la Organización.
- La Administración de Riesgos debe ser parte integral del proceso administrativo utilizado por la Dirección de la Organización.

La Administración de Riesgos es un proceso multifacético y participativo, el cual es frecuentemente mejor llevado a cabo por un equipo multidisciplinario.

2.1.4.4. Proceso de Administración de Riesgos de TI: A continuación se describen las principales etapas definidas para el Proceso de Administración de Riesgos de TI.

FIGURA 2.2.

PROCESO DE ADMINISTRACIÓN DE RIESGO de TI



2.1.4.4.1. Establecimiento de la Metodología de TI: Permite, a través del conocimiento del entorno y de la organización, establecer criterios generales que serán utilizados para implementar el enfoque de Administración de Riesgos de TI en el área de sistemas de la Organización.

Durante esta etapa se debe establecer la metodología que será utilizada para la Administración de Riesgos de TI en el área de sistemas de la empresa.

Consiste en analizar los riesgos existentes en el área y de acuerdo a este análisis, determinar cual de las alternativas propuestas (metodologías) va a ser la mejor opción para la realización del trabajo.

2.1.4.4.2. Identificación de Riesgos de TI: Mediante el establecimiento de un marco de acción específico se puede entender el objeto sobre el cual se aplicará el proceso de Administración de Riesgos de TI.

El propósito final de esta etapa es proveer los mecanismos necesarios para recopilar la información relacionada con los riesgos, impactos y sus causas.

Algo importante en esta etapa, es tener claro la definición de Riesgo. Para la mayoría de partes, los riesgos son percibidos como cualquier cosa o evento que podría apoyar la forma en que la organización alcance sus objetivos.

Por consiguiente, la Administración de Riesgos de TI no está dirigida exclusivamente a evitarlos. Su enfoque está en identificar, evaluar, controlar y "dominar" los riesgos.

2.1.4.4.3. Análisis del Riesgos de TI: En esta etapa se busca obtener el entendimiento y conocimiento de los riesgos identificados de tal manera que se pueda recopilar información que permita el cálculo del nivel de riesgo al cual está expuesto el objeto, Identificar los controles existentes implementados para mitigar el impacto ante la ocurrencia de los riesgos de TI, permitiendo de esta manera valorar los niveles del riesgo, la efectividad de los controles y el nivel de exposición.

El riesgo de TI es analizado a través de la combinación de estimativos de probabilidad y de las consecuencias en el contexto de las medidas de control existentes. El análisis de riesgos de TI involucra un debido examen de las fuentes de riesgo, sus consecuencias y la probabilidad de que esas consecuencias puedan ocurrir. Pueden llegar a identificarse factores que afectan tanto las consecuencias como la probabilidad.

Los estimativos pueden determinarse utilizando análisis, estadísticas y cálculos. Alternativamente donde no hay datos históricos disponibles, se pueden hacer estimativos subjetivos que reflejen el grado de creencia de un grupo o de un individuo en que un evento en particular o suceso ocurran.

2.1.4.4.4. Evaluación y Priorización de Riesgos de TI: La evaluación de riesgos de TI incluye comparar el nivel de riesgo encontrado durante el proceso de análisis contra el criterio de riesgo establecido previamente, y decidir si los riesgos pueden ser aceptados.

El análisis de riesgos y los criterios contra los cuales los riesgos son comparados en la valoración deben ser considerados sobre la misma base. Así, evaluaciones cualitativas incluyen la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y evaluaciones cuantitativas involucran la comparación de niveles estimados de riesgo contra criterios que pueden ser expresados como números específicos, tales como fatalidad, frecuencia o valores monetarios.

El resultado de una evaluación de riesgos es una lista priorizada de riesgos para definirles acciones de tratamiento posteriores.

Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

2.1.4.4.5. Tratamiento de Riesgos de TI (Controles Definitivos):

Después de valorar y priorizar los riesgos de TI, y dependiendo del nivel de exposición, se debe determinar la opción de tratamiento que más conviene aplicar en cada caso. El tratamiento de riesgos de TI incluye la identificación de la gama de opciones de tratamiento del riesgo de TI, la evaluación de las mismas, la preparación de planes de tratamiento de riesgos de TI y su posterior implementación por parte de la Gerencia de la empresa.

Las opciones de tratamiento que se relacionan a continuación no son mutuamente exclusivas ni serán apropiadas en todas las circunstancias:

EVITAR el riesgo: Se decide, donde sea práctico, no proceder con procesos y/o actividades que podrían generar riesgos inaceptables, buscando con ello eludir el riesgo inherente asociado a esos objetos. Es siempre la primera alternativa que debe considerarse.

REDUCIR el riesgo: La organización decide prevenir y/o reducir el riesgo de TI. Si el riesgo no se puede evitar porque crea grandes dificultades en el departamento, el siguiente paso es reducirlo al más bajo nivel posible, el cual debe ser compatible con las actividades del área. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

REDUCIR la probabilidad de ocurrencia: Prevención del riesgo a través de la implementación de acciones tendientes a controlar su frecuencia o probabilidad.

REDUCIR las consecuencias o MITIGAR el riesgo: reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste ocurre.

ASUMIR el riesgo: La organización decide aceptar los riesgos como ellos existen en la actualidad, y establece políticas o estrategias apropiadas para su tratamiento.

Otra manera de ASUMIR los riesgos, pero debe hacerse a un nivel adecuado en la entidad y considerando que puede ser mucho mayor el costo de la inseguridad que el de la seguridad, lo que a veces sólo se sabe cuando ha ocurrido algo. ¿Cuál es el riesgo máximo admisible que puede permitirse una entidad? Alguna vez se nos ha hecho la pregunta, y depende de lo crítica que sea para la entidad la información así como disponer de ella, e incluso puede depender del momento.

2.1.4.4.6. Monitoreo y Revisión: Pocos riesgos permanecen estáticos. Por ello, los riesgos y la efectividad de sus medidas de control necesitan ser monitoreados continuamente para asegurar que circunstancias cambiantes no alteren las prioridades.

Revisiones progresivas son esenciales para asegurar que los planes de la administración permanecen relevantes. Los factores que afectan

la probabilidad y la consecuencia de un resultado puede cambiar, al igual que los factores que afectan la viabilidad o el costo de las opciones de tratamiento.

2.1.4.5. Metodologías de Administración de Riesgos de TI y Seguridad:

2.1.4.5.1. Introducción a las Metodologías: Según el Diccionario, Método es el "modo de decir o hacer con orden una cosa". Asimismo define el diccionario la palabra Metodología como "conjunto de métodos que se siguen en una investigación científica". Esto significa que cualquier proceso cinético debe estar sujeto a una disciplina de proceso defina con anterioridad que llamaremos Metodología.

La Informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta la auditoria de los sistemas de información.

Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo, y están directamente relacionadas con su

experiencia profesional acumulada como parte del comportamiento humano de "acierto / error".

Asimismo una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo, por lo que resulta habitual el uso de metodologías en las empresas auditoras / consultoras profesionales, desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

La proliferación de metodologías en el mundo de la auditoria y el control informático se pueden observar en los primeros años de la década de los ochenta, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas. Pero el uso de métodos de auditoria es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas cuyo uso de metodologías constituye una práctica habitual. Una de ellas es la seguridad de los sistemas de información.

Aunque de forma simplista se trata de identificar la seguridad informática a la seguridad lógica de los sistemas, nada está más lejos

de la realidad hoy en día, extendiéndose sus raíces a todos los aspectos que suponen riesgos para la informática.

Si definimos la "Seguridad delos Sistemas de Información" como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso.

Por lo tanto, el nivel de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y sus medios de proceso.

2.1.4.5.1.1. Los Procedimientos de Control: Son los procedimientos operativos de las distintas áreas de a empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control y, por tanto, deben de estar documentados y aprobados por la dirección. La tendencia habitual de los informáticos es la de dar más peso a la herramienta que al "control o contramedida", pero no se debe olvidar que "una herramienta nunca es una solución sino una

ayuda para conseguir un control mejor". Sin la existencia de estos procedimientos, las herramientas de control son sólo una anécdota.

2.1.4.5.1.2. Dentro de la **Tecnología de Seguridad** están todos los elementos ya sean hardware o software, que ayudan a controlar un riesgo informático. Dentro de este concepto están los cifradores, autentificadores, equipos "tolerantes al fallo", las herramientas de control, etc.

2.1.4.5.1.3. Las herramientas de control son los elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Todos estos factores están relacionados entre sí, así como la calidad de cada uno con la de los demás. Cuando se evalúa el nivel de Seguridad de Sistemas en una institución, se están evaluando todos estos factores y se plantea un Plan de Seguridad nuevo que mejore todos los factores, aunque conforme se vayan realizando los distintos proyectos del plan, no se irán mejorando todos por igual. Al finalizar el plan se habrá conseguido una situación nueva en la que el nivel de control sea superior al anterior.

Se llamará Plan de Seguridad a una estrategia planificada de acciones y productos que lleven a un sistema de información y sus centros de proceso de una situación inicial determinada (y a mejorar) a una situación mejorada.

2.1.4.5.2. Metodologías de Evaluación de Sistemas:

2.1.4.5.2.1. Conceptos Fundamentales: En el mundo de la seguridad de sistemas se utilizan todas las metodologías necesarias para realizar un plan de seguridad además de las de auditoría informática.

Las dos metodologías de evaluación de sistemas por excelencia son las de Análisis de Riesgos y las de Auditoría Informática, con dos enfoques distintos. La auditoría informática sólo identifica el nivel de "exposición" por la falta de controles, mientras el análisis de riesgos facilita la "evaluación" de los riesgos y recomienda acciones en base al costo-beneficio de las mismas.

Se introducirán una serie de definiciones para profundizar en estas metodologías.

Amenaza: Una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Ejemplo: inundación, incendio, robo de datos, sabotaje, aplicaciones mal diseñadas, etc.

Vulnerabilidad: La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera suceder y así afectar el entorno informático. Ejemplos: falta de control de acceso lógico, inexistencia de un control de soportes magnéticos, falta de cifrado en las telecomunicaciones, etc.

Riesgo: La probabilidad de que una amenaza llegue a suceder por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes.

Exposición o Impacto: La evaluación del efecto del riesgo. Ejemplo: es frecuente evaluar el impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imagen de la empresa, honor, defensa nacional, etc.

Todos los riesgos que se presentan podemos:

- Evitarlos (por ejemplo: no construir un centro donde hay peligro constante de inundaciones).
- Transferirlos (por ejemplo: uso de un centro de cálculo controlado).
- Reducirlos (por ejemplo: sistema de detección y extinción de incendios).
- Asumirlos. Que es lo que se hace si no se controla el riesgo en absoluto.

Para los tres primeros, se actúa si se establecen controles o contramedidas. Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que la probabilidad de que las amenazas se materialicen en hechos (por falta de control) sea lo más baja posible o al menos quede reducida de una forma razonable en costo – beneficio.

2.1.4.5.2.2. Tipos de Metodologías: Todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informático, se pueden agrupar en dos grandes familias. Éstas son:

- Cuantitativas: Basadas en un modelo matemático numérico que ayuda a la realización del trabajo.
- Cualitativas: Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

2.1.4.5.2.2.1. Metodologías Cuantitativas: Este tipo de metodologías han sido diseñadas para producir una lista de riesgos que pueden comparables entre sí, con facilidad de poder asignarles valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos, son datos de probabilidad de ocurrencia de una situación o evento que se debe extraer de un registro de incidencias donde el número de incidencias sea suficientemente grande o tienda al infinito. Esto no se aplica con precisión en la práctica, pero se aproxima ese valor de forma subjetiva restando así rigor científico al cálculo. Pero dado que el cálculo se hace para ayudar a elegir el método entre varias contramedidas podría ser aceptado.

Hay varios coeficientes que conviene definir:

- A.L.E. (Annualized Loss Expentacy): multiplicar la pérdida máxima posible de cada bien /recurso por la amenaza con probabilidad más alta.
- Retorno de la Inversión (R.O.I.): A.L.E. original menos A.L.E. reducido (como resultado de la medida), dividido por el coste anualizado de la medida.
- Reducción del A.L.E. (Annualized Loss Expectancy): Es el cociente entre el coste anualizado de la instalación y el mantenimiento de la medida contra el valor total del bien /recurso que se está protegiendo, en tanto por ciento.

Estos coeficientes y algunos otros son utilizados para la simulación que permite elegir entre varias contramedidas en el análisis de riesgos.

Por consiguiente, se nota con claridad los dos grandes inconvenientes o problemas que presentan estas metodologías: por una parte la debilidad de los datos de la probabilidad de ocurrencia por los pocos registros y la poca significación de los mismos a nivel mundial, y por otra la imposibilidad o dificultad de evaluar económicamente todos los

impactos que pueden suceder frente a la ventaja de poder usar un modelo matemático para el análisis.

2.1.4.5.2.2.2. Metodologías Cualitativas: Precisan de la involucración de un profesional experimentado. Basadas en métodos estadísticos y lógica borrosa (humana, no matemática). Pero requieren menos recursos humanos / tiempo que las metodologías cuantitativas.

La tendencia de uso en la realidad es la mezcla de ambas. A continuaciones muestra un cuadro comparativo de las comparaciones entre estos dos tipos de metodologías:

TABLA VI

COMPARACIÓN ENTRE LAS METODOLOGÍAS CUANTITATIVAS Y CUALITATIVAS

	Cuantitativa	Cualitativa
Pros	- Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas. - Proporciona una cifra justificante para cada contramedida.	- Enfoque lo amplio que se desee. - Plan de trabajo flexible o reactivo. - Se concentra en la identificación de eventos. - Incluye factores intangibles.
Contras	- Estimación de probabilidad depende de estadísticas fiables inexistentes. - Estimación de las pérdidas potenciales sólo si son valores cuantificables. - Metodologías estándares. - Difíciles de mantener o modificar. - Dependencia de un profesional.	- Depende fuertemente de la habilidad y calidad del personal involucrado. - Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar la guía). - Identificación de eventos reales más claros al no tener que aplicarles probabilidades complejas de calcular. - Dependencia de un profesional.

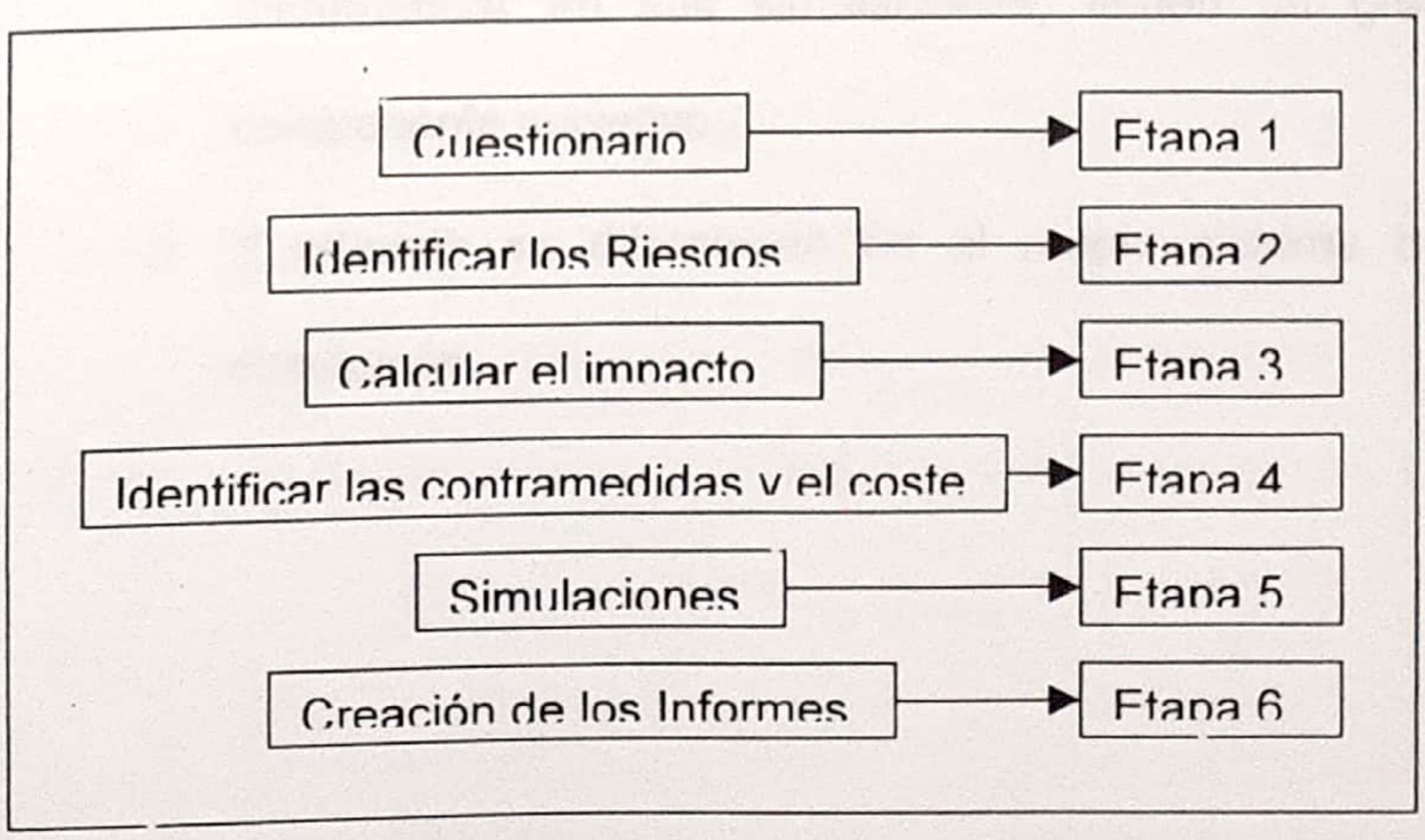
2.1.4.5.2.3. Metodologías más comunes: Las metodologías más comunes de evaluación de sistemas que podemos encontrar son de análisis de riesgos o de diagnósticos de seguridad, las de plan de contingencias, y las de auditoría de controles generales.

2.1.4.5.2.3.1. Metodologías de Análisis de Riesgo: Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas, de las que existen gran cantidad de ambas clases y sólo citaremos algunas de ellas.

El esquema básico de una metodología de análisis de riesgos es, en esencia, el representado a continuación:

FIGURA 2.3.

FUNCIONAMIENTO ESQUEMÁTICO BÁSICO DE CUALQUIER METODOLOGÍA



En base a estos cuestionarios se identifican vulnerabilidades y riesgos y se evalúa el impacto para más tarde identificar las contramedidas y el coste. La siguiente etapa es la más importante, pues mediante un juego de simulación (que se llamará "¿Qué pasa si..?") que analizará el efecto de las distintas contramedidas en la disminución de los riesgos analizados, eligiendo de esta manera un plan de contramedidas (plan de seguridad) que compondrá el informe final de la evaluación.

De forma genérica las metodologías existentes se diferencian en:

- Si son cuantitativas o cualitativas, o sea si para el "¿Qué pasa si...?" utilizan un modelo matemático o algún sistema cercano a la elección subjetiva. Aunque, bien pensado, al aproximar las probabilidades por esperanzas matemáticas subjetivamente, las metodologías cuantitativas, aunque utilicen aparatos matemáticos en sus simulaciones, tienen un gran componente subjetivo.
- Y además se diferencian en el propio sistema de simulación.

Se han identificado 66 metodologías. Entre ellas están: ANALIZY, BDSS, BIS RISK ASESOR, BUDDY SYSTEM, COBRA, CRAMM, DDIS MARION AP+, MELISA, RISAN, RISKPAC, RISKWATCH.

Después de estas metodologías han nacido muchas otras como la MAGERIT, desarrollada por la administración española; MARION, PRIMA (Prevención de Riesgos Informáticos con Metodología Abierta) y DELPHI. A continuación se detallan algunas de las metodologías:

2.1.4.5.2.3.1.1. Metodología MAGERIT (Metodología de Análisis y Sesión de Riesgos de los Sistemas de Información): El esquema completo de Etapas, Actividades y Tareas del Submodelo de Procesos de MAGERIT es el siguiente:

Etapa 1. Planificación del Análisis y Gestión de Riesgos

Actividad 1.1. Oportunidad de Realización

Tarea 1.1.1. (única) Clarificar la oportunidad de realización

Actividad 1.2. Definición de Dominio y Objetivos

Tarea 1.2.1. Especificar los objetivos del proyecto

Tarea 1.2.2. Definir el dominio y los límites del proyecto

Tarea 1.2.3. Identificar el entorno y restricciones generales

Tarea 1.2.4. Estimar dimensión, costos y retornos del proyecto

Actividad 1.3. Planificación del Proyecto

Tarea 1.3.1. Evaluar cargas y planificar entrevistas

Tarea 1.3.2. Organizar a los participantes

Tarea 1.3.3. Planificar el trabajo

Actividad 1.4. Lanzamiento del Proyecto

Tarea 1.4.1. Adaptar los cuestionarios

Tarea 1.4.2. Seleccionar criterios de evaluación y técnicas para el proyecto

Tarea 1.4.3. Asignar los recursos necesarios

Tarea 1.4.4. Sensibilizar (campaña informativa)

Etapa 2. Análisis de Riesgos

Actividad 2.1. Recogida de Información

Tarea 2.1.1. Preparar la información

Tarea 2.1.2. Realización de las entrevistas

Tarea 2.1.3. Analizar la información recogida

Actividad 2.2. Identificación y Agrupación de Activos

Tarea 2.2.1. Identificar Activos y grupos de Activos

Tarea 2.2.2. Identificar mecanismos de salvaguarda existentes

Tarea 2.2.3. Valorar Activos

Actividad 2.3. Identificación y Evaluación de Amenazas

Tarea 2.3.1. Identificar y Agrupar Amenazas

Tarea 2.3.2. Establecer los árboles de fallos generados por amenazas

Actividad 2.4. Identificación y Estimación de Vulnerabilidades

Tarea 2.4.1. Identificar vulnerabilidades

Tarea 2.4.2. Estimar vulnerabilidades

Actividad 2.5. Identificación y Valoración de Impactos

Tarea 2.5.1. Identificar Impactos

Tarea 2.5.2. Tipificar Impactos

Tarea 2.5.3. Valorar impactos

Actividad 2.6. Evaluación del Riesgo

Tarea 2.6.1. Evaluar el riesgo intrínseco

Tarea 2.6.2. Analizar las funciones de salvaguarda existentes

Tarea 2.6.3. Evaluar el riesgo efectivo

Etapa 3. Gestión del Riesgo

Actividad 3.1. Interpretación del Riesgo

Tarea 3.1.1. (única) Interpretar los riesgos

Actividad 3.2. Identificación y Estimación de Funciones de salvaguarda

Tarea 3.2.1. Identificar funciones de salvaguarda

Tarea 3.2.2. Estimar la efectividad de las funciones de salvaguarda

Actividad 3.3. Selección de Funciones de Salvaguarda

Tarea 3.3.1. Aplicar los parámetros de selección

Tarea 3.3.2. Evaluar el riesgo

Actividad 3.4. Cumplimiento de Objetivos

Tarea 3.4.1. (única) Determinar el cumplimiento de los objetivos

Etapa 4. Selección de Salvaguardas

Actividad 4.1. Identificación de mecanismos de salvaguarda

Tarea 4.1.1. Identificar los mecanismos posibles

Tarea 4.1.2. Estudiar mecanismos implantados

Tarea 4.1.3. Incorporar restricciones

Actividad 4.2. Selección de mecanismos de salvaguarda

Tarea 4.2.1. Identificar mecanismos a implantar

Tarea 4.2.2. Evaluar el riesgo (mecanismos elegidos)

Tarea 4.2.3. Seleccionar mecanismos a implantar

Actividad 4.3. Especificación de los mecanismos a implantar

Tarea 4.3.1. (única) Especificar los mecanismos a implantar

Actividad 4.4. Planificación de la Implantación

Tarea 4.4.1. Priorizar mecanismos

Tarea 4.4.2. Evaluar los recursos necesarios

Tarea 4.4.3. Elaborar cronogramas tentativos

Actividad 4.5. Integración de resultados

Tarea 4.5.1. (única) Integrar los resultados

2.1.4.5.2.3.1.2. Metodología MARION: Método documentado en dos libros de los cuales el más actual es La Securité des reseaux-Methodes et Techniques de J.M. Lamere y Leroux, J. Tourly. Tiene dos productos: MARION AP+, para sistemas individuales, y MARION RSX para sistemas distribuidos y conectividad.

Es un método cuantitativo y se basa en la encuesta anual de miembros la base de incidentes francesa (C.L.U.S.I.F.). No contempla probabilidades, sino esperanzas matemáticas que son aproximaciones numéricas (valores subjetivos).

La MARION AP+ utiliza cuestionarios y parámetros correlacionados enfocados a las distintas soluciones de contramedidas, en seis categorías. Las categorías son: seguridad informática general, factores socioeconómicos, concienciación sobre la seguridad de software y materiales, seguridad en explotación y seguridad de desarrollo.

El análisis de riesgos lo hace sobre diez áreas problemáticas. Estas áreas son: riesgos materiales, sabotajes físicos, averías,

comunicaciones, errores de desarrollo, errores de explotación, fraude, robo de información, robo de software, problemas de personal.

2.1.4.5.2.3.1.3. Metodología RISCKPAC: Todas las metodologías que se desarrollan en la actualidad están pensadas para su aplicación en herramientas. La primera de esta familia la desarrolló PROFILE ANÁLISIS CORPORATION, y la primera instalación en cliente data de 1984. Según DATAPRO es el software más vendido.

Su enfoque es metodología cualitativa. Sus resultados son exportables a procesadores de texto, bases de datos, hoja electrónica o sistemas gráficos. Está estructurada en tres niveles: Entorno, Procesador y Aplicaciones con 26 categorías de riesgo en cada nivel. Tiene un "¿Qué pasa si...?" con un nivel de riesgo de evaluación subjetiva del 1 al 5 y ofrece una lista de contramedidas o recomendaciones básicas para ayudar al informe final o plan de acciones.

2.1.4.5.2.3.1.4. Metodología CRAMM: Se desarrolló entre 1985 y 1987 por BIS y CCTA (Central Computer & Telecomunication Agency Risk Análisis & Management Meted, Inglaterra). Implantado en más de

750 organizaciones en Europa, sobre todo de la administración pública. Es una metodología cualitativa y permite hacer análisis "¿Qué pasa si...?".

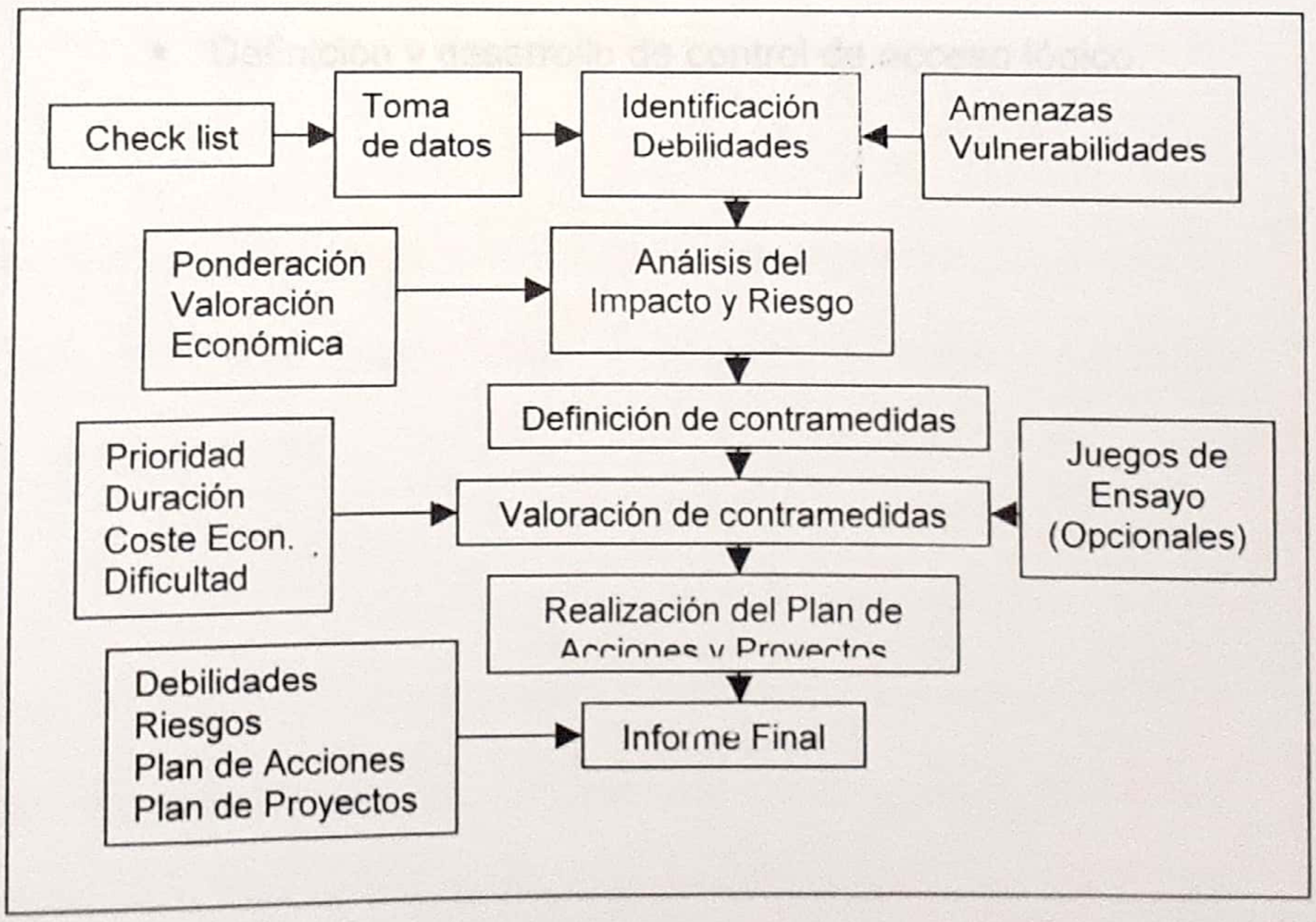
2.1.4.5.2.3.1.5. Metodología PRIMA (Prevención de Riesgos Informáticos con Metodología Abierta): Es un conjunto de metodologías españolas desarrolladas entre los años 1990 y la actualidad con un enfoque subjetivo. Sus características esenciales son:

- Cubrir las necesidades de los profesionales que desarrollan cada uno de los proyectos necesarios de un plan de seguridad.
- Fácilmente adaptable a cualquier tipo de herramienta.
- Posee cuestionarios de preguntas para la identificación de debilidades o faltas de controles.
- Posee listas de ayuda para los usuarios menos experimentados de debilidades, riesgos y contramedidas (sistema de ayuda).
- Permite fácilmente la generación de informes finales.

- Las "Listas de Ayuda" (Ver Figura 2.6.) y los cuestionarios son abiertos, y por tanto es posible introducir información nueva o cambiar la existente. De ahí la expresión abierta de su nombre.
- Tiene un "¿Qué pasa si...?" cualitativo, y capacidad de aprendizaje al poseer una base de conocimiento o registro de incidentes que van variando las esperanzas matemáticas de partida y adaptándose a los entornos de trabajo.

FIGURA 2.4.

FASES DE LA METODOLOGÍA PRIMA

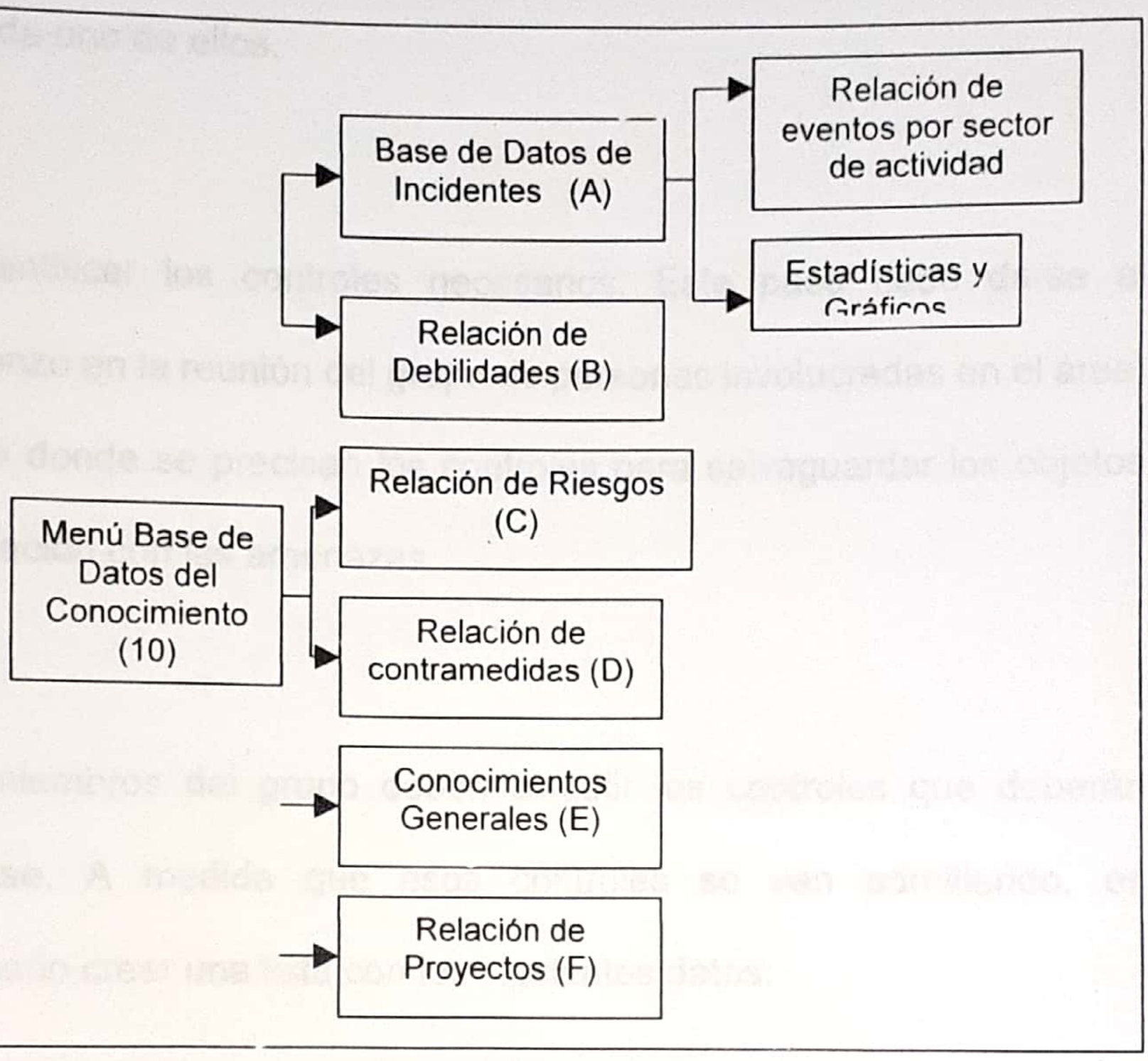


Con la misma filosofía abierta existen en la actualidad las siguientes metodologías:

- Análisis de Riesgos.
- Plan de Contingencias Informática y de recuperación del negocio.
- Plan de restauración interno informático.
- Clasificación de la información.
- Definición y desarrollo de procedimientos de control informáticos.
- Plan de cifrado.
- Auditoría Informática.
- Definición y desarrollo de control de acceso lógico.

FIGURA 2.5.

LISTA DE AYUDA DE LA METODOLOGÍA PRIMA



2.1.4.5.2.3.1.6. Metodología DELPHI: La siguiente metodología analizada, es la Metodología Delphi. El esquema completo del método Delphi es el siguiente:

1. Crear la matriz de Amenazas y Objetos: Al comienzo se debe realizar una reunión con todo el personal involucrado en el trabajo. Esta reunión tiene por objeto no sólo identificar las amenazas y los

objetos del área, sino también establecer nombres cortos para denominar las amenazas y los objetos y redactar una breve definición de cada uno de ellos.

2. Identificar los controles necesarios: Este paso debe darse al comienzo en la reunión del grupo de personas involucradas en el área. Es allí donde se precisan los controles para salvaguardar los objetos en relación con las amenazas.

Los miembros del grupo deben discutir los controles que deberán incluirse. A medida que esos controles se van admitiendo, es necesario crear una lista con los siguientes datos:

- Número de Identificación,
- Nombre corto que distingue a cada control,
- Breve descripción sobre la funcionalidad y utilidad del control,
- Identificación de la persona responsable de la implementación de los controles.

3. Registrar los controles dentro de la matriz: Este paso se ejecuta para colocar dentro de las celdas el número de identificación de los controles

4. Categorizar los riesgos: Aquí se identifican las áreas de alto, medio y bajo riesgo, colocándolas en orden de nivel de exposición. Para la ejecución de este paso se utiliza el método Delphi y la comparación de los niveles de riesgo.

El método Delphi, consiste en reunir a un grupo de expertos para solucionar determinados problemas. Dicho grupo realiza la categorización individual de las amenazas y de los objetos de riesgo. El equipo Delphi sesiona conjuntamente para combinar sus experiencias en la realización de las siguientes tareas:

- Categorizar las amenazas por niveles de riesgos. (Ver Anexo 6) Para efecto de este ejercicio, se ha organizado un grupo de cinco personas, quienes se someten a votación hasta completar la matriz. (Ver Anexo 7) La categorización se obtiene sumando como se muestra en el anexo 8. Luego se suman los dos votos para obtener el total final de cada

amenaza. El resultado se utiliza para producir una lista de categorización de amenazas, por niveles de riesgo de mayor a menor. (Ver Anexo 8).

- Categorizar la Sensibilidad de los Objetos: Este proceso se inicia copiando los objetos que registra la matriz de control de riesgos en una hoja de comparación de categorías de riesgos (Ver Anexo 9). Para categorizar la sensibilidad de los objetos se utiliza la percepción que tenga cada uno de los miembros del equipo Delphi sobre cuál objeto de cada pareja de objetos puede causar mayor pérdida económica si se daña o causa demoras en el procesamiento. El grupo vota hasta completar la matiz (Ver Anexo 10). Después se suman los resultados derechos de diagonales de las columnas, en forma vertical, y luego se sumnan los resultados izquierdos de las diagonales de las columnas, en forma horizontal, en el sentido de las filas de la matriz. Se suman los resultados para obtener el total final. (Ver Anexo 11).

- Combinar las dos Categorías: Una vez terminadas las dos categorías, se elabora una matriz de control de riesgos,

colocando los totales en orden de mayor a menor, en los dos casos. (Ver Anexo 12).

- Seguidamente se multiplican los correspondientes valores y con los resultados se organiza una matriz. Terminada esta operación se procede a obtener el nivel de riesgo / sensibilidad de las celdas de acuerdo con el valor del producto. Puede ser que al terminar este proceso se presenten repeticiones.

- Dividir las celdas en regiones de mayor, mediano y menor riesgo: Este proceso se realiza dividiendo la cantidad de niveles de riesgo / sensibilidad por cinco (número de personas del grupo). El cociente se utiliza para indicar las celdas de mayor o menor riesgo. De manera que las celdas con niveles de riesgo / sensibilidad inferiores o iguales al cociente son las celdas de mayor riesgo. Las celdas con niveles de riesgo / sensibilidad superiores al cociente e inferiores o iguales a tres veces el cociente son las celdas de mediano riesgo y las celdas con niveles de riesgo /

sensibilidad superiores a tres veces el cociente son las celdas de bajo riesgo.

En la matriz se resta al número de celdas las repeticiones (si es que las hay), para efectos del cálculo. Este valor es dividido para el número de personas del grupo obteniendo un cociente con el cual se organiza el cuadro de riesgo / sensibilidad y la matriz correspondiente. (Ver Anexo 13)

5. Diseñar los controles Definitivos: Con el resultado del trabajo apoyados en el método Delphi, se diseñan y documentan definitivamente los controles a nivel: preventivo, detectivo y correctivo, de acuerdo con el área que se esté analizando.

Este es un trabajo dispendioso, debido a que todo depende del conocimiento que se tenga del área informática y del sistema de control interno informático deseable.

6. Resultados del Análisis de Riesgos. Los resultados del análisis de riesgos, deben ser escritos y dados a conocer oportunamente para que sean incorporados en el área analizada.

2.1.4.5.3. Metodologías de Auditoria Informática: Las únicas metodologías que podemos encontrar en la auditoría informática son dos familias distintas: las auditorias de Controles Generales como producto estándar de la de Auditores Profesionales, que son una homologación de las mismas a nivel internacional, y las Metodologías de los auditores internos.

Entre las dos metodologías de valuación de sistemas (análisis de riesgos y auditoría) existen similitudes y grandes diferencias. Ambas tienen papeles de trabajo obtenidos del trabajo de campo tras el plan de entrevistas, pero los cuestionarios son totalmente distintos.

Las metodologías de auditoria son del tipo cualitativo / subjetivo. Se puede decir que son las subjetivas por excelencia. Por lo tanto, están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación continuada. Sólo así

esta función se consolidará en las entidades, esto es, por el "respeto profesional" a los que ejercen la función.

El concepto de las metodologías de análisis de riesgos de "tiempos medios" es más bien para consultores profesionales que para auditores internos.

2.1.4.5.4. Metodologías de Clasificación de la Información y de Obtención de los Procedimientos de Control:

2.1.4.5.4.1. Clasificación de la Información: No es frecuente encontrar metodologías de este tipo, pero la metodología PRIMA tiene dos módulos que desarrollan estos dos aspectos que se muestran a continuación.

Se podría preguntar si es suficiente con un análisis de riesgos para obtener un plan de contramedidas que nos llevará a una situación de control como se desea. La respuesta es no, dado que todas las entidades de información a proteger no tienen el mismo grado de importancia, y el análisis de riesgos metodológicamente no permite

aplicar una diferenciación de contramedidas según el activo o recurso que protege, sino por la probabilidad del riesgo analizado.

Tiene que ser otro concepto, esto es "si se identifican distintos niveles de contramedidas para distintas entidades de información con distinto nivel de criticidad, se estará optimizando la eficiencia de las contramedidas y reduciendo los costos de las mismas".

Esta metodología es del tipo cualitativo, y como el resto de la metodología PRIMA tiene listas de ayuda con el concepto abierto, esto es, que el profesional puede añadir en la herramienta niveles o jerarquías, estándares y objetivos a cumplir por nivel, y ayudas de contramedidas.

O sea los factores a considerar son los requerimientos legislativos, la sensibilidad a la divulgación (confidencialidad), a la modificación (integridad), y a la destrucción.

Las jerarquías suelen ser cuatro, y según se trate de óptica de preservación o de protección, los cuatro grupos serían: Vital, Crítica, valuada y No sensible.

PRIMA, aunque permite definirla a voluntad, básicamente define:

- Estratégica (información muy restringida, muy confidencial, vital para la subsistencia de la empresa).
- Restringida (a los propietarios de la información).
- De uso interno (a todos los empleados).
- De uso general (sin restricción).

Los pasos de la metodología son los siguientes:

1. Identificación de la Información.
2. Inventario de Entidades de Información Residentes y Operativas. Inventario de programas, archivos de datos, estructuras de datos, soportes de información, etc.
3. Identificación de Propietarios. Son los que necesitan para su trabajo, usan o custodian la información.
4. Definición de jerarquías de información. Suelen ser cuatro, por que es difícil distinguir entre más niveles.
5. Definición de la Matriz de Clasificación. Esto consiste en definir las políticas, estándares, objetivos de control y contramedidas por tipos y jerarquías de información.

6. Confección de la Matriz de Clasificación. En esta fase se complementa toda la matriz, asignándole a cada entidad un nivel de jerarquía, lo que se asocia a una serie de hitos a cumplir, para cuyo cumplimiento se deberán desarrollar acciones concretas en el punto siguiente.
7. Realización del Plan de Acciones. Se confecciona el plan detallado de acciones. Por ejemplo, se reforma una aplicación de nóminas para que un empleado utilice el programa de subidas de salario y su supervisor lo apruebe.
8. Implantación y Mantenimiento. Se implanta el plan de acciones y se mantiene actualizado.

Y así se completa esta metodología.

2.1.4.5.4.2. Obtención de los Procedimientos de Control: Otra Metodología necesaria para la obtención de los controles es "la Obtención de los Procedimientos de Control". Es frecuente encontrar manuales de procedimientos en todas las áreas de la empresa que explican las funciones y cómo se realizan las distintas tareas diariamente, siendo éstos necesarios para que los auditores realicen sus revisiones operativas, evaluando si los procedimientos son correctos y están aprobados y sobre todo si se cumplen.

Pero se podría preguntar si desde el punto de vista de control informático es suficiente y cómo se podrían mejorar.

La respuesta es dada por la metodología que se expone a continuación, que dará otro plan de acciones que contribuirá sumándose a los distintos proyectos de un plan de seguridad para mejorar el entramado de contramedidas.

La metodología se muestra a continuación:

Fase I. Definición de Objetivos de Control.

Tarea 1: Análisis de la empresa. Se estudian los procesos, organigramas y funciones.

Tarea 2: Recopilación de estándares. Se estudian todas las fuentes de información necesarias para conseguir definir en la siguiente fase los objetivos de control a cumplir (por ejemplo: ISO, CISA, etc).

Tarea 3: Definir los objetivos de control.

Fase II. Definición de los Controles.

Tarea 1: Definir los controles. Con los objetivos de control definidos, se analizan los procesos y se va definiendo los distintos controles que se necesiten.

Tarea 2: Definición de Necesidades Tecnológicas (hardware y herramientas de control).

Tarea 3: Definición de los Procedimientos de Control. Se desarrollan los distintos procedimientos que se generan en las áreas usuarias, informática, control informático y control no informático.

Tarea 4: Definición de las necesidades de recursos humanos.

Fase III. Implantación de los Controles.

Una vez definidos los controles, las herramientas de control y los recursos humanos necesarios, no resta más que implantarlos en forma de acciones específicas.

Terminado el proceso de implantación de acciones habrá que documentar los procedimientos nuevos y revisar los afectados de cambio. Los procedimientos resultantes serán:

- Procedimientos propios de control de la actividad informática (control interno informático).
- Procedimientos de distintas áreas usuarias de la informática, mejorados.
- Procedimientos de áreas informáticas, mejorados.
- Procedimientos de control dual entre control interno informática y el área informática, los usuarios informáticos, y el área de control no informático.

2.1.4.5.5. Metodología de Evaluación de Riesgos: Este tipo de metodología, conocida también por risk oriented approach, es la que propone la ISACA, y empieza fijando los objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno.

2.2. Definiciones Conceptuales

Alcance: Distancia a que llega una cosa. Efectuada la revisión de antecedentes, se procede a preparar el programa de auditoria, precisando periodo y alcance del examen.

Antecedente: Todo lo que sirve para juzgar hechos posteriores. Acordada la realización de una auditoria, el grupo designado para practicarla efectúa una revisión de antecedentes con el estudio de papeles de trabajo e informes anteriores.

Auditoría: Examen objetivo, sistemático, profesional e independiente, aplicado a una organización por un auditor competente.

Características: Cualidades o rasgos que sirven para distinguir una persona o una cosa de sus semejantes. La consideración de las características de la organización es fundamental en la implantación y desarrollo de la auditoria interna.

Control en TI: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonable-mente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos

Criterio: Pauta, norma, regla para conocer la verdad; juicio, discernimiento frente a un asunto determinado. El auditor fundamenta su trabajo en la evaluación del cumplimiento de criterios establecidos. Ningún tipo de auditoria es posible si no hay criterios establecidos sobre los cuales un auditor debe evaluar.

Cronograma: Relación de actividades por desarrollar en fechas determinadas, las cuales hacen parte de los planes y programas de las organizaciones y a su vez se constituye en un mecanismo del control interno.

Desempeñar: Hacer aquello a lo que uno está obligado, lo cual debe estar garantizado en un alto grado por los mecanismos de control.

Diagnóstico: Análisis que permite determinar el conjunto de síntomas o características de la evolución o el desarrollo de un proceso determinado, el cuál resulta muy útil para conocer el grado de desarrollo y fortalecimiento del sistema de control interno de una organización.

Diseño: Bosquejo formal de un proceso o cosa. Diseño de los elementos y mecanismos del sistema de control interno.

Economía: Administración recta y prudente de los bienes. A este requisito que debe tener toda organización debe contribuir permanentemente el sistema de control interno y de auditoria interna.

Eficacia: Virtud, fuerza y poder para obrar.

Eficiencia: Logro de metas y objetivos en términos de cantidad y calidad. Virtud y facultad para lograr un efecto determinado.

Énfasis: Fuerza de expresión o entonación. Los programas de auditoria se confeccionan sobre la base de poner énfasis en las áreas

más importantes y las áreas donde los controles internos son deficientes.

Estrategia: Procedimiento o plan que se aplica para lograr un propósito u objetivo.

Ética: Parte de la filosofía que trata de la moral y de las obligaciones del hombre. El auditor cuenta con su propia ética profesional para el desarrollo de sus funciones.

Evaluar: Valorar, estimar el valor de las cosas o situaciones.

Evidencia: La evidencia se constituye en el soporte y respaldo a las afirmaciones dadas.

Fase: Cualquiera de los aspectos o cambios dentro de un proceso.

Función: Es el conjunto de actividades u operaciones que dan características propias y definidas a un cargo, para determinar niveles de responsabilidad y autoridad, y deben estar formuladas y

documentadas en un manual de funciones y procedimientos el que a su vez se constituye en el elemento de control.

Gobierno de TI: Una estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de lograr sus objetivos al añadir valor mientras se equilibran los riesgos contra el re-torno sobre TI y sus procesos.

Implantar: Establecer y poner en ejecución doctrinas nuevas, prácticas o costumbres.

Informática: Aplicación racional, sistemática de la información para el desarrollo económico, social y político.

Inherente: Unido inseparablemente y por naturaleza a una cosa. El riesgo es inherente al desarrollo de las actividades de una organización por lo que no se pueden orientar todos los recursos a eliminarlo totalmente. Lo importante es identificarlo y manejarlo.

Integridad: Calidad de íntegro. Que tiene todas sus partes. Los papeles de trabajo protegen la integridad profesional del auditor y ayudan a justificar su actuación.

Manual: Documento guía que describe asuntos o actividades de acuerdo con un ordenamiento lógico, y está sujeto a permanente evaluación y actualización. Es una de las fuentes de criterios a evaluar dentro del análisis de riesgos.

Mecanismos: Combinación de partes que producen o transforman un movimiento. Para que exista un buen control se deben establecer mecanismos de seguimiento y control.

Método: Modo de obrar con orden. La evaluación de control interno por el método de cuestionario consiste en convertir en preguntas todas las normas de control interno, de tal manera que una respuesta afirmativa indique la existencia y observación de la norma y una respuesta negativa indique su ausencia o incumplimiento.

Normas: Son los requisitos de calidad relativos a la persona del auditor, al trabajo que realiza y a la emisión de su opinión.

Objetivo: Relativo al objeto en sí y no a nuestro modo de pensar o sentir. El informe debe presentar comentarios, conclusiones y recomendaciones en forma objetiva.

Objetivo de Control: Una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

Oportunidad: Se refiere a la época en que se deben aplicar los procedimientos del análisis, de tal forma que se obtengan los resultados más eficientes que sean posibles.

Organización: Unión voluntaria de una serie de individuos; está integrada por múltiples vínculos contractuales entre factores (personas, servicio y procesos) con una función de asignación eficiente de los recursos y bajo la dirección y coordinación de una autoridad directiva.

Planear: Trazar, formar, disponer el plan de una obra. Forjar planes.

Ponderar: Pesar, determinar el peso de una cosa. Examinar con atención las razones de una cosa para formar un juicio de ella.

Principios: Base, origen, fundamento máximo por el que cada quien rige sus actuaciones. La actuación del auditor está regida por principios éticos profesionales.

Procedimiento: Método para hacer alguna cosa. Entonces podemos referirnos a procedimientos operativos, administrativos y de control.

Proceso: Conjunto de fases sucesivas de un fenómeno o asunto, las cuales son controladas, supervisadas y evaluadas por el sistema de control interno.

Programa: Escrito que indica las condiciones de un análisis. El auditor debe formular un programa general de trabajo que incluye un resumen de las actividades a desarrollar.

Recomendación: Encargo que se hace a una persona respecto de otra o de alguna cosa. El informe del análisis debe tener recomendaciones que permitan subsanar las deficiencias encontradas.

Recursos Materiales: Todo lo referente a mobiliario de oficina y equipos de computación con que cuenta la organización.

Relevante: Sobresaliente, excelente, importante. El informe del análisis debe brindar la información necesaria y relevante relacionada con el examen practicado.

Sábana: Refiérase a los reportes largos que se imprimían antes.

Semicuantificar: Asignar rangos numéricos a las características Alto, Medio, y Bajo.

Sistemático: Que sigue un sistema. Dícese de quien procede por principios sometiéndose a un sistema fijo en su conducta, escritos, opiniones. Es una de las características del examen de auditoría.

Técnica: Conjunto de procedimientos de un arte o ciencia. Habilidad para usar esos procedimientos. En el desarrollo del examen de auditoría se hace uso de las técnicas de auditoría.

Técnicas: Son los recursos prácticos de investigación y prueba que el auditor utiliza para obtener la información que necesita.

Verificar: Probar que es verdad una cosa que se duda. La auditoría es un examen que verifica y evalúa determinadas áreas de una empresa.

CAPÍTULO 3

3. NORMATIVAS Y/O ESTÁNDARES INTERNACIONALES.

En vista de continuos cambios en Tecnología de Información, el desarrollo de este capítulo concerniente a normas y/o estándares internacionales, pretende difundir las normativas que se han venido desarrollando conforme ha ido evolucionado la tecnología.

Estas normativas constituyen el fundamento para el progreso efectivo en el campo de los controles en el área de sistemas y de información.

En este capítulo se documentarán algunas leyes, normas y estándares internacionales que hablan del riesgo como aspecto importante a analizar en toda la organización.

3.1. Ley Sarbanes – Oxley

La Ley Sarbanes-Oxley de 2002 promulgada en los Estados Unidos a raíz de los "escándalos contables" al abrir el nuevo Siglo XXI, lleva mucho más lejos las disposiciones sobre la obligación de la gerencia de asegurar adecuados controles internos.

Dentro de la ley Sarbanes Oxley, se encuentra la sección 404 que hace referencia al tema de Administración de Riesgo de TI, la cual se muestra a continuación:

3.1.1. SEC. 404: Evaluación de la Gerencia de los Controles Internos:

Regulaciones Requeridas.- La Comisión prescribirá regulaciones requiriendo que cada informe anual requerido por la sección 13 (a) ó 15 (d) del Acta de Intercambio de Valores de 1934 contenga un informe de control interno, el cual :

- determinará la responsabilidad de la gerencia por establecer y mantener una estructura adecuada de control interno y los procedimientos para información financiera, y

- contendrá una evaluación, al final del año fiscal más reciente del emisor, de la estructura de control interno y los procedimientos del emisor para información financiera.

3.1.1.2. Evaluación e Informe del Control Interno: Con respecto a la evaluación del control interno requerido por la sub-sección (a), cada firma de contabilidad pública registrada que prepara o emite el informe de auditoria para el emisor testificará, e informará sobre la evaluación hecha por la gerencia del emisor. Una testificación bajo esta sub-sección será hecha de acuerdo con las normas para compromisos de testificación emitidas o adoptadas por la Junta. La testificación no estará sujeta a un compromiso separado.

3.2.- Normas COBIT: Control Objectives for Information and related Technology

La Information Systems Audit and Control Foundation (ISACF) desarrolló los Objetivos de Control para la Información y Tecnología relacionada (COBIT) para servir como una estructura generalmente aplicable y prácticas de seguridad para el control de la tecnología de la

información. Esta estructura COBIT le permite a la gerencia comparar la seguridad y prácticas de control de los ambientes de TI.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Por lo tanto, el objetivo principal de COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta de COBIT es desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa.

3.2.1. Audiencia: Administración, Usuarios y Auditores.- COBIT está diseñado para ser utilizado por tres audiencias distintas:

3.2.1.1. Administración / Gerencia: Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

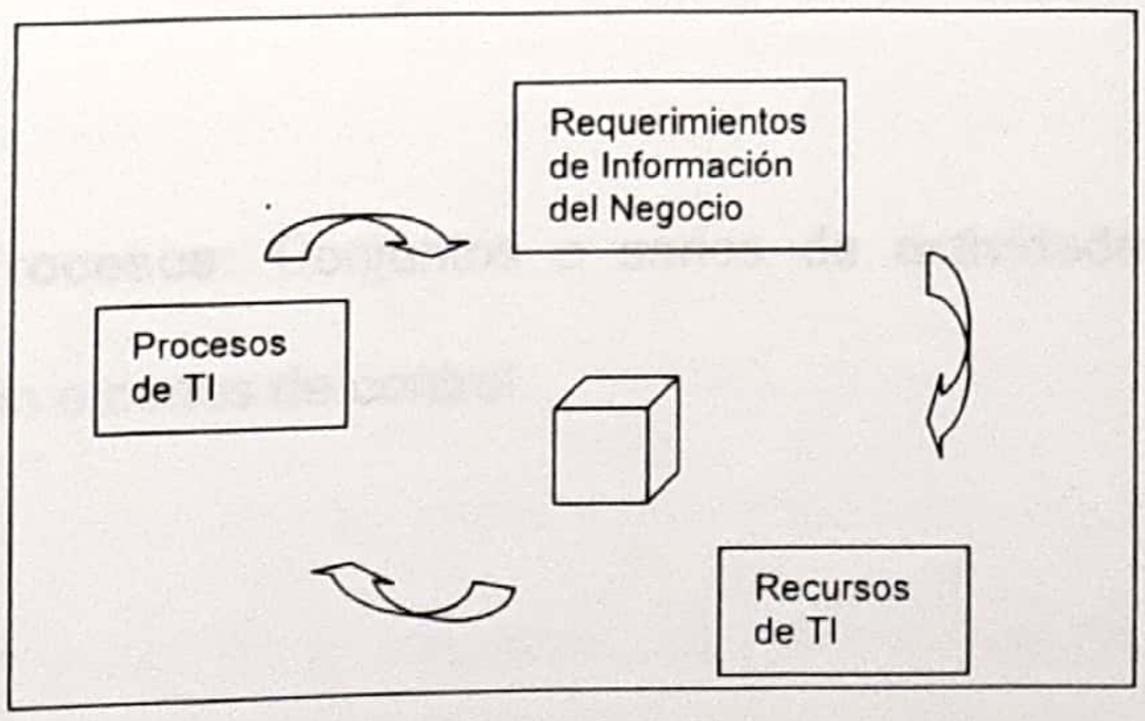
3.2.1.2. Usuarios: Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

3.2.1.3. Auditores: Para soportar su opinión y/o proporcionar consejos a la Administración sobre los controles internos.

3.2.2. Principios.-

FIGURA 3.1.

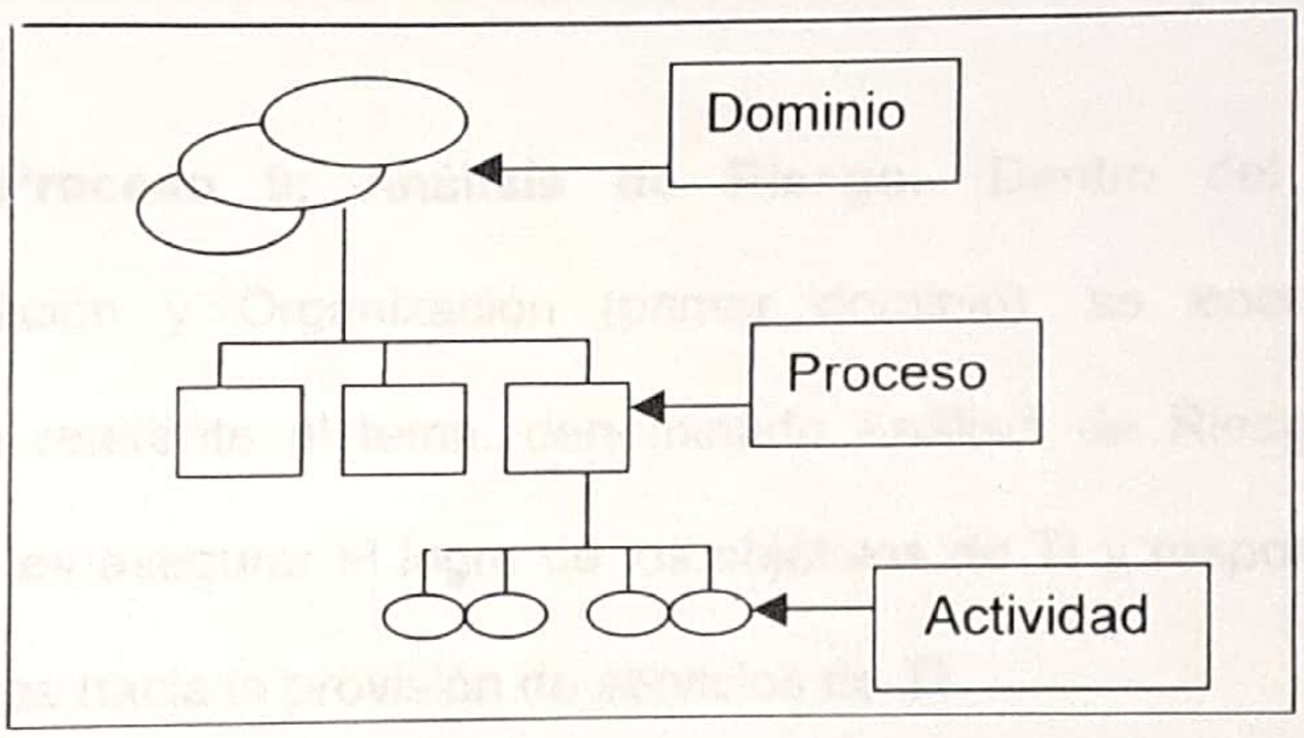
PRINCIPIOS DE COBIT



3.2.3. Procesos de TI.- La estructura de COBIT se define a partir de una premisa simple: "Los recursos de las Tecnologías de Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".

FIGURA 3.2.

NIVELES DE COBIT



3.2.3.1. Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

3.2.3.2. Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.

3.2.3.3. Actividades: Acciones requeridas para lograr un resultado medible.

Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios. De estos se tomará en consideración aquellos que se refieren a riesgos.

3.2.4. Proceso 9: Análisis de Riesgo.- Dentro del Dominio: Planificación y Organización (primer dominio), se encuentra un proceso referente al tema, denominado Análisis de Riesgo y cuyo objetivo es asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

3.2.4.1. Actividad 1: Evaluación de Riesgos del Negocio: Objetivo de Control: La Gerencia deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información relevantes para el logro de los objetivos del negocio, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar

evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema, para nuevos proyectos y para casos recurrentes y con participación multidisciplinaria. La Administración deberá asegurar que se realicen reevaluaciones y que la información sobre evaluación de riesgos sea actualizada como resultado de audito-rías, inspecciones e incidentes identificados.

3.2.4.2. Actividad 2: Enfoque de Evaluación de Riesgos: Objetivo de Control: La Gerencia deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La Gerencia debe adelantar la identificación de soluciones para la mitigación de riesgos e involucrar-se en la identificación de vulnerabilidades. Especialistas de seguridad deben realizar identificación de amenazas y especialistas de TI deben dirigir la selección de controles. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

3.2.4.3. Actividad 3: Identificación de Riesgos: Objetivo de Control: La evaluación de riesgos deberá enfocarse al examen de los

elementos esenciales de riesgo y las relaciones causa / efecto entre ellos. Los elementos esenciales de riesgo incluyen activos tangibles e intangibles, valor de los activos, amenazas, vulnerabilidades, protecciones, consecuencias y probabilidad de amenaza. El proceso de identificación de riesgos debe incluir una clasificación cualitativa y, donde sea apropiado, clasificación cuantitativa de riesgos y debe obtener in- sumos de las tormentas de ideas de la Gerencia, de planeación estratégica, auditorias anteriores y otros análisis. El análisis de riesgos debe considerar el negocio, regulaciones, aspectos legales, tecnología, comercio entre socios y riesgos del recurso humano.

3.2.4.4. Actividad 4: Medición de Riesgos: Objetivo de Control: El enfoque de la evaluación de riesgos deberá asegurar que la información del análisis de la identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Así mismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

3.2.4.5. Actividad 5: Plan de Acción contra Riesgos: Objetivo de Control: El enfoque de evaluación de riesgos deberá proporcionar la

definición de un plan de acción contra riesgos para asegurar que el costo–efectividad de los controles y las medidas de seguridad mitiguen los riesgos en forma continua. El plan de acción contra los riesgos debe identificar la estrategia de riesgos en términos de evitar, mitigar o aceptar el riesgo.

3.2.4.6. Actividad 6: Aceptación de Riesgos: Objetivo de Control: El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y el costo-efectividad de la implementación de protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada, compromisos de negociación contractual y autoaseguramiento.

3.2.4.7. Actividad 7: Selección de Garantías o Protecciones: Objetivo de Control: Mientras se logra un sistema de controles y garantías razonable, apropiado y proporcional, controles con el más alto retorno de inversión y aquellos que provean ganancia rápida deben recibir la primera prioridad. El sistema de control necesita además balancear las medidas de prevención, detección, corrección y

recuperación. Adicionalmente, la Gerencia necesita comunicar el propósito de las medidas de control, manejar el conflicto y moni-torear continuamente la efectividad de las medidas de control.

3.2.4.8. Actividad 8: Compromiso con el Análisis de Riesgos:

Objetivo de Control: La Gerencia deberá motivar el análisis de riesgos como una herramienta importante para proveer información para el diseño e implementación de controles internos, en la definición del plan estratégico de tecnología de información y en los mecanismos de evaluación y monitoreo.

3.3.- COSO Report

COSO es el marco más extendido y utilizado, que se concentra en el control interno de manera integrada y comprensiva. Adoptado por el sector público y privado en USA, por el Banco Mundial y el BID, y se extiende rápidamente por todo Latino América.

El nombre de COSO proviene del "Committee of Sponsoring Organizations of the Treadway Commission", una iniciativa del sector privado esponsorizada por las cinco mayores asociaciones

profesionales financieras de los Estados Unidos (Instituto Americano de Contadores Públicos, Instituto de Auditores Internos, Asociación Americana de Contabilidad, Instituto de Contadores de Gestión e Instituto de Ejecutivos Financieros).

El Comité, que es independiente de sus cinco espónsores, incluyó representantes de la industria, la contaduría, las firmas de inversiones, y la bolsa de Nueva York.

En 1992, publicó un informe denominado "Control Interno – Marco Integrado", con recomendaciones para establecer una definición común de control interno y proveer guía en la creación y mejoramiento de la estructura de control interno.

En 1999, el GAO (Contraloría en EEUU), publica Estándares para Control Interno en el Gobierno Federal, basado en COSO.

En 2001, el GAO publica Herramienta para Evaluación de Controles Internos basado en COSO.

En 2002, se aprueba la ley Sarbanes Oxley con obligaciones en materia de control interno para empresas que cotizan en bolsa.

En 2003, COSO publica el borrador del nuevo documento para el marco conceptual de la Administración de Riesgos

3.3.1. Conceptos Fundamentales.- Según el informe COSO hay ciertos conceptos fundamentales implícitos en el control interno:

- El control interno es un proceso...un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- El control interno lo llevan acabo las personas...no por medio de las reglas, manuales, u otros impresos...sino por medio de los servidores de la empresa.
- El control interno solo puede aportar un grado de seguridad razonable...no la seguridad total.
- El control interno está pensado para facilitar la consecución de objetivos en una o más de las diferentes categorías que, al mismo tiempo, se solapan.

La autoevaluación de control interno es un proceso que guía a los gerentes y empleados de una entidad, organización o departamentos dentro de la organización a través de un análisis de control interno diseñado para identificar y mejorar las fortalezas del control interno y rectificar las debilidades.

El análisis o autoevaluación de control se realiza utilizando un marco tal como el "Control Interno – Sistema Integrado" el título formal del informe COSO. Este sistema establece una definición común de control interno y proporciona un estándar con el cual las organizaciones pueden evaluar y mejorar sus sistemas de control. El marco COSO incluye todos aquellos elementos de una organización que apoyan a los empleados para alcanzar los objetivos de la misma. El objetivo de COSO es guiar a los gerentes, directores y otros que desean mejorar su comprensión acerca del control interno y su efectividad.

3.3.2. Componentes.- Los componentes presentes e interrelacionados para alcanzar los objetivos de una organización según el informe COSO son:

- Ambiente de Control: Ética de trabajo, liderazgo, trabajo en equipo, moral.
- Evaluación de Riesgos: Mecanismos para identificar riesgos para alcanzar los objetivos de trabajo, incluyendo los riesgos particulares asociados con el cambio.
- Actividades de Control: Políticas, procedimientos, atribuciones (incluyendo aquellos que pueden ser redundantes o que no agregan valor).
- Información y Comunicación: Horizontal y vertical que es crítica en todos los niveles arriba mencionados
- Monitoreo y Aprendizaje: Realizar cambios basados en ese aprendizaje.

El ambiente de control provee la base para los otros componentes. El mismo abarca factores tales como filosofía y estilo operativo de la gerencia, políticas y prácticas de recursos humanos, la integridad y valores éticos de los empleados, la estructura organizacional, y la atención y dirección del directorio. El informe COSO brinda una guía para evaluar cada uno de estos factores. Por ejemplo, la filosofía gerencial y el estilo operativo pueden ser evaluados examinando la naturaleza de los riesgos del negocio que acepta la gerencia, la

frecuencia de su interacción con los subordinados, y su actitud hacia los informes financieros.

La evaluación de riesgo consiste en la identificación del riesgo y el análisis del riesgo. La identificación del riesgo incluye examinar factores externos tales como los desarrollos tecnológicos, la competencia y los cambios económicos, y factores internos tales como calidad del personal, la naturaleza de las actividades de la entidad, y las características de procesamiento del sistema de información. El análisis de riesgo involucra estimar la significación del riesgo, evaluar la probabilidad de que ocurra y considerar cómo administrarlo.

Las actividades de control consisten en las políticas y procedimientos que aseguran que los empleados lleven a cabo las directivas de la gerencia. Las actividades de control incluyen revisiones del sistema de control, los controles físicos, la segregación de tareas y los controles de los sistemas de información. Los controles sobre los sistemas de información incluyen los controles generales y los controles de las aplicaciones. Controles generales son aquellos que cubren el acceso, el desarrollo de software y sistemas. Controles de las aplicaciones son

aquellos que previenen que ingresen errores en el sistema o detectan y corrigen errores presentes en el sistema.

La entidad obtiene información pertinente y la comunica a través de la organización. El sistema de información identifica, captura y reporta información financiera y operativa que es útil para controlar las actividades de la organización. Dentro de la organización, el personal debe recibir el mensaje que ellos deben comprender sus roles en el sistema de control interno, tomar seriamente sus responsabilidades por el control interno, y, si es necesario, reportar problemas a los altos niveles de gerencia. Fuera de la entidad, los individuos y organizaciones que suministran o reciben bienes o servicios deben recibir el mensaje de que la entidad no tolerará acciones impropias.

La gerencia monitorea el sistema de control revisando el output generado por las actividades regulares de control y realizando evaluaciones especiales. Las actividades regulares de control incluyen comparar los activos físicos con los datos registrados, seminarios de entrenamiento, y exámenes realizados por auditores internos y externos. Las evaluaciones especiales pueden ser de distinto alcance y frecuencia. Las deficiencias encontradas durante las actividades

regulares de control son normalmente reportadas al supervisor a cargo; las deficiencias detectadas durante evaluaciones especiales son normalmente comunicadas a los niveles altos de la organización.

3.3.3. Controles.- Los tipos de actividad de control son (Según COSO):

- Controles generales
- Ambientes de control
- Controles directos

3.3.3.1. Controles generales:

- Planeamiento de requerimientos para las instalaciones
- Controles del departamento de Sistemas

3.3.3.2. Ambientes de control:

- Enfoque hacia el control
- Organización gerencia
- Administración de Seguridad de las instalaciones

3.3.3.3. Controles directos:

- Controles de las instalaciones
- Controles de procesamiento y funciones de procesamiento computarizadas
- Controles para salvaguardar equipos

3.4. ISO 17999

La norma internacional ISO 17799:2000 esta basada en la norma BS 7799 (esta última publicada por el Instituto Británico de Normas Técnicas en 1995, y revisada y ampliada en una segunda versión en 1999). Actualmente, es un estándar a seguir dentro de la práctica de Seguridad Informática.

Propone 10 áreas o dominios de control, conteniendo una serie de recomendaciones prácticas "exitosas" de seguridad que toda organización debería poder aplicar independientemente de su tamaño o sector.

Existen programas de certificación de cumplimiento con la norma. Asimismo, la ISO 17799 puede servir de guía para definir Políticas de

seguridad en la empresa y/o para implantar un programa de administración de la seguridad.

En la Argentina la ISO 17799:2000 fue adoptada por IRAM. Así como es un estándar a seguir con referencia a la seguridad informática, también hace referencia a los riesgos y sus posibles controles a implementar, de tal manera que los minimiza, teniendo muy claro que los riesgos no se pueden anular.

3.4.1. Estructura de la Norma ISO 17799:2000.-

3.4.1.1. Política de Seguridad de la Información: Refleja las expectativas y el compromiso de la organización en materia de seguridad a fin de brindar administración, dirección y soporte.

3.4.1.2. Organización de la Seguridad: Relacionada con el diseño de una estructura de administración dentro de la organización que establezca la responsabilidad de los grupos en áreas de seguridad y un procesos para el manejo de respuesta a incidentes.

3.4.1.3. Clasificación y Control de Activos: Relacionado con la necesidad de inventariar y clasificar los activos de la organización en cuanto a su criticidad, grado de exposición al riesgo y nivel de protección necesario, y la designación de responsables por la custodia de los mismos.

3.4.1.4. Seguridad del Personal: Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad, integrándolos de esta forma en la cadena de detección y respuesta a incidentes.

3.4.1.5. Seguridad Física y Ambiental: Responde a la necesidad de proteger las áreas de procesamiento e instalaciones de la organización.

3.4.1.6. Gestión de Comunicaciones y Operaciones:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información

- Minimizar el riesgo de falla de los sistemas
- Proteger la integridad del software y la información
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información
- Garantizar la protección de la información en las redes y de la infraestructura de soporte
- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

3.4.1.7. Control de Accesos: Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos y externos.

3.4.1.8. Desarrollo y mantenimiento de Sistemas: En toda labor de tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso de desarrollo e implantación de software.

3.4.1.9. Administración de la Continuidad de los Negocios: La organización debe estar preparada para contrarrestar las interrupciones en las actividades y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

3.4.1.10. Cumplimiento: Establece la necesidad de que las organizaciones verifiquen si el cumplimiento con la Norma Técnica ISO 17799 concuerda con otros requisitos jurídicos, como la Directiva de la Unión Europea que concierne la Privacidad, la Ley de Responsabilidad y Transferibilidad del Seguro Médico (HIPAA por su sigla en Inglés) y la Ley Gramm-Leach-Billey (GLBA por su sigla en inglés). Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

3.4.2. Beneficios de la Norma.- Una empresa que pudiese estar certificada con la norma técnica ISO 17799 puede ganar frente a los competidores no certificados. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante,

por lo general optará por la empresa certificada. Además una empresa certificada tendrá en cuenta lo siguiente:

- Mayor seguridad en la empresa.
- Planeación y manejo de la seguridad más efectivos.
- Alianzas comerciales más seguras.
- Mayor confianza en el cliente.
- Auditorias de seguridad más precisas y confiables.
- Menor Responsabilidad civil

3.5. S.A.C. (Systems Auditability and Control)

El informe SAC define el sistema de control interno, describe sus componentes, provee varias clasificaciones de los controles, describe objetivos de control y riesgos, y define el rol del auditor interno. El informe provee una guía sobre el uso, administración y protección de los recursos de tecnología informática y discute los efectos de la computación de usuario final, las telecomunicaciones y las tecnologías emergentes.

3.5.1. Definición.- El informe SAC define a un sistema de control interno como: un conjunto de procesos, funciones, actividades, subsistemas, y gente que son agrupados o concientemente segregados para asegurar el logro efectivo de los objetivos y metas.

El informe enfatiza el rol e impacto de los sistema computarizados de información sobre el sistema de control interno. El mismo acentúa la necesidad de evaluar los riesgos, pesar los costos y beneficios y construir controles en los sistemas en lugar de agregarlos luego de la implementación.

3.5.2. Componentes.- El sistema de control interno consiste en tres componentes: el ambiente de control, los sistemas manuales y automatizados y los procedimientos de control. El ambiente de control incluye la estructura de la organización, la estructura de control, las políticas y procedimientos y las influencias externas. Los sistemas automatizados consisten en sistemas y software de aplicación. SAC discute los riesgos de control asociados con los sistemas de usuario final y departamentales pero no describe ni define los sistemas manuales. Los procedimientos de control consisten en controles generales, de aplicaciones y compensatorios.

3.5.3. Clasificaciones.- SAC provee cinco esquemas de clasificación para los controles internos en los sistemas informáticos:

- Preventivos, detectivos, correctivos
- Discrecionales, no discrecionales
- Voluntarios, obligatorios
- Manuales, Automatizados
- Controles de Aplicaciones y Generales

Estos esquemas se enfocan en cuándo se aplica el control, si el control puede ser evitado, quién impone la necesidad del control, cómo se implementa el control, y dónde se implementa el control en el software.

3.5.3.1. Controles Preventivo, Detectivo, Correctivo: El enfoque de la clasificación depende del momento en que se aplica el control. Estos momentos son: Antes, durante o después de que ocurra un error. Ejemplos:

- Se requiere el uso de claves privadas para acceder a los sistemas (Preventivo)
- Preparación de informes de excepción para revisiones subsecuentes(Detectivo)
- Procedimientos automáticos de recuperación de archivos para recrear archivos dañados (Correctivo)

3.5.3.2. Discrecional vs. No Discrecional: El enfoque de la clasificación depende de quien realiza el control (ser humano vs. automatizado) y el grado al cual puede ser evitado. Ejemplos:

- Revisión de firmas autorizadas (Discrecional)
- Requerimiento de ingreso de número de identificación personal (PIN) para el uso de cajeros automáticos (ATMs) (No discrecional)

3.5.3.3. Voluntario vs. Mandatorio: El enfoque de la clasificación depende de quien impone la necesidad de control (interno vs. externo). Ejemplos:

- Controles de razonabilidad sobre los volúmenes de desembolso (Voluntario)
- Los informes de transacciones significativas deben cumplir con los requerimientos de las instituciones financieras (Mandatorio)

3.5.3.4. Manual vs. Automático: El enfoque de la clasificación depende de cuando se implementa el control con o sin automatización. Ejemplos:

- Reconciliaciones efectuadas por empleados(Manual).
- Actualización automática de la cuenta corriente al momento de ingresar una factura(Automático)

3.5.3.5. Aplicación vs. General: El enfoque de la clasificación depende de una transacción individual o el ambiente en el cual se procesan las transacciones. Ejemplos:

- Procedimientos de balanceo computarizados entre subfunciones de un sistema automatizado(Aplicación)
- Mantenimiento de una fuerte función de seguridad de sistemas de información(General)

3.5.4. Objetivos de Control y Riesgos.- Los riesgos incluyen fraudes, errores, interrupción del negocio, y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad, y el cumplimiento. La integridad de la información es resguardada por los controles de calidad del input, procesamiento, output y software. Las medidas de seguridad incluyen los controles de seguridad de los datos, física y de programas. Los controles de cumplimiento aseguran conformidad con las leyes y regulaciones, los estándares contables y de auditoría, y las políticas y procedimientos internos.

CAPÍTULO 4

4. CASO PRÁCTICO: ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN (TI) DE UNA EMPRESA DEL SECTOR INFORMÁTICO .

4.1. Información Preliminar

4.1.1. Introducción.- El presente trabajo ha sido desarrollado en una empresa cuyo nombre se mantendrá en reserva por ética profesional, pero que para referirnos a ella la llamaremos "Admitec".

Admitec ubicada al norte de la ciudad, es una empresa nueva en el ámbito informático, teniendo por ello, un mercado competitivo muy grande de donde quiere resaltar por la calidad y combinación de sus servicios.

Tiene una gama extensa de clientes ya que a pesar de ser nueva, pertenece a un grupo de empresas y por consiguiente presta sus

servicios a los clientes del grupo, además de las empresas del mismo grupo.

La empresa Admitec cuenta con un Departamento de Sistemas destinado al uso del desarrollo tanto informático como electrónico. En el área informática se cuenta con el desarrollo de software utilizados para su venta; además del mantenimiento de los equipos (Hardware) tanto para las empresas del grupo (incluyendo la empresa) como de los clientes. En el área electrónica, la empresa se encarga de dar soporte a los diferentes departamentos de sistemas del grupo. Este soporte consiste en: Networking, aplicaciones de desarrollados, además del soporte a usuario que lo realizan localmente. Todo esto sumado a la garantía de la satisfacción del cliente.

El responsable de este departamento tendrá que buscar el equilibrio deseado entre todos los elementos. Su objetivo, en la Administración de Riesgos de TI, será aquel balance entre los departamentos de sistema del grupo y la satisfacción del cliente.

Las evaluaciones de los controles y seguridades de los sistemas de la empresa constituye uno de los pilares básicos que contribuyen a alcanzar los objetivos y por ende el crecimiento y desarrollo de la empresa.

4.1.2. Motivos del Análisis de Riesgos.- Entre los principales justificativos o motivos del análisis de riesgo encontramos los siguientes:

- Ausencia de personal técnico en el tema de riesgo.
- Desconocimiento de los riesgos informáticos que existen en la organización.
- Desconocimiento de Metodologías de Administración de Riesgos

Estos justificativos son considerados de mayor relevancia en la Administración de Riesgos de TI, por parte de la organización. Por ello se detallada brevemente cada uno de ellos:

4.1.2.1. Ausencia de Personal Técnico en el tema de Riesgos: El recurso humano en las empresas es un factor primordial, ya que son ellos quienes realizan el trabajo día a día. Debido a esto, se le debe prestar la atención necesaria en caso de presentarse algún inconveniente.

Para el mejor desarrollo de la empresa es necesario que el personal sea especializado en el ámbito que se requiera, de no ser así, la capacitación es una de las alternativas para satisfacer el requerimiento del área. En este caso, la necesidad se presenta en el departamento de Sistemas, debido a la ausencia de personal técnico que sea especializado en el tema de riesgos informáticos.

4.1.2.2. Desconocimiento de los Riesgos Informáticos que existen en la organización: El riesgo informático es un tema que en la actualidad se ha difundido en las empresas, motivo por el cual es un foco de análisis por parte de los expertos.

En toda empresa hay riesgos informáticos, ya que hoy en día toda la información se maneja en procesadores. Partiendo de que los riesgos

no son eliminados sino mas bien controlados, los controles y las seguridades cada vez se vuelven más indispensables para la protección de la información.

El desconocimiento del tema de los riesgos informáticos, es un peligro latente ya que las empresas pueden perder la eficiencia y la eficacia en el desarrollo de sus actividades.

4.1.2.3. Desconocimiento de Metodologías de Administración de

Riesgos de TI: Debido a la gran cantidad de riesgos informáticos que pueden haber en una empresa, y a la gama de controles que se pueden aplicar a ellos, existen diferentes maneras de administrarlos, por lo que se han determinado metodologías para su administración.

Para el mejor control de los riesgos latentes en las empresas, existen diferentes metodologías de Administración de Riesgos de TI, que pueden ser aplicadas en el área informática de las empresas.

Para este estudio se han considerado dos metodologías: Magerit y Delphi. Las cuales serán detalladas más adelante.

4.1.3. Objetivo General del Análisis de Riesgos de TI.- El objetivo general del análisis de riesgo es identificar los riesgos potenciales, en una determinada área, que en este caso es el departamento de Sistemas de la empresa, determinar los riesgos existentes y cualificarlos, para poder tener información suficiente al respecto y optar por la metodología de análisis de riesgos a fin de minimizar los efectos de los riesgos dentro del área de Sistemas.

4.1.3.1. Objetivos Específicos del Análisis de Riesgos de TI: Los objetivos de una Administración de riesgos pueden ser varios, todos dependen del análisis de la situación informática .

Entre los principales objetivos que motivan una Administración de Riesgos tenemos:

- Revisar, Evaluar y Actualizar aspectos relacionados tendientes a un control efectivo de la Administración de Riesgos,
- Conocer la situación actual del área de sistemas,
- Establecer la metodología adecuada para la Administración de Riesgos de TI,
- Dar a conocer información acerca de los riesgos informáticos que existen en la empresa,
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información, mediante la recomendación de controles generales.

4.1.3.1.1. Revisar, Evaluar y Actualizar aspectos relacionados tendientes a un control efectivo de la Administración de Riesgos:

Debido a que los riesgos existen desde siempre en toda organización, ha sido necesario buscar la manera de administrarlos de tal manera que se logre tener control sobre ellos.

Con el pasar del tiempo, la administración de riesgos ha ido cambiando de acuerdo a las necesidades actuales de las

organizaciones, por lo que es necesario mantenerse actualizado en este tema.

Para la elaboración de este trabajo ha sido necesario revisar si existían mecanismos de administración de riesgos, evaluarlos y por consiguiente actualizarlos, si así hubiese sido el caso.

4.1.3.1.2. Asegurar una mayor integridad, confidencialidad y confiabilidad de la información: Se entiende por integridad la veracidad y legitimidad de la información de la empresa, a la cual sólo debe de tener acceso el personal autorizado de la empresa.

Además se entiende por confidencialidad el salvaguardo de la información con caracteres reservados y exclusivos a los funcionarios autorizados. La confidencialidad de la información permite el acceso de datos e información sólo a personal autorizado de manera que las transacciones realizadas por un usuario queden registradas como responsabilidad absoluta de la persona que está autorizada a efectuar alguna transacción.

La confiabilidad de la información se refiere a la confianza que pueden tener los clientes sobre dicha información. Una razón más para que no sea de manipulación de cualquier persona de la organización.

4.1.3.1.3. Dar a conocer información acerca de los riesgos informáticos que existen en la empresa: Los riesgos informáticos se vuelven cada vez más un tema importante dentro de las empresas, por lo que es necesario que éstas tengan un personal preparadc en esta área.

Es imprescindible también que dentro el personal del área de sistemas de la empresa, exista un responsable del tema de riegos y seguridad, aunque no sea un experto, éste debe tener conocimientos básicos acerca de los riesgos informáticos.

4.1.4. Alcance del Análisis de Riesgos.- Habiéndose sometido a consideración de los directivos de la empresa, después de realizarse un análisis global, se determinó que el Análisis de Riesgo, se realizará en el área informática del departamento de Sistemas; aunque algunos de los riesgos a tratar involucran implícitamente al área electrónica. El

análisis de riesgos consistirá en aplicar la metodología seleccionada y determinar el nivel de riesgo.

En base a los objetivos y justificativos planteados anteriormente el alcance del trabajo radica en:

4.1.4.1. Evaluar las seguridades físicas del departamento: Estas seguridades tiene como finalidad:

- Establecer seguridades en los accesos de entrada y salida a la empresa y por consiguiente al departamento de sistemas.
- Establecer respaldos actualizados de la información (bases de datos) que tiene el departamento y mantenerlos seguros.
- Contratar un seguro de tal manera que los equipos puedan ser resguardados.

4.1.4.2. Evaluar las seguridades lógicas del departamento: Estas seguridades tienen como finalidad:

- Mantener la confiabilidad, confidencialidad e integridad de la información de la empresa, por medio de la utilización adecuada de la misma.
- Establecer claves de acceso, mediante algún software de seguridad existente en el mercado o desarrollado por la empresa.

4.1.4.3. Definir los controles que deben implantarse: Luego de la observación realizada se debe crear los controles adecuados con la finalidad de garantizar la integridad del servicio, sean éstos:

- Controles Preventivos: Detección y documentación de condiciones anormales relacionadas con los sistemas, programas, hardware, etc
- Controles Correctivos: Tomar acciones luego del daño ocasionado, conjuntamente con su respectiva documentación.
- Controles Detectivos: Evaluar la operatoria actual para proponer mejoras

4.2. Descripción del Entorno Informático (Anexo 3)

La empresa cuenta con equipos de alta tecnología. El entorno informático esta acorde a las necesidades imperantes de la actividad y operación que desarrolla.

El Departamento de Sistemas existe con la finalidad de satisfacer a los usuarios organizacionales otorgando un servicio definido a través de objetivos planteados por la empresa, en un contrato pertinente establecido con la empresa.

Los servicios que presta el Departamento de Sistemas a los usuarios son:

- Desarrollo de Software,
- Venta de Software,
- Soporte Técnico a los departamentos de Sistema del grupo de empresas, y;
- Mantenimiento de equipos.

Desarrollo de Software.- Para el desarrollo de software, la empresa considera las necesidades de las empresas que forman parte del grupo así como las de sus clientes internos y externos.

Venta de Software.- Para la venta de software, la empresa primero analiza las exigencias del usuario, envía la cotización correspondiente y si el usuario acepta la cotización, ésta es reenviada a la empresa, donde se procede a la elaboración de la factura. El departamento de Sistemas recibe una copia de la factura para verificar y luego se procede a la venta del software.

Soporte Técnico.- Para el Soporte Técnico a los departamentos de Sistema del grupo de empresas, primero la empresa que requiere el servicio debe presentar la solicitud correspondiente para el soporte técnico, y ésta a su vez planifica el día que va a brindar dicho soporte técnico.

Mantenimiento de Equipos.- Para el mantenimiento de equipos, el usuario o cliente solicita el servicio al departamento, se planifica la agenda para que el técnico revise el/los equipo(s), el cual luego de haber realizado la revisión, elabora un reporte técnico y es entregado

al jefe del departamento con una copia para el cliente. El jefe del departamento evalúa el reporte técnico y emite un detalle de los costos de materiales, mano de obra y ganancia por la prestación del servicio. Se elabora la cotización, se envía el original al cliente y se archiva la copia. El usuario recibe la cotización original y la analiza, si acepta se ejecuta el trabajo de mantenimiento; y si no, se da por finalizada la transacción.

Una vez aceptada la cotización, se ingresan los datos del cliente y del trabajo, se coordina con el cliente la fecha, se planifica la agenda y el técnico procede a realizar la visita, luego elabora el reporte del trabajo realizado entregándole al cliente la copia y al jefe del departamento el original, quien informa a Contabilidad del cumplimiento del servicio para que prosiga con la facturación.

Si el mantenimiento es realizado a el /los equipo(s) de la empresa, sólo es necesario realizar el informe técnico del trabajo que se ha realizado para contabilizar los gastos de materiales.

4.2.1. Arquitectura Informática

4.2.1.1. Entorno de Red: La empresa cuenta con una red de computadoras donde interactúan veinte y siete máquinas entre servidor y estaciones de trabajo.

En el Departamento de Sistemas, la empresa cuenta con una red BackOffice de Microsoft instalada en el servidor y Windows XP instalado en las terminales.

4.2.1.2. Equipos Disponibles: La empresa cuenta con 27 equipos distribuidos de la siguiente manera: 7 equipos en el área de sistemas y los 20 restantes están distribuidos en los demás departamentos de la empresa.

El departamento Sistemas cuenta con dos servidores: Un servidor de aplicaciones y un servidor de internet. Además cuenta con una PC y cuatro laptop's.

La PC es utilizada por la persona que asiste todo lo referente a coordinación y facturación. Las cuatro laptop's son utilizadas por desarrolladores.

4.2.1.3. Sistema Operativo: El Sistema Operativo que utilizan es Windows XP.

4.2.1.4 Software de Sistemas y Utilitarios

4.2.1.4.1. Lenguaje de Programación: La empresa utiliza el lenguaje de Programación Visual Basic de Visual Studio.

4. 2.1.4.2. Sistemas de Aplicación: En la empresa se han desarrollado los siguientes sistemas:

- Sisterna de Facturación y Puntos de venta,
- Infatech,
- Liquidación de horas trabajadas,
- ControlSys
- Sistema Prepago para centrales telefónicas,
- Teleadmcomp,

- Aplicaciones para manejo de equipos:
    - Equipos de recolección de datos:
        - Accestool
        - Data Online
        - FPUAnalizer
        - Accestool IP
        - Bio_IP
    - Equipos de Comunicaciones:
        - Consola 327
- Aplicaciones de Bajo Nivel (Todas las desarrolladas para los equipos que fabrican)

Todos los sistemas son comercializados, además de ser utilizados en la empresa excepto Consola 327.

También se da mantenimiento técnico a los sistemas ya sea que estén implementados en la empresa o hayan sido comercializados.

4.2.1.4.3. Utilitarios: Con respecto a utilitarios la empresa utiliza el paquete MsOffice.

4.3. Estrategia de Administración de Riesgos de TI

4.3.1. Establecer Metodología.- Luego de una evaluación de las diferentes metodologías que existen para analizar y administrar el Riesgo de Tecnología de Información, la decisión se inclinó por considerar la del criterio de los expertos, que es la metodología Delphi, que consiste en reunir un grupo de personas que conozcan del negocio y tengan noción mínima de los riesgos.

La directiva de la empresa se inclinó por esta metodología ya que consideraron que para poder establecer soluciones en la empresa era imprescindible que se considere la opinión de las personas que colaboran en la organización, en este caso los expertos del departamento de Sistemas, que son cuatro personas conjuntamente con el jefe del departamento de sistemas, las que participan en el desarrollo de la metodología.

4.3.2. Identificar Riesgos de TI.- Una vez definidos los objetivos y el alcance del trabajo a realizar, se desarrollaron criterios de evaluación de riesgos de TI, que es el aspecto en el que se va a centrar esta evaluación, para el Área de Informática.

Para la identificación de los riesgos, se entrevistó a cada uno de los expertos (Ver Anexos 4 al 7), donde explicando el proceso de identificación de riesgos y analizando los problemas que afectan al departamento, se estableció la Matriz de Ponderaciones, proceso que se da mediante una lluvia de ideas de todos los riesgos que han sido observados por cada uno de los expertos dentro del Dpto. desde el inicio de sus actividades, además de las categorías seleccionadas donde afectan estos riesgos (cada riesgo afecta con diferente impacto a cada categorización), (Anexo 8) se llega a la conclusión de que los riesgos más relevantes son los siguientes:

- Accesos ilegales a las Bases de Datos
- Accesos no autorizados al programa aplicativo de ventas
- Falta de Integridad de los Paquetes Comerciales
- Pérdida y/o Destrucción de las Bases de Datos
- Alteración, Destrucción y/o Pérdida de información relevante para la empresa
- Inundaciones
- Incendios
- Mal uso o destrucción de los reportes de trabajo
- Falta de Inventario de los Activos del Dpto.

- Falta de Inventario de las partes y/o piezas de los computadores del Dpto.
- Desactualización de las claves de acceso
- Ausencia de bitácoras de trabajos realizados por el Dpto.
- Ausencia de documentación técnica y formal de los sistemas diseñados y de pruebas
- Ausencia de actualizaciones de respaldos de las Bases de Datos fuera de la empresa
- Ausencia de medidas de seguridad de los equipos del Dpto.
- Ausencia de control en la destrucción de los activos del Dpto.

Para un mejor manejo de los riesgos encontrados, los expertos determinaron clasificar dichos riesgos y la determinación de las amenazas que compondrán la matriz. (Ver Anexo 10).

4.3.3. Análisis del Riesgos.-

4.3.3.1. Valorar el Riesgo Inherente: Para la valoración de los riesgos que se analizan, se definió una escala de valoración

Cualitativa, que es la asignación de las características Alto, Medio y Bajo a los diferentes riesgos encontrados.

4.3.3.2. Determinar Controles Existentes: El Departamento tiene ciertos controles, pero carece de otros controles que son necesarios ya sea para prevenir, detectar o corregir la materialización de los Riesgos (Ver Anexo 9).

4.3.3.3. Identificar Nivel de Exposición : Cabe recalcar que el Nivel de Exposición es igual a decir Riesgo Inherente menos Controles. Por determinación del grupo involucrado en el trabajo, se pudo determinar que la empresa tiene un nivel de exposición medio-alto, ya que no tiene los suficientes controles necesarios para restarle a los riesgos inherentes. Esto se puede definir dependiendo de las siguientes afirmaciones:

Exposición Alta: Tiene una exposición al riesgo alta.

Exposición Media: Tiene una exposición al riesgo media

Exposición Baja: Es baja la exposición que tiene al riesgo.

4.3.3.4. Método Matricial para el Análisis de Riesgos: Este método utiliza una matriz que muestra gráficamente tanto las amenazas a que están expuestos los sistemas computarizados y la información del departamento, como los objetos que comprenden el departamento de Sistemas.

Se describe a continuación los pasos para el desarrollo del método:

- Crear la matriz de amenazas (causas de riesgo) y de objetos del sistema a analizar.
- Categorizar los riesgos.

4.3.3.4.1. Crear la matriz de amenazas y de objetos: Luego de ponderar los riesgos y determinar las amenazas existentes dentro del Departamento, (trabajo realizado por el grupo de expertos), se determinaron los que compondrán la Matriz de Control de Riesgos (Amenazas y Objetos). (Ver Anexo 11)

4.3.3.4.2. Categorización de Riesgos: Se categorizan las amenazas por niveles de riesgo, de mayor a menor en orden de importancia, como haya sido determinado por el grupo Delphi. (Ver Anexo 12)

Luego los cinco expertos proceden a votar. La votación se realiza de manera vertical y horizontal. (Ver Anexo 13)

Después se suman los votos derechos de las columnas y los votos izquierdos de las filas; y para la cifra total se suman los resultados antes obtenidos. (Ver Anexo 14)

Paso a seguir, se procede a categorizar la sensibilidad de los objetos. Proceso que se inicia pasando los objetos que registra la matriz de control de riesgos en una hoja de comparación de categorías de riesgos. Para categorizar la sensibilidad de los objetos se utiliza como criterio la percepción que tenga cada uno de los miembros del equipo Delphi sobre objetos que puedan causar mayor pérdida económica si se daña o causa demoras en el procesamiento. (Ver Anexo 15)

A seguir, se procede a la votación del grupo de igual manera como se realizó con la categorización de las amenazas. (Ver Anexo 16)

De igual manera se procede a sumar de la misma manera que se realizó con las amenazas. (Ver Anexo 17)

Con la categorización tanto de las amenazas como los objetos, se realiza la combinación de las dos categorías, elaborando una matriz de combinaciones, colocando los totales en orden de mayor a menor (de izquierda a derecha y de arriba abajo), en los dos casos. (Ver Anexo 18)

Después se procede a realizar los cálculos correspondientes, multiplicando los valores de las amenazas con los de los objetos para así poder obtener el nivel de riesgo / sensibilidad de las celdas de acuerdo con el valor del producto. Puede que al terminar este proceso se presenten repeticiones, las cuales no son consideradas para determinar el nivel de riesgos de las celdas. Luego dividimos las celdas en regiones de mayor, menor y mediano riesgo. (Ver Anexo 19)

Como en este caso no existen repeticiones en los productos, se consideran las 36 celdas para la determinación del nivel de riesgo. Se procede a dividir las 36 celdas para el número de expertos (36 / 5 = 7,2 = 7). La escala de valoración es Semicuantitativa ya que se asignan rangos numéricos a las características Alto, Medio y Bajo. Se toman las siete celdas con los productos más altos para determinarlas con un nivel de riesgo alto, las siete celdas con los productos más

bajos para determinarlas con un nivel de riesgo bajo; y las veinte y dos celdas restantes se las determina con un nivel de riesgo medio. (Ver Anexo 19)

4.3.4. Diseñar los controles definitivos.- Finalmente, con el resultado del trabajo realizado, apoyados en el Método Delphi y en el modelo matricial Riesgo / Sensibilidad, se diseñan y documentan de controles a nivel: preventivo, detectivo y correctivo; de acuerdo al área informática del Departamento de Sistemas, que servirán como referencia a los expertos del Dpto. (Ver Anexo 20)

4.3.5. Presentar los Resultados.- La Gerencia de la empresa debe de conocer el resultado del análisis de riesgo de manera oportuna, el cual será presentado en un informe detallado. De esta manera la Gerencia podrá tomar las acciones necesarias para su implantación. A continuación colocaremos los resultados.

4.3.5.1. Informe de los Resultados: Luego de concluir el Análisis de Riesgo de TI, se ha determinado el grado de prioridad de los riesgos que afectan al área de Sistemas, para lo cual se realizan las respectivas recomendaciones.

Categoría 1: Archivos de Seguridades de las Bases de Datos.

Riesgo 1: Accesos Ilegales a las Bases de Datos

Recomendación: Es necesario que se establezca quienes son las personas autorizadas al acceso de las Bases de Datos, ya que no es conveniente que no se tenga restricciones a esta parte de la información. Los autorizados deberán tener otro código o clave de acceso al momento de acceder a esta información y deberán cerrar esta sesión una vez realizado el trabajo que se haya establecido. Las claves establecidas deberán ser cambiadas constantemente para mantener un control sobre dichos accesos.

Riesgo 2: Alteración, Destrucción y/o Pérdida de información relevante para la empresa.

Recomendación: Parte de la información relevante para la empresa, son los archivos de seguridades de las bases de datos; archivos a los cuales sólo debe de tener acceso la persona encargada de las bases. Estas seguridades deberán ser cambiadas en determinado periodo de tiempo que podría ser un mes, de tal manera que se dificulte cualquier tipo de acceso ilegal a estos archivos.

Por otro lado toda la información que la empresa considere relevante, deberá mantenerse bajo resguardo ya sea mediante claves, respaldos, etc. Mediante el acceso adecuado de las personas a determinada

información que se encuentre en el Dpto., se mantendrá un mejor control sobre la seguridad de ésta.

Riesgo 3: Desactualización de las Claves de Acceso

Recomendación: Las claves de acceso a la información del Dpto. es una medida de seguridad a la cual se le debe de prestar la importancia que amerita. La No actualización de éstas, podría ocasionar no sólo la pérdida de la información sino pérdidas económicas, además de la imagen de la empresa en el mercado. Por lo que se sugiere la actualización de éstas en determinados periodos de tiempo, los cuales pueden ser establecidos por el Jefe del Área en conjunto con la Gerencia. Estas actualizaciones servirán como un monitoreo continuo de la seguridad de la información.

Categoría 2: Bases de Datos de Clientes y Proveedores.

Riesgo 4: Pérdida y/o Destrucción de las Bases de Datos

Recomendación: Las Bases de Datos (Clientes y Proveedores), son parte esencial del desarrollo de la empresa, por lo que se debe poner énfasis en la seguridad de esta clase de información. Además de las claves de accesos que poseen las Bases de Datos, el servidor o servidores donde se encontrarán éstas, deben de estar en un lugar

fuera del alcance de terceros, de ser posible en una oficina con seguridad que podría ser la del Jefe del Departamento de Sistemas, lugar al cual sólo debería tener acceso el encargado de las Bases (el Jefe). Además de mantener los respaldos actualizados tanto dentro como fuera de la empresa. De esta manera se podrán evitar tanto la pérdida como la destrucción de las bases, riesgos que podrían acarrear con consecuencias mayores a sólo la pérdida de la información.

Riesgo 5: Inexistencia de actualizaciones de Respaldos de las Bases de Datos fuera de la empresa.

Recomendación: Las actualizaciones de las Bases, es otra medida de asegurar la información en caso de incidentes. Además del respaldo que se encontrará en otra área diferente al de las computadoras, se deberá mantener dos respaldos de las Bases de Datos, tanto de clientes como de proveedores, fuera de la empresa, con sus respectivas actualizaciones en los periodos de tiempo que sean determinados por la empresa, de acuerdo a los cambios de información que se realicen en el Dpto. Las actualizaciones que se encontrarán fuera de la empresa, también deberán encontrarse en lugares seguros; lugares que serán de conocimiento sólo de la Gerencia de la empresa para mayor seguridad.

Categoría 3: Paquetes Comerciales

Riesgo 6: Falta de integridad de los Paquetes Comerciales

Recomendación: Una de las actividades que proporcionan ingresos, es la venta de los Paquetes Comerciales, los cuales son adaptados de acuerdo con las necesidades de los clientes. Por esta razón es importante que esta información sea integra. Los desarrolladores de estos paquetes comerciales, no deberán tener acceso a éstos una vez realizados; a no ser que se necesite realizar alguna modificación de acuerdo a los requerimientos del cliente, para lo cual se realizará una orden de modificaciones, y sólo así el desarrollador tendrá acceso al programa. Una vez realizadas las modificaciones, deberán realizase pruebas para asegurarse del correcto funcionamiento del programa. Los archivos de programación de estos paquetes, es parte de la información relevante que mantiene la empresa por lo que están dentro de las recomendaciones emitidas anteriormente.

Categoría 4: Programa Aplicativo de Ventas

Riesgo 7: Acceso no autorizado al Programa Aplicativo de Ventas

Recomendación: El programa aplicativo de Ventas, es el software con mayores modificaciones debido a la variedad de requerimientos de los clientes. Razón por la cual el acceso a éste es muy concurrente y sólo debe ser realizado por el Técnico al cual se le haya emitido la

Orden de Modificaciones, y una vez terminadas las éstas y sus respectivas pruebas, se deberá volver a resguardar esta información, de tal manera que nadie tenga acceso a más de la persona encargada de la seguridad de la información. Esta medida ayudará no sólo ala integridad de la información, sino también la confidencialidad dela misma.

Categoría 5: Reportes de la realización de trabajos de Mantenimiento

Riesgo 8: Mal uso o Destrucción de los Reportes de Trabajo

Recomendación: Otra manera de generar ingresos a la empresa, es la realización de mantenimiento de equipos ya sea de clientes o del Grupo al cual pertenece la empresa. Los reportes realizados por los técnicos deben de ser confirmados por el jefe del Dpto. para asegurarse de que el trabajo fue realizado correctamente. La elaboración de estos informes deberán ser realizados si es posible en órdenes preimpresas o por lo menos con una secuencia en su emisión, para controlar que no haya posibilidad de destrucción o pérdida de alguno de los reportes. Para un monitoreo futuro es recomendable que cada cierto tiempo se realice un checklist de los reportes de los trabajos que se hayan realizado.

Riesgo 9: Ausencia de Bitácoras de trabajos realizados por el Dpto.

Recomendación: Para la realización de esta actividad, se deberá emitir una orden de trabajo, mediante la cual se notificará al técnico el trabajo a realizar. Una vez realizado el trabajo, es de prioridad del técnico la realización del reporte respectivo. Los reportes de los trabajos realizados se deberán entregar al Jefe del Dpto. para confirmar la culminación de éste. A su vez el jefe deberá archivar cada uno de los reportes, de manera tal que se tenga constancia de los trabajos que se han realizado para futuras correcciones o simples revisiones. Estas bitácoras deberán ser mantenidas en un lugar seguro de manera que se evite el deterioro de las mismas. Cabe recalcar la recomendación del punto anterior: La preimpresión o la secuencia de los reportes.

Riesgo 10: Inexistencia de documentación técnica formal de los sistemas diseñados y de pruebas.

Recomendación: Cada sistema que se ha desarrollado en el Dpto. deberá tener una documentación de la realización del mismo, detallando de manera comprensible para cualquier otro desarrollador, la elaboración del sistema. Esta documentación técnica escrita, deberá ser archivada conjuntamente con cada uno de los reportes o

documentación de modificaciones de los sistemas y sus respectivas pruebas.

Categoría 6: Partes y/o Piezas del Computador

Riesgo 11: Falta de inventario de las partes y/o piezas de los computadores del Dpto.

Recomendación: Aunque no sea una pérdida económica significativa, no deja de ser una pérdida. Los mantenimientos de equipos que se hacen en el Dpto. de Sistemas de la empresa, suelen demoran un mínimo de 24 horas. Para dichas pruebas se utilizan piezas o partes de los computadores que se encuentran en el Dpto. Razón por la cual es recomendable que se mantenga un inventario de las partes y/o piezas de los equipos que forman parte del Dpto. Por ser piezas relativamente pequeñas es muy fácil la pérdida de éstas. El inventario ayudará a manera de monitoreo cada cierto tiempo a controlar la existencia de las piezas que formen parte de dicho inventario. Las partes y/o piezas nuevas, deberán ser puestas en inventario antes que pasen a formar parte de algún computador.

Riesgo 12: Falta de Inventarios de Activos del Dpto.

Recomendación: A más de las piezas y/o partes de los computadores, el Dpto. cuenta con una serie de activos sobre los cuales no existe inventario alguno. Motivo por el cual se recomienda la realización de un inventario de existencias físicas, inventario que deberá ser realizado bajo supervisión. Una medida de control para tiempos posteriores es la verificación continua (tiempo que puede ser determinado aleatoriamente para no prevenir a nadie) de los activos, disminuyendo así la probabilidad de pérdida de algún activo del Dpto.

Riesgo 13: Ausencia de medidas de seguridad de los equipos.

Recomendación: Los computadores son los medios de trabajo del Dpto. y es donde se almacena la información de la empresa. Por lo que es preciso contratar un seguro para proteger no sólo los activos de la empresa sino también los equipos del área de sistemas, ya que la ausencia de un seguro acarrearía pérdidas aún mayores a las que podrían darse con un de estos. Además que es la manera de recuperar en dinero parte de lo que se perdería en caso de algún incidente.

Riesgo 14: Ausencia de Control en la Destrucción de los Activos del Dptc.

Recomendación: A más del inventario que es una manera de controlar las existencias, es necesario que esas existencias se conserven en buen estado, para lo cual se sugiere establecer un control semanal del buen funcionamiento de los equipos, ya que si estos funcionan bien, por ende sus piezas también. En caso del daño de algún activo, deberá comunicarse la situación y su(s) causas. Se analizará las causas y de llegarse a determinar algun responsable, la Gerencia deberá señalar alguna sanción para el(los) implicado(s).

Riesgo 15: Incendios

Recomendación: Una de los accidentes que aunque no ocurren con frecuencia pero que si ocasionan pérdidas económicas grandes, son los incendios, para lo cual se requiere la implementación de alarmas contra incendios. De no ser posible la implementación inmediata de éstos, se deberá por lo menos dar el correcto mantenimiento a los extintores (2) del Dpto. y de la empresa en general.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La Administración de Riesgos de TI es importante ya que es una aproximación científica del comportamiento de los riesgos, anticipando posibles perdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

2. La Administración de Riesgos de TI es un proceso multifacético y participativo, el cual es frecuentemente mejor llevado a cabo por un equipo multidisciplinario.

3. El principal objetivo de la Administración de Riesgos de TI, como primera ley de la naturaleza, garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos. Muchos de los defectos en la administración de riesgos radica en la ausencia de objetivos claros.

4. Se debe enfatizar y relevar la importancia y la significación de la Administración de Riesgos de TI, debido a la trascendencia de los controles y seguridades de los sistemas de procesamiento de información que ameritan ser implementados en toda la organización.

5. La Administración de Riesgos de TI, dentro de la empresa, es una herramienta muy útil para el mejor desarrollo de las actividades de un departamento o de todos los departamentos de la organización.

6. La Administración de Riesgos de Tecnología de Información, nos muestra los principales controles y seguridades que deben implementarse en uno de los departamentos de la empresa como es el caso del departamento de sistemas.

7. El análisis de riesgos de TI, desarrollado en la empresa, ha contribuido a ampliar aún más los conocimientos sobre los problemas significativos que pueda tener el área de sistemas de una empresa y sobre las múltiples ideas de soluciones que se pueden aplicar.

8. En el trabajo se pudieron determinar una serie de hallazgos como:

   - Inexistencia de Respaldos de las Bases de Datos (Clientes y Proveedores)
   - Ausencia de seguridades de la Información
   - Inexistencia de Bitácoras de las Actividades del Departamento de Sistemas
   - Inexistencia de Planes de Contingencia
   - Inexistencia de seguros para la protección de los Equipos
   - Carencia de seguridades en la empresa
   - Inexistencia de documentación y de seguridad de la Información
   - Inexistencia de Manuales de Funciones

9. Este trabajo tiene como una de sus metas primordiales el orientar a las generaciones futuras, sobre los aspectos importantes que se deben considerar en la administración de riesgos de Tecnología de Información de las empresas del sector informático.

10. Este trabajo así como es un apoyo a la empresa, también es una guía para quienes en un futuro desarrollen actividades sobre la Administración de Riesgos de TI en una empresa determinada.

RECOMENDACIONES

1. La empresa Admitec debería designar un área o un grupo de personas que se encarguen de implementar los controles determinados en el trabajo y posteriores monitoreos de revisión de éstos.

2. El departamento de sistemas debería poner énfasis en su organización, ya que el no hacerlo le podría acarrear costos aún mayores.

3. Con el crecimiento de las empresa crecen también los riesgos y aparecen nuevos, por lo que la empresa en conjunto con el Departamento de Sistemas deben realizar el Análisis de Riesgos cada cierto tiempo (Establecido dependiendo de la situación de la empresa).

4. Antes de la elaboración de un Análisis de Riesgo, es necesario tener el suficiente conocimiento acerca del tema, para tener un mejor desarrollo del trabajo.

5. Es necesario que las personas que conforman el Departamento de Sistemas, tengan el conocimiento tanto para la elaboración del análisis como para la revisión y monitoreo del trabajo una vez implementado.

6. A las generaciones futuras que deseen trabajar en este campo, es necesario que estén actualizados tanto de la metodología como de los riesgos y su efecto en las empresas tanto grandes como pequeñas.

BIBLIOGRAFÍA

1. **Cepeda Gustavo**, 1997. Auditoría y Control Interno, Segunda Edición, McGraw-Hill Interamericana S.A., Colombia, Páginas 208-224, 227-232

2. **Gill Morell M.,** 2000. Informática y Comunicaciones, GIGA Nº 2, Revista Cubana de Computación, Cuba.

3. **Mc Connell Steve,** 1996. Desarrollo y Gestión de Proyectos Informáticos: Gestión de Riesgos, Primera Edición, McGraw-Hill, España.

4. **Piattini Mario y Del Peso Emilio,** 2004. Auditoría Informática: Un Enfoque Práctico, Segunda Edición, Editorial RA-MA, España, Páginas 45-89, 310-317, 394-401, 570-581, 616

5. **Pinilla Forero José Dagoberto,** 1997. Auditoría Informática - Aplicaciones en Producción: Análisis de Riesgos, Primera Edición, ECOE Ediciones, Colombia, Páginas 129-141, 165-186.

6. **Sallenave Jean Paul,** 1996. Gerencia y Planeación Estratégica: El Método Delphi, Segunda Edición, Editorial Norma, Colombia.

7. **Wesberry Jim,** 1998. Prácticas Corporativas para minimizar el Riesgo, Revista americana, Georgia-EE.UU. Páginas 2-7.

8. **AUDISIS,** 2003. Ideas para considerar en el Control Interno y la Auditoria de su Empresa, Boletín Nº 2, www.audisis.com, Colombia, Páginas 1-4

9. **Comité Directivo de COBIT e ISACA,** 1998. COBIT. Directrices de Auditoría, Segunda Edición, www.isaca.org, EE.UU., Páginas 8-18, 23-27, 70-73.

10. **Comité Directivo de COBIT y El IT Governance Institute,** 2002. COBIT. Objetivos de Control, Tercera Edición, www.isaca.org, www.ltgovernance.org, EE.UU., Páginas 5-20, 52-54.

11. **KPMG LLP,** 2003. Sarbanes-Oxley. Section 404: Management Assessment of Internal Control and the proposed Auditing Standards, Primera Edición, www.kpmg.com, EE.UU. Páginas 9-12, 17-20.

12. **Procuraduría General de la Nación,** 2003. Programa de Administración de Riesgos. Publicación de la Oficina de Control Interno, Colombia, Páginas 7-15.

13. **2001,** http://microsoft.com/spain/technet/recursos/articulos/srsgchoz.mspx, EE.UU.

14. **2002,** http://www.atlatl.com.mx/docs/wesb_practcorp.pdf, EE.UU.

15. **2002,** http://www.sarbanesoxley-comp.com/directory/acta-sarbanes-oxley.html, EE.UU.

16. **2003,** http://www.monografias.com, Auditoria de Sistemas, Chile.

17. **2004,** http://www.s2grupo.com, Gestión de la Seguridad de la Información, España.

18. **2004,**http://www.gestiopolis.com/recursos/documentos/fulldocs/ger1/sistecinf or.htm, Colombia

ANEXOS

ANEXO 1

PROGRAMA DE TRABAJO

Empresa: Admitec **Dpto:** Sistemas

OBJETIVOS/PROCEDIMIENTOS	REF.	H. Por	FECHA
RELEVAMIENTO DE INFORMACIÓN			
Objetivo			
Adquirir conocimiento del entorno informático de la organización.			
Procedimientos			
1. Realizar una Guía de Visita previa que nos permita identificar el objetivo y	Anexo 2	J. Maxitana	
estructura orgánica del departamento de sistemas, modificaciones en la misma,			
y la existencia de manuales de usuario y funciones del departamento.			
2. Entrevistar al Jefe del Departamento para tener información más precisa	Anexo 3	J. Maxitana	
acerca del área informática: los servicios que presta el departamento, detallan-			
do cada uno y su funcionamiento), los software's que utilizan por medio de los			
cuales interactúan todos los sistemas, los equipos con los que cuenta el dpto.,			
la manera en que están distribuidos, el sistema operativo que manejan, su			
lenguaje de programación, los sistemas desarrollados en la empresa, los que			
usan dentro de la misma, y los utilitarios utilizados. (Cuestionario del Entorno			
Informático)			

3. Entrevista al Técnico denominado # 1 para determinar los controles	Anexo 4	J. Maxitana	
y vulnerabilidades considera que afectan al departamento de sistemas.			
4. Entrevista al Técnico denominado # 2 para determinar los controles	Anexo 5	J. Maxitana	
y vulnerabilidades considera que afectan al departamento de sistemas.			
5. Entrevista al Técnico denominado # 3 para determinar los controles	Anexo 6	J. Maxitana	
y vulnerabilidades considera que afectan al departamento de sistemas.			
6. Entrevista al Técnico denominado # 4 para determinar los controles	Anexo 7	J. Maxitana	
y vulnerabilidades considera que afectan al departamento de sistemas.			
ANÁLISIS DE RIESGOS			
Objetivo			
Establecer los niveles de riesgo / sensibilidad en el departamento de sistemas.			
Procedimientos			
1. Realizar la Matriz e Ponderación de Risgos que se encuetran en el Dpto.	Anexo 8	J. Maxitana	
2. Establecer el Cuadro de la Valoración de los Riesgos Existentes	Anexo 9	J. Maxitana	
3. Establecer el Cuadro de los Controles Necesarios	Anexo 10	J. Maxitana	
4. Establecer la Matriz de Amenazas y Objetos.	Anexo 11	J. Maxitana	
5. Realizar la Comparación de Categorías de Riesgos (Amenazas)	Anexo 12	J. Maxitana	
6. Realizar el Proceso de Votación (Amenazas)	Anexo 13	J. Maxitana	

7. Realizar la suma de votos de las Amenazas	Anexo 14	J. Maxitana	
8. Elaborar la Comparación de Categorías de Riesgos (Objetos)	Anexo 15	J. Maxitana	
9. Elaborar el Proceso de Votación (Objetos)	Anexo 16	J. Maxitana	
10. Realizar la suma de los votos de los Objetos	Anexo 17	J. Maxitana	
11. Realizar la Matriz de Combinación de las 2 Categorías	Anexo 18	J. Maxitana	
12. Ralizar la Matriz de Resultados con Riesgos de Sensibilidad e Identificación de Niveles de Riesgo.	Anexo 19	J. Maxitana	
13. Establecer y documentar los Controles Definitivos.	Anexo 20	J. Maxitana	
		ELAB: J. MAXITANA	**FECHA:**
		REV.	**FECHA:**

ANEXO 2

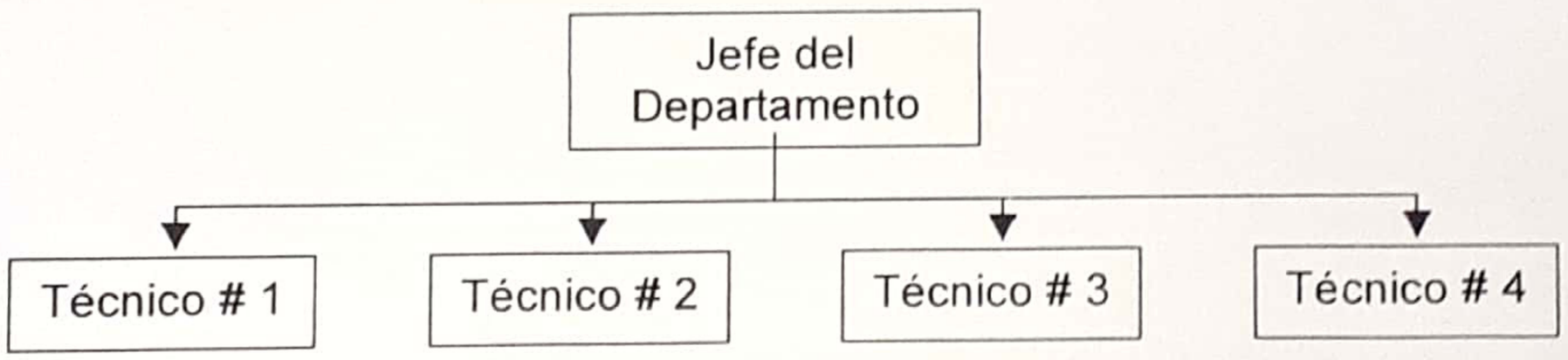
GUIA DE VISITA PREVIA

INFORMACIÓN GENERAL

Nombre de la entidad: Admitec
Nombre del Departamento: Sistemas
Persona Entrevistada: Jefe del Departamento

1. ¿Cuál es el objetivo del Departamento de Sistemas?
El objetivo del departamento de Sistemas es satisfacer las necesidades del cliente o de los usuarios de las empresas que conforman el grupo.

2. ¿Cuál es la estructura orgánica del Departamento?



3. ¿Ha existido alguna modificación en la estructura orgánica?

Si No

4. ¿Existe un manual de las usuario del Departamento?

Si No

5. ¿Existe un manual de funciones del Departamento?

Si No

6. ¿Existe un manual de procedimientos del Departamento?

Si No

7. ¿ Qué funciones realizan los diferentes técnicos del Departamento de Sistemas?

Los técnicos del área están desde la iniciación de la empresa, y la iniciación se dio a la organización de un grupo de colegas, los que ahora son técnicos del Departamento.

Todos conocen de las operaciones que se desarrollan dentro del departamento, por lo que todos están capacitados para realizar las diferentes actividades.

Las actividades que realizan se las van asignando de acuerdo a como se vayan desocupando de tareas anteriores.

OBSERVACIÓN: Por ética profesional se omitirá los nombres de los técnicos en la entrevistas a cada uno de ellos. Por lo que se los denominará: Técnico 1, Técnico 2, Técnico 3 y Técnico 4.

ANEXO 3

CUESTIONARIO
DESCRIPCIÓN DEL ENTORNO INFORMÁTICO

Empresa: Admitec
Departamento: Sistemas
Persona Entrevistada: Jefe del Departamento

1. ¿Qué servicios presta el Departamento de Sistemas (Detalle cada servicio y su funcionamiento)?
El servicio está dividido en dos grupos y se los describe a continuación:

Para el Grupo: Nuestra empresa por ser la única empresa del grupo que se dedica al desarrollo tanto informático como electrónico, somos los que nos encargamos de dar el soporte técnico a los diferentes departamentos de sistemas del grupo que conformamos. Damos soporte Networking; aplicaciones de desarrolladas y el soporte a usuarios se lo realiza localmente. Además del mantenimiento de los equipos del grupo.

Para el cliente: La empresa se encarga de desarrollar software que se los comercializa. Además del mantenimiento de los equipos de los clientes. Y en muchas ocasiones damos soporte vía telefónica y presencial a nuestros distribuidores.

2. ¿Qué software es utilizado por la empresa por medio del cual interactúan todos los sistemas?
Estamos trabajando con una red BackOffice instalada en el servidor y en terminales con XP.

3. ¿Con qué equipos cuenta el Departamento de Sistemas?
Tenemos dos servidores: Aplicaciones e Internet. Además de una PC y cuatro laptop's.

4. ¿Cómo están distribuidos los equipos con que cuenta el Departamento de Sistemas?

La PC es utilizada por la persona que asiste en todo lo que significa coordinación y facturación, y las 4 laptop son utilizadas por los desarrolladores.

5. ¿Qué sistema Operativo manejan?
Windows XP

6. ¿Qué lenguaje de programación utiliza el Departamento?
Se maneja Vb Studio

7.- ¿Cuáles son los sistemas desarrollados en la empresa?
En la empresa se han desarrollado los siguientes sistemas:

- Sistema de Facturación y Puntos e Venta,
- Infatech,
- Liquidación de horas trabajadas,
- ControlSys,
- Sistema Prepago para centrales telefónicas,
- Teleadmcomp,
- Aplicaciones para manejo de equipos:
    - Equipos de recolección de datos:
        - Accestool,
        - Data Online,
        - FPUAnalizer,
        - Accestool IP,
        - Bio_IP,
    - Equipos de Comunicaciones:
        - Consola 327,
- Aplicaciones de Bajo Nivel (Todas las desarrolladas para los equipos que fabrican).

8. ¿De los sistemas antes mencionados, cuáles son los que se aplican en la empresa?
La empresa maneja todos menos Consola 327.

9. ¿Cuáles son los utilitarios que se utilizan en el departamento?
Al igual que el resto de la empresa, el departamento de Sistemas maneja el paquete MsOffice.

ANEXO 4

ENTREVISTAS A TÉCNICOS DEL DEPARTAMENTO DE SISTEMAS DE ADMITEC

Persona Entrevistada: Técnico 1 (Nombre Ficticio)

CONTROL SOBRE INFORMACIÓN IMPRESA

1. ¿Cómo utiliza los reportes de trabajos realizados por el Departamento?
Una vez realizado el reporte de algún cliente, éste es entregado al Jefe del Departamento y éste a su vez debería ser el encargado de archivarlo.

2. ¿Qué criterio tiene en cuanto a la eliminación o modificación desautorizadas de reportes?
Si se llegase a dar el caso, todo depende del Jefe del Departamento ya que es él quien se encarga de ellos.

3. ¿Se cuenta con un manual de usuario por Sistema?
1.- SI (**X**) 2.- NO ( )

4. Si existe. ¿Es claro y objetivo el manual del usuario?
1.- SI (**X**) 2.- NO ( )

5. ¿Conoce Ud. de la existencia de manuales técnicos en el departamento de Sistemas?
1.- SI ( ) 2.- NO (**X**)

6. ¿Conoce Ud. de la existencia de documentos que detallen las pruebas de sistemas?
1.- SI ( ) 2.- NO (**X**)

SEGURIDADES LÓGICAS Y FÍSICAS

1.¿Qué piensa de la seguridad en el manejo de la información en el Departamento de Sistema?
1.- Nula ( ) 2.- Riesgosa (**X**)
3.- Satisfactoria ( ) 4.- Excelente ( )
5.- Lo desconoce ( ) ¿Por que?

2. Indique cuál(es) control(es) interno(s) existe(n) en el Dpto. de Sistemas:

1.- Procedimientos para operar en el Dpto. departamento (**X**)
2.- Inventario de activos ( )
3.- Claves de acceso a los sistemas ( ),
4.- Seguridades de las Bases de Datos ( )
5.- Manuales de Funciones (**X**)
6.- Control de archivos de seguridades ( )
7.- Paquetes Comerciales ( )

3. ¿Quién(es) tiene(n) acceso a las Bases de Datos?

El Jefe del Departamento y mi persona.

4. ¿Existe un registro de anomalías de los Programas?

No, por que todo se escribe en una pizarra.

5. ¿La solicitud de modificaciones a los programas se hacen en forma?

1.- Oral? (**X**)
2.- Escrita? ( )

6. ¿Cuál de los programas es el que presenta más anomalías y quién realiza sus modificaciones?

El programa de Ventas y las modificaciones son realizadas por mi persona que soy quien maneja mejor el programa.

7. ¿Se hace un reporte diario, semanal o mensual de las actividades del Dpto. a la Gerencia?

1.- SI (**X**) 2.- NO ( )

8. ¿Se tienen respaldos de las Bases?

1.- SI (**X**) 2.- NO ( ) Sólo al que está en la empresa

9. ¿Se cuenta con respaldos actualizados de las bases en lugar distinto al de las computadoras?

1.- SI ( ) 2.- NO (**X**)

10. ¿Existen procedimientos de actualización de las copias que se encuentran fuera de la empresa?

1.- SI ( ) 2.- NO (**X**)

11. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:

0 ( ) 1 ( ) 2 ( ) 3 (**X**)

12. ¿Dónde se almacenan estas copias?
1.- Departamento de Sistemas ( )
2.- Otra área de la empresa (X) 3.- Fuera de la empresa (X)

13. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?
1.- SI ( ) 2.- NO (X)

14. ¿Se tienen seguros sobre todos los equipos?
1.- SI ( ) 2.- NO (X)

15. ¿Se han adoptado medidas de seguridad en el departamento de sistemas?
1.- SI ( ) 2.- NO (X)

16. ¿Existen una persona responsable de la seguridad?
1.- SI ( ) 2.- NO (X)

17. ¿Existe vigilancia en el departamento durante las horas laborales?
1.- SI (X) 2.- NO ( )

18. El edificio donde se encuentra la computadora esta situado a salvo de:
1) Inundación? ( ) 2) Terremoto? ( )
3) Fuego? ( ) 4) Sabotaje? ( )

19. El centro de cómputo tiene salida al exterior al exterior?
1.- SI ( ) 2.- NO (X)

20. ¿Existe alarma para:
1.- Detectar fuego(calor o humo) en forma automática? ( )
2.- Avisar en forma manual la presencia del fuego? (X)
3.- Detectar una fuga de agua? (X) **Diciendo**
4.- Detectores magnéticos? ( ) 5.- No existe ( )

21. Existen extintores de fuego:
1.- Manuales? (X) 2.- Automáticos? ( ) 3.- No existen ( )

22. ¿Se ha adiestrado el personal en el manejo de los extintores?
1.- SI ( ) 2.- NO (X)

23. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
1.- SI (X) 2.- NO ( )

24. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
1.- SI (**X**) 2.- NO ( )

25. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
1.- Evitando artículos inflamables en el departamento de cómputo (**X**)
2.- Prohibiendo fumar a los operadores en el interior (**X**)
3.- Vigilando y manteniendo el sistema eléctrico (**X**)
4.- No se ha previsto ( )

CONTROL DE OPERACIÓN

1. ¿Existen procedimientos formales para la operación del Departamento de Sistema?
1.- SI (**X**) 2.- NO ( )

2. ¿Están actualizados los procedimientos?
1.- SI (**X**) 2.- NO ( )

3. Determine la eficiencia con que se ejecutan los trabajos dentro del Departamento de Sistemas, tomando en cuenta equipo y técnico, a través de inspección visual.
1.-Mala ( ) 2.-Regular ( ) 3.-Buena ( ) 4.-Muy Buena (**X**) 5.-Excelente ( )

4. ¿Tiene el conocimiento necesario para actuar en caso de errores en los sistemas?
1.- SI ( ) 2.- NO (**X**)

5. Las intervenciones de los técnicos en los sistemas son:
Son muy numerosas? 1.- SI ( ) 2.- NO (**X**)
Se limitan a los mensajes? 1.- SI (**X**) 2.- NO ( )

6. ¿Se tiene un control adecuado sobre los programas que están en operación?
1.- SI ( ) 2.- NO (**X**)

7. ¿Cuentan los técnicos con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?
1.- Si, por máquina ( ) 2.- Si, escrita manualmente ( ) 3.- NO (**X**)

8. ¿Existe un lugar para archivar las bitácoras de los sistemas diseñados por el Dpto.?
1.- SI ( ) 2.- NO (**X**)

ANEXO 5

ENTREVISTAS A TÉCNICOS DEL DEPARTAMENTO DE SISTEMAS DE ADMITEC

Persona Entrevistada: Técnico 2 (Nombre Ficticio)

CONTROL SOBRE INFORMACIÓN IMPRESA

1. ¿Cómo utiliza los reportes de trabajos realizados por el Departamento?
No siempre se realizan reportes de los trabajos realizados.

2. ¿Qué criterio tiene en cuanto a la eliminación o modificación desautorizadas de reportes?
No estoy de acuerdo, pero en tal caso, no sería algo de fácil detección.

3. ¿Se cuenta con un manual de usuario por Sistema?
1.- SI (**X**) 2.- NO ( )

4. Si existe. ¿Es claro y objetivo el manual del usuario?
1.- SI (**X**) 2.- NO ( )

5. ¿Conoce Ud. de la existencia de manuales técnicos en el departamento de Sistemas?
1.- SI ( ) 2.- NO (**X**)

6. ¿Conoce Ud. de la existencia de documentos que detallen las pruebas de sistemas?
1.- SI ( ) 2.- NO (**X**)

SEGURIDADES LÓGICAS Y FÍSICAS

1.¿Que piensa de la seguridad en el manejo de la información en el Departamento de Sistema?
1.- Nula ( )
2.- Riesgosa (**X**)
3.- Satisfactoria ( )
4.- Excelente ( )
5.- Lo desconoce ( ) ¿Por que?

2. Indique cuál(es) control(es) interno(s) existe(n) en el Dpto. de Sistemas:

1.- Procedimientos para operar en el departamento (X)
2.- Inventario de activos ( )
3.- Claves de acceso a los sistemas ( )
4.- Seguridades de las Bases de Datos ( )
5.- Manuales de Funciones (**X**)
6.- Control de archivos de seguridades ( )
7.- Paquetes Comerciales ( )

3. ¿Quién(es) tiene(n) acceso a las Bases de Datos?

El Jefe del Departamento y el técnico 1

4. ¿Existe un registro de anomalías de los Programas?

Por lo general si se tiene que realizar alguna modificación por anomalías, se apunta en una pizarra hasta que el técnico encargado la realice.

5. ¿La solicitud de modificaciones a los programas se hacen en forma?

1.- Oral? (**X**)
2.- Escrita? ( )

6. ¿Cuál de los programas es el que presenta más anomalías y quién realiza sus modificaciones?

El de Ventas y las modificaciones las realiza el técnico 1

7. ¿Se hace un reporte diario, semanal o mensual de las actividades del Dpto. a la Gerencia?

1.- SI (**X**) 2.- NO ( )

3. ¿Se tienen respaldos de las Bases?

1.- SI (**X**) 2.- NO ( ) Al de la empresa

9. ¿Se cuenta con respaldos actualizados de las bases en lugar distinto al de las computadoras?

1.- SI ( ) 2.- NO (**X**)

10. ¿Existen procedimientos de actualización de las copias que se encuentran fueran fuera de la empresa?

1.- SI ( ) 2.- NO (**X**)

11. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:

0 ( ) 1 ( ) 2 ( ) 3 (**X**)

12. ¿Dónde se almacenan estas copias?
1.- Departamento de Sistemas ( )
2.- Otra área de la empresa ( ) 3.- Fuera de la empresa (**X**)

13. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?
1.- SI ( ) 2.- NO (**X**)

14. ¿Se tienen seguros sobre todos los equipos?
1.- SI ( ) 2.- NO (**X**)

15. ¿Se han adoptado medidas de seguridad en el departamento de sistemas?
1.- SI ( ) 2.- NO (**X**)

16. ¿Existen una persona responsable de la seguridad?
1.- SI ( ) 2.- NO (**X**)

17. ¿Existe vigilancia en el departamento durante las horas laborales?
1.- SI (**X**) 2.- NO ( )

18. El edificio donde se encuentra la computadora esta situado a salvo de:
1.- Inundación? ( ) 2.- Terremoto? ( )
3.- Fuego? ( ) 4.- Sabotaje? ( )

19. El centro de cómputo tiene salida al exterior al exterior?
1.- SI ( ) 2.- NO (**X**)

20. ¿Existe alarma para:
1.- Detectar fuego(calor o humo) en forma automática? ( )
2.- Avisar en forma manual la presencia del fuego? (**X**)
3.- Detectar una fuga de agua? (**X**) **Diciendo**
4.- Detectores magnéticos? ( ) 5.- No existe ( )

21. Existen extintores de fuego:
1.- Manuales? (**X**) 2.- Automáticos? ( ) 3.- No existen ( )

22. ¿Se ha adiestrado el personal en el manejo de los extintores?
1.- SI ( ) 2.- NO (**X**)

23. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
1.- SI (**X**) 2.- NO ( )

24. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
1.- SI (X) 2.- NO ( )

25. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
1.- Evitando artículos inflamables en el departamento de cómputo? (X)
2.- Prohibiendo fumar a los operadores en el interior? (X)
3.- Vigilando y manteniendo el sistema eléctrico? (X)
4.- No se ha previsto ( )

CONTROL DE OPERACIÓN

1. ¿Existen procedimientos formales para la operación del Departamento de Sistema?
1.- SI (X) 2.- NO ( )

2. ¿Están actualizados los procedimientos?
1.- SI ( ) 2.- NO (X)

3. Determine la eficiencia con que se ejecutan los trabajos dentro del Departamento de Sistemas, tomando en cuenta equipo y técnico, a través de inspección visual.
1.-Mala ( ) 2.-Regular ( ) 3.-Buena ( ) 4.-Muy Buena (X) 5.-Excelente ( )

4. ¿Tiene el conocimiento necesario para actuar en caso de errores en los sistemas?
1.- SI ( ) 2.- NO (X)

5. Las intervenciones de los técnicos en los sistemas son:
Son muy numerosas? 1.- SI ( ) 2.- NO (X)
Se limitan a los mensajes? 1.- SI (X) 2.- NO ( )

6. ¿Se tiene un control adecuado sobre los programas que están en operación?
1.- SI ( ) 2.- NO (X)

7. ¿Cuentan los técnicos con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?
1.- Si, por máquina ( ) 2.- Si, escrita manualmente ( ) 3.- NO (X)

8. ¿Existe un lugar para archivar las bitácoras de los sistemas diseñados por el Dpto.?
1.- SI ( ) 2.- NO (X)

ANEXO 6

ENTREVISTAS A TÉCNICOS DEL DEPARTAMENTO DE SISTEMAS DE ADMITEC

Persona Entrevistada: Técnico 3 (Nombre Ficticio)

CONTROL SOBRE INFORMACIÓN IMPRESA

1. ¿Cómo utiliza los reportes de trabajos realizados por el Departamento?
Están en poder del Jefe del Dpto., pero no hay un fólder o archivo donde estén todos.

2. ¿Qué criterio tiene en cuanto a la eliminación o modificación desautorizadas de reportes?
No comparto esa idea.

3. ¿Se cuenta con un manual de usuario por Sistema?
SI (**X**) NO ( )

4. Si existe. ¿Es claro y objetivo el manual del usuario?
SI (X) NO ( )

5. ¿Conoce Ud. de la existencia de manuales técnicos en el departamento de Sistemas?
1.- SI ( ) 2.- NO (**X**)

6. ¿Conoce Ud. de la existencia de documentos que detallen las pruebas de sistemas?
1.- SI ( ) 2.- NO (X)

SEGURIDADES LÓGICAS Y FÍSICAS

1.¿Que piensa de la seguridad en el manejo de la información en el Departamento de Sistema?
1.- Nula (**X**) 2.- Riesgosa ( )
3.- Satisfactoria ( ) 4.-Excelente ( )
5.- Lo desconoce ( ) ¿Por que?

2. Indique cuál(es) control(es) interno(s) existe(n) en el Dpto. de Sistemas:

1.- Procedimientos para operar en el departamento (**X**)
2.- Inventario de activos ( )
3.- Claves de acceso a los sistemas ( )
4.- Seguridades de las Bases de Datos ( )
5.- Manuales de Funciones (**X**)
6.- Control de archivos de seguridades ( )
7.- Paquetes Comerciales ( )

3. ¿Quién(es) tiene(n) acceso a las Bases de Datos?

El Técnico 1 y el Jefe.

4. ¿Existe un registro de anomalías de los Programas?

No, por lo general no se guarda ese tipo de información.

5. ¿La solicitud de modificaciones a los programas se hacen en forma?

1.- Oral? (**X**)
2.- Escrita? ( )

6. ¿Cuál de los programas es el que presenta más anomalías y quién realiza sus modificaciones?

El de ventas es el que tiene más anomalías. Lo revisa ya sea el jefe o el Técnico 1.

7. ¿Se hace un reporte diario, semanal o mensual de las actividades del Dpto. a la Gerencia?

1.- SI (**X**) 2.- NO ( )

8. ¿Se tienen respaldos de las Bases?

1.- SI (**X**) 2.- NO ( ) Al de la empresa

9. ¿Se cuenta con respaldos actualizados de las bases en lugar distinto al de las computadoras?

1.- SI ( ) 2.- NO (**X**)

10. ¿Existen procedimientos de actualización a estas copias?

1.- SI ( ) 2.- NO (**X**)

11. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:

0 ( ) 1 ( ) 2 ( ) 3 (**X**)

12. ¿Dónde se almacenan estas copias?
1.- Departamento de Sistemas ( )
2.- Otra área de la empresa (**X**) 3.- Fuera de la empresa (**X**)

13. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?
1.- SI ( ) 2.- NO (**X**)

14. ¿Se tienen seguros sobre todos los equipos?
1.- SI ( ) 2.- NO ( ) La verdad desconozco.

15. ¿Se han adoptado medidas de seguridad en el departamento de sistemas?
1.- SI ( ) 2.- NO (**X**)

16. ¿Existen una persona responsable de la seguridad?
1.- SI ( ) 2.- NO (**X**)

17. ¿Existe vigilancia en el departamento durante las horas laborales?
1.- SI (**X**) 1.- NO ( )

18. El edificio donde se encuentra la computadora esta situado a salvo de:
1.- Inundación? ( ) 2.- Terremoto? ( )
3.- Fuego? ( ) 4.- Sabotaje? ( )

19. El centro de cómputo tiene salida al exterior al exterior?
1.- SI ( ) 2.- NO (**X**)

20. ¿Existe alarma para:
1.- Detectar fuego(calor o humo) en forma automática? ( )
2.- Avisar en forma manual la presencia del fuego? (**X**)
3.- Detectar una fuga de agua? (**X**)
4.- Detectores magnéticos? ( ) 5.- No existe ( )

21. Existen extintores de fuego:
1.- Manuales? (**X**) 2.-Automáticos? ( ) 3.- No existen ( )

22. ¿Se ha adiestrado el personal en el manejo de los extintores?
1.-SI ( ) 2.-NO (**X**)

23. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
1.-SI (**X**) 2.-NO ( )

24. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
1.-I (X) 2.-NO ( )

25. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
1.- Evitando artículos inflamables en el departamento de cómputo? (X)
2.- Prohibiendo fumar a los operadores en el interior? (X)
3.- Vigilando y manteniendo el sistema eléctrico? (X)
4.- No se ha previsto ( )

CONTROL DE OPERACIÓN

1. ¿Existen procedimientos formales para la operación del Departamento de Sistema?
1.-SI (X) 2.-NO ( )

2. ¿Están actualizados los procedimientos?
1.-SI (X) 2.-NO ( )

3. Determine la eficiencia con que se ejecutan los trabajos dentro del Departamento de Sistemas, tomando en cuenta equipo y técnico, a través de inspección visual.
1.-Mala ( ) 2.-Regular ( ) 3.-Buena ( ) 4.-Muy Buena (X) 5.-Excelente ( )

4. ¿Tiene el conocimiento necesario para actuar en caso de errores en los sistemas?
1.-SI ( ) 2.-NO (X)

5. Las intervenciones de los técnicos en los sistemas son:
Son muy numerosas? 1.-SI ( ) 2.-NO (X)
Se limitan a los mensajes? 1.-SI (X) 2.-NO ( )

6. ¿Se tiene un control adecuado sobre los programas que están en operación?
1.-SI ( ) 2.-NO (X)

7. ¿Cuentan los técnicos con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?
1.-Si, por máquina ( ) 2.-Si, escrita manualmente ( ) 3.-NO (X)

8. ¿Existe un lugar para archivar las bitácoras de los sistemas diseñados por el Dpto.?
1.-SI ( ) 2.-NO (X)

ANEXO 7

ENTREVISTAS A TÉCNICOS DEL DEPARTAMENTO DE SISTEMAS DE ADMITEC

Persona Entrevistada: Técnico 4 (Nombre Ficticio)

CONTROL SOBRE INFORMACIÓN IMPRESA

1. ¿Cómo utiliza los reportes de trabajos realizados por el Departamento?
Cuando se hacen los reportes aunque no siempre, se los entrega al Jefe como constancia de lo que se hizo.

2. ¿Qué criterio tiene en cuanto a la eliminación o modificación desautorizadas de reportes?
Es algo de lo cual no se darían cuenta hasta después de un tiempo, pero personalmente no estoy de acuerdo.

3. ¿Se cuenta con un manual de usuario por Sistema?
SI (**X**) NO ( )

4. Si existe. ¿Es claro y objetivo el manual del usuario?
SI (**X**) NO ( )

5. ¿Conoce Ud. de la existencia de manuales técnicos en el departamento de Sistemas?
1.- SI ( ) 2.- NO (**X**)

6. ¿Conoce Ud. de la existencia de documentos que detallen las pruebas de sistemas?
1.- SI ( ) 2.- NO (**X**)

SEGURIDADES LÓGICAS Y FÍSICAS

1.¿Que piensa de la seguridad en el manejo de la información en el Departamento de Sistema?
1.- Nula ( ) 2.- Riesgosa (**X**)
3.- Satisfactoria ( ) 4.- Excelente ( )
5.- Lo desconoce ( ) ¿Por que?

2. Indique cuál(es) control(es) interno(s) existe(n) en el Dpto. de Sistemas:

1.- Procedimientos para operar en el departamento (X)
2.- Inventario de activos ( )
3.- Claves de acceso a los sistemas ( )
4.- Seguridades de las Bases de Datos ( )
5.- Manuales de Funciones (X)
6.- Control de archivos de seguridades ( )
7.- Paquetes Comerciales ( )

3. ¿Quién(es) tiene(n) acceso a las Bases de Datos?

Jefe y Técnico 1

4. ¿Existe un registro de anomalías de los Programas?

No.

5. ¿La solicitud de modificaciones a los programas se hacen en forma?

1.- Oral? (X)
2.- Escrita? ( )

6. ¿Cuál de los programas es el que presenta más anomalías y quién realiza sus modificaciones?

Ventas. Técnico 1 o el Jefe

7. ¿Se hace un reporte diario, semanal o mensual de las actividades del Dpto. a la Gerencia?

SI (X) NO ( )

8. ¿Se tienen respaldos de las Bases?

SI (X) NO ( ) Al de la empresa

9. ¿Se cuenta con respaldos actualizados de las bases en lugar distinto al de las computadoras?

SI ( ) NO (X)

10. ¿Existen procedimientos de actualización de las copias que se encuentran fuera de la empresa?

SI ( ) NO (X)

11. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:

0 ( ) 1 ( ) 2 ( ) 3 (X)

12. ¿Dónde se almacenan estas copias?
1.- Departamento de Sistemas ( )
2.- Otra área de la empresa (**X**) 3.- Fuera de la empresa (**X**)

13. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?
SI ( ) NO (**X**)

14. ¿Se tienen seguros sobre todos los equipos?
SI ( ) NO (**X**)

15. ¿Se han adoptado medidas de seguridad en el departamento de sistemas?
SI ( ) NO (**X**)

16. ¿Existen una persona responsable de la seguridad?
SI ( ) NO (**X**)

17. ¿Existe vigilancia en el departamento durante las horas laborales?
SI (**X**) NO ( )

18. El edificio donde se encuentra la computadora esta situado a salvo de:
1.- Inundación? ( ) 2.- Terremoto? ( )
3.- Fuego? ( ) 4.- Sabotaje? ( )

19. El centro de cómputo tiene salida al exterior al exterior?
SI ( ) NO (**X**)

20. ¿Existe alarma para:
1.- Detectar fuego(calor o humo) en forma automática? ( )
2.- Avisar en forma manual la presencia del fuego? (**X**)
3.- Detectar una fuga de agua? (**X**) **Diciendo.**
4.- Detectores magnéticos? ( ) 5.- No existe ( )

21. Existen extintores de fuego:
1.- Manuales? (**X**) 2.- Automáticos? ( ) 3.- No existen ( )

22. ¿Se ha adiestrado el personal en el manejo de los extintores?
SI ( ) NO (**X**)

23. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
SI (**X**) NO ( )

24. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
SI (**X**) NO ( )

25. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
1.- Evitando artículos inflamables en el departamento de cómputo? (**X**)
2.- Prohibiendo fumar a los operadores en el interior? (**X**)
3.- Vigilando y manteniendo el sistema eléctrico? (**X**)
4.- No se ha previsto ( )

CONTROL DE OPERACIÓN

1. ¿Existen procedimientos formales para la operación del Departamento de Sistema?
SI (**X**) NO ( )

2. ¿Están actualizados los procedimientos?
SI (**X**) NO ( )

3. Determine la eficiencia con que se ejecutan los trabajos dentro del Departamento de Sistemas, tomando en cuenta equipo y técnico, a través de inspección visual.
1.-Mala ( ) 2.-Regular ( ) 3.-Buena ( ) 4.-Muy Buena (**X**) 5.-Excelente ( )

4. ¿Tiene el conocimiento necesario para actuar en caso de errores en los sistemas?
SI ( ) NO (**X**)

5. Las intervenciones de los técnicos en los sistemas son:
Son muy numerosas? SI ( ) NO (**X**)
Se limitan a los mensajes? SI (**X**) NO ( )

6. ¿Se tiene un control adecuado sobre los programas que están en operación?
SI ( ) NO (**X**)

7. ¿Cuentan los técnicos con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?
1.- Si, por máquina ( ) 2.- Si, escrita manualmente ( ) 3.-NO (**X**)

8. ¿Existe un lugar para archivar las bitácoras de los sistemas diseñados por el Dpto.?
SI ( ) NO (**X**)

ANEXO 8
PONDERACIÓN DE LOS RIESGOS

ANEXO 9
VALORACIÓN DE RIESGOS EXISTENTES

Nº	Riesgos Existentes controlados	Ponderación
1	Falta de Manuales de Usuarios	2,0
2	Falta de un registro de Horarios de Trabajo	3,0
3	Falta de reportes periódicos de las actividades del Dpto.a la Gerencia	2,0
4	No actualización de los respaldos de las Bases de Datos dentro de la empresa	2,2
5	Ausencia de vigilancia en el Dpto.	2,2
6	Mala Ubicación del Dpto. de Sistemas	2,6
7	Mala ubicación de los Interruptores de Energía	3,0
8	Desconocimiento de qué hacer en caso de incendios	2,5
9	Ausencia de medidas para minimiar la posibilidad de incendios	2,8
10	Falta de procedimientos formales para operar dentro del Dpto.	2,0

Dentro de la Ponderación de los Riesgos, también se determinaron los controles existentes dentro del Dpto., ya que la ponderación de sus riesgos fue alta (por encima de 2,0)

Por lo tanto los controles que existen en el Dpto. son:
Rangos: (2,5 - 3,0) = Control Alto (2,0 - 2,4) = Control Medio-Alto

Nº	Controles	Valoración
1	Manuales de Usuarios de los sistemas diseñados	Medio-Alto
2	Archivos de Horarios de Entrada y salida	Alto
3	Reportes quincenales a la Gerencia de las actividades del Dpto.	Medio-Alto
4	Actualizaciones periódicas de respaldos de las Bases de Datos dentro de la empresa	Medio-Alto
5	Vigilancia constane del Dpto.	Medio-Alto
6	Buena ubicación del Dpto. de Sistemas (No da el sol a los equipos y no	Alto
	es de fácil acceso a personas ajenas a la empresa).	
7	Los interruptores de energía están protegidos, etiquetados y sin obstáculos	Alto
8	Personal capacitado para casos de emergencia	Alto
9	Medidas adecuadas para evitar incendios	Alto
10	Procesos para operar dentro del Dpto.	Medio-Alto

ANEXO 10
CLASIFICACIÓN DE RIESGOS EXISTENTES

II°	OBJETOS	#RIESGO
1	Programas Aplicativos de Ventas	
	Acceso no autorizado al programa aplicativo de Vtas.	2
2	Archivos de Sequridades de las Bases de Datos	
	Accesos ilegales a las Bases de Datos	1
	Alteración, Destrucción y/o Pérdida de Información relevante para la empresa	5
	Desactualización de las claves de acceso	11
3	Partes y/o Piezas del Computador	
	Falta de Inventario de las partes y/o piezas de los computadores del Dpto.	10
	Falta de Inventario de los activos del Dpto.	9
	Ausencia de medidas de seguridad de los equipos	15
	Ausencia de control en la destrucción de los activos del Dpto.	16
4	Bases de Datos de Clientes y Proveedores	
	Destrucción y/o Pérdida de las Bases de Datos	4
	Ausencia de actualizaciones de respaldos de las Bases de Datos fuera de la empresa	14
5	Reportes de la realización de trabajos de mantenimiento	
	Mal uso o destrucción de los reportes de trabajo	8
	Ausencia de bitácoras de trabajos realizados por el Dpto.	12
	Ausencia de documentación técnica y formal de los sistemas diseñados y de pruebas	13
6	Paquetes Comerciales	
	Falta de Integridad de los Paquetes Comerciales	3

Las Amenazas Generales que fueron determinadas y que afectan tanto a la parte Física como a la Intangible son:

N°	AMENAZAS	# AMENAZA
1	Pérdida y/o Destrucción de la Información	1
2	Alteraciones de la Información	2
3	Destrucción de Recursos Materiales	3
4	Fraude y/o Robo de Recursos Materiales	4
5	Desastre Físico (Incendios)	5
6	Desastre Físico (Inundaciones)	6

ANEXO 11
MATRIZ DE CONTROL DE RIESGOS (AMENAZAS Y OBJETOS)

Amenazas / Objetos	Pérdida y/o Destrucción de Información	Alteraciones de la Información	Destrucción de Recursos Materiales	Fraude y/o Robo de Recursos Materiales	Desastre Físico (Incendios)	Desastre Físico (Inundaciones)
Programas aplicativos de Ventas						
Archivos de seguridades en la Base de D.						
Partes y/o piezas del computador						
Bases de Datos de clientes y Proveedores						
Reportes de la realización de trabajos de mant.						
Paquetes Comerciales						

ANEXO 12
COMPARACIÓN DE CATEGORÍAS DE RIESGO (AMENAZAS)

Pérdida y/o Destrucción de Información	Pérdida y/o Destrucción de Información				
Alteraciones de la Información		Alteraciones de la Información			
Destrucción de Recursos Materiales			Destrucción de Recursos Materiales		
Fraude y/o Robo de Recursos Materiales				Fraude y/o Robo de Recursos Materiales	
Desastre Físico (Inundaciones)					Desastre Físico (Incendios)
Desastre Físico (Temblores)					Desastre Físico (Inundaciones)

ANEXO 13
PROCESO DE VOTACIÓN DEL GRUPO DELPHI (AMENAZAS)

Pérdida y/o Destrucción de Información	Pérdida y/o Destrucción de Información					
Alteraciones de la Información	III / II	Alteraciones de la Información				
Destrucción de Recursos Materiales	IIII / I	III / II	Destrucción de Recursos Materiales			
Fraude y/o Robo de Recursos Materiales	II / III	II / III	II / III	Fraude y/o Robo de Recursos Materiales		
Desastre Físico (Inundaciones)	III / II	IIII / I	III / II	IIII / I	Desastre Físico (Incendios)	
Desastre Físico (Temblores)	IIII / I	IIII / I	IIII / I	IIII / I	III / II	Desastre Físico (Inundaciones)

ANEXO 14
SUMA DE LOS RESULTADOS (AMENAZAS).

Pérdida y/o Destrucción de Información	Pérdida y/o Destrucción de Información	3+4+2+3+4=16 0=0				
		16 (2)				
Alteraciones de la Información	III / II	Alteraciones de la Información	3+2+4+4=13 2=2			
			15 (3)			
Destrucción de Recursos Materiales	IIII / I	III / II	Destrucción de Recursos Materiales	2+3+4=9 1+2=3		
				12 (4)		
Fraude y/o Robo de Recur-sos Materiales	II / III	II / III	II / III	Fraude y/o Robo de Recur-sos Materiales	4+4=8 3+3+3=9	
					17 (1)	
Desastre Físico (Inundaciones)	III / II	IIII / I	III / II	IIII / I	Desastre Físico (Incendios)	3=3 2+1+2+1=6
						9 (5)
Desastre Físico (Temblores)	IIII / I	IIII / I	IIII / I	IIII / I	III / II	Desastre Físico (Inundaciones)	0=0 1+1+1+1+2=6
						6 (6)

ANEXO 15
COMPARACIÓN DE CATEGORÍAS DE RIESGOS (OBJETOS).

Programas aplicativos de Ventas	Programas aplicativos de Ventas				
Archivos de seguridades en la Base de D.		Archivos de seguridades en la Base de D.			
Partes y/o piezas del computador			Partes y/o piezas del computador		
Bases de Datos de clientes y Proveedores				Bases de Datos de clientes y Proveedores	
Reportes de la realización de trabajos de mant.					Reportes de la realización de trabajos de mant.
Paquetes Comerciales					Paquetes Comerciales

ANEXO 16
PROCESO DE VOTACIÓN DEL GRUPO DELPHI (OBJETOS).

Programas aplicativos de Ventas	Programas aplicativos de Ventas					
Archivos de seguridades en la Base de D.	II / III	Archivos de seguridades en la Base de D.				
Partes y/o piezas del computador	III / II	IIII / I	Partes y/o piezas del computador			
Bases de Datos de clientes y Proveedores	II / III	II / II	II / III	Bases de Datos de clientes y Proveedores		
Reportes de la realización de trabajos de mant.	IIII / I	IIII / I	II / III	IIII / I	Reportes de la realización de trabajos de mant.	
Paquetes Comerciales	II / III	III / II	I / IIII	III / II	II / III	Paquetes Comerciales

ANEXO 17
SUMA DE LOS RESULTADOS (OBJETOS).

Programas aplicativos de Ventas	Programas aplicativos de Ventas	2+3+2+4+2=13 0=0						
			13 (4)					
Archivos de seguridades en la Base de D.	II III	Archivos de seguridades en la Base de D.	4+3+4+3=14 3=3					
				17 (1)				
Partes y/o piezas del computador	III II	IIII I	Partes y/o piezas del computador	2+1+1=4 2+1=3				
					7 (6)			
Bases de Datos de clientes y Proveedores	II III	III II	II III	Bases de Datos de clientes y Proveedores	4+3=7 3+2+3=8			
						15 (2)		
Reportes de la realización de trabajos de mant.	IIII I	IIII I	I IIII	IIII I	Reportes de la realización de trabajos de mant.	2=2 1+1+4+1=7		
							9 (5)	
Paquetes Comerciales	II III	III II	I IIII	III II	II III	Paquetes Comerciales	0=0 3+2+4+2+3=14	
								14 (3)

ANEXO 18
MATRIZ DE COMBINACIONES DE LAS 2 CATEGORIZACIONES (AMENAZAS Y OBJETOS)

Amenazas / Objetos	Fraude y/o Robo de Recursos Materiales (17)	Pérdida y/o Destrucción de Información (16)	Alteraciones de la Información (15)	Destrucción de Recursos Materiales (12)	Desastre Físico (Incendios) (9)	Desastre Físico (Inundaciones) (6)
Archivos de seguridades en la Base de D. (17)						
Bases de Datos de clientes y Proveedores (15)						
Paquetes Comerciales (14)						
Programas aplicativos de Ventas (13)						
Reportes de la realización de trabajos de mant. (9)						
Partes y/o piezas del computador (7)						

ANEXO 19
MATRIZ DE RESULTADOS CON RIESGOS DE SENSIBILIDAD E IDENTIFICACIÓN DE NIVELES DE RIESGO (ALTO, MEDIO Y BAJO)

Amenazas / Objetos	Fraude y/o Robo de Recursos Materiales (17)	Pérdida y/o Destrucción de Información (16)	Alteraciones de la Información (15)	Destrucción de Recursos Materiales (12)	Desastre Físico (Incendios) (9)	Desastre Físico (Inundaciones) (6)
Archivos de seguridades en la Base de D. (17)	289 1	272 2	255 3	204 11	153 16	102 25
Bases de Datos de clientes y Proveedores (15)	255 3R	240 4	225 6	180 13	135 18R	90 26
Paquetes Comerciales (14)	238 5	224 7	210 9	168 14	126 19	84 27
Programas aplicativos de Ventas (13)	221 8	208 10	195 12	156 15	117 21	78 29
Reportes de la realización de trabajos de mant. (9)	153 16R	144 17	135 18	108 23	81 28	54 31
Partes y/o piezas del computador (7)	119 20	112 22	105 24	84 27R	63 30	42 32

32/5 = 6,4 = 6

de 1 a 6 = 6 — Alto Riesgo
de 7 a 26 = 20 — Mediano Riesgo
de 27 a 32 = 6 — Bajo Riesgo

ANEXO 20
CUADRO DE LOS CONTROLES DEFINITIVOS.

Nº Ident.	Nombre corto	Nivel Preventivo	Nivel Detectivo	Nivel Correctivo	Responsabilidad	Amenazas y Objetos que cubren
1	Respaldos de las Bases de Datos	Se necesita respaldar la Base de Datos de acuerdo a la actualización de la información.	Respaldar la Base de Datos al momento del problema para evitar futuros incovenientes.	Respaldar la BD luego de reconstruir la información que éstas contenían.	Gerencia	**Amenazas:** Pérdida y/o destrucción de la información, Alteraciones de la Información. **Objetos:** Archivos de S. De la BD, BD de clientes y Proveedores.
2	Seguridades de la Información	Colocar claves de acceso a los diferentes computadores de los diferentes técnicos del área así como del jefe del Departamento.	Revisar el problema de acceso a la información de los equipos y colocar las claves correspondientes.	Revisar que información se ha perdido, realizar los procedimientos de recuperación y colocar las claves de acceso pertinentes.	Departamento de Sistemas	**Amenazas:** Fraude y/o Robo de Recursos Materiales, Pérdida y/o destrucción de la Información, Alteraciones de la Información, Destrucción de RRMM. **Objetos:** Archivos de S. De la BD, BD de clientes y Proveedores, Paquetes Comerciales.
3	Bitácoras de las actividades del departamento	Se requiere de bitácoras donde se detallen las actividades realizadas.	Preparación de bitácoras para constatación de activid. Subsecuentes.	Procedimientos de recuperación de archivos para recrear archivos dañados	Gerencia y Dpto. de Sistemas	**Amenazas:** Pérdida y/o destrucción de la información, Alteraciones de la Información. **Objetos:** Programas aplicativos de Ventas, Reportes de la realización de trabajos de mantenimiento.
4	Alarmas de Seguridades (Incendios)	Es indispensable la implementación de alarmas contra incendios o el correcto mantenimiento de los extintores	Procurar mantener en buen estado los extintores o colocar las respectivas alarmas contra incendios	Analizar los motivos del siniestro y colocar las correspondientes alarmas o colocar en mejor ubicación los extintores en toda la empresa.	Departamento de Sistemas	**Amenazas:** Cubren cualquier amenaza de incendios tanto en el departamento como la empresa **Objetos:** Cubre cada uno de los objetos del dpto. y empresa.

RRMM: Recursos Materiales
BD: Bases de Datos

5	Seguros de los equipos (computadores)	Es preciso contratar un seguro para la protección de los activos de la empresa y por consiguiente de los equipos	Revisar el problema encontrado y contratar el servicio para evitar futuros inconvenientes.	Realizar un inventario de los equipos, determinar las pérdidas y contratar el seguro.	Gerencia	**Amenazas:** Destrucción de RRMM, Desastres Físicos: Inundaciones y Temblores.**Objetos:** Cubre lo referente a Hardware
6	Seguridades en la Empresa	Es necesario reforzar las puertas y ventanas que tiene la empresa. Además de la instalación de un intercomunicador en la entrada.	Reparar el acceso dañado a la empresa y reforzar los demás accesos.	Inventariar los activos de la empresa (incluyendo PC`s) y reforzar las entradas a la misma, con énfasis en el acceso destruido para evitar futuros inconvenientes.	Gerencia y Dpto. de Sistemas	**Amenazas:** Fraude y/o Robo de RRMM, Pérdida y/o Destrucción de la Información, Destrucción de RRMM. **Objetos:** Cubre todos los objetos del departamento de Sistemas.
7	Documentación Técnica y Doc. de Pruebas	Elaborar toda la documentación técnica correspondiente a los sistemas a implementar y de los ya implementados. Además de elaborar y archivar la documentación de pruebas.	Archivar la documentación técnica de los sistemas ya implementados además de las pruebas y modificaciones de los sistemas.	Recuperar información de los sistemas implementados y documentalos. Además de la recuperación de pruebas y sus respectivas modificaciones.	Departamento de Sistemas	**Amenazas:** Pérdida y/o destrucción de la Información, Alteraciones de la Información. **Objetos:** Paquetes Comerciales, Programas aplicativos de Ventas, Reportes de la realización de trabajos de mantenimiento.