ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMATICA Y ELECTRÓNICA

"DESARROLLO DE UNA METODOLOGÍA PARA LA AUDITORÍA DE RIESGOS INFORMÁTICOS (FÍSICOS Y LÓGICOS) Y SU APLICACIÓN AL DEPARTAMENTO DE INFORMÁTICA DE LA DIRECCIÓN PROVINCIAL DE ´PICHINCHA DEL CONSEJO DE LA JUDICATURA"

TESIS DE GRADO

Previa la obtención del título de:

INGENIERO EN SISTEMAS INFORMÁTICOS

Presentado por:

GEOMAYRA ALEXANDRA PAREDES FIERRO

MAYRA ALEXANDRA VEGA NOBOA

RIOBAMBA – ECUADOR

2011

Agradecemos a Dios por habernos permitido llegar a culminar con éxito una etapa importante en nuestra vida profesional.

A la Escuela Superior Politécnica de Chimborazo, como también a sus distinguidos catedráticos quienes durante nuestros estudios nos guiaron en la preparación académica.

Al Ing. Danilo Pastor, Director de Tesis al Ing. Eduardo Villa Asesor de Tesis, Por su colaboración para el desarrollo de este trabajo.

A Dios Todopoderoso por iluminarme el camino a seguir ya que siempre está con nosotros en todo momento, por haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mis padres Luis y Amelia por el apoyo incondicional ya que son los pilares fundamentales en mi vida, por su amor, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, quienes son dignos de ejemplo de trabajo y constancia que siempre me brindan todo el apoyo necesario para alcanzar mis metas y sueños.

Geomy

Dedico este trabajo y toda mi carrera politécnica, a Dios por ser quien ha estado a mi lado en todo momento dándome las fuerzas necesarias para continuar luchando día tras día y seguir adelante rompiendo todas las barreras que se me presenten.

A mi hija que es la bendición más grande que Dios me ha dado, ella es el motivo de todos mis esfuerzos, el motor que me obliga a funcionar y ser cada día mejor, la fuente de mi inspiración y motivación para culminar con este trabajo y cumplir con mis dos más grandes sueños; ser madre de una preciosura "Emily Samantha Gavilánez Vega" y mi título de Ingeniera en Sistemas Informáticos.

A mis padres por haberme educado y soportar mis errores. Gracias a sus consejos, por el amor que siempre me han brindado, por cultivar e inculcar ese sabio don de la responsabilidad con valores, principios, perseverancia y empeño, y todo ello con una gran dosis de amor y sin pedir nunca nada a cambio.

Mayra

FIRMAS DE RESPONSABILIDADES

NOMBRE	FIRMA	FECHA
Ing. Iván Menes .C. **DECANO DE LA FACULTAD DE INFORMATICA Y ELECTRONICA**	…….	…….
Ing. Raúl Rosero **DIRECTOR DE LA ESCUELA DE INGENIERIA EN SISTEMAS**	…….	…….
Ing. Danilo Pastor **DIRECTOR DE TESIS**	…….	…….
Ing. Eduardo Villa **MIEMBRO DEL TRIBUNAL**	…….	…….
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACIÓN**	…….	…….
NOTA DE LA TESIS	…….	

“Nosotras, Geomayra Alexandra Paredes Fierro y Mayra Alexandra Vega Noboa somos responsables de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO”.

Geomayra Alexandra Paredes Fierro

Mayra Alexandra Vega Noboa

Índice General

INDICE DE TABLAS
INDICE DE FIGURAS
INTRODUCCIÓN
CAPÍTULO I 15
I. MARCO REFERENCIAL 15
1.1 ANTECEDENTES 15
1.2 OBJETIVOS 19
1.3 JUSTIFICACIÓN 19
1.4 HIPÓTESIS 21
1.5 MÉTODOS Y TÉCNICAS 22
CAPITULO II 23
2. MARCO TEÓRICO 23
2.1 Información 23
2.2 Seguridad 24
2.2.1 Seguridad de la Información 25
2.3 Auditoría 32
2.4 Riesgos Informáticos 36
CAPÍTULO III 46
3. ESTUDIO DE LAS METODOLOGÍAS 46
3.1 Metodologías de Auditoria Informática 47
3.1.1 COBIT 48
3.1.2 ITIL 90
3.1.3 ISO 17799 100
3.1.4 MAGERIT 109
3.1.5 CRMR 116
CAPITULO IV 121

4. ANÁLISIS DE LAS METODOLOGÍAS Y DESARROLLO DE LA METODOLOGÍA 121
4.1 Introducción 121
4.2 Determinación de las metodologías a analizar 122
4.3 Análisis de metodologías seleccionadas 128
4.3.1 COBIT 128
4.3.2 ISO 17799 135
4.3.3 MAGERIT 138
4.4 Diseño y Definición de la Metodología 142
4.4.1 Fases de la Metodología MACORI 146
CAPÍTULO V 188
5. AUDITORÍA INFORMÁTICA 188
5.1 FASE I: DEFINICIÓN DEL PLAN 188
5.1.1 Recogida de información 188
5.1.2 Definir un plan, los objetivos y una política de seguridad. 189
5.1.3 Prestación y Organización de servicios 192
5.2 FASE II GESTIÓN INFORMÁTICA 194
5.2.1 Planificación de la seguridad de los Sistemas de Información 194
5.2.2 Diseño y mantenimiento de un plan de infraestructura tecnológica. 201
5.2.3 Gestionar la calidad de proyectos 209
5.2.4 Desarrollo y mantenimiento de sistemas. 215
5.2.5 Control de accesos 218
5.2.6 Gestionar los datos, comunicaciones y operaciones 224
5.3 FASE III CONTROL Y COMUNICACIÓN 226
5.3.1 Análisis y Control de Activos 226
5.3.2 Control de Recursos Humanos 226
5.3.3 Comunicar las Aspiraciones y la Dirección de la Gerencia 227
5.3.4 Capacitación a los usuarios 227
5.4 FASE IV ANÁLISIS Y GESTIÓN DE RIESGOS 227

5.4.1 Identificación y Evaluación del Riesgo 227
5.5 FASE V MONITOREO Y CUMPLIMIENTO DE LEYES 232
5.5.1 Monitoreo del Proceso 232
5.5.2 Garantizar el cumplimiento de las leyes 232
5.5.3 Conclusiones 233
5.6 COMPROBACIÓN DE LA HIPOTESIS 235
CONCLUSIONES
RECOMENDACIONES
RESUMEN
SUMMARY
ABREVIATURAS
GLOSARIO
BIBLIOGRAFIA

ÍNDICE DE TABLAS

Tabla. IV. 1. Características de la Metodologías…… 126
Tabla. IV. 2. Cobit – Dominio Planear y Organizar…….. 133
Tabla. IV. 3. Cobit – Dominio Adquirir e Implantar…….. 134
Tabla. IV. 4. Cobit – Dominio Entregar y Dar Soporte……. 137
Tabla. IV. 5. Cobit – Dominio Monitorear y Evaluar…… 138
Tabla. IV. 6. Dominios de ISO 17799…… 141
Tabla. IV. 7. MAGERIT – Actividades AGR…….. 142
Tabla. IV. 8. MAGERIT – Actividades Planificación de Gestión de riesgos – Planificación……. 143
Tabla. IV. 9. MAGERIT – Actividades Planificación de Gestión de riesgos – Análisis…….. 144
Tabla. IV. 10. MAGERIT – Actividades Planificación de Gestión de riesgo – Gestión…….. 144
Tabla. IV. 11. MAGERIT – Actividades Planificación de Gestión de riesgos – Selección de Salvaguardas…… 145
Tabla. IV. 12. Definición de la metodología……... 149
Tabla. IV. 13. Capacitación a los Usuarios…… 188
Tabla. V. 14. Planificación del Desarrollo de la Auditoria…… 193
Tabla. V. 15 .Planificación…….. 198
Tabla. V. 16. Coordinación……. 199
Tabla. V. 17. Supervisión …… 200
Tabla. V. 18. Funcionalidad de los Módulos…….. 202
Tabla. V. 19. Seguridad de los Sistemas…….. 204
Tabla. V. 20. Seguridades Físicas…… 206
Tabla. V. 21. Seguridades Lógicas…….. 207
Tabla. V. 22. Infraestructura de la red…… 209
Tabla. V. 23. Inventario de Hardware……. 211
Tabla. V. 24. Necesidades de Hardware…….. 212

Tabla. V. 25. Normas y Estándares……. 214
Tabla. V. 26. Planeación de la Calidad del Proyecto…….. 215
Tabla. V. 27. Aseguramiento de la calidad del Proyecto…… 217
Tabla. V. 28. Control de la Calidad del Proyecto……... 219
Tabla. V. 29. Desarrollo y Mantenimiento de Sistemas…… 221
Tabla. V. 30. Actividades del Programador…….. 230
Tabla. V. 31. Identificación y Evaluación del Riesgo…….. 234
Tabla. V. 32. Criterios de la Evaluación de la Probabilidad……. 234
Tabla. V. 33. Criterios de la Evaluación del Impacto…… 234
Tabla. V. 34. Criterios de la Evaluación de la Exposición al riesgo…… 235
Tabla. V. 35. Valorización de Riesgos…… 236

ÍNDICE DE FIGURAS

Figura 1: Información……. 24

Figura 2: Seguridad……. 25

Figura 3: Riesgo…….. 37

Figura 4: Administración de la Información……. 53

Figura 5: Áreas Focales del Gobierno de TI……. 55

Figura 6: Productos Cobit…….. 57

Figura 7: Interrelaciones de los componentes de COBIT…… 59

Figura 8: Principio Básico COBIT……..... 64

Figura 9: Definiendo metas de TI y Arquitectura Empresarial para TI…….…. 66

Figura 10: Administración de recursos de TI para garantizar las metas de TI…….. 68

Figura 11: Modelo de Control…… 71

Figura 12: Representación gráfica de los modelos de madurez……... 80

Figura 13. Modelo genérico de Madurez……...…… 82

Figura 14: Las tres dimensiones de la madurez…… 83

Figura 15. Atributos de Madurez……... 86

Figura 16: Relación entre proceso, metas y métrica (DS5)……. 88

Figura 17: Administración, Control, Alimentación y Monitoreo COBIT…… 89

Figura 18: El cubo COBIT…… 90

Figura 19: Marco de trabajo general de COBIT……. 91

Figura 20: Soluciones para ITIL…….. 93

Figura 21: Procesos ITIL…….. 95

Figura 22: Proceso de manejo de problemas……..... 97

Figura 23: Proceso de manejo de configuraciones……... 98

Figura 24: Proceso de control de cambios…… 99

Figura 25: Proceso de manejo de entregas…….. 101

Figura 26: ISO 17799……..... 103

Figura 27: Gestión de seguridad de la información……. 105

Figura 28: Análisis y Gestión de Riesgos MARGERIT……... 113

Figura 29: Modelo de MARGERIT……..... 114
Figura 30: Submodelo de Procesos de MAGERIT…… 115
Fig. IV. 31. Resultados Encuesta ……. 130
Fig. IV. 32. Diagrama de Venn de las Metodologías…….. 146
Fig. IV. 33. Fases de la metodología MACORI……. 150
Fig. IV. 34. Gestión de la Calidad del Proyecto……... 163
Fig. IV. 35. Planeación de la Calidad del Proyecto – Insumos…….. 163
Fig. IV. 36. Planeación de la Calidad del Proyecto – Salidas…… 164
Fig. IV. 37. Métricas de Calidad…….. 165
Fig. IV. 38. Lista de chequeo……. 165
Fig. IV. 39. Aseguramiento de la Calidad del Proyecto – Insumos…….. 166
Fig. IV. 40. Mediciones de Control de Calidad…….. 167
Fig. IV. 41. Técnicas para el aseguramiento de la calidad…..…….. 168
Fig. IV. 42. Control de la Calidad del Proyecto…….. 168
Fig. IV. 43. Control de la Calidad del Proyecto - Insumos…….. 169
Fig. IV. 43. Control de la Calidad del Proyecto – Salidas…… 169

INTRODUCCIÓN

Actualmente el trabajo que se desempeña en las empresas, son actividades que en la mayoría de las instituciones no intervienen personas expertas en llevar a cabo una evaluación correcta de las funciones de la organización y una identificación de los riesgos que se exteriorizan en las áreas en las cuales debería ser controlado el funcionamiento de la tecnología informática ya que es el pilar fundamental en una empresa, misma q corresponde la integración de un control de datos y de información.

Por ello se hace necesario la elaboración de una metodología que involucre los aspectos necesarios que ayuden a la organización a evaluar eficientemente cada uno de los aspectos que ayudaran a identificar los riesgos físicos y lógicos de la empresa.

El trabajo desarrollado a continuación, se lo llevo previo a un estudio y análisis de metodologías, tomando lo relevante en cada una de ellas llegando a desarrollar la Metodología MACORI, esta fue aplicada en una de las empresas que necesita contar con el apoyo de una auditoría de riesgos informáticos (físicos y lógicos) es el Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura en la ciudad de Quito y desconocen la existencia de riesgos informáticos, la seguridad implantada, el tiempo de uso de los equipos y otras vulnerabilidades que puedan presentarse en este tipo de empresas.

CAPÍTULO I

I. MARCO REFERENCIAL

1.1 ANTECEDENTES

Hoy en día el trabajo que se desempeña en las empresas, son actividades que en la mayoría de las instituciones no son controladas por personas especializadas en realizar este tipo de trabajo, sobre todo se hace un enfoque directamente al área en donde se aplica la tecnología informática ya que es el centro en el cual se lleva a cabo el control de los datos y de la información que se maneja en las empresas.

Para tener un trabajo de calidad se debe seguir un proceso ordenado y de calidad para que los resultados obtenidos por la investigación sean eficientes, den valor y ayuden a la organización a la toma de decisiones, para ello existen las metodologías las cuales se elaboran con el propósito de dar seguimiento a un proceso de investigación.

El maravilloso "mundo de las computadoras" ha proporcionado un verdadero avance en diferentes áreas y en ellas es menester realizar gestiones de manera dinámica, eficiente y precisa. Al aplicarse esta tecnología en todo tipo de gestiones automatizadas, se establece

un gran paso en la creación de mejores métodos y procedimientos que ayuden al hombre a desempeñar más eficientemente las tareas que realiza en serie y, lo más común, aquellas de rutina.

En las compañías y empresas, actualmente existe un factor nuevo de preocupación a nivel departamental: los sistemas de información operan en un ambiente que está lleno de peligros latentes.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de personas tanto internas como externas de la organización, desastres naturales, servicios, suministros y trabajos no confiables e imperfectos, la incompetencia y las deficiencias cotidianas, el abuso en el manejo de los sistemas informáticos, el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

A finales del siglo XX, los Sistemas Informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la empresa.

La Informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "Tiene Auditoría" como sinónimo de que, en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallas.

El concepto de auditoría es mucho más que esto. Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc., que ayudaran determinar el nivel de cumplimiento de las actividades a desarrollarse en la Institución.

Para tener un trabajo de calidad se debe seguir un proceso ordenado y de calidad para que los resultados obtenidos por la investigación sean eficientes, den valor y ayuden a la organización a la toma de decisiones, para ello existen las metodologías las cuales se elaboran con el propósito de dar seguimiento a un proceso de investigación.

Metodología es una secuencia de pasos lógica y ordenada de proceder para llegar a un resultado. Generalmente existen diversas formas de obtener un resultado determinado, y de esto se deriva la existencia de varias metodologías para llevar a cabo una auditoria informática.

Las metodologías que existen para realizar una auditoría informática como tienen sus beneficios, tienen partes y en las cuales incluimos las fases en la cual el usuario está en desacuerdo con las mismas, ya que llegan a esta conclusión debido a un respectivo estudio de las mismas y determinan las falencias que existen en cada una de las metodologías, cabe destacar la razón fundamental para la no conformidad completa es que cada una de ellas se enfocan a fondo en un ámbito en el cual tal vez quien lo usa no se inmiscuye respectivamente en esa área.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido

de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

Todos estos aspectos hacen que sea necesario replantear la seguridad con que cuenta hasta ahora la empresa.

Una de las empresas que necesita contar con el apoyo de una auditoría de riesgos informáticos (físicos y lógicos) es El Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura en la ciudad de Quito debido a que se encuentran a cargo de varios edificios (Benalcazar Mil, Cornejo, Palacio de Justicia, Corte Provincial de Pichincha, Tribunal Contencioso Administrativo, Tribunal Fiscal y Tribunal Penal) y desconocen la existencia de riesgos informáticos, la seguridad implantada, el tiempo de uso de los equipos y otras vulnerabilidades que puedan presentarse en este tipo de empresas, todos estos puntos son causa para que la empresa requiera mejorar la eficiencia del departamento y reforzar su seguridad para la toma de decisiones importantes.

El Consejo de la Judicatura es el órgano único de gobierno, administración, vigilancia y disciplina de la Función Judicial, que comprende: órganos jurisdiccionales, órganos administrativos, órganos auxiliares y órganos autónomos.

El Consejo de la Judicatura es un órgano instrumental para asegurar el correcto, eficiente y coordinado funcionamiento de los órganos jurisdiccionales, autónomos y auxiliares. En ningún caso, el Consejo de la Judicatura se considerará jerárquicamente superior ni podrá atentar contra la independencia para ejercer las funciones específicas de las juezas y jueces, de las y los fiscales y de las defensoras y defensores públicos.

El Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura lleva a cabo las actividades necesarias y suficientes para asegurar la automatización integral de los procesos judiciales en todas las dependencias de la Provincia de Pichincha, mediante la utilización óptima de los recursos humanos y tecnológicos disponibles.

1.2 OBJETIVOS

2.3.1 Objetivo general

Desarrollar una metodológica para la auditoria de Riesgos Informáticos(físicos y lógicos), mediante el análisis de recursos y herramientas de auditoría informática, y su aplicación al Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura

2.3.2 Objetivos específicos

- ✓ Estudiar los conceptos, recursos y herramientas de Auditoría Informática.
- ✓ Analizar las herramientas consideradas como mejores prácticas tales como: ITIL, COBIT, CRMR y MARGERIT
- ✓ Desarrollar una metodológica de Auditoría de Riesgos Informáticos (físicos y lógicos) tomando las etapas más importantes de las herramientas analizadas.
- ✓ Realizar una Auditoría de Riesgos Informáticos del Departamento de Sistemas de la Empresa.

1.3 JUSTIFICACIÓN

Ignorar las amenazas y riesgos que acechan a las unidades informáticas o trivializarlas, es como jugar a la ruleta rusa: se puede ser afortunado durante algún tiempo, pero tarde o temprano esa fortuna terminará. Desgraciadamente, la mayoría de las amenazas son invisibles hasta que es demasiado tarde, mucho más si se hace referencia a los sistemas de información, los mismos que manejan activos tan intangibles como los datos y la información que se obtiene de estos.

Es muy importante identificar los riesgos informáticos para garantizar la supervivencia de la organización.

La implementación de mejores prácticas tales como **ITIL, COBIT, CRMR y MAGERIT** constituye hoy en día algunas de las prioridades de aquellos departamentos de Tecnologías

de Información (TI) alineados con brindar servicios de Información Tecnológica de calidad y el entendimiento de las necesidades de negocio, es por ello que se ha optado por estas metodologías para la realización de nuestro estudio. No obstante la aplicación de estas prácticas supone una inversión considerable de tiempo y esfuerzo, por lo que para aplicar cualquier buena práctica de TI dentro de la organización debemos considerar el valor de negocio que cada una de ellas aporta de forma incluyente o excluyente.

El objetivo del trabajo práctico se divide en dos partes. En primer lugar, describir las metodologías de auditoría informática en forma general. En segundo lugar proponer una metodología la misma que será utilizada para el caso práctico en la empresa auditada.

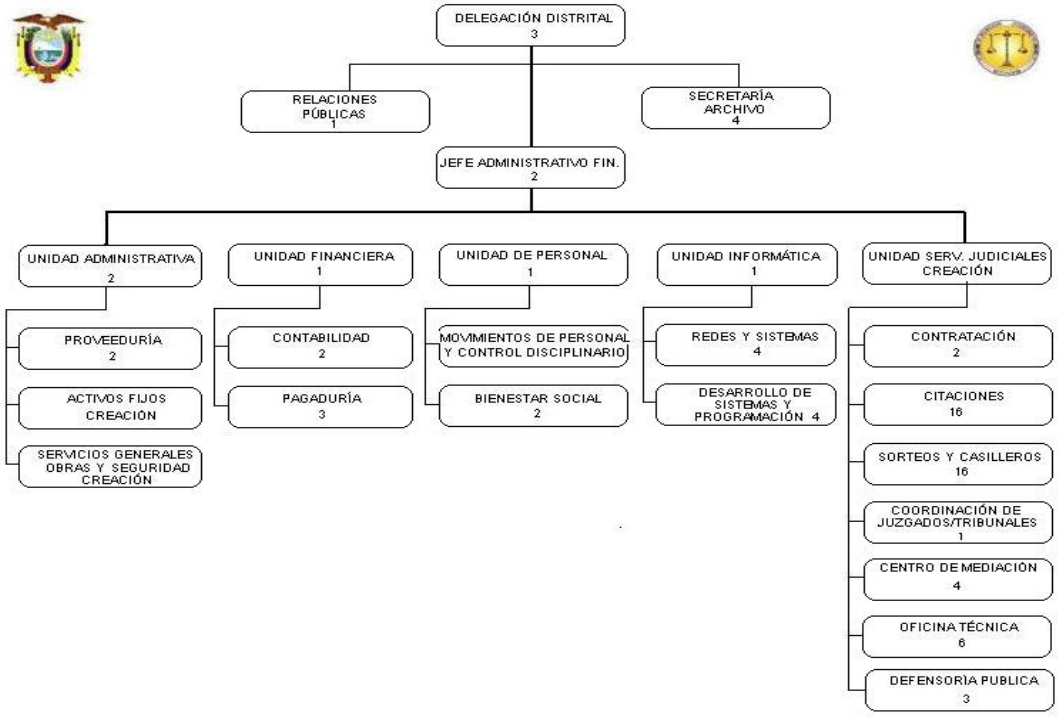
Como todas las metodologías tienen sus desventajas en algunas de sus fases o les falta identificar fases, por ello se elaborará una metodología para lo cual se realizará el estudio y análisis de recursos y herramientas de auditoría informática.

Analizar los Riesgos Informáticos y tomar acciones con respecto a sus causas es un factor muy importante, ya que los mismos constituyen un elemento crítico para el éxito y la supervivencia de las organizaciones, en el presente caso se enfocará al Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura; en donde surge la necesidad de realizar una Auditoria de Riesgos Informáticos, con el fin de proporcionar un documento técnico; el mismo que brindará una metodología adecuada para que el Departamento de informática de la Organización pueda controlar los Riesgos Informáticos (físicos y lógicos) y tomar las acciones necesarias para evitar que estos se materialicen como problemas inminentes y mejorar de alguna manera su productividad.

El Consejo de la Judicatura es el órgano único de gobierno, administración, vigilancia y disciplina de la Función Judicial, que comprende: órganos jurisdiccionales, órganos administrativos, órganos auxiliares y órganos autónomos.

En el presente organigrama se observa la estructura de la Función Judicial y cabe mencionar que el departamento de informática controla el funcionamiento de cada una de estas unidades más los edificios (Benalcazar Mil, Cornejo, Palacio de Justicia, Corte

Provincial de Pichincha, Tribunal Contencioso Administrativo, Tribunal Fiscal y Tribunal Penal), por ello es que la empresa necesita conocer los riesgos a los que puede estar propensa, pues manejan información muy valiosa e incluso confidencial.



La mayoría de las metodologías están enfocadas en resolver problemas de grandes empresas que por sus avances tecnológicos requieren de mayores estudios, el desarrollo de la metodología estará orientado a resolver problemas específicamente de una sola área como es la informática y contendrán actividades que puedan ser aplicadas en organizaciones de nuestro medio y que satisfagan las necesidades de la empresa.

1.4 HIPÓTESIS

El desarrollo y la aplicación de la metodológica para la auditoria de riesgos informáticos (físicos y lógicos) basados en varias herramientas y metodologías de auditoría informática; proporcionará resultados eficientes para el departamento de informática de la organización auditada.

1.5 MÉTODOS Y TÉCNICAS

Método Científico

Método utilizado con el fin de alcanzar conocimientos válidos sobre Metodologías de Auditoría de Sistemas y Riesgos Informáticos.

Método Deductivo

Método que será utilizado en el análisis de las Metodologías de auditoría; ya que se estudiará desde su definición y características, fases y módulos que posee cada una buscando los beneficios más relevantes de las mismas.

Método Comparativo

Permitirá comparar y seleccionar los beneficios de calidad que proporciona cada una de ellas con el fin de establecer una nueva metodología de Auditoría Informática para el desarrollo de la metodología de Auditoría de Riesgos Informáticos enfocando el caso práctico para el Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura.

TÉCNICAS

Brindarán apoyo a la recolección de la información sobre Metodologías de Auditoría de Sistemas, Políticas de Seguridad y Riesgos Informáticos; así como también sobre las características de cada metodología a comparar. Las técnicas empleadas son:

Entrevistas y encuestas

Se realizarán entrevistas a los empleados del Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura de su conocimiento sobre la organización y funcionamiento así como el estado actual del departamento.

Observación y Trabajo de Campo

Mediante esta técnica se busca obtener datos sobre los Riesgos Informáticos presentes en el Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura.

CAPITULO II

2. MARCO TEÓRICO

2.1 Información

Para empezar con la base de este capítulo mencionaremos el factor más importante que involucra el argumento "Auditoría de Riesgos Informáticos", conceptualizando e incluyendo el contenido que conlleva el término *información*.

Iniciamos señalando que la expresión información "Proviene de los vocablos latinos, *in - formare (*poner en forma*)*, proceso físico, mecánico de transmisión de datos que posee una connotación vinculada a una de nuestras más grandes libertades que son la de opinión y/o expresión de ideas [[1]].

---

[1] *Información*
http://www.mailxmail.com/curso-codigo-etica-informaticos/conceptos-basicos-informatica

[2] *Información*
http://es.wikipedia.org/wiki/Informaci%C3%B3n

De esta forma se define la Información como un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno, por ende es considerado como un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada [2].

Figura 1: Información

2.2 Seguridad

Podemos entender como seguridad un estado de cualquier tipo de información o la (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

Figura 2: Seguridad

2.2.1 Seguridad de la Información

Como resultado de la creciente inter conectividad en el ambiente de los negocios, la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.

El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Necesidad de seguridad a la información

La información y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad de la información es importante en negocios tanto del sector público como del privado y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, por ejemplo lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes públicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos.

Es necesario que exista seguridad en el activo más importante de la organización por las siguientes razones:

- ✓ Gran variedad de Riesgos y Amenazas: Fraudes, espionaje, sabotaje, vandalismo, incendio, inundación, Hacking, virus, denegación de servicio, etc.
- ✓ Provenientes de múltiples fuentes.
- ✓ Mayor vulnerabilidad a las amenazas por la dependencia de los sistemas y servicios de información interconectados.
- ✓ La mayoría de los sistemas de información no han sido diseñados para ser seguros.
- ✓ La seguridad de la información se define como la preservación de:

    - Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso
    - Integridad. Garantía de la exactitud y totalidad de la información y de los métodos de procesamiento.

- Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y a los recursos relacionados.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse: seguridad organizacional, seguridad lógica, seguridad física y seguridad legal.

Seguridad Organizacional Dentro de este, se establece el marco formal de seguridad que debe sustentar la institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, Integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Lógica Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

Seguridad Física Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

Seguridad Legal Integra los requerimientos de seguridad que deben cumplir todos los empleados, socios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la Universidad de Oriente en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

Las Normas de Seguridad

Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por

éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red institucional.

Organización de la Seguridad Informática

Gerencia.- Autoridad de nivel superior que integra el comité de seguridad. Bajo su administración están la aceptación y seguimiento de las políticas y normativa de seguridad en concordancia con las autoridades de nivel superior.

Gestor de Seguridad.- Persona dotada de conciencia técnica, encargada de velar por la seguridad de la información, realizar auditorías de seguridad, elaborar documentos de seguridad como, políticas, normas; y de llevar un estricto control con la ayuda de la unidad de informática referente a los servicios prestados y niveles de seguridad aceptados para tales servicios.

Unidad de Informática.- Entidad o Departamento dentro de la institución, que vela por todo lo relacionado con la utilización de computadoras, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación en sí, a través de medios electrónicos.

Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad está ligada a una Amenaza y el Riesgo a un Impacto.

La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma. Desde el punto de vista de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos. Una persona no autorizada podría**:** Clasificar y desclasificar los datos, Filtrar información, Alterar la información, Borrar la información, Usurpar datos, Hojear información clasificada.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Copia de seguridad completa, Todos los datos (la primera vez), Copias de seguridad incrementales, Sólo se copian los ficheros creados o modificados desde el último backup, Elaboración de un plan de backup en función del volumen de información generada

¿De qué nos queremos proteger?

En seguridad informática en general, se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestra información, sistema, red, etc. A continuación se presenta una relación de los elementos que potencialmente pueden considerarse peligrosos.

Personas.- La mayoría de ataques que se da a los factores importantes de la empresa van a provenir en última instancia de personas que, intencionada o bienintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible. Pero con demasiada frecuencia se suele olvidar que los piratas "clásicos" no son los únicos que amenazan nuestros equipos.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas. Generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor.

- ✓ **Personal.-** Las amenazas a la seguridad de un sistema proveniente del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento, etc.) puede comprometer la seguridad de los equipos. Aunque los ataques pueden ser intencionados lo normal es que más que de ataques se trate de

accidentes causados por un error o por desconocimiento de las normas básicas de seguridad.

- ✓ **Ex-empleados.-** Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Personas descontentas con la organización que pueden aprovechar debilidades de la empresa, que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo.
- ✓ **Curiosos.-** Junto con los crackers, los curiosos son los atacantes más habituales de sistemas Unix en redes de I+D. Aunque en la mayoría de situaciones se trata de ataques no destructivos, parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.
- ✓ **Crackers.-** Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Las redes son generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas; por otro lado, el gran número y variedad de sistemas Unix conectados a estas redes provoca, que al menos algunos de sus equipos sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple exploit los equipos que presentan vulnerabilidades; esto convierte a las redes de I+D, a las de empresas, o a las de ISPs en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos.
- ✓ **Terroristas.-** Por "terroristas" no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.
- ✓ **Intrusos remunerados.-** Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes,

información confidencial sobre las posiciones de satélites espía.) o simplemente para dañar la imagen de la entidad afectada.

- ✓ **Amenazas lógicas.-** Bajo la etiqueta de "amenazas lógicas' encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros). Algunas de las amenazas con que nos podemos encontrar son:
- ✓ **Herramientas de seguridad.-** Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como nessus, saint o satan pasan de ser útiles a ser peligrosas cuando las utilizan crackers que buscan información sobre las vulnerabilidades de un host o de una red completa.
- ✓ **Puertas traseras.-** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se los denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos.
- ✓ **Bombas lógicas-.-** Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.
- ✓ **Canales cubiertos.-** Los canales cubiertos (o canales ocultos) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema. No constituyen una amenaza demasiado habitual en redes de I+D, sin embargo, es posible su existencia, y en este caso su detección suele ser difícil.
- ✓ **Virus.-** Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también

lo hace, insertándose a sí mismo en otros programas. Aunque los virus existentes para entornos Unix son más una curiosidad que una amenaza real, en sistemas sobre plataformas IBM-PC o compatibles (Linux, FreeBSD, NetBSD, Minix, Solaris.) ciertos virus, especialmente los de boot, pueden tener efectos nocivos, como dañar el sector de arranque.

- ✓ **Gusano.-** Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.
- ✓ **Caballos de Troya.-** Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas, es decir que ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.
- ✓ **Programas conejo o bacterias.-** Son los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.), produciendo una negación de servicio.
- ✓ **Técnicas salami.-** Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección.
- ✓ **Catástrofes.-** Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar).

2.3 Auditoría

Hoy por hoy las tecnologías de la información son vitales para una organización en la medida en la que éstas dan soporte a sus procesos esenciales de negocio, no obstante, todos los beneficios que de esto se deriva se ven amenazados por numerosos riesgos que

requieren ser controlados para garantizar que este soporte sea efectivo; en otras palabras se requiere de un sistema de control interno eficaz, eficiente y una labor periódica de supervisión o de auditoría en la organización.

Auditoría es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para la adecuada toma de decisiones [3].
El concepto de auditoría es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc. La Informática hoy, está dentro de la gestión integral de la empresa, y por eso, las normas y estándares propiamente informáticos deben estar, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el “management” o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, desde el momento en que es una herramienta adecuada de colaboración [4].

La Informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

---

[3] *Auditoria*
http://pdf.rincondelvago.com/auditoria_7.html
[4] *Auditoria*
http://www.eisi.ues.ed.terminologia.ppt

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas.

El concepto de auditoría es mucho más que esto. Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones

Síntomas de Necesidad de una Auditoría Informática:
Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

1. Síntomas de descoordinación y desorganización:

- No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

[Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante]

2. Síntomas de mala imagen e insatisfacción de los usuarios:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
- No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

3. Síntomas de debilidades económico-financieras:

- Incremento desmesurado de costes.
- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Desviaciones Presupuestarias significativas.
- Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

4. Síntomas de Inseguridad: Evaluación de nivel de riesgos

- Seguridad Lógica
- Seguridad Física
- Confidencialidad

[Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales]

Continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia* Totales y Locales.

Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoría. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio.

El proceso que conlleva realizar una auditoría, incluye una serie de actividades, se menciona las principales que se lleva a cabo en una metodología general.

- Estudiar y actualizar las áreas susceptibles de revisión

- Apegarse a las normas, políticas, procedimientos y técnicas de auditoría establecidos.
- Evaluar y verificar las áreas requeridas por la alta dirección o responsables
- Elaboración del informe de auditoria

2.4 Riesgos Informáticos

Un riesgo se define como la incertidumbre que ocurra un evento que podría tener un impacto en el logro de los objetivos.

Los riesgos son hechos o acontecimientos cuya probabilidad de ocurrencia es incierta. La trascendencia del riesgo, se basa en que su probable manifestación y el impacto que puede causar en la organización, pone en peligro la consecución de los objetivos de la misma [5].

A un riesgo se le conoce también como la eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado.

En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo el riesgo de perder datos a rotura de disco, virus informáticos, etc.) [6].

Figura 3: *Riesgo*

5 Riesgo
http://www.circulo-icau.cl/uploads/documentos/descarga_0/coso007.pdf

6 Riesgo
http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf

La acepción “riesgo informático” es un concepto nuevo en la terminología jurídica sin existir por tanto una definición específica.

El riesgo se refiere a la incertidumbre o probabilidad de que ocurra o se realice una eventualidad, la cual puede estar prevista; en este sentido podemos decir que el riesgo es la contingencia de un daño.

En función de lo anterior, podemos aseverar que los riesgos informáticos se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos como por ejemplo los equipos informáticos, periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, responsabilidad civil que estos ocasionan frente a terceros por la prestación de un servicio informático, etcétera.

En nuestro medio los riesgos informáticos no constituyen una figura jurídica especial, aunque se pueden aplicar en su tratamiento ordenamientos tales como la Ley del Contrato de seguro y la Ley General de Instituciones de Seguro; sin embargo, lo que motiva y justifica el señalar los riesgos informáticos como un fenómeno jurídico especial es la complejidad de los problemas que presentan en la práctica.

Por otra parte, es conveniente enunciar que la forma de apreciar un riesgo de esta índole es muy diferente al tratamiento que se les da a los riesgos comúnmente conocidos en el mercado de seguros.

De esta forma, el concepto de **Riesgo Informático** es una noción in extenso que se desarrolla al parejo de la tecnología, siendo objeto de estudio del llamado derecho informático bajo el rubro de los contratos informáticos [7].

Cuando ya ocurra la presencia del riesgo en la organización se debería realizar un tratamiento de cómo actuar frente a este factor, lo que se denominaría la gestión de los riesgos.

---

7 Riesgo Informático

http://www.bibliojuridica.org/libros/2/909/5.pdf

LA GESTION DE LOS RIESGOS

El principal objetivo de la administración de riesgos, como primera ley de la naturaleza, es garantizar la supervivencia de la organización, minimizando los costos asociados con los riesgos. Muchos de los defectos en la administración de riesgos radican en la ausencia de objetivos claros.

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

Los objetivos de la administración de riesgos están formalizados en una *"política corporativa de administración de riesgos"*, la cual describe las políticas y medidas tomadas para su consecución. Idealmente los objetivos y las políticas de administración de riesgos deben ser producto de las decisiones de la Alta Dirección de la compañía.

La administración de riesgos se ha considerado como un área funcional especial de la organización, por lo cual se han ido formalizando sus principios y técnicas.

El factor más importante para determinar cuáles riesgos requiere alguna acción específica es el máximo potencial de pérdida, algunas pérdidas pueden ser potencialmente devastadoras literalmente fuera del alcance de la organización mientras tanto otras envuelven menores consecuencias financieras, si el máximo potencial de pérdida de una amenaza es grande, la perdida sería inmanejable, por lo que el riesgo requiere de un tratamiento especial.

LOS RIESGOS INFORMATICOS

Es importante en toda organización contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

Viendo la necesidad en el entorno empresarial de este tipo de herramientas y teniendo en cuenta que, una de las principales causas de los problemas dentro del entorno informático, es la inadecuada administración de riesgos informáticos, esta información sirve de apoyo para una adecuada gestión de la administración de riesgos, basándose en los siguientes aspectos :

- La evaluación de los riesgos inherentes a los procesos informáticos.
- La evaluación de las amenazas ó causas de los riesgos.
- Los controles utilizados para minimizar las amenazas a riesgos.
- La asignación de responsables a los procesos informáticos.
- La evaluación de los elementos del análisis de riesgos.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de:

- Personas tanto internas como externas de la organización.
- Desastres naturales.
- Por servicios, suministros y trabajos no confiables e imperfectos.
- Por la incompetencia y las deficiencias cotidianas.
- Por el abuso en el manejo de los sistemas informáticos.
- Por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

Es fundamental que los directivos de las organizaciones que no se han ocupado lo suficiente en implementar un estricto sistema de seguridad se preocupen en:

- Reconocer la necesidad de establecer normas de seguridad para los datos, políticas, normas y directrices.
- Comprender que el papel que desempeñan en la organización, está relacionado con la seguridad del ciclo de vida del sistema de información.
- Establecer una planificación formalizada para la seguridad informática.
- Gestionar los medios necesarios para administrar correctamente la función de la seguridad informática.

RIESGOS RELACIONADOS CON LA INFORMATICA

En efecto, las principales áreas en que habitualmente ha incursionado la seguridad en los centros de cómputos han sido:

- Seguridad física.
- Control de accesos.
- Protección de los datos.
- Seguridad en las redes.

Los principales riesgos informáticos de los negocios son los siguientes:

Riesgos de Integridad: Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:

- *Interface del usuario:* Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones. Otros riesgos en esta área se relacionan a controles que aseguren la validez y completitud de la información introducida dentro de un sistema.
- *Procesamiento:* Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles detectivos y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.
- *Procesamiento de errores:* Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores (*Exceptions)* sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

- *Interface:* Los riesgos en esta área generalmente se relacionan con controles preventivos y detectivos que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.
- *Administración de cambios:* Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con la administración inadecuada de procesos de cambios organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.
- *Información:* Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos. La integridad puede perderse por: Errores de programación (*buena información es procesada por programas mal construídos)*, procesamiento de errores (*transacciones incorrectamente procesadas)* ó administración y procesamiento de errores (*Administración pobre del mantenimiento de sistemas).*

Riesgos de relación: Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (*Información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).*

Riesgos de acceso: Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

- *Procesos de negocio:* Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.

- *Aplicación:* La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.
- *Administración de la información:* El mecanismo provee a los usuarios acceso a la información específica del entorno.
- *Entorno de procesamiento:*
- Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.
- *Redes:* En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.
- *Nivel físico:* Protección física de dispositivos y un apropiado acceso a ellos. Algunos de los métodos de prevenir el acceso ilegal a los servicios informáticos incluyen:
    - Claves y contraseñas para permitir el acceso a los equipos.
    - Uso de cerrojos y llaves.
    - Fichas ó tarjetas inteligentes.
    - Dispositivos biométricos (Identificación de huellas dactilares, lectores de huellas de manos, patrones de voz, firma/escritura digital, análisis de pulsaciones y escáner de retina, entre otros).

Riesgos de utilidad: Estos riesgos se enfocan en tres diferentes niveles de riesgo:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
- Backups y planes de contingencia controlan desastres en el procesamiento de la información.

Riesgos en la infraestructura: Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (*hardware, software, redes, personas y procesos)* para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de

procesamiento de información y las aplicaciones asociadas (*servicio al cliente, pago de cuentas, etc.)*. Estos riesgos son generalmente se consideran en el contexto de los siguientes procesos informáticos:

- *Planeación organizacional:* Los proceso en esta área aseguran la definición del impacto, definición y verificación de la tecnología informática en el negocio. Además, verifica si existe una adecuada organización (*gente y procesos)* asegura que los esfuerzos de la tecnología informática será exitosa.
- *Definición de las aplicaciones:* Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio. Estos procesos abarcan: la determinación de comprar una aplicación ya existente ó desarrollar soluciones a cliente. Estos procesos también aseguran que cualquier cambio a las aplicaciones (*compradas o desarrolladas)* sigue un proceso definido que confirma que los puntos críticos de proceso/control son consistentes (*Todos los cambios son examinados por usuarios antes de la implementación).*
- *Administración de seguridad:* Los procesos en esta área aseguran que la organización está adecuadamente direccionada a establecer, mantener y monitorizar un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de fraudes a niveles aceptables.
- *Operaciones de red y computacionales:* Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutados por personal operativo definido, medido y monitoreado.
- También aseguran que los sistemas son consistentes y están disponibles a los usuarios a un nivel de ejecución satisfactorio.
- *Administración de sistemas de bases de datos:* Los procesos en esta área están diseñados para asegurar que las bases de datos usadas para soportar aplicaciones críticas y reportes tengan consistencia de definición, correspondan con los requerimientos y reduzcan el potencial de redundancia.

- *Información / Negocio:* Los proceso en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesitan.

Riesgos de seguridad general: Los estándar IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

- *Riesgos de choque de eléctrico:* Niveles altos de voltaje.
- *Riesgos de incendio:* Inflamabilidad de materiales.
- *Riesgos de niveles inadecuados de energía eléctrica.*
- *Riesgos de radiaciones:* Ondas de ruido, de láser y ultrasónicas.
- *Riesgos mecánicos:* Inestabilidad de las piezas eléctricas.

Seguidamente veremos otros riesgos que afectan a la protección informática puesto que aumentan los puntos de vulnerabilidad de los sistemas

Concentración de procesamiento de aplicaciones más grandes y de mayor complejidad: Una de las causas más importantes del incremento en los riesgos informáticos probablemente sea el aumento en la cantidad de aplicaciones o usos que se le da a las computadoras y la consecuente concentración de información y tecnología de software para el procesamiento de datos, generalmente la información y programas están concentrados en las manos de pocas personas.

Como consecuencia de ello, se corre el riesgo de sufrir lo que en la jerga de seguridad informática suele denominarse "Amnesia Corporativa" debido a algún desastre ocurrido en las computadoras, y de quedar expuesta a una suspensión prolongada del procesamiento y por ende el mal funcionar de la compañía generándose una situación de caos para la misma y en todos los niveles de la organización.

Dependencia en el personal clave: Además del peligro que encierra algún desastre en los sistemas informáticos, existen otras situaciones potencialmente riesgosas de las cuales la más importante es, quizá, la dependencia hacia individuos clave. La dependencia en individuos clave, algunos de los cuales poseen un alto nivel de desempeño técnico, con frecuencia pone a la compañía en manos de relativamente pocas personas, siendo que éstas por lo general son externas a la organización. Este tipo de situaciones ha conducido a

situaciones donde las empresas se han visto expuestas al chantaje, la extorsión, mal uso y fraudes en la explotación de los sistemas informáticos.

La amenaza no solo se restringe al abuso del tipo descrito aquí. Este personal especializado con frecuencia posee el conocimiento único y no registrado de las modificaciones o el funcionamiento de las aplicaciones. La supervisión y el control de su trabajo resulta difícil como lo es el conocimiento de lo que si funcionaría sin contar con las habilidades del especialista.

Desaparición de los controles tradicionales*:* Muchas de las nuevas y extensas aplicaciones omiten las auditorías tradicionales y los controles impresos por razones de volumen. Las aplicaciones contienen verificadores automáticos que aseguran la integridad de la información que se procesa. Este gran cambio en el criterio sobre el control de los empleados y las brechas respecto a la comunicación, crean situaciones de seguridad totalmente diferentes.

Huelgas, terrorismo e inestabilidad social: El nivel actual de riesgo en computación se debe revisar también dentro del contexto de inestabilidad social en muchas partes del mundo. Ha habido ataques físicos a diversas instalaciones, sin embargo algunas veces se trata de la incursión de personal interno y no de agitadores. Este tipo insidioso de riesgo es, en potencia, la fuente de más alto perjuicio para la institución. Este riesgo, solo, genera una amplia posibilidad de nuevas amenazas ante las cuales hay que responder.

Los ataques internos por parte del personal de una institución pueden tomar la forma de huelga; ésta, aunque no sea violenta, puede ser tan perjudicial como el ataque físico. Las huelgas han sucedido en grandes instalaciones que operan en línea en diferentes partes del mundo y por tanto en nuestro país también.

Mayor conciencia de los proveedores: Hasta hace pocos años este tema no constituía motivo de gran preocupación para los proveedores, pero la conciencia acerca de la exposición a los riesgos los ha obligado a destinar presupuestos considerables para la investigación acerca de la seguridad. Como resultado, se dispone de un mayor número de publicaciones de alta calidad para los usuarios, lo que permite mejorar la estructura y el enfoque para la seguridad de las computadoras; asimismo, ha intensificado el interés por reducir en forma progresiva el riesgo causado por un desastre en las computadoras.

CAPÍTULO III

3. ESTUDIO DE LAS METODOLOGÍAS

Metodología

Una metodología es un conjunto de etapas formalmente estructuradas, de manera que brinden a los interesados los siguientes parámetros de acción en el desarrollo de sus proyectos: plan general y detallado, tareas y acciones, tiempos, aseguramiento de la calidad, involucrados, etapas, revisiones de avance, responsables, recursos requeridos, entre otros [8].

La 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.

---

[8] *Metodología*
http://www.angelfire.metodologia.doc

3.1 Metodologías de Auditoria Informática

Las metodologías son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.

La auditoria informática solo 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 la misma. Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que la productividad de que las amenazas se materialicen en hechos sea lo más baja posible o al menos quede reducida de una forma razonable en costo-beneficio

Las metodologías de auditoría informática son de tipo cualitativo/subjetivo. Se puede decir que son subjetivas por excelencia. Están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen en gran profesionalidad y formación continua. Solo existen dos tipos de metodologías para la auditoría informática:

- **Controles Generales.-** Son el producto estándar de los auditores profesionales. El objetivo aquí es dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera, es resultado es escueto y forma parte del informe de auditoría, en donde se hacen notar las vulnerabilidades encontradas. Están desprestigiadas ya que dependen en gran medida de la experiencia de los profesionales que las usan.
- **Metodologías de los auditores internos.-** Están formuladas por recomendaciones de plan de trabajo y de todo el proceso que se debe seguir. También se define el objetivo de la misma, que habrá que describirlo en el memorando de apertura al auditado. De la misma forma se describe en forma de cuestionarios genéricos, con una orientación de los controles a revisar. El auditor interno debe crear sus metodologías necesarias para auditar los distintos aspectos o áreas en el plan auditor.

3.1.1 COBIT

Historia

Modelo desarrollado por la ISACA y el IT Governance Institute (ITGI) para llevar a la práctica el Gobierno de TI en las organizaciones.

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores [9].

COBIT (Control Objectives for Information and Related Technology) define una serie de procesos relacionados con TI, los cuales agrupa en cuatro dominios (Planificación y organización, desarrollo y adquisición, Soporte y Monitoreo), y los cuales estructura en distintas actividades. Estos procesos son adaptables a las distintas organizaciones y son la base para cualquiera de los enfoques utilizados para su implementación (usuarios, administradores de TI y auditores)

Independientemente de la realidad tecnológica de cada caso concreto, COBIT determina, con el respaldo de las principales normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en TI que son necesarias para alinear TI con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.

La misión COBIT es " para investigar, desarrollar, hacer público y promover un juego autoritario, actualizado, internacional de objetivos de control de tecnología de información generalmente aceptados para el empleo cotidiano por directores comerciales e interventores. "

---

[9] *COBIT*
http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf

Los gerentes, interventores, y usuarios se benefician del desarrollo de COBIT porque esto les ayuda a entender sus sistemas TI y decidir el nivel de seguridad (valor) y control que es necesario para proteger el activo de sus empresas por el desarrollo de un modelo de gobernación 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.

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI. La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI. **El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos organizacionales.** Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI de la empresa sirve como base a los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte al Committee Of Sponsoring Organisations Of The Treadway Commission
Control interno—Marco de Referencia integrado, el marco de referencia de control ampliamente aceptado para gobierno de la empresa y para la administración de riesgos, así

como a marcos compatibles similares. Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para la TI y decidir qué tipo de gobierno y de control debe aplicar.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien. Para que la TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implantar un sistema de control interno o un marco de trabajo.

El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de TI a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en vincular las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y de TI. El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural. Pero, ¿cómo puede la empresa poner bajo control la TI de tal manera que genere la información que la empresa necesita? ¿Cómo puede administrar los riesgos y asegurar los recursos de TI de los cuales depende tanto? ¿Cómo puede la empresa asegurar que TI logre sus objetivos y soporte los del negocio?

Primero, la dirección requiere objetivos de control que definan la última meta de implantar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar un nivel razonable para garantizar que:

- Se alcancen los objetivos del negocio.
- Se prevengan o se detecten y corrijan los eventos no deseados.

En segundo lugar, en los complejos ambientes de hoy en día, la dirección busca continuamente información oportuna y condensada, para tomar decisiones difíciles respecto a riesgos y controles, de manera rápida y exitosa. ¿Qué se debe medir y cómo? Las empresas requieren una medición objetiva de dónde se encuentran y dónde se requieren mejoras, y deben implantar una caja de herramientas gerenciales para monitorear esta mejora. **La figura 4** muestra algunas preguntas frecuentes y las herramientas gerenciales de información usadas para encontrar las respuestas, aunque estos tableros de control requieren indicadores, los marcadores de puntuación requieren mediciones y los Benchmarking requieren una escala de comparación.

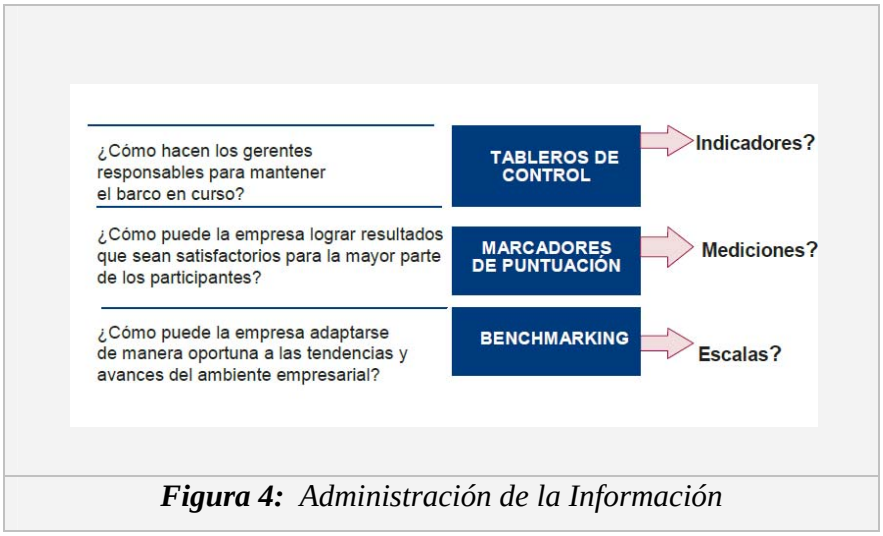


Figura 4: *Administración de la Información*

Una respuesta a los requerimientos de determinar y monitorear el nivel apropiado de control y desempeño de TI son las definiciones específicas de COBIT de los siguientes conceptos:

• **Benchmarking** de la capacidad de los procesos de TI, expresada como modelos de madurez, derivados del Modelo de Madurez de la Capacidad del Instituto de Ingeniería de Software

• **Metas y métricas** de los procesos de TI para definir y medir sus resultados y su desempeño, basados en los principios de balanced business Scorecard de Robert Kaplan y David Norton

• **Metas de actividades** para controlar estos procesos, con base en los objetivos de control detallados de COBIT La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI. Después de identificar los procesos y controles críticos de TI, el modelado de la madurez permite identificar y demostrar a la dirección las brechas en la capacidad. Entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado. COBIT da soporte al gobierno de TI **(figura 5)** al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI capacita el negocio y maximiza los beneficios
- Los recursos de TI se usen de manera responsable
- Los riesgos de TI se administren apropiadamente

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. Mientras las otras áreas consideradas contribuyen, la transparencia se logra de forma principal por medio de la medición del desempeño.

Figura 5: *Áreas Focales del Gobierno de TI*

Alineación estratégica se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de valor se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.

Administración de recursos se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI:, aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

Administración de riesgos requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del deseo de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

Medición del desempeño rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega

del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.

Estas áreas focales de gobierno de TI describen los tópicos en los que la dirección ejecutiva requiere poner atención para gobernar la TI en sus empresas. La dirección operacional usa procesos para organizar y administrar las actividades cotidianas de TI. COBIT brinda un modelo de procesos genéricos que representa todos los procesos que normalmente se encuentran en las funciones de TI, ofreciendo un modelo de referencia común entendible para los gerentes operacionales de IT y del negocio. Se establecieron equivalencias entre los modelos de procesos COBIT y las áreas focales del gobierno de TI (vea apéndice II), ofreciendo así un puente entre lo que los gerentes operacionales deben realizar y lo que los ejecutivos desean gobernar. Para lograr un gobierno efectivo, los ejecutivos esperan que los controles a ser implementados por los gerentes operacionales se encuentren dentro de un marco de control definido para todo los procesos de TI. Los objetivos de control de TI de COBIT están organizados por proceso de TI; por lo tanto, el marco de trabajo brinda un vínculo claro entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI. COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI, (vea apéndice IV). COBIT actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se vincula con los requerimientos de gobierno y de negocios.

COSO (y similares marcos de trabajo) es generalmente aceptado como el marco de trabajo de control interno para las empresas. COBIT es el marco de trabajo de control interno generalmente aceptado para TI.

Los productos COBIT se han organizado en tres niveles **(figura 6)** diseñados para dar soporte a:

- Administración y consejos ejecutivos
- Administración del negocio y de TI
- Profesionales en Gobierno, aseguramiento, control y seguridad.

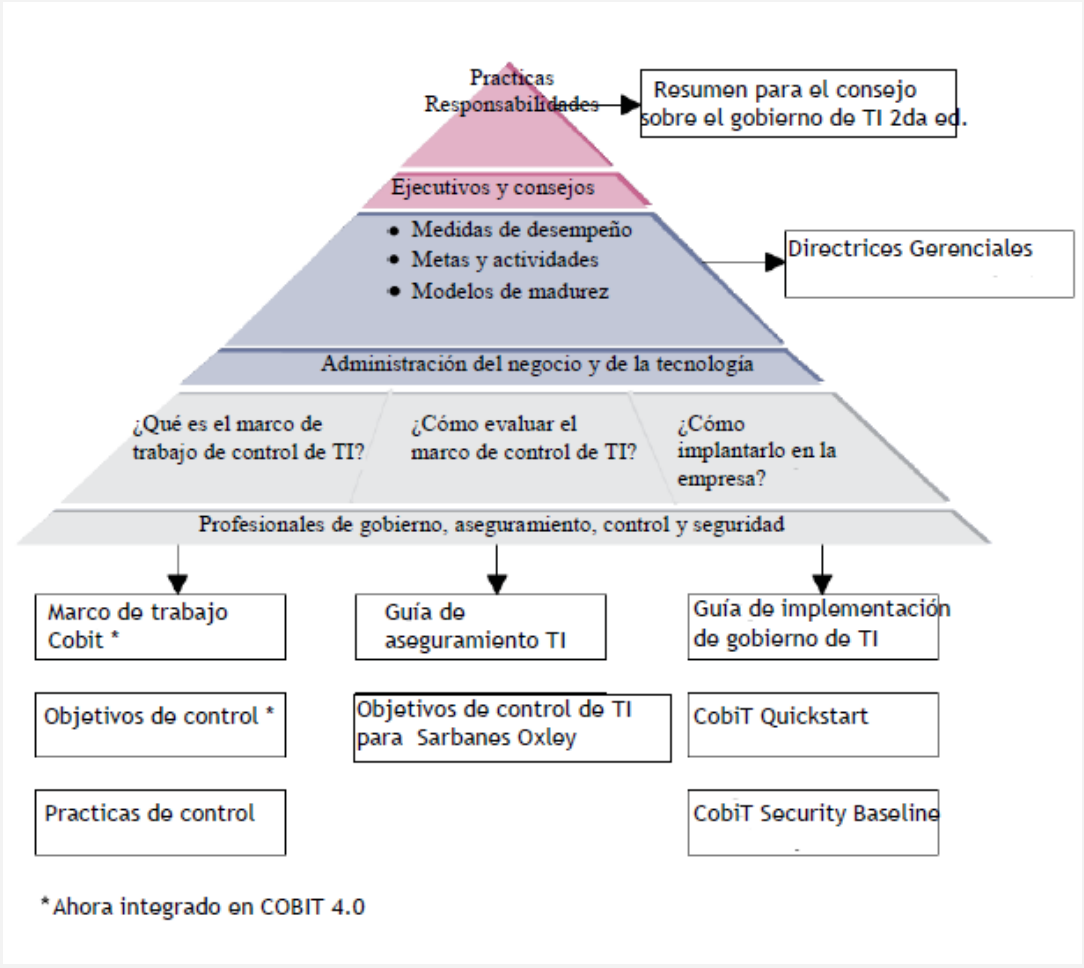


Figura 6: *Productos Cobit*

Es de interés primordial para los ejecutivos:

• *El resumen informativo al consejo sobre el gobierno de TI, 2da Edición.*- Diseñado para ayudar a los ejecutivos a entender porqué el gobierno de TI es importante, cuáles son sus intereses y sus responsabilidades para su administración

Es de primordial interés para la dirección del negocio y de tecnología:

• *Directrices Gerenciales.*- Herramientas para ayudar a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad. Las directrices

ayudan a brindar respuestas a preguntas comunes de la administración: ¿Qué tan lejos podemos llegar para controlar la TI?, y ¿el costo justifica el beneficio? ¿Cuáles son los indicadores de un buen desempeño? ¿Cuáles son las prácticas administrativas clave a aplicar? ¿Qué hacen otros? ¿Cómo medimos y comparamos?

Es de primordial interés para los profesionales de gobierno, aseguramiento, control y seguridad:

• *Marco de Referencia*.- Explicar cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los vincula a los requerimientos del negocio

• *Objetivos de control*.- Brindar objetivos a la dirección basados en las mejores prácticas genéricas para todas las actividades de TI

• *Prácticas de control*.- Brindar guía de por qué vale la pena implementar controles y cómo implantarlos

• *Guía de aseguramiento de TI*.- Ofrecer un enfoque genérico de auditoría y una guía de soporte para la auditoria de todos los procesos TI de COBIT

• *Objetivos de control de IT para Sarbanes-Oxley*.- Proporcionar una guía sobre cómo garantizar el cumplimiento para el ambiente de TI basado en los objetivos de control COBIT

• *Guía de implementación del Gobierno de TI*.- Ofrecer un mapa genérico para implementar el gobierno de TI usando los recursos COBIT y un juego de herramientas de soporte

• COBIT *Quickstart*TM.- Brindar una línea base de control para pequeñas organizaciones y un posible primer paso para las grandes

• COBIT *Security Baseline*TM .- Enfocar la organización a los pasos esenciales para implementar la seguridad de la información dentro de la Empresa

Todos estos componentes de COBIT se interrelacionan, ofreciendo soporte para las necesidades de gobierno, de administración, de control y de auditoría de los distintos interesados, como se muestra en la **figura 7.**

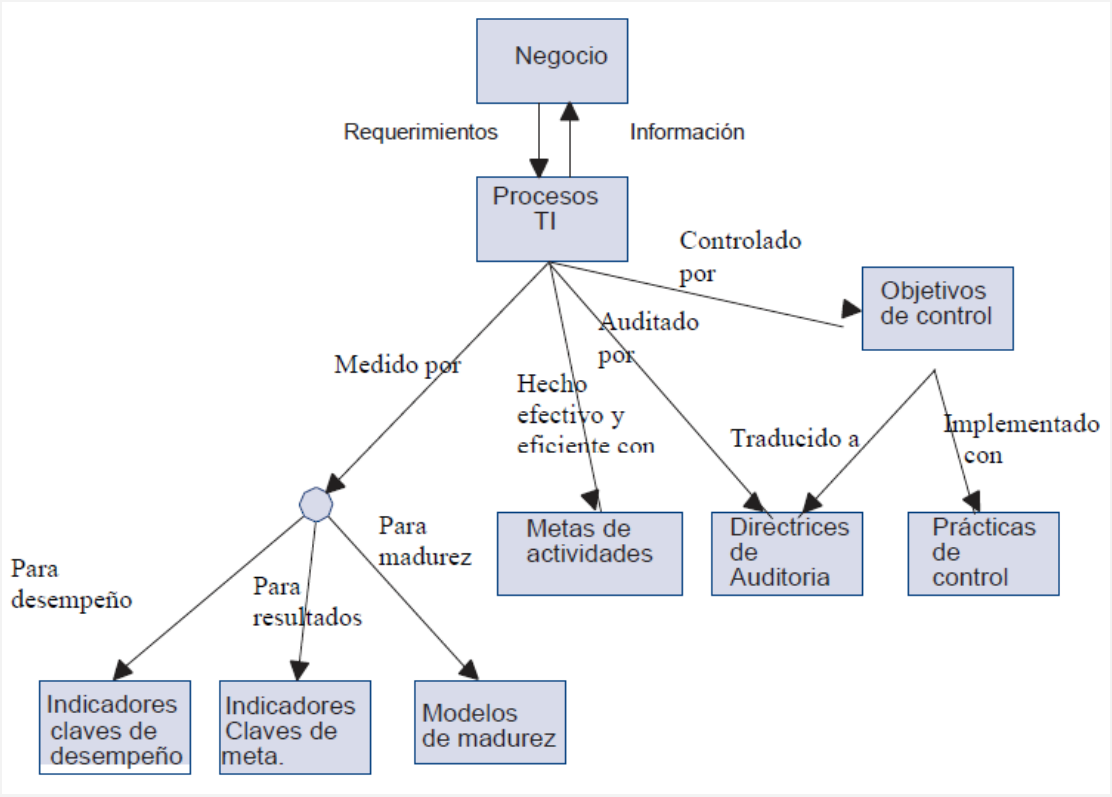


Figura 7: *Interrelaciones de los componentes de COBIT*

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar

acerca de TI. Los beneficios de implementar COBIT como marco de referencia de gobierno sobre la TI incluyen:

• Mejor alineación, con base en su enfoque de negocios

• Una visión, entendible para la gerencia, de lo que hace TI

• Propiedad y responsabilidades claras, con base en su orientación a procesos

• Aceptación general de terceros y reguladores

• Entendimiento compartido entre todos los participantes, con base en un lenguaje común

• Cumplimiento de los requerimientos COSO para el ambiente de control de TI El resto de este documento brinda una descripción del marco de trabajo COBIT, así como todos los componentes esenciales COBIT organizados por los dominios TI de COBIT y 34 procesos de TI.

MARCO DE TRABAJO COBIT

La necesidad de un marco de trabajo para el control del gobierno de TI

Por qué

Cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información (TI) es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva. En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Garantice el logro de sus objetivos
- Tenga suficiente flexibilidad para aprender y adaptarse
- Cuente con un manejo juicioso de los riesgos que enfrenta
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas

Las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI, y encuentran maneras para:

- Alinear la estrategia de TI con la estrategia del negocio

- Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa
- Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas
- Crear relaciones constructivas y comunicaciones efectivas entre el negocio y TI, y con socios externos
- Medir el desempeño de TI

Las empresas no pueden responder de forma efectiva a estos requerimientos de negocio y de gobierno sin adoptar e implementar un marco de Referencia de gobierno y de control para TI, de tal manera que:

- Se forme un vínculo con los requerimientos del negocio
- El desempeño real con respecto a los requerimientos sea transparente
- Organice sus actividades en un modelo de procesos generalmente aceptado
- Identifique los principales recursos a ser aprovechados
- Se definan los objetivos de control Gerenciales a ser considerados

Además, el gobierno y los marcos de trabajo de control están siendo parte de las mejores prácticas de la administración de TI y sirven como facilitadores para establecer el gobierno de TI y cumplir con el constante incremento de requerimientos regulatorios. Las mejores prácticas de TI se han vuelto significativas debido a un número de factores:

Directores de negocio y consejos directivos que demandan un mayor retorno de la inversión en TI, es decir, que TI genere lo que el negocio necesita para mejorar el valor de los participantes

Preocupación por el creciente nivel de gasto en TI

La necesidad de satisfacer requerimientos regulatorios para controles de TI en áreas como privacidad y reportes financieros (por ejemplo, Sarbanes-Oxley Act, Basel II) y en sectores específicos como el financiero, farmacéutico y de atención a la salud.

La selección de proveedores de servicio y el manejo de Outsourcing y de Adquisición de servicios

Riesgos crecientemente complejos de la TI como la seguridad de redes

Iniciativas de gobierno de TI que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de TI, aumentar el valor del negocio y reducir los riesgos de éste

La necesidad de optimizar costos siguiendo, siempre que sea posible, un enfoque estandarizado en lugar de enfoques desarrollados especialmente

La madurez creciente y la consecuente aceptación de marcos de trabajo respetados tales como COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2

La necesidad de las empresas de valorar su desempeño en comparación con estándares generalmente aceptados y con respecto a su competencia (Benchmarking)

Quién

Un marco de referencia de gobierno y de control requiere servir a una variedad de interesados internos y externos, cada uno de los cuales tiene necesidades específicas:

• Interesados dentro de la empresa que tengan un interés en generar valor de las inversiones en TI:

- ✓ Aquellos que tomen decisiones de inversiones
- ✓ Aquellos que deciden respecto a los requerimientos
- ✓ Aquellos que utilicen los servicios de TI

• Interesados internos y externos que proporcionen servicios de TI:

- ✓ Aquellos que administren la organización y los procesos de TI
- ✓ Aquellos que desarrollen capacidades
- ✓ Aquellos que operen los servicios

• Interesados internos y externos con responsabilidades de control/riesgo:

- ✓ Aquellos con responsabilidades de seguridad, privacidad y/o riesgo
- ✓ Aquellos que realicen funciones de cumplimiento
- ✓ Aquellos que requieran o proporcionen servicios de aseguramiento

Qué

Para satisfacer los requerimientos previos, un marco de referencia para el gobierno y el control de TI deben satisfacer las siguientes especificaciones generales:

• Brindar un enfoque de negocios que permita la alineación entre los objetivos de negocio y de TI.

• Establecer una orientación a procesos para definir el alcance y el grado de cobertura, con una estructura definida que permita una fácil navegación en el contenido.
• Ser generalmente aceptable al ser consistente con las mejores prácticas y estándares de TI aceptados, y que sea independiente de tecnologías específicas.
• Proporcionar un lenguaje común, con un juego de términos y definiciones que sean comprensibles en lo general para todos los Interesados.
• Ayudar a satisfacer requerimientos regulatorios, al ser consistente con estándares de gobierno corporativo generalmente aceptados (COSO) y con controles de TI esperados por agentes reguladores y auditores externos.

COMO SATISFACE COBIT LA NECESIDAD

Como respuesta a las necesidades descritas en la sección anterior, el marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

Orientado al negocio

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los propietarios de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio **(figura 8):** proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información. El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

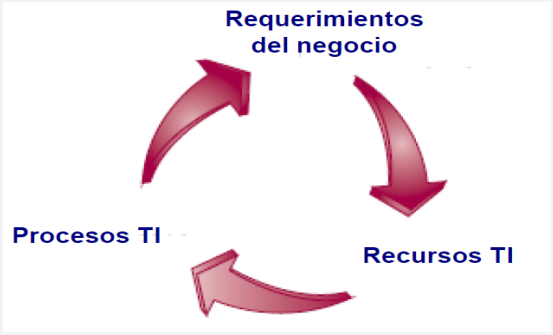


Figura 8: *Principio Básico COBIT*

CRITERIOS DE INFORMACIÓN DE COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

• La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

• La eficiencia consiste en que la información sea generada optimizando los recursos (más productivo y económico).

• La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.

• La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

• La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.

• El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
• La confiabilidad significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

METAS DE NEGOCIOS Y DE TI

Mientras que los criterios de información proporcionan un método genérico para definir los requerimientos del negocio, la definición de un conjunto de metas genéricas de negocio y de TI ofrece una base más refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas. Cada empresa usuaria de TI, habilita las iniciativas del negocio y estas pueden ser representadas como metas del negocio para TI. El Apéndice I proporciona una matriz de metas genéricas de negocios y metas de TI y como se asocian con los criterios de la información. Estos ejemplos genéricos se pueden utilizar como guía para determinar los requerimientos, metas y métricas específicas del negocio para la empresa.
Si se pretende que la TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una propiedad y una dirección clara de los requerimientos por parte del negocio (el cliente) y un claro entendimiento para TI, de cómo y qué debe entregar (el proveedor).
La **Figura 9** ilustra como la estrategia de la empresa se debe traducir por parte del negocio en objetivos para su uso de iniciativas facilitadas por TI (Las metas de negocio para TI). Estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de la TI (las metas de TI), y luego éstas a su vez definir los recursos y capacidades de TI (la arquitectura empresarial para TI) requeridos para ejecutar de forma exitosa la parte que le corresponde a TI de la estrategia empresarial. Todos estos objetivos se deben expresar en términos de negocios significativos para el cliente, y esto, combinado con una alineación efectiva de la jerarquía de objetivos, asegurará que el negocio pueda confirmar que TI puede, con alta probabilidad, dar soporte a las metas del negocio.

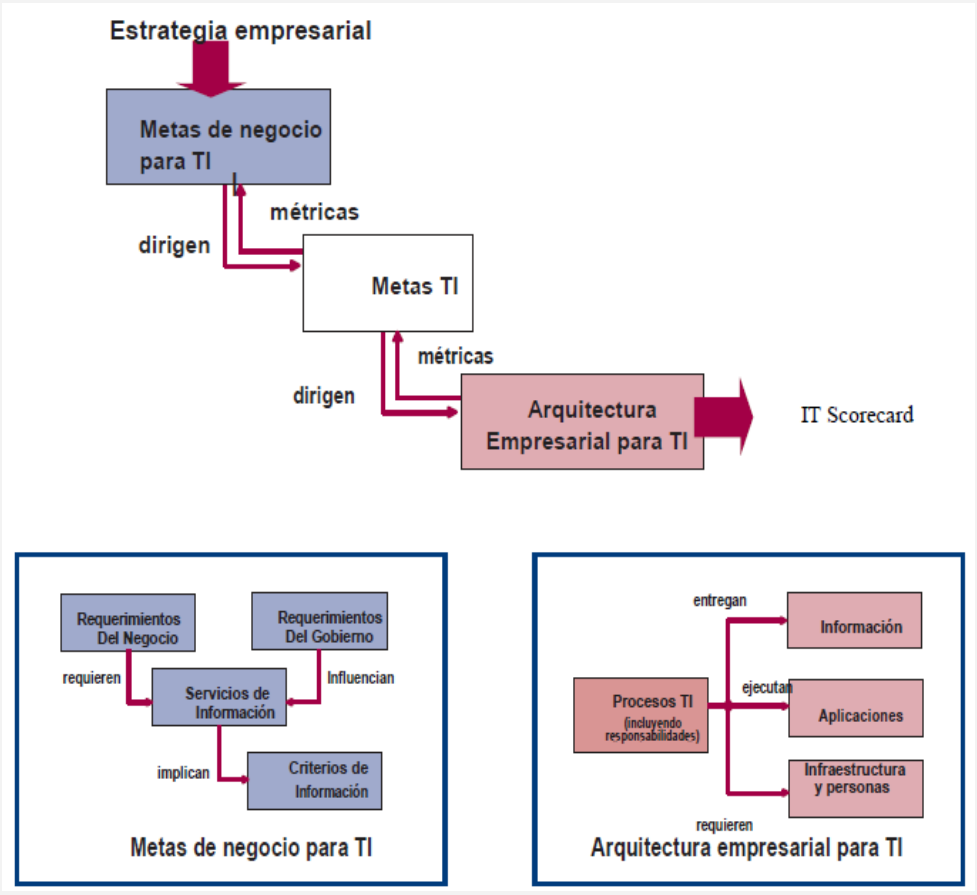


Figura 9: *Definiendo metas de TI y Arquitectura Empresarial para TI*

Una vez que las metas alineadas han sido definidas, requieren ser monitoreadas para garantizar que la entrega cumple con las expectativas. Esto se logra con métricas derivadas de las metas y capturadas en scorecard de TI que el cliente pueda entender y seguir, y que permita al proveedor enfocarse en sus propios objetivos internos. El apéndice I ofrece una visión global de cómo las metas genéricas del negocio se relacionan con las metas de TI, con los procesos de TI y con los criterios de la información. La tabla ayuda a demostrar el

alcance de COBIT y la relación general de negocios entre COBIT y los impulsores del negocio.

RECURSOS DE TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI, como se muestra en la **figura 9.** Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (ej., implementando una cadena de suministro) que genere el resultado deseado (ej., mayores ventas y beneficios financieros). Los recursos de TI identificados en COBIT se pueden definir como sigue:

• Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

• La información son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.

• La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

• Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

La **figura 10** resume cómo las metas de negocio para TI influencian la manera en que se manejan los recursos necesarios de TI por parte de los procesos de TI para lograr las metas de TI.

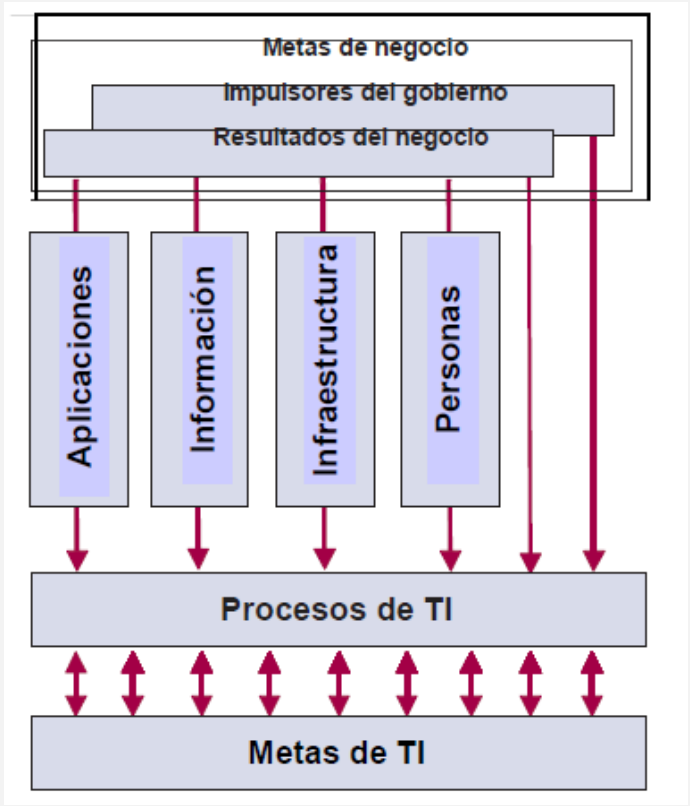


Figura 10: *Administración de recursos de TI para garantizar las metas de TI*

Procesos orientados

COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la

medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades. Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

PLANEAR Y ORGANIZAR (PO) Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios afectarán las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Por lo general aclara las siguientes preguntas de la gerencia:

• ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?

• ¿Están optimizados los costos de TI?

• ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?

• ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

Basado en controles

LOS PROCESOS REQUIEREN CONTROLES

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT.

La guía se puede obtener del modelo de control estándar mostrado en la **figura 11**. Sigue los principios que se evidencian en la siguiente analogía: cuando se ajusta la temperatura ambiente (estándar) para el sistema de calefacción (proceso), el sistema verificará de forma constante (comparar) la temperatura ambiente (inf. de control) e indicará (actuar) al sistema de calefacción para que genere más o menos calor.

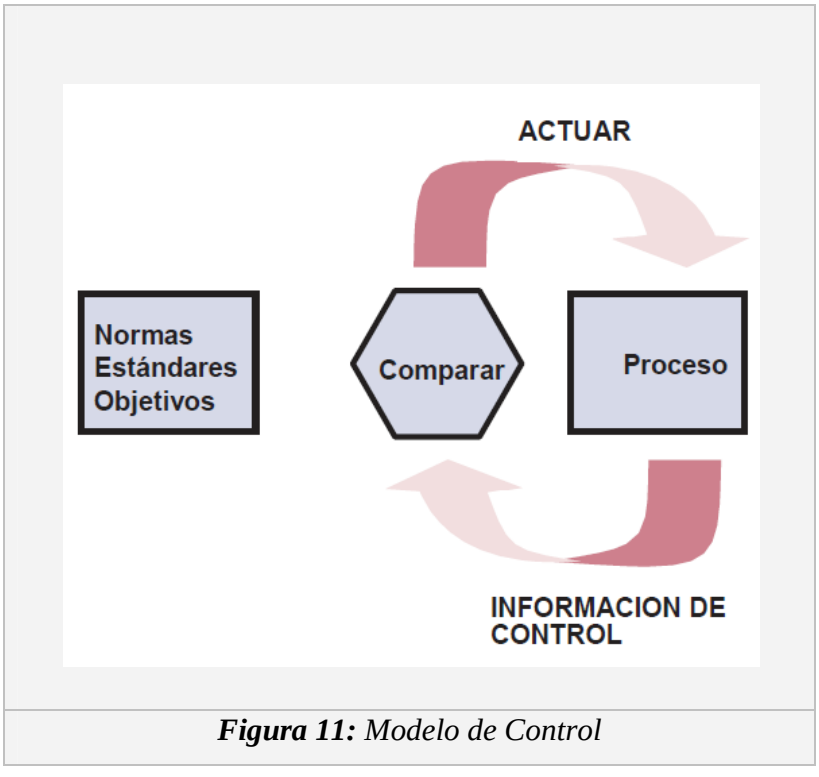


Figura 11: *Modelo de Control*

La gerencia operacional usa los procesos para organizar y administrar las actividades de TI en curso. COBIT brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia operacional de TI y para la gerencia administrativa. Para lograr un gobierno efectivo, los gerentes operacionales deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI. Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado. Los objetivos de control detallados se identifican por dos caracteres que representan el dominio más un número de proceso y un número de objetivo de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa número de control de proceso. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

PC1 Dueño del proceso.- Asignar un dueño para cada proceso COBIT de tal manera que la responsabilidad sea clara.

PC2 Reiterativo.- Definir cada proceso COBIT de tal forma que sea repetitivo.

PC3 Metas y objetivos.- Establecer metas y objetivos claros para cada proceso COBIT para una ejecución efectiva.

PC4 Roles y responsabilidades.- Definir roles, actividades y responsabilidades claros en cada proceso COBIT para una ejecución eficiente. *PC5 Desempeño del proceso* Medir el desempeño de cada proceso COBIT en comparación con sus metas. *PC6 Políticas, planes y procedimientos* Documentar, revisar, actualizar, formalizar y comunicar a todas las partes involucradas cualquier política, plan ó procedimiento que impulse un proceso COBIT. Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia debido a que habrá menos errores y un enfoque administrativo más

consistente. Además, COBIT ofrece ejemplos ilustrativos para cada proceso, los cuales no son exhaustivos o anticuados / caducos, de:

Entradas y salidas genéricas

Actividades y guías sobre roles y responsabilidades en una gráfica RACI

Metas de actividades clave (las cosas más importantes a realizar)

Métricas Además de evaluar qué controles son requeridos, los propietarios de procesos deben entender qué entradas requieren de otros procesos y que requieren otros de sus procesos.

COBIT brinda ejemplos genéricos de las entradas y salidas clave para cada proceso incluyendo los requerimientos externos de TI. Existen algunas salidas que son entradas a todos los demás procesos, marcadas como “TODOS” en las tablas de salidas, pero no se mencionan como entradas en todos los procesos, y por lo general incluyen estándares de calidad y requerimientos de métricas, el marco de trabajo de procesos de TI, roles y responsabilidades documentados, el marco de control empresarial de TI, las políticas de TI, y roles y responsabilidades del personal. El entendimiento de los roles y responsabilidades para cada proceso es clave para un gobierno efectivo. COBIT proporciona una gráfica RACI (quién es responsable, quién rinde cuentas, quién es consultado y quien informado) para cada proceso. Rendir cuentas significa la responsabilidad termina aquí, esta es la persona que provee autorización y direccionamiento a una actividad. Responsabilidad se refiere a la persona que realiza la actividad. Los otros dos roles (consultado e informado) garantizan que todas las personas que son requeridas están involucradas y dan soporte al proceso.

CONTROLES DEL NEGOCIO Y CONTROLES DE TI

El sistema empresarial de controles internos impacta a TI en tres niveles:

- Al nivel de dirección ejecutiva, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte del consejo y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.

- Al nivel de procesos de negocio, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones, la separación de funciones y las conciliaciones manuales. Los controles al nivel de procesos de negocio son, por lo tanto, una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Ambos son responsabilidad del negocio en cuanto a su definición y administración aunque los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.
- Para soportar los procesos de negocio, TI proporciona servicios, por lo general de forma compartida, por varios procesos de negocio, así como procesos operacionales y de desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de integridad.

CONTROLES GENERALES DE TI Y CONTROLES DE APLICACIÓN

Los controles generales son aquellos que están incrustados en los procesos y servicios de TI. Algunos ejemplos son:

- Desarrollo de sistemas
- Administración de cambios
- Seguridad
- Operación del computador

Los controles incluidos en las aplicaciones del proceso de negocios se conocen por lo general como controles de aplicación. Ejemplos:

- Integridad (Completitud)
- Precisión
- Validez
- Autorización
- Segregación de funciones

COBIT asume que el diseño e implementación de los controles de aplicación automatizados son responsabilidad de TI, y están cubiertos en el dominio de Adquirir e Implementar, con base en los requerimientos de negocio definidos, usando los criterios de información de COBIT. La responsabilidad operacional de administrar y controlar los controles de aplicación no es de TI, sino del propietario del proceso de negocio. TI entrega y da soporte a los servicios de las aplicaciones y a las bases de datos e infraestructura de soporte. Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales de TI, pero no los controles de las aplicaciones, debido a que son responsabilidad de los dueños de los procesos del negocio, y como se describió anteriormente, están integrados en los procesos de negocio. La siguiente lista ofrece un conjunto recomendado de objetivos de control de las aplicaciones identificados por ACn, número de Control de Aplicación (por sus siglas en inglés):

Controles de origen de datos/ autorización

AC1 Procedimientos de preparación de datos

Los departamentos usuarios implementan y dan seguimiento a los procedimientos de preparación de datos. En este contexto, el diseño de los formatos de entrada asegura que los errores y las omisiones se minimicen. Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable que los errores y las irregularidades son detectadas, reportadas y corregidas.

AC2 Procedimientos de autorización de documentos fuente

El personal autorizado, actuando dentro de su autoridad, prepara los documentos fuente de forma adecuada y existe una segregación de funciones apropiada con respecto a la generación y aprobación de los documentos fuente.

AC3 Recolección de datos de documentos fuente

Los procedimientos garantizan que todos los documentos fuente autorizados son completos y precisos, debidamente justificados y transmitidos de manera oportuna para su captura.

AC4 Manejo de errores en documentos fuente

Los procedimientos de manejo de errores durante la generación de los datos aseguran de forma razonable la detección, el reporte y la corrección de errores e irregularidades.

AC5 Retención de documentos fuente Existen procedimientos para garantizar que los documentos fuente originales son retenidos o pueden ser reproducidos por la organización durante un lapso adecuado de tiempo para facilitar el acceso o reconstrucción de datos así como para satisfacer los requerimientos legales.

Controles de entrada de datos

AC6 Procedimientos de autorización de captura de datos Los procedimientos aseguran que solo el personal autorizado capture los datos de entrada.

AC7 Verificaciones de precisión, integridad y autorización

Los datos de transacciones, ingresados para ser procesados (generados por personas, por sistemas o entradas de interfaces) están sujetos a una variedad de controles para verificar su precisión, integridad y validez. Los procedimientos también garantizan que los datos de entrada son validados y editados tan cerca del punto de origen como sea posible.

AC8 Manejo de errores en la entrada de datos

Existen y se siguen procedimientos para la corrección y re-captura de datos que fueron ingresados de manera incorrecta.

Controles en el Procesamiento de datos

AC9 Integridad en el procesamiento de datos

Los procedimientos para el procesamiento de datos aseguran que la separación de funciones se mantiene y que el trabajo realizado de forma rutinaria se verifica. Los procedimientos garantizan que existen controles de actualización adecuados, tales como totales de control de corrida-a-corrida, y controles de actualización de archivos maestros.

AC10 Validación y edición del procesamiento de datos

Los procedimientos garantizan que la validación, la autenticación y la edición del procesamiento de datos se realizan tan cerca como sea posible del punto de generación. Los individuos aprueban decisiones vitales que se basan en sistemas de inteligencia artificial.

AC11 Manejo de errores en el procesamiento de datos Los procedimientos de manejo de errores en el procesamiento de datos permiten que las transacciones erróneas sean identificadas sin ser procesadas y sin una indebida interrupción del procesamiento de otras transacciones válidas.

Controles de salida de datos

AC12 Manejo y retención de salidas

El manejo y la retención de salidas provenientes de aplicaciones de TI siguen procedimientos definidos y tienen en cuenta los requerimientos de privacidad y de seguridad.

AC13 Distribución de salidas

Los procedimientos para la distribución de las salidas de TI se definen, se comunican y se les da seguimiento.

AC14 Cuadre y conciliación de salidas

Las salidas cuadran rutinariamente con los totales de control relevantes. Las pistas de auditoría facilitan el rastreo del procesamiento de las transacciones y la conciliación de datos alterados.

AC15 Revisión de salidas y manejo de errores

Los procedimientos garantizan que tanto el proveedor como los usuarios relevantes revisan la precisión de los reportes de salida. También existen procedimientos para la identificación y el manejo de errores contenidos en las salidas.

AC16 Provisión de seguridad para reportes de salida

Existen procedimientos para garantizar que se mantiene la seguridad de los reportes de salida, tanto para aquellos que esperan ser distribuidos como para aquellos que ya están entregados a los usuarios.

Controles de límites

AC17 Autenticidad e integridad

Se verifica de forma apropiada la autenticidad e integridad de la información generada fuera de la organización, ya sea que haya sido recibida por teléfono, por correo de voz, como documento en papel, fax o correo electrónico, antes de que se tomen medidas potencialmente críticas.

AC18 Protección de información sensitiva durante su transmisión y transporte

Se proporciona una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión y el transporte.

Generadores de mediciones

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar la empresa. La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora. Para decidir cuál es el nivel correcto, la gerencia debe preguntarse a sí misma: ¿Qué tan lejos debemos ir, y está justificado el costo por el beneficio? COBIT atiende estos temas por medio de:

- Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad.
- Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para

medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard).

- Metas de actividades para facilitar el desempeño efectivo de los procesos.

MODELOS DE MADUREZ

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que se considere qué tan bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del costo beneficio y éstas preguntas relacionadas:

- ¿Qué están haciendo nuestra competencia en la industria, y cómo estamos posicionados en relación a ellos?
- ¿Cuáles son las mejores prácticas aceptables en la industria, y cómo estamos posicionados con respecto a estas prácticas?
- Con base en estas comparaciones, ¿se puede decir que estamos haciendo lo suficiente?
- ¿Cómo identificamos lo que se requiere hacer para alcanzar un nivel adecuado de administración y control sobre nuestros procesos de TI?

Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación por benchmarking y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el propietario del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control. Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa
2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

El modelado de la madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí

misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control. Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Si se usan los procesos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la administración podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentarán como un medio para dar soporte al caso de negocio para planes futuros, se requiere contar con un método gráfico de presentación **(figura 12).**

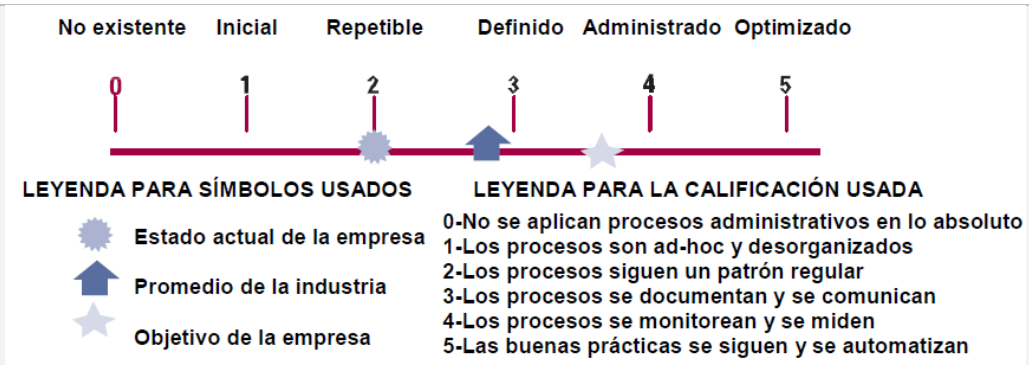


Figura 12: *Representación gráfica de los modelos de madurez*

Se ha definido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición creciente a partir de 0, no existente, hasta 5, optimizado. El desarrollo se basó en las descripciones del modelo de madurez genérico descritas en la **figura 13**.
COBIT es un marco de referencia desarrollado para la administración de procesos de TI con un fuerte enfoque en el control. Estas escalas deben ser prácticas en su aplicación y razonablemente fáciles de entender. El tema de procesos de TI es esencialmente complejo y subjetivo, por lo tanto, es más fácil abordarlo por medio de evaluaciones fáciles que aumenten la conciencia, que logren un consenso amplio y que motiven la mejora. Estas evaluaciones se pueden realizar ya sea contra las descripciones del modelo de madurez como un todo o con mayor rigor, en cada una de las afirmaciones individuales de las descripciones. De cualquier manera, se requiere experiencia en el proceso de la empresa que se está revisando.

0 No existente. Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1 Inicial. Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2 Repetible. Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3 Definido. Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4 Administrado. Es posible monitorear y medir el cumplimiento de los procedimientos y

tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5 Optimizado. Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.
Figura 13. Modelo genérico de Madurez

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada. Sin embargo, la capacidad administrativa de un proceso no es lo mismo que el desempeño.

La capacidad requerida, como se determina en el negocio y en las metas de TI, puede no requerir aplicarse al mismo nivel en todo el ambiente de TI, es decir, de forma inconsistente o solo a un número limitado de sistemas o unidades. La medición del desempeño, como se cubre en los próximos párrafos, es esencial para determinar cuál es el desempeño real de la empresa en sus procesos de TI.

Aunque una capacidad aplicada de forma apropiada reduce los riesgos, una empresa debe analizar los controles necesarios para asegurar que el riesgo sea mitigado y que se obtenga el valor de acuerdo al apetito de riesgo y a los objetivos del negocio. Estos controles son dirigidos por los objetivos de control de COBIT.

Cobit muestra un modelo de madurez para el control interno que ilustra la madurez de una empresa con respecto al establecimiento y desempeño del control interno. Con frecuencia, este análisis se inicia como respuesta a impulsores externos, aunque idealmente debería ser institucionalizado como se documenta en los procesos de COBIT PO6 *Comunicar los objetivos y el rumbo de la dirección* y ME2 Monitore*ar y evaluar el control interno.* La

capacidad, el desempeño y el control son dimensiones de la madurez de un proceso como se ilustra en la **figura 14**.

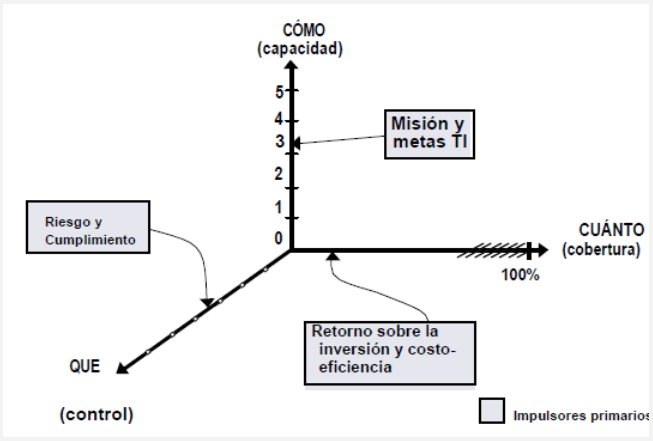


Figura 14: *Las tres dimensiones de la madurez*

El modelo de madurez es una forma de medir qué tan bien están desarrollados los procesos administrativos, esto es, qué tan capaces son en realidad. Qué tan bien desarrollados o capaces deberían ser, principalmente dependen de las metas de TI y en las necesidades del negocio subyacentes a la cuales sirven de base. Cuánta de esa capacidad es realmente utilizada actualmente para retornar la inversión deseada en una empresa. Por ejemplo, habrá procesos y sistemas críticos que requieren de una mayor administración de la seguridad que otros que son menos críticos. Por otro lado, el grado y sofisticación de los controles que se requiere aplicar en un proceso están más definidos por el apetito de riesgo de una empresa y por los requerimientos aplicables. Las escalas del modelo de madurez ayudarán a los profesionales a explicarle a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran. El nivel de madurez correcto estará influenciado por los objetivos de negocio de una empresa, por el ambiente operativo y por las prácticas de la industria. Específicamente, el nivel de madurez en la administración se basará en la dependencia que tenga la empresa en la TI, en su sofisticación tecnológica y, lo más importante, en el valor de su información. Un punto de

referencia estratégico para una empresa que ayuda a mejorar la administración y el control de los procesos de TI se puede encontrar observando los estándares internacionales y las mejores prácticas. Las prácticas emergentes de hoy en día se pueden convertir en el nivel esperado de desempeño del mañana y por lo tanto son útiles para planear dónde desea estar la empresa en un lapso de tiempo. Los modelos de madurez se desarrollan empezando con el modelo genérico cualitativo (consulte la **figura 13**) al cual se añaden, en forma creciente, algunos principios contenidos en los siguientes atributos, a través de niveles:

- Conciencia y comunicación
- Políticas, estándares y procedimientos
- Herramientas y automatización
- Habilidades y experiencia
- Responsabilidad y rendición de cuentas
- Establecimiento y medición de metas

La tabla de atributos de madurez que se muestra en la **figura 15** lista las características de cómo se administran los procesos de TI y describe cómo evolucionan desde un proceso no existente hasta uno optimizado. Estos atributos se pueden usar para una evaluación más integral, para un análisis de brechas y para la planeación de mejoras. En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI, estos son:

- Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez
- Una escala donde la diferencia se puede medir de forma sencilla
- Una escala que se presta a sí misma para una comparación práctica
- La base para establecer el estado actual y el estado deseado
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado
- Tomado en conjunto, una vista de cómo se administra la TI en la empresa

Los modelos de madurez COBIT se enfocan en la capacidad, y no necesariamente en el desempeño. No son un número al cual hay que llegar, ni están diseñados para ser una base

formal de certificación con niveles discretos que formen umbrales difíciles de atravesar. Sin embargo, se diseñaron para ser aplicables siempre, con niveles que brindan una descripción que una empresa pueda reconocer como la mejor para sus procesos. El nivel correcto está determinado por el tipo de empresa, por su medio ambiente y por la estrategia.

El desempeño, o la manera en que la capacidad se usa y se implanta, es una decisión de rentabilidad. Por ejemplo, un alto nivel de administración de la seguridad quizá se tenga que enfocar sólo en los sistemas empresariales más críticos. Para finalizar, mientras los niveles de madurez más altos aumentan el control del proceso, la empresa aún necesita analizar, con base en los impulsadores de riesgo y de valor, cuáles mecanismos de control debe aplicar. Las metas genéricas de negocio y de TI, como se definen en este marco de trabajo, ayudarán a realizar este análisis.

Los objetivos de control de COBIT guían los mecanismos de control y éstos se enfocan en qué se hace en el proceso; los modelos de madurez se enfocan principalmente en qué tan bien se administra un proceso. El apéndice III brinda un modelo de madurez genérico que muestra el estatus del ambiente de control interno y el establecimiento de controles en una empresa. Un ambiente de control implantado de forma adecuada, se logra cuando se han conseguido los tres aspectos de madurez (capacidad, desempeño y control). El incremento en la madurez reduce el riesgo y mejora la eficiencia, generando menos errores, más procesos predecibles y un uso rentable de los recursos.

Conciencia y comunicación	Políticas, estándares y procedimientos	Herramientas y automatización	Habilidades y experiencia	Responsabilidad y rendición de cuentas	Establecimiento y medición de metas
1 Surge el reconocimiento de la necesidad del proceso Existe comunicación esporádica de los problemas.	Existen enfoques *ad hoc* hacia los procesos y las prácticas Los procesos y las prácticas no están definidos	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio No existe un enfoque planeado para el uso de herramientas	No están definidas las habilidades requeridas para el proceso No existe un plan de entrenamiento y no hay entrenamiento formal	No existe definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva.	Las metas no están claras y no existen las mediciones.
2 Existe conciencia de la necesidad de actuar La gerencia comunica los problemas generales	Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual Algunos aspectos de los procesos son repetibles debido a la experiencia individual, y puede existir alguna documentación y entendimiento informal de las políticas y procedimientos	Existen enfoques comunes para el uso de herramientas pero se basan en soluciones desarrolladas por individuos clave. Pueden haberse adquirido herramientas de proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse.	Se identifican los requerimientos mínimos de habilidades para áreas críticas Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha.	Un individuo asume su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confusión acerca de la responsabilidad cuando ocurren problemas y una cultura de culpas tiende a existir.	Existen algunas metas; se establecen algunas mediciones financieras pero solo las conoce la alta dirección. Hay monitoreo inconsistente en áreas aisladas.
3 Existe el entendimiento de la necesidad de actuar La gerencia es más formal y estructurada en su comunicación	Surge el uso de buenas prácticas Los procesos, políticas y procedimientos están definidos y documentados para todas las actividades clave	Existe un plan para el uso y estandarización de las herramientas para automatizar el proceso Se usan herramientas por su propósito básico, pero pueden no estar de acuerdo al plan acordado, y pueden no estar integradas entre sí	Se definen y documentan los requerimientos y habilidades para todas las áreas. Existe un plan de entrenamiento formal pero todavía se basa en iniciativas individuales	La responsabilidad y la rendición de cuentas sobre los procesos están definidas y se han identificado a los propietarios de los procesos de negocio. Es poco probable que el propietario del proceso tenga la autoridad plena para ejercer las responsabilidades.	Se establecen algunas mediciones y metas de efectividad, pero no se comunican, y existe una relación clara con las metas del negocio. Surgen los procesos de medición pero no se aplican de modo consistente. Se adoptan ideas de un balanced scorecard de TI así como la aplicación intuitiva ocasional de análisis de causas raíz.
4 Hay entendimiento de los requerimientos completos Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación	El proceso es sólido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado las políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento de procesos y procedimientos.	Se implantan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles críticos	Los requerimientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación Se aplican técnicas maduras de entrenamiento de acuerdo al plan y se fomenta la compartición del conocimiento. Todos los expertos internos están involucrados y se evalúa la efectividad del plan de entrenamiento.	Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al propietario del proceso descargar sus responsabilidades. Existe una cultura de recompensas que activa la acción positiva.	La eficiencia y la efectividad se miden y comunican y están ligadas a las metas del negocio y al plan estratégico de TI. Se implementa el balanced scorecard de TI en algunas áreas, con excepciones conocidas por la gerencia y se está estandarizando el análisis de causas raíz. Surge la mejora continua.
5 Existe un entendimiento avanzado y a futuro de los requerimientos Existe una comunicación proactiva de los problemas, basada en las tendencias, se aplican técnicas maduras de comunicación y se usan herramientas integradas de comunicación	Se aplican las mejores prácticas y estándares externos La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Los procesos, las políticas y los procedimientos están estandarizados e integrados para permitir una administración y mejoras integrales	Se usan juegos de herramientas estandarizados a lo largo de la empresa. Las herramientas están completamente integradas con otras herramientas relacionadas para permitir un soporte integral de los procesos. Se usan las herramientas para dar soporte a la mejora del proceso y detectar de forma automática las excepciones de control	La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizacionales claramente definidas. El entrenamiento y la educación dan soporte a las mejores prácticas externas y al uso de conceptos y técnicas de vanguardia. La compartición del conocimiento es parte de la cultura empresarial y se implementan sistemas basados en conocimiento. Se usan a expertos externos y a líderes de la industria como guía.	Los propietarios de procesos tienen la facultad de tomar decisiones y medidas. La aceptación de la responsabilidad ha descendido en cascada a través de la organización de forma consistente.	Existe un sistema de medición de desempeño integrado que liga al desempeño de TI con las metas del negocio por la aplicación global del balanced scorecard de TI. La dirección nota las excepciones de forma global y consistente y el análisis de causas raíz se aplica. La mejora continua es una forma de vida.

Figura 15. Tabla Atributos de Madurez

MEDICIÓN DEL DESEMPEÑO

Las métricas y las metas se definen en COBIT a tres niveles:

- Las metas y métricas de TI que definen lo que el negocio espera de TI (lo que el negocio usaría para medir a TI)
- Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI (cómo sería medido el propietario del proceso de TI)
- Métricas de desempeño de los procesos (miden qué tan bien se desempeña el proceso para indicar si es probable alcanzar las metas)

COBIT utiliza dos tipos de métrica: indicadores de metas e indicadores de desempeño. Los indicadores de metas de bajo nivel se convierten en indicadores de desempeño para los niveles altos. Los indicadores clave de metas (KGI) definen mediciones para informar a la gerencia—después del hecho—si un proceso TI alcanzó sus requerimientos de negocio, y se expresan por lo general en términos de criterios de información:

- Disponibilidad de información necesaria para dar soporte a las necesidades del negocio • Ausencia de riesgos de integridad y de confidencialidad
- Rentabilidad de procesos y operaciones
- Confirmación de confiabilidad, efectividad y cumplimiento

Los indicadores clave de desempeño (KPI) definen mediciones que determinan qué tan bien se está desempeñando el proceso de TI para alcanzar la meta. Son los indicadores principales que indican si será factible lograr una meta o no, y son buenos indicadores de las capacidades, prácticas y habilidades. Miden las metas de las actividades, las cuales son las acciones que el propietario del proceso debe seguir para lograr un efectivo desempeño del proceso. Las métricas efectivas deben tener las siguientes características:

- Una alta proporción entendimiento-esfuerzo (esto es, el entendimiento del desempeño y del logro de las metas en contraste con el esfuerzo de lograrlos)
- Deben ser comparables internamente (esto es, un porcentaje en contraste con una base o números en el tiempo)
- Deben ser comparables externamente sin tomar en cuenta el tamaño de la empresa o la industria

- Es mejor tener pocas métricas (quizá una sola muy buena que pueda ser influenciada por distintos medios) que una lista más larga de menor calidad
- Debe ser fácil de medir y no se debe confundir con las metas

La **figura 16** ilustra la relación entre los procesos, TI y las metas del negocio, y entre las diferentes métricas, con ejemplo tomados de DS5 *Garantizar la seguridad de los sistemas*.

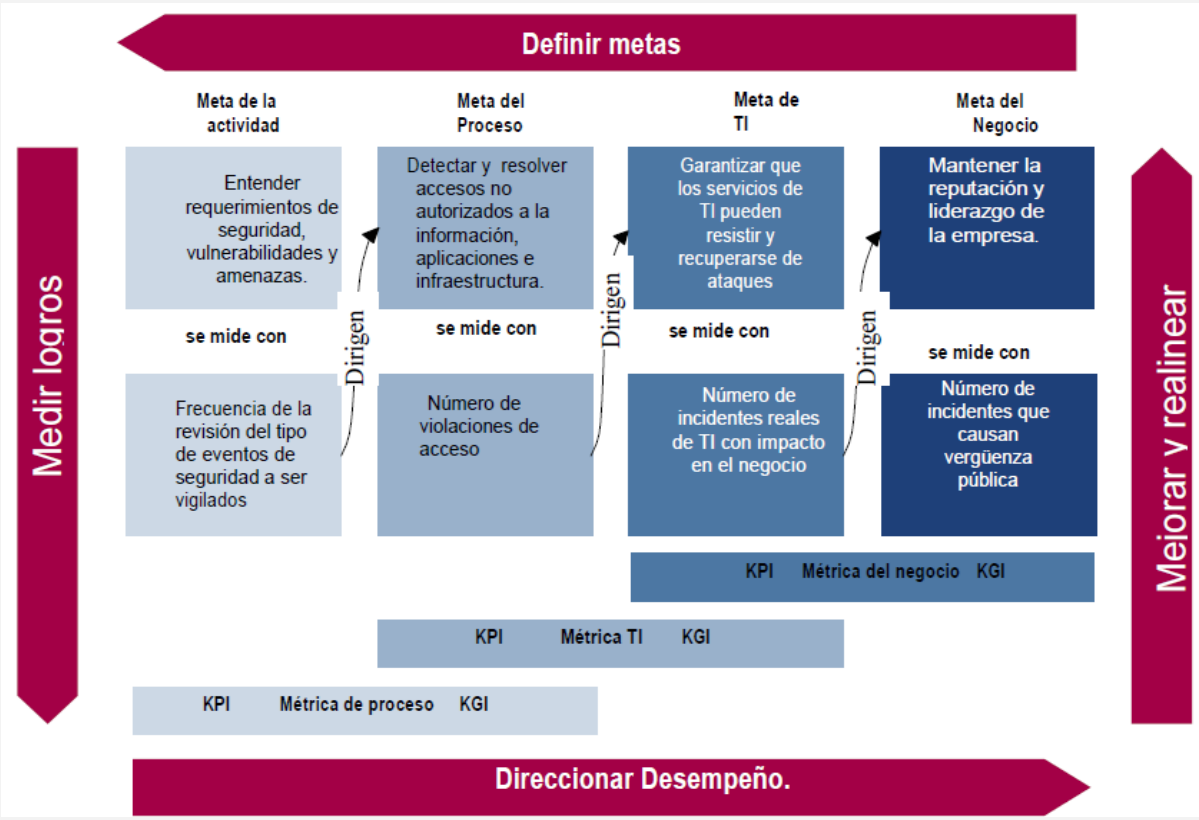


Figura 16: *Relación entre proceso, metas y métrica (DS5)*

Las metas se definen de arriba hacia abajo con base en las metas de negocio que determinarán el número de metas que soportará TI, las metas de TI decidirán las diferentes necesidades de las metas de proceso, y cada meta de proceso establecerá las metas de las actividades. El logro de metas se mide con las métricas de resultado (llamadas indicadores clave de metas, o KGIs) y dirigen las metas de más alto nivel. Por ejemplo, la métrica que midió el logro de la meta de la actividad es un motivador de desempeño (llamado indicador

clave de desempeño, o KPI) para la meta del proceso. Las métricas permiten a la gerencia corregir el desempeño y realinearse con las metas.

EL MODELO DEL MARCO DE TRABAJO COBIT

El marco de trabajo COBIT, por lo tanto, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicio de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las métricas KGI y KPI de COBIT, como se ilustra en la **figura 17.**

Figura 14. Administración, Control, Alimentación y Monitoreo COBIT

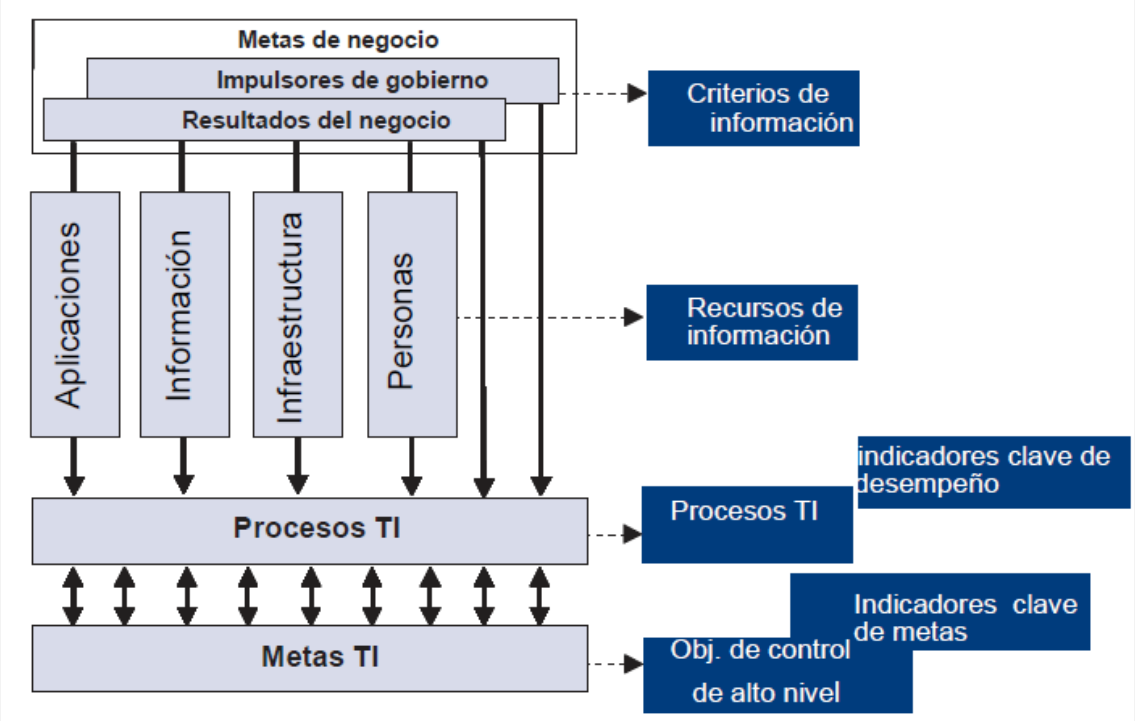


Figura 17: *Administración, Control, Alimentación y Monitoreo COBIT*

Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT **(figura 18)**

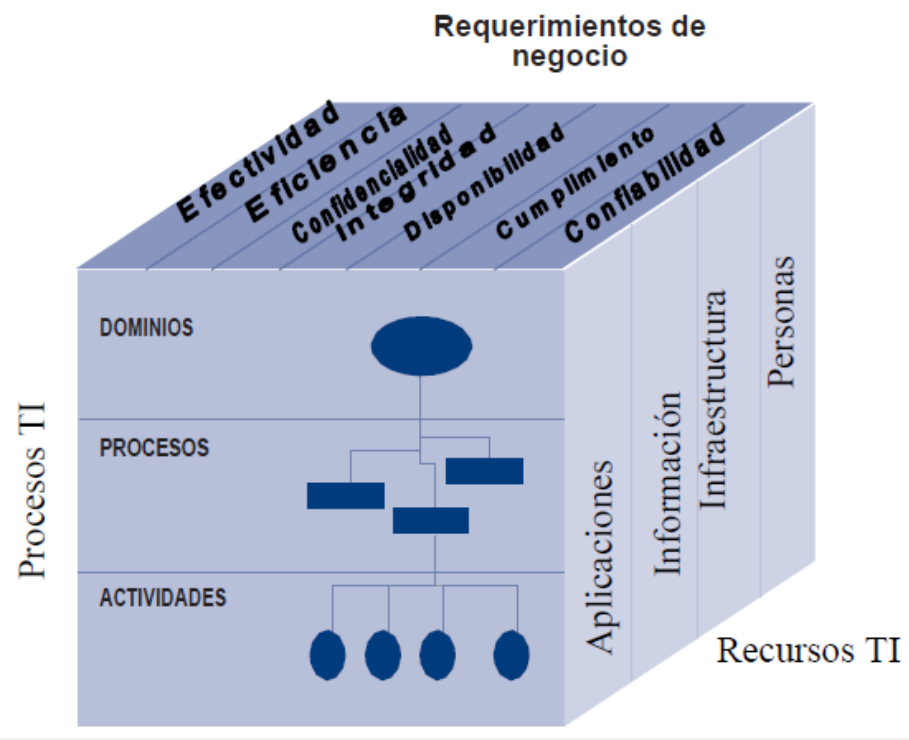


Figura 18: *El cubo COBIT*

En detalle, el marco de trabajo general COBIT se muestra gráficamente en la **figura 19,** con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

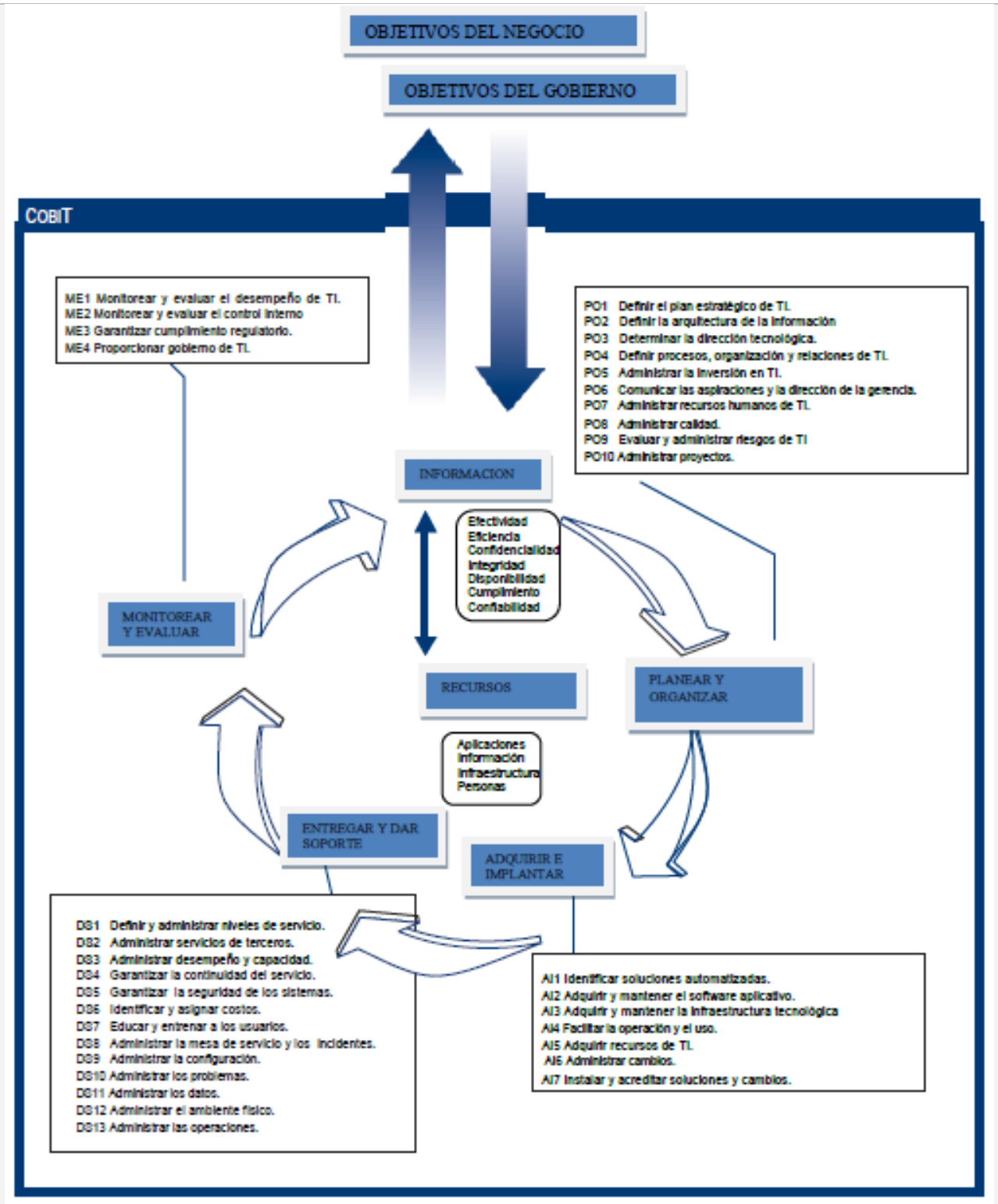


Figura 19: *Marco de trabajo general de COBIT*

3.1.2 ITIL

Historia

Desarrollada a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL) se ha convertido en el estándar mundial de de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, la estructura base ha demostrado ser útil para las organizaciones en todos los sectores a través de su adopción por innumerables compañías como base para consulta, educación y soporte de herramientas de software. Hoy, ITIL es conocido y utilizado mundialmente. Pertenece a la OGC, pero es de libre utilización [10].

Las siglas de ITIL significan (Information Technology Infrastructure Library) o Librería de Infraestructura de Tecnologías de Información.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

El objetivo de usar ITIL en Managed Services

ITIL como metodología propone el establecimiento de estándares que nos ayuden en el control, operación y administración de los recursos (ya sean propios o de los clientes). Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua.

10ITIL

http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

Otra de las cosas que propone es que para cada actividad que se realice se debe de hacer la documentación pertinente, ya que ésta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda la gente esté al tanto de los cambios y no se tome a nadie por sorpresa.

Concepto de soluciones para ITIL desde el punto de vista de negocio

Según este diagrama vemos como aparentemente tenemos segmentos del negocio aislados, pero en realidad todos tienen algo que ver para la obtención de las soluciones. Por ejemplo la prestación de servicios muchas veces no sería posible sin la gestión de infraestructura, asimismo las perspectivas del negocio no se darían sin la prestación de servicio y los servicios no serian posibles sin un soporte al servicio. Y el punto de interacción que se da entre estos segmentos del negocio es la búsqueda de soluciones, donde lo que se busca es que las perspectivas del negocio estén soportadas en base a la prestación de servicios; la prestación de servicios requiere que se le de un soporte al servicio para que esté siempre disponible, la disponibilidad la podemos lograr mediante una gestión de la infraestructura y en lugar de tener al centro las soluciones vamos a tener a los clientes satisfechos.

Figura 20: *Soluciones para ITIL*

Forma de uso de ITIL en Managed Services

ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de cinco procesos:

- Manejo de Incidentes
- Manejo de problemas
- Manejo de configuraciones
- Manejo de cambios y
- Manejo de entregas
- Proceso de manejo de incidentes

Su objetivo primordial es reestablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, esto se hace con la finalidad de que se minimicen los efectos de la operación. Se dice que el proveedor se debe de encargar de que el cliente no debe percibir todas aquellas pequeñas o grandes fallas que llegue a presentar el sistema. A este concepto se le llama disponibilidad (que el usuario pueda tener acceso al servicio y que nunca se vea interrumpido).

Para este proceso se tiene un diagrama que en cada una de sus fases maneja cuatro pasos básicos que son: propiedad, monitoreo, manejo de secuencias y comunicación.

En el proceso de manejo de incidentes vemos que se da como primera etapa la **detección del incidente** (es cuando el sistema presenta alguna anomalía o falla, y que esto se puede traducir en un error en el sistema o que el usuario no puede hacer algo y recurre a pedir ayuda); ya que lo tenemos identificado se hace una **clasificación del incidente** (vemos si el error que se presenta es conocido o si nunca se ha presentado) y de la mano va el soporte inicial (es el punto en el que el cliente llega a la mesa de servicio a solicitar ayuda, porque no sabe o no puede hacer algo); en caso de que el incidente sea conocido se hace el **procedimiento de solicitud de servicio** (se ejecutan los pasos a seguir según el manual de procedimientos para poder llegar a la solución de una forma viable y eficiente); una vez que ya que se la dio una solución al incidente por medio del manual de procedimientos se recurre a la documentación y contabilización del incidente, para ver qué tanta incidencia tiene este caso; finalmente se hace una evaluación para ver si efectivamente se **resolvió el incidente** de forma satisfactoria y en supuesto de ser afirmativa se **cierra el incidente** y el

otro supuesto seria que de la solución que se planteo no es lo suficientemente eficiente o acertada para que resuelva el problema y se recurre a hacer una investigación y un diagnostico de la situación para ver cómo es que se puede atacar el problema de frente y resolverlo; una vez que se tiene todo un contexto analizado se recurre a la ejecución de la propuesta de solución del incidente y se hace un estudio para ver si el incidente es recuperable o si es caso perdido (la mayoría de los casos son recuperables, peo cuando el nivel de daño es muy fuerte, se da el caso de que se dé por perdido); y finamente se cierra el incidente y esta solución se documenta en una base de datos a la que se le llama base del conocimiento o Knowledge Data Base (aquí vienen documentadas todas las soluciones, y se establecen los pasos a seguir para que se hagan de forma eficiente) para que al momento de volverse a presentar el incidente ya va a estar documentado y esto hace que sea mas fácil, rápida y eficiente su resolución.

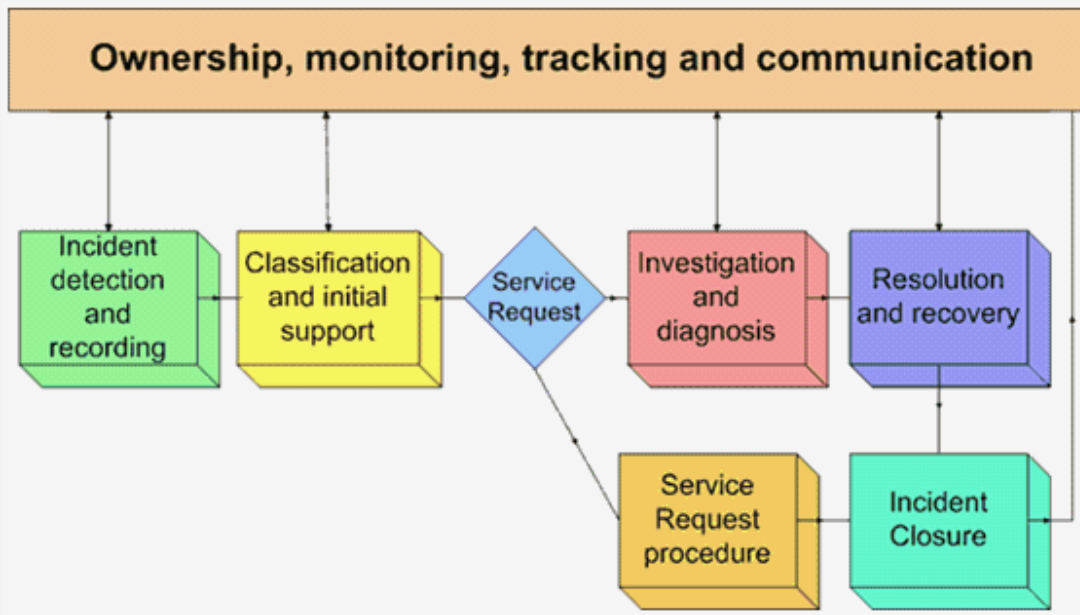


Figura 21: *Procesos ITIL*

Proceso de manejo de problemas

El Objetivo de este proceso es prevenir y reducir al máximo los incidentes, y esto nos lleva a una reducción en el nivel de incidencia. Por otro lado nos ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.

En este proceso lo que se busca es que se pueda tener pleno control del problema, esto se logra dándole un seguimiento y un monitoreo al problema.

El diagrama de este proceso es muy particular, ya que se maneja en dos fases: la primera está relacionada con lo que es el control del problema y la segunda es con el control del error.

En lo que respecta a la ***Fase De Control Del Problema***: primero se tiene que identificar el problema en base a alguna sintomatología; ya que tenemos este antecedente, pasamos a la clasificación de los problemas (en este proceso al igual que en el proceso de manejo de incidentes tenemos que ver si es un problema conocido), en caso de ser conocido, se recurre al procedimiento de solicitud de servicio, donde se van a aplicar las soluciones de acuerdo a como están en el manual de procedimientos; y en caso de no ser conocido se tendría que hacer una fase de investigación para ver que es lo que genera el problema y mas tarde hacer un diagnostico; ya que tenemos un diagnóstico tenemos que hacer un RFC (Request For Change o Solicitud de Cambio),

Esta solicitud de cambio implica que se va a tener que implementar la solución y finalmente se va a hacer una evaluación para ver si se resolvió el problema de raíz. En caso de que si se funcione esta solución se pasa a la documentación.

Con lo que respecta a la ***Segunda Fase Del Modelo***, el control del error se hace por medio de una identificación del error en general, posteriormente se hace una especie de registro, y este va a servir para clasificar el error; ya que se tiene una clasificación y se recurre a una evaluación de que tanto daño genero o puede llegar a generar el error, esto con la finalidad de cuantificar los desperfectos que podría llegar a causar en caso de que el error prevalezca y no se solucione; posteriormente se hace la resolución o corrección del error (este puede deberse a varios aspectos: configuraciones, falta de seguridad, inconsistencia de datos, etc.); y este modelo tiene una fase muy difícil, que es determinar que problemas están asociados o como es que al momento de cambiar algo el sistema, se va a cambiar de forma

uniforme y no se va a alterar, y que presente inconsistencias. Por ejemplo que es lo que pasaría si cambio algunos de los datos en la configuración del sistema, se tendría que afectar el sistema de manera uniforme para que siga en equilibrio y no esté cambiado en algunas partes y en otras que se quede como estaba antes.

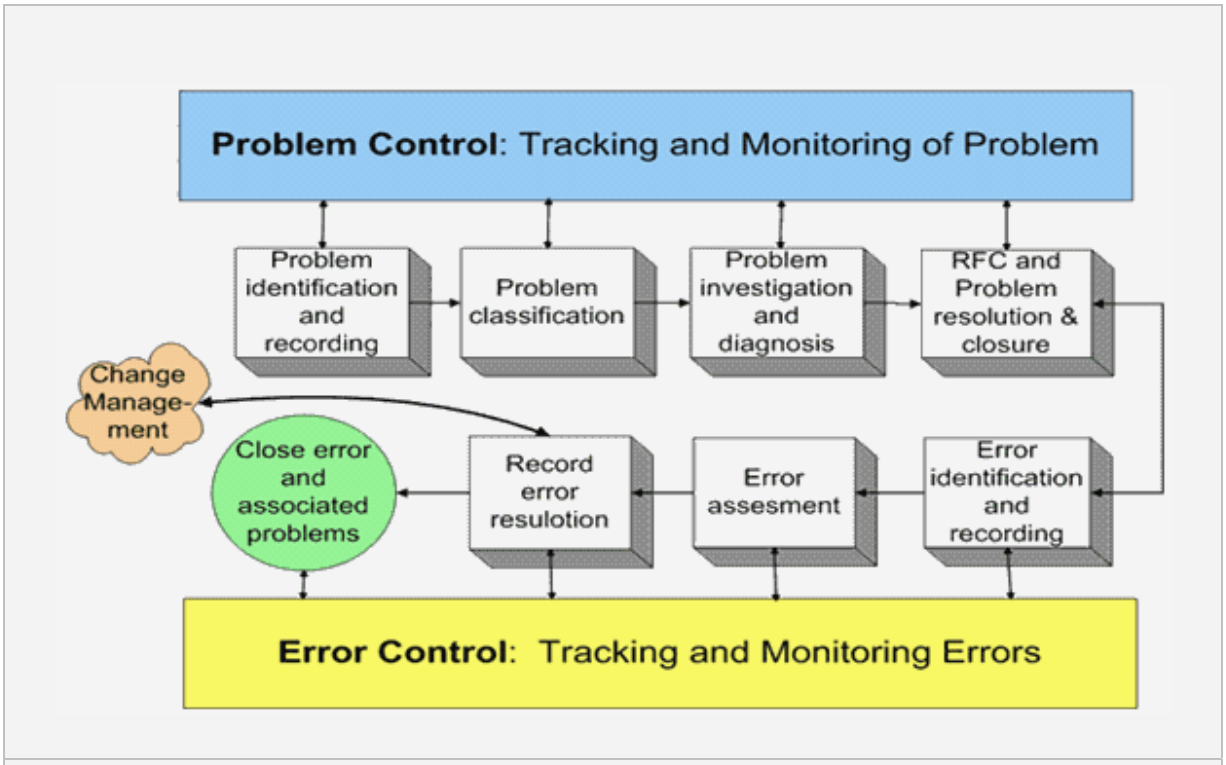


Figura 22: *Proceso de manejo de problemas*

Proceso de manejo de configuraciones

Su objetivo es proveer con información real y actualizada de lo que se tiene configurado e instalado en cada sistema del cliente.

Este proceso es de los más complejos, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.

El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y muchas de ellas son dinámicas, entonces al cambiar una o varias de ellas se afecta el sistema en

general, lo que hace que sea muy difícil de manipular. Aunque es lo más parecido a la realidad, porque nuestro entorno es dinámico y las decisiones de unos afectan a otros.

Por ejemplo en lo que respecta a la administración de cambios vemos que se relaciona directamente con la administración de incidentes y de problemas, lo que conlleva una planeación, identificación, control, seguimiento del status, verificación y auditoria de configuraciones, lo que hace que haya muchas variables.

En otro ejemplo la implementación de cambios implica que se tiene que hacer la liberación y distribución de nuevas versiones, esto se da por una fase de planeación, identificación, control, revisión del status, verificación y auditoria, y puede depender de la administración de las capacidades, ya que si no se cuenta con el software o con el hardware esta fase no se podría llevar a cabo; y así se haría con todos los niveles hasta llegar al cierre del control de cambios.

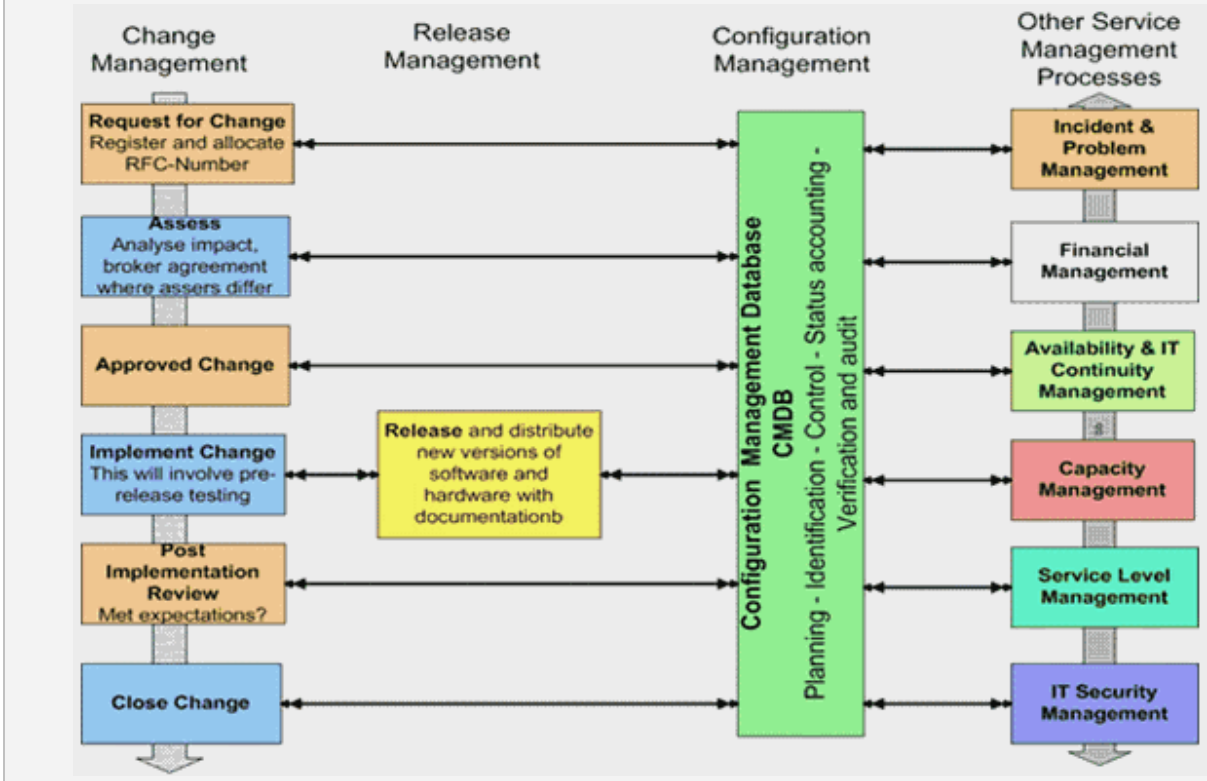


Figura 23: *Proceso de manejo de configuraciones*

Proceso de control de cambios

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de los cambios. Este diagrama al parecer es muy fácil de seguir, pero en realidad no lo es, ya que entre etapa y etapa se da una fase de monitoreo para ver que no se han sufrido desviaciones de los objetivos.

Primero vemos que tenemos un registro y clasificación del cambio que se tiene que hacer, se pasa a la **fase de monitoreo y planeación**, si el rendimiento es satisfactorio se da la aprobación del cambio, y en caso de que el rendimiento sea malo se pasa a la **fase de reingeniería** hasta que el proceso funcione adecuadamente, ya que se aprueban los cambio, se construyen prototipos o modelos en los que se van a hacer las pruebas, se hacen las pruebas pertinentes para ver las capacidades del sistema, ya que el proceso está probado se da la autorización e implementación; ya implementado se ve que no se hayan tenido desviaciones y se ajusta a las necesidades actuales que también se le considera como revisión post-implementación.

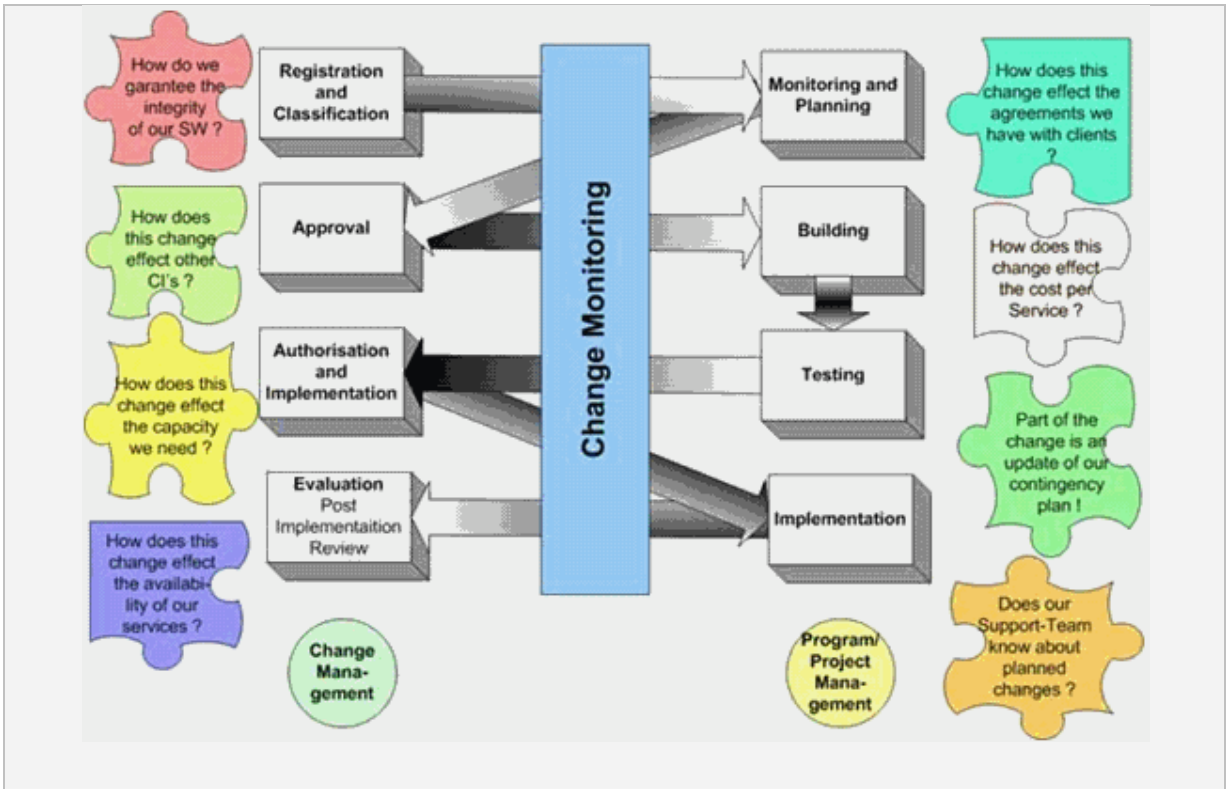


Figura 24: *Proceso de control de cambios*

Proceso de manejo de entregas

Su objetivo es planear y controlar exitosamente la instalación de Software y Hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real.

Este proceso tiene un diagrama que marca la transición que se da de acuerdo a los ambientes por los que se va dando la evolución del proyecto.

En lo que respecta al ambiente de desarrollo vemos que se tiene que hacer la liberación de las políticas, la liberación de la planeación, el diseño lógico de la infraestructura que se va a implementar y la adquisición de software y hardware están entre los ambientes de desarrollo y de pruebas controladas; ya que se requiere que ambos hagan pruebas sobre ellos; en el ambiente de pruebas controladas vemos que se hace la construcción y liberación de las configuraciones (nivel lógico), se hacen las pruebas para establecer los acuerdos de aceptación; se da la aceptación total de versiones y de modelos, se arranca la planeación y finalmente las pruebas y comunicaciones; y en lo que es el ambiente real vemos que se da la distribución e instalación.

En la etapa del ambiente real es la que se ve de forma más concreta, ya que muchas veces no tenemos idea de todo lo que pasa hasta antes de la instalación.

En el proceso de entrega del servicio es el punto en el que el usuario hace uno del servicio y no sabe que detrás del servicio que está recibiendo hay un sin fin de actividades y de decisiones que se tuvieron que tomar para que llegar a este punto.

Este proceso es en el que más cuidado debemos de poner, ya que en caso de haber fallas, el primero en detectarlas o en percibirlas es el usuario, y eso nos genera que el cliente este insatisfecho o molesto. Por lo general los usuarios no saben que para que puedan hacer uso de los servicios, se paso por una fase de planeación, monitoreo, análisis y por un sin fin de pruebas, con la intención de que en caso de que algo no funcione, se de en la fase de pruebas controladas y no en la fase de pruebas en ambiente real, donde el mayor afectado es el cliente.

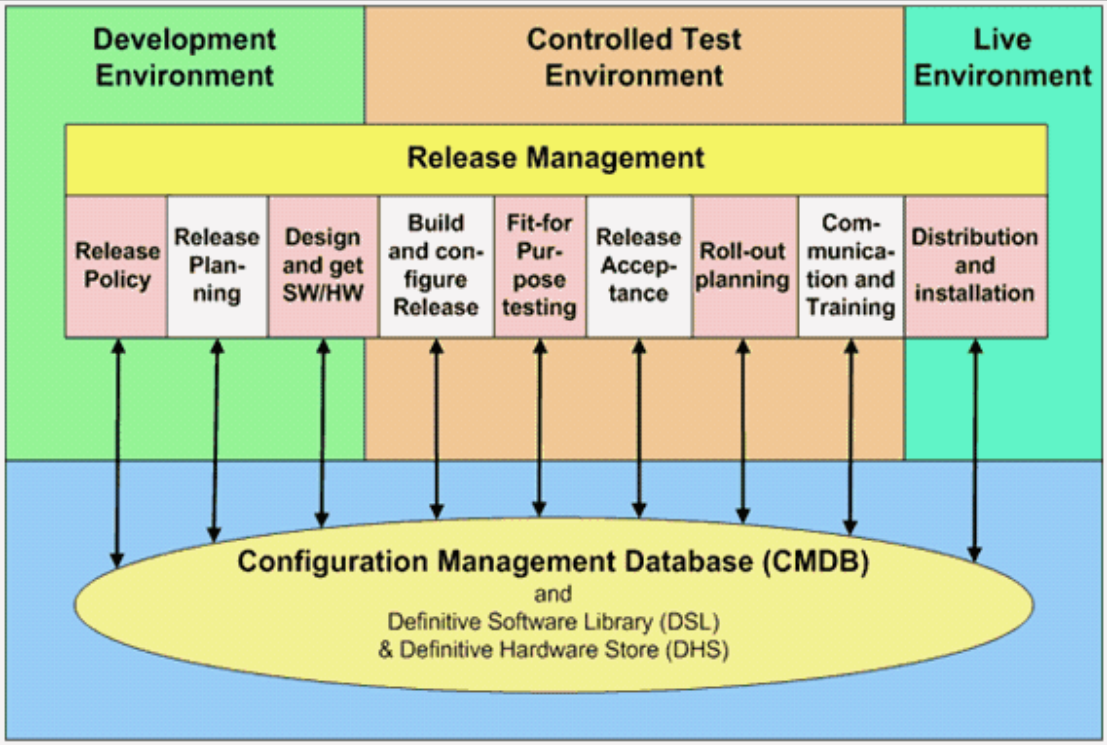


Figura 25: *Proceso de manejo de entregas*

Conclusiones:

ITIL es una metodología que nos va a ayudar a que las cosas se puedan hacer de una forma más eficiente, ya que lo que se propone es que se adopten ciertas métricas y procedimientos que otros proveedores de IT adoptaron y que gracias a ellas son catalogadas como mejores prácticas.

El hecho de adoptar mejores prácticas implica que no tengamos que descubrir el hilo negro y que si alguien sabe cómo hacer las cosas y explotar los recursos nos podemos apoyar en el para que nosotros también podamos hacerlo. E mayor objetivo es que todos lleguemos a un nivel de eficiencia que se traduzca en una buena prestación de servicios.

Ventajas de ITIL

Hay varios beneficios para el uso de la Biblioteca de Infraestructura de Tecnología de la Información para muchas de sus necesidades de negocios de TI y un beneficio principal es que a través de las directrices y las mejores prácticas que se imparten en la biblioteca, su empresa puede ahorrar una enorme cantidad de dinero una vez ejecutados.

Otra de las ventajas de ITIL es que ayudará a organizar su departamento de TI y gestión de diferentes disciplinas mediante un amplio volumen. ITIL es el líder en ÉL las directrices y las mejores prácticas de publicaciones, que ha sido probado en entornos del mundo real durante más de una década y está demostrado que funciona.

Desventajas de ITIL

Aunque por lo general las ventajas superan con creces los inconvenientes, hay un par de críticas que son de destacar en particular la idea de que la mayoría de los profesionales de TI ITIL considerar un enfoque holístico a la administración de TI. Aunque ITIL es amplia, incluso la publicación en sí no se considera un enfoque holístico a la administración de TI.

Además, también hay acusaciones por parte de algunos profesionales de TI que sólo los siguientes ITIL debido a su aceptación por muchos administradores de TI como la fuente autorizada ha llevado a muchas empresas a saltar de soluciones pragmáticas para sus necesidades empresariales específicas. Por último, otra de las críticas de ITIL es que mientras que algunos temas se tratan ampliamente y son de gran valor, otros temas pueden no recibir suficiente atención con calidad de ser desiguales en algunas publicaciones.

3.1.3 ISO 17799

Historia

La problemática de la seguridad en los sistemas de información surge del acelerado desarrollo e implantación de este tipo de tecnologías, denominadas comúnmente TICs. La rápida implantación que ha tenido Internet en nuestras vidas ha conllevado que cantidades enormes de información (en muchos casos confidencial) estén a disposición de cualquiera.

Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información

que estuviera sujeto a auditoría y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

Desde su publicación por parte de la Organización Internacional de Normas en diciembre de 2000, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

Figura 26: *ISO 17799*

Definición

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización [11].

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada.

11ISO 17799

http://www.mvausa.com/Colombia/Presentaciones/INTRODUCCION_ISO_17799.pdf

El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Integridad:** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

La adaptación española de la norma se denomina UNE 71502, que será explicada posteriormente.

La norma ISO 17799 no incluye la segunda parte de BS 7799, que se refiere a la implementación. ISO 17799 hoy en día es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector.

La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes.

ESTRUCTURA DE LA NORMA:

Dominios de control y objetivos.

La norma UNE-ISO/IEC 17799 establece diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad.

2. Aspectos organizativos para la seguridad.

3. Clasificación y control de activos.

4. Seguridad ligada al personal.

5. Seguridad física y del entorno.

6. Gestión de comunicaciones y operaciones.

7. Control de accesos.

8. Desarrollo y mantenimiento de sistemas.

9. Gestión de continuidad del negocio.

10. Conformidad con la legislación.

Figura 27: *Gestión de seguridad de la información*

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

A continuación se comentan los detalles de cada dominio de control:

1.- Política de seguridad.

Su objetivo principal es dirigir y dar soporte a la gestión de la seguridad de la información. La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.

La política se constituye en la base de todo el sistema de seguridad de la información.

La alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

2.- Aspectos organizativos para la seguridad.

Gestionan la seguridad de la información dentro de la organización. Mantienen la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros. Mantienen también la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma. Dicha estructura debe poseer un enfoque multidisciplinar: los problemas de seguridad no son exclusivamente técnicos.

3.- Clasificación y control de activos.

Mantener una protección adecuada sobre los activos de la organización. Asegurar un nivel de protección adecuado a los activos de información. Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario

actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

4.- Seguridad ligada al personal.

Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo. Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Las implicaciones del factor humano en la seguridad de la información son muy elevadas. Todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.

Debe haber diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc, y procesos de notificación de incidencias claros, ágiles y conocidos por todos.

5.- Seguridad física y del entorno.

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización. Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

Las áreas de trabajo de la organización y sus activos deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio...).

6.- Gestión de comunicaciones y operaciones.

Asegurar la operación correcta y segura de los recursos de tratamiento de información.

Minimizar el riesgo de fallos en los sistemas. Proteger la integridad del software y de la información. Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación. Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo. Evitar daños a los activos e interrupciones de actividades de la organización. Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

Se debe garantizar la seguridad de las comunicaciones y de la operación de los sistemas críticos para el negocio.

7.- Control de accesos.

Controlar los accesos a la información, evitar accesos no autorizados a los sistemas de información, evitar el acceso de usuarios no autorizados, proteger los servicios en red. Evitar accesos no autorizados a ordenadores, el acceso no autorizado a la información contenida en los sistemas. Detectar actividades no autorizadas. Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y tele-trabajo.

Se deben establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc.

8.- Desarrollo y mantenimiento de sistemas.

Asegurar que la seguridad está incluida dentro de los sistemas de información.

Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

Proteger la confidencialidad, autenticidad e integridad de la información. Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura. Mantener la seguridad del software y la información de la aplicación del sistema.

Debe contemplarse la seguridad de la información en todas las etapas del ciclo de vida del software en una organización: especificación de requisitos, desarrollo, explotación, mantenimiento.

9.- Gestión de continuidad del negocio.

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres. Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.

Los planes de contingencia deben ser probados y revisados periódicamente.

Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

10.- Conformidad con la legislación.

Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad. Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma. Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.

Se debe identificar convenientemente la legislación aplicable a los sistemas de información corporativos (en nuestro caso, LOPD, LPI, LSSI...), integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.

Se debe definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

Niveles de seguridad:

- Lógica: Confidencialidad, integridad y disponibilidad del software y datos de un SGI.
- Organizativa: Relativa a la prevención, detección y corrección de riesgos.
- Física: Protección de elementos físicos de las instalaciones: servidores, PCs…
- Legal: Cumplimiento de la legislación vigente.

En España: LOPD (Ley Orgánica de Protección de Datos).

APLICACIÓN DE LA NORMA ISO 17799.

Auditoría.

Un trabajo de auditoría ISO 17799 consiste en la valoración del nivel de adecuación, implantación y gestión de cada control de la norma en la organización. Valora la seguridad desde 4 puntos de vista:

- Seguridad lógica.
- Seguridad física.
- Seguridad organizativa.
- Seguridad legal.

Se trata de una referencia de la seguridad de la información estándar y aceptada internacionalmente. Una vez conocemos el estado actual de la seguridad de la información en la organización, podemos planificar correctamente su mejora o su mantenimiento. Una auditoría ISO 17799 proporciona información precisa acerca del nivel de cumplimiento de la norma a diferentes niveles: global, por dominios, por objetivos y por controles.

VENTAJAS

La adopción de la norma ISO 17799 proporciona diferentes ventajas a cualquier organización:

Aumento de la seguridad efectiva de los sistemas de información.

- Correcta planificación y gestión de la seguridad.
- Garantías de continuidad del negocio.
- Alianzas comerciales y e-commerce más seguras.
- Mejora contínua a través del proceso de auditoría interna.
- Incremento de los niveles de confianza de nuestros clientes y partners.
- Aumento del valor comercial y mejora de la imagen de la organización.
- Auditorías de seguridad más precisas y fiables.
- Menor Responsabilidad Civil.

CONCLUSIONES.

- ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información, adoptada en España como norma UNE-ISO/IEC 17799 (UNE 71502).
- La norma se estructura en diez dominios de control que cubren por completo todos los aspectos relativos a la seguridad de la información.
- Implantar ISO 17799 requiere de un trabajo de consultoría que adapte los requerimientos de la norma a las necesidades de cada organización concreta.
- La adopción de ISO 17799 presenta diferentes ventajas para la organización, entre ellas el primer paso, para la certificación según UNE 71502.

3.1.4 MAGERIT

Historia

MAGERIT ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática.

La generalización del uso de las tecnologías de la información y de las comunicaciones es potencialmente beneficiosa para los ciudadanos, las empresas y la propia Administración Pública, pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización.

No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a estos riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas).

Definición

La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos [12].

Objetivos de MAGERIT

- **Estudiar los riesgos** que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un ***análisis de los riesgos*** que implica la evaluación del *impacto* que una violación de la seguridad tiene en la organización; señala los *riesgos* existentes, identificando las *amenazas* que acechan al sistema de información, y determina la *vulnerabilidad* del sistema de prevención de dichas amenazas, obteniendo unos resultados.

- Los resultados del análisis de riesgos permiten a la ***gestión de riesgos*** **recomendar las medidas** apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

- Como **objetivo a más largo plazo**, MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información (ITSEC, Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información).

MAGERIT ha tenido en cuenta los estándares y métodos más avanzados y asentados en SSI.

La Aplicación de MAGERIT permite:

- *Aportar racionalidad en el conocimiento del estado de seguridad* de los Sistemas de Información y en la introducción de medidas de seguridad;
- *Ayudar a garantizar una adecuada cobertura en extensión*, de forma que no haya elementos del sistema de información que queden fuera del análisis, y *en intensidad*, de forma que se alcance la profundidad necesaria en el análisis del sistema.

12MARGERIT
http://www.coit.es/publicac/publbit/bit128/bitcd1/legisla/pg5m21.htm

La incrustación de mecanismos de seguridad en el corazón mismo de los sistemas de información:

a) Para paliar las insuficiencias de los sistemas vigentes;

b) Para asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento.

El **Análisis y Gestión de Riesgos** es el 'corazón' de toda actuación organizada en materia de seguridad y, por tanto, de la gestión global de la seguridad. Influye en las Fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento).

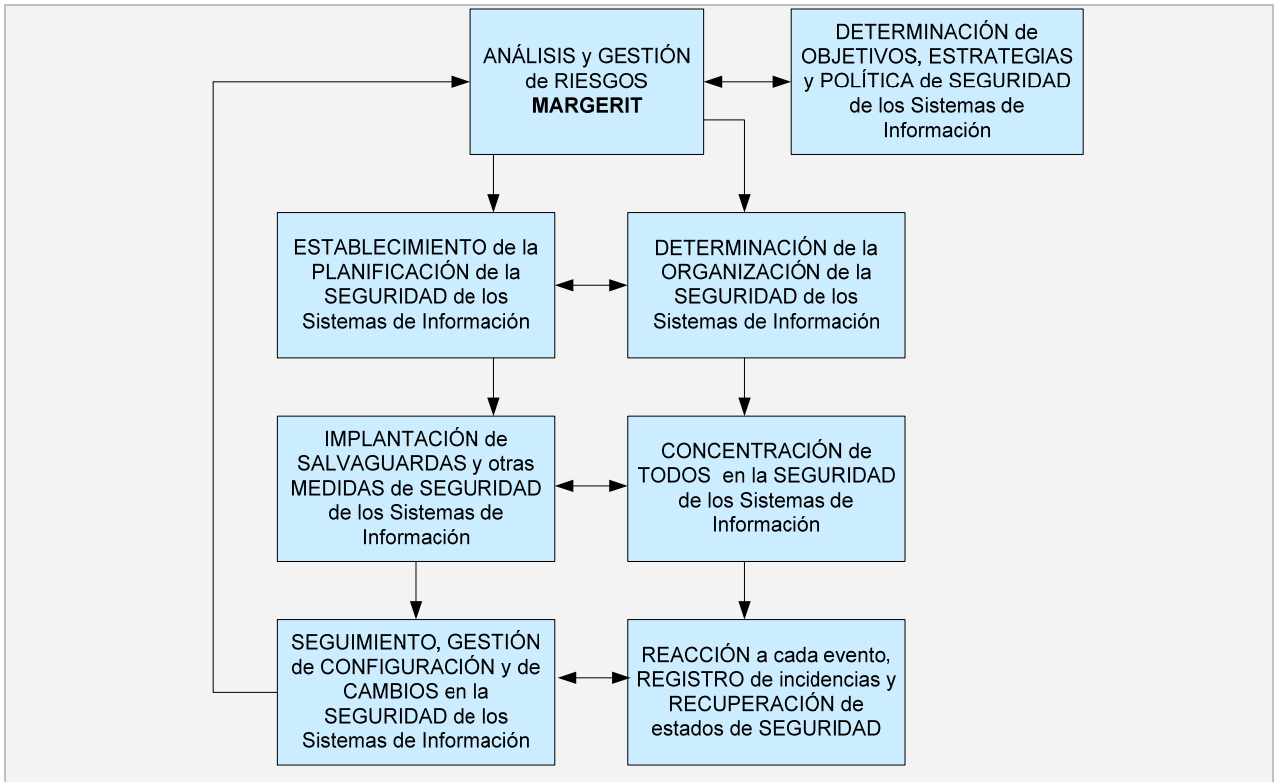


Figura 28: *Análisis y Gestión de Riesgos MAGERIT*

Tipos de proyectos

MAGERIT responde a las necesidades de un espectro amplio de intereses de usuarios con un enfoque de adaptación a cada organización y a sensibilidades diferentes en Seguridad de los Sistemas de Información. Las diferencias residen en tres cuestiones fundamentales:

- **Situación** dentro del "ciclo de estudio": marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- **Envergadura**: complejidad e incertidumbre relativas del Dominio estudiado, tipo de estudio más adecuado a la situación (corto, simplificado,...), granularidad adoptada.
- **Problemas específicos** que se desee solventar: Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para homologación de sistemas o productos, Auditorías de seguridad.

Estructura de MAGERIT

El modelo normativo de MAGERIT se apoya en tres submodelos: El *Submodelo de Elementos* proporciona los "componentes" que el *Submodelo de Eventos* va a relacionar entre sí y con el tiempo, mientras que el *Submodelo de Procesos* será la descripción funcional ("el esquema explicativo") del proyecto de seguridad a construir.

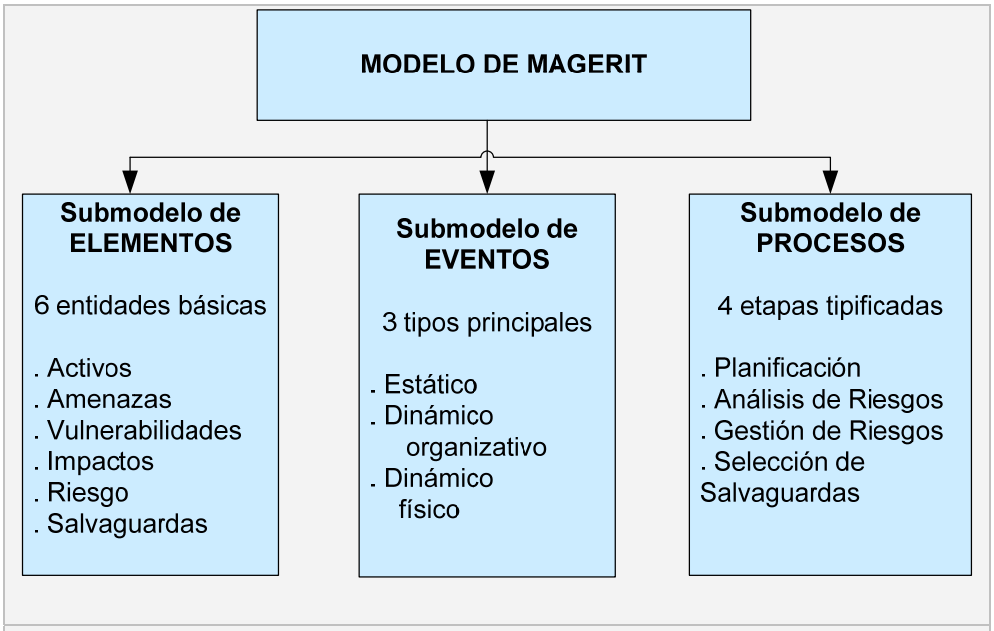


Figura 29: *Modelo de MAGERIT*

El Submodelo de Procesos de MAGERIT comprende 4 Etapas:

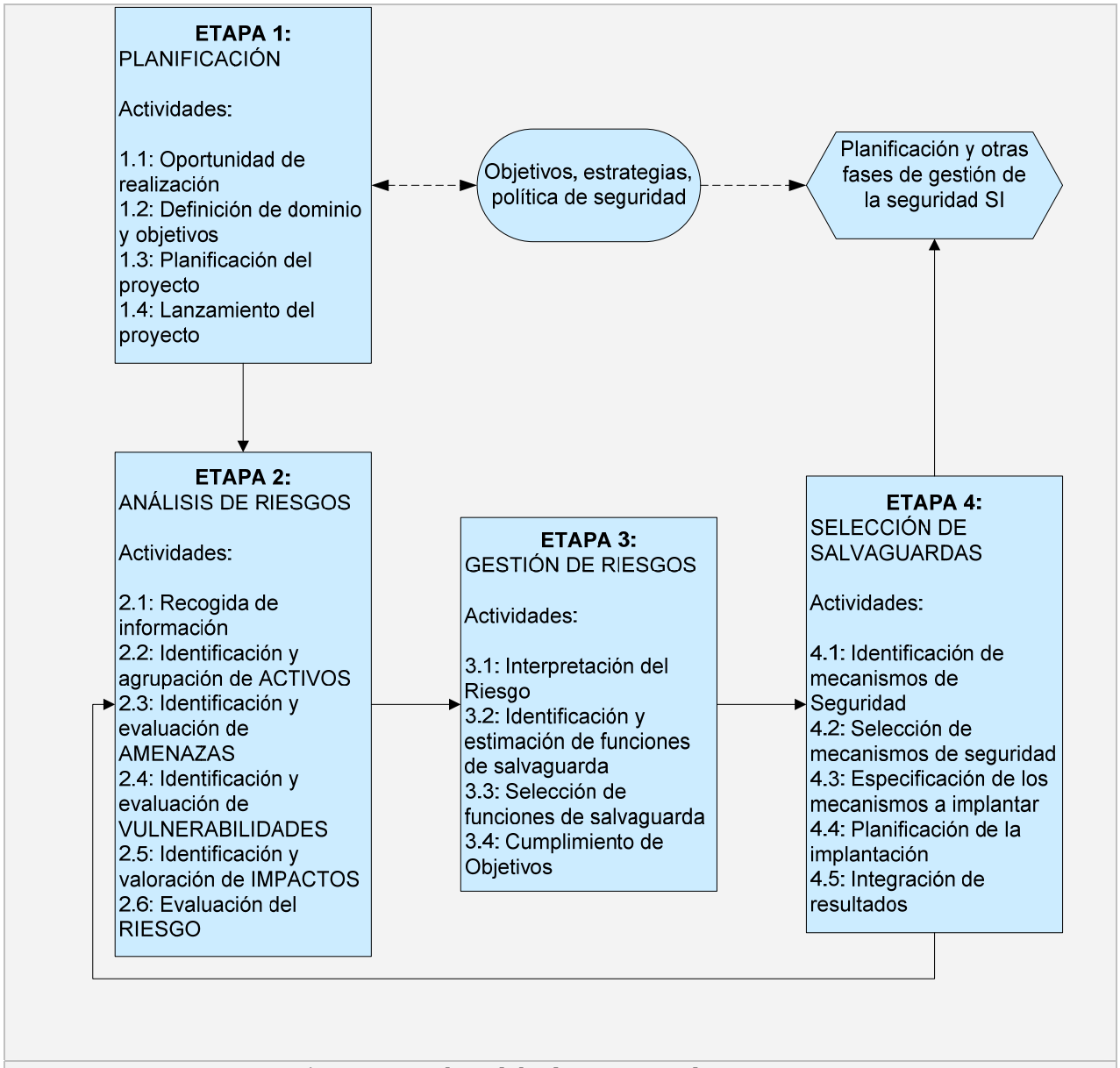


Figura 30: *Submodelo de Procesos de MAGERIT*

1. ***Planificación del Proyecto de Riesgos***. Como consideraciones iniciales para arrancar el proyecto de Análisis y Gestión de Riesgos (AGR), se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito

que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto

2. ***Análisis de riesgos***. Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.

3. ***Gestión de riesgos***. Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

4. ***Selección de salvaguardas***. Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del Análisis y Gestión de Riesgos (AGR), para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

Para poder construir proyectos específicos de seguridad, MAGERIT posee interfaces de enlace con **MÉTRICA VERSIÓN 2.1**. MAGERIT permite añadir durante el desarrollo del Sistema la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento. Estas interfaces tienen ventajas inmediatas: analizar la seguridad del Sistema antes de su desarrollo, incorporar defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema.

Tipos de Técnicas usadas en MAGERIT

Cada una de las Tareas del Submodelo de Procesos en la Guía de Procedimientos indica las técnicas empleadas para realizarla. MAGERIT tipifica las técnicas recomendadas como:

- Técnicas Comunes con METRICA v2.1 y con EUROMÉTODO.
- Técnicas características de MAGERIT, tales como matriciales, algorítmicas y de lógica difusa.

- Técnicas Complementarias.

MAGERIT consta de siete guías:

- **Guía de Aproximación**. Presenta los conceptos básicos de seguridad de los sistemas de información, con la finalidad de facilitar su comprensión por persona no especialista y ofrece una introducción al núcleo básico de MAGERIT, constituido por las Guías de Procedimientos y de Técnicas.

- **Guía de Procedimientos**. Representa el núcleo del método, que se completa con la Guía de Técnicas. Ambas constituyen un conjunto autosuficiente, puesto que basta su contenido para comprender la terminología y para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información.

- **Guía de Técnicas**. Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.

- **Guía para Responsables del Dominio protegible**. Explica la participación de los directivos "responsables de un dominio" en la realización del análisis y gestión de riesgos de aquellos sistemas de información relacionados con los activos cuya gestión y seguridad les están encomendados.

- **Guía para Desarrolladores de Aplicaciones**. Está diseñada para ser utilizada por los desarrolladores de aplicaciones, y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica v2.1.

- **Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos**. La interfaz para intercambio de datos posibilita que un usuario de MAGERIT establezca la comunicación con otras aplicaciones y sistemas facilitando la incorporación de sus productos a la herramienta MAGERIT y viceversa.

- **Referencia de Normas legales y técnicas**. Lista de normas en materia de seguridad a fecha 31 de Diciembre de 1996.

En su primera versión MAGERIT consta de dos herramientas de apoyo sobre plataforma PC:

- **Herramienta 1, Introductoria**. Permite una primera aproximación al Análisis y Gestión de Riesgos y constituye un apoyo en la identificación de riesgos menores a los que bastará aplicar globalmente medidas básicas de seguridad 'práctica' y de riesgos mayores a cada uno de los cuales será necesario aplicar un nuevo Análisis y Gestión de Riesgos más detallado. Se apoya en el uso de técnicas matriciales y no requiere que el usuario tenga necesariamente un nivel avanzado de especialización en seguridad de los sistemas de información. Se ofrece completamente con la publicación.
- **Herramienta 2, Avanzada**. Permite realizar un Análisis y Gestión de riesgos detallado y afrontar así proyectos de complejidad media o alta en materia de seguridad. Se apoya en el uso de técnicas algorítmicas, de lógica difusa y de Bayés. Permite un análisis detallado de los Activos del Dominio y de sus dependencias, de la relación entre éstos y las Amenazas, las Funciones y los Mecanismos de Seguridad, y de los Riesgos (intrínseco, efectivo, residual). Requiere que el usuario tenga un cierto nivel de especialización en seguridad de los sistemas de información.

3.1.5 CRMR

CRMR son las siglas de <<Computer Resource Management Review>>; su traducción más adecuada, Evaluación de la gestión de recursos informáticos. En cualquier caso, esta terminología quiere destacar la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio del management.

Una revisión de esta naturaleza no tiene en sí misma el grado de profundidad de una auditoría informática global, pero proporciona soluciones más rápidas a problemas concretos y notorios.

Supuestos de aplicación:

En función de la definición dada, la metodología abreviada CRMR es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un Centro de Procesos de Datos.

El método CRMR puede aplicarse cuando se producen algunas de las situaciones que se citan:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.
- Existen costes excesivos de proceso en el Centro de Proceso de Datos.

Efectivamente, son éstas y no otras las situaciones que el auditor informático encuentra con mayor frecuencia. Aunque pueden existir factores técnicos que causen las debilidades descritas, hay que convenir en la mayor incidencia de fallos de gestión.

Áreas de aplicación:

Las áreas en que el método CRMR puede ser aplicado se corresponden con las sujetas a las condiciones de aplicación señaladas en punto anterior:

- Gestión de Datos.
- Control de Operaciones.
- Control y utilización de recursos materiales y humanos.
- Interfaces y relaciones con usuarios.
- Planificación.
- Organización y administración.

13CRMR

http://www.monografias.com/trabajos5/audi/audi2.shtml

Ciertamente, el CRMR no es adecuado para evaluar la procedencia de adquisición de nuevos equipos (Capacity Planning) o para revisar muy a fondo los caminos críticos o las holguras de un Proyecto complejo.

Objetivos:

CRMR tiene como objetivo fundamental evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un Centro de Proceso de Datos. Las Recomendaciones que se emitan como resultado de la aplicación del CRMR, tendrán como finalidad algunas de las que se relacionan:

- Identificar y fijas responsabilidades.
- Mejorar la flexibilidad de realización de actividades.
- Aumentar la productividad.
- Disminuir costes
- Mejorar los métodos y procedimientos de Dirección.

Alcance

Se fijarán los límites que abarcará el CRMR, antes de comenzar el trabajo.

Se establecen tres clases:

- Reducido. El resultado consiste en señalar las áreas de actuación con potencialidad inmediata de obtención de beneficios.
- Medio. En este caso, el CRMR ya establece conclusiones y Recomendaciones, tal y como se hace en la auditoría informática ordinaria.
- Amplio. El CRMR incluye Planes de Acción, aportando técnicas de implementación de las Recomendaciones, a la par que desarrolla las conclusiones.

Información necesaria para la evaluación del CRMR

Se determinan en este punto los requisitos necesarios para que esta simbiosis de auditoría y consultoría pueda llevarse a cabo con éxito.

El trabajo de campo del CRMR ha de realizarse completamente integrado en la estructura del Centro de Proceso de Datos del cliente, y con los recursos de éste.

Se deberá cumplir un detallado programa de trabajo por tareas.

El auditor-consultor recabará determinada información necesaria del cliente.

Se tratan a continuación los tres requisitos expuestos:

Integración del auditor en el Centro de Procesos de Datos a revisar

No debe olvidarse que se están evaluando actividades desde el punto de vista gerencial. El contacto permanente del auditor con el trabajo ordinario del Centro de Proceso de Datos permite a aquél determinar el tipo de esquema organizativo que se sigue.

Programa de trabajo clasificado por tareas

Todo trabajo habrá de ser descompuesto en tareas. Cada una de ellas se someterá a la siguiente sistemática:

- Identificación de la tarea.
- Descripción de la tarea.
- Descripción de la función de dirección cuando la tarea se realiza incorrectamente.
- Descripción de ventajas, sugerencias y beneficios que puede originar un cambio o modificación de tarea
- Test para la evaluación de la práctica directiva en relación con la tarea.
- Posibilidades de agrupación de tareas.
- Ajustes en función de las peculiaridades de un departamento concreto.
- Registro de resultados, conclusiones y Recomendaciones.

Información necesaria para la realización del CRMR

El cliente es el que facilita la información que el auditor contrastará con su trabajo de campo.

Se exhibe a continuación una Checklist completa de los datos necesarios para confeccionar el CRMR:

- Datos de mantenimiento preventivo de Hardware.
- Informes de anomalías de los Sistemas.

- Procedimientos estándar de actualización.
- Procedimientos de emergencia.
- Monitorización de los Sistemas.
- Informes del rendimiento de los Sistemas.
- Mantenimiento de las Librerías de Programas.
- Gestión de Espacio en disco.
- Documentación de entrega de Aplicaciones a Explotación.
- Documentación de alta de cadenas en Explotación.
- Utilización de CPU, canales y discos.
- Datos de paginación de los Sistemas.
- Volumen total y libre de almacenamiento.
- Ocupación media de disco.
- Manuales de Procedimientos de Explotación.

Esta información cubre ampliamente el espectro del CRMR y permite ejercer el seguimiento de las Recomendaciones realizadas.

CAPITULO IV

4. ANÁLISIS DE LAS METODOLOGÍAS Y DESARROLLO DE LA METODOLOGÍA

4.1 Introducción

La determinación de la metodología, que se va a utilizar para la implementación de una auditoria de riesgos (físicos y lógicos), debe ser una de las decisiones más importantes que deben tomar los auditores, la cual debe estar basada en un profundo y minucioso análisis de acuerdo a criterios de comparación o parámetros y también deben cumplir con los requerimientos de la empresa para la cual se va a desarrollar la auditoría de riesgos informáticos.

La determinación de los criterios para realizar un análisis entre las metodologías para realizar una auditoría de riesgos informáticos se basa en sus características más importantes, por lo que se tomaran en cuenta los aspectos que presenten mayor relevancia para tomar una decisión. En este capítulo se realizará un análisis de las metodologías para el desarrollo de una auditoría de riesgos informáticos con la finalidad de obtener una metodología compuesta por los procesos más importantes de todos los analizados acorde a

las necesidades de la empresa, los resultados obtenidos del presente estudio se expresan en el informe que se genera al termino de la auditoría.

4.2 Determinación de las metodologías a analizar

En la actualidad existe en el mercado varias metodologías para desarrollar auditorías de riesgos informáticos, actuales, bastante populares, y de gran importancia para los auditores, de las cuales hemos investigado las siguientes: ITIL, COBIT, ISO 17799, MAGERIT y CRMR.

En el presente cuadro se muestra un breve resumen de los objetivos y el trabajo que desempeña las actividades en cada una de las metodologías.

HERRAMIENTA / CARACTERÍSTICA	COBIT	ITIL	ISO 17799	MAGERIT	CRMR
Objetivo	Determina, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en el negocio con el respaldo de las principales normas técnicas internacionales.	Desarrollada para alcanzar objetivos corporativos. Ayudará a organizar el departamento	Definir un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información.	Investigar los riesgos que soportan los Sistemas de Información, y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.	Evalúa la gestión de recursos informáticos. Evalúa la eficiencia de utilización de los recursos por medio de la administración.
¿Que ofrece?	Brinda métricas y modelos de madurez para medir logros del negocio. Brinda un modelo de procesos genéricos (procesos que se encuentran en las funciones de TI).	El beneficio principal es que a través de las directrices y las mejores prácticas que se imparten en la biblioteca, su empresa puede ahorrar una enorme cantidad de dinero una vez ejecutados.	Ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización	Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información. Incrustar de mecanismos de seguridad en el corazón mismo de los sistemas de información:	Evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un Centro de Proceso de Datos
	COBIT define 4	ITIL define cinco	La norma ISO 17799	Influye en las Fases y	CRMR define 4 fases:

Marco de trabajo/Fases/Actividades/Procesos	dominios que son: ✓ Planear y Organizar(Incluye 11 Procesos) ✓ Adquirir e Implementar(Incluye 6 Procesos) ✓ Entregar y Dar Soporte (Incluye 13 Procesos) ✓ Monitorear y Evaluar(Incluye 4 Procesos)	procesos: ✓ Manejo de Incidentes ✓ Manejo de problemas ✓ Manejo de configuraciones ✓ Manejo de Cambios ✓ Manejo de entregas	establece diez dominios de control: ✓ Política de seguridad. ✓ Aspectos- Seguridad. ✓ Clasificación-Control de activos. ✓ Seguridad-Personal. ✓ Seguridad-Entorno. ✓ Gestión (Comunicaciones y Operaciones). ✓ Control de accesos. ✓ Desarrollo-Sistemas. ✓ Gestión del negocio. ✓ Conformidad con la legislación.	actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento). Incluyendo 3 sub-modelos	✓ Causas de la realización del ciclo de seguridad. ✓ Estrategia y logística del ciclo de seguridad. ✓ Cálculos y resultados del ciclo de seguridad. ✓ Confección del informe del ciclo de seguridad.

Tabla. IV. 1. Características de la Metodologías

En el cuadro presentado, señala los objetivos principales, lo más importante que ofrece y menciona cada una de las tareas y procesos que incluye en cada una de las metodologías estudiadas.

Con respecto a sus objetivos, podemos señalar que COBIT, ITIL, ISO 17799 y MAGERIT coinciden en el trabajo de seguridad tanto de la información como de los sistemas de información, mientras que CRMR se enfoca más en el trabajo de Gestión de los Recursos Informáticos.

En lo que respecta a lo que ofrece cada una de las herramientas, determinamos que COBIT se enfoca en medir logros del negocio, mientras que ITIL ayuda a la empresa ahorrar grandes cantidades de dinero, así como también ISO y MAGERIT brinda seguridad a la información y CRMR ofrece evaluar la eficiencia del Centro de Proceso de Datos.

Para el trabajo que realiza cada una de las metodologías proporcionan sus actividades y fases, en las que luego del respectivo análisis se puede definir que COBIT e ISO brindan un trabajo largo pero muy bien estructurado y muy completo mientras que ITIL, MAGERIT Y CRMR ofrecen un marco de trabajo no muy complejo con cada una de las actividades que se puedan desarrollar en menos tiempo y sin la necesidad de un especialista.

Para el proceso de análisis se han seleccionado 3 metodologías por las razones que se explican a continuación:

En un artículo ” **El desarrollo de la Relación de Bussines**” el cual es un estudio en el que se explora como las empresas están desarrollando el valor de negocio ITIL, manifestando los resultados de una encuesta realizada en septiembre la Conferencia Nacional de itSMF a 100 ejecutivos de 90 empresas, quienes mencionan que aunque las organizaciones se centran claramente en sus prioridades de ITIL (calidad del servicio y de entrega) y de sus principales iniciativas de ITIL (CMDB, Incidentes and Problemas de Administración, Servicio de Catálogo y el cambio y de prensa Gestión), la mayoría siguen tropezando con el problema de la cuantificación y articular el valor de estas iniciativas para la empresa.

En otro de los estudios realizados se presenta el que titula”**RESULTADOS DE LA ENCUESTA: ITIL ® BUENAS PRÁCTICAS EN ENTORNOS SAP**”, localizado en el siguiente link: www.pinkelephant.com, el cual menciona que:

- ✓ El proceso de ITIL más común aplicarse en primer lugar es de Manejo de Incidentes, seguida de Service Desk y Gestión del Cambio

Otro resultado denominado "**Resultados encuesta mundial 2008 de ITGI acerca de gobierno de IT**" el cual menciona que el ITGI comisionó una encuesta global de 749 ejecutivos del nivel CEO/CIO en 23 países para determinar sus prioridades de gobierno y los problemas con las TI que han tenido que enfrentar. De acuerdo a la *Encuesta Global de Gobierno de TI del 2008*, 58% de los encuestados mencionaron que el personal insuficiente es un problema, comparado con sólo el 35% en el 2005. Así mismo, el 48% dijo que los problemas con la entrega de servicio continuaban siendo el segundo problema más común y un 38% apunta hacia problemas de personal con pocas habilidades. 30% de los encuestados reportaron problemas en la anticipación del retorno de la inversión para gastos de TI.

El estudio es una continuación a las encuestas del 2003 y el 2005 y da seguimientos a las tendencias en TI en los cuatro últimos años. Muchos avances importantes en el ámbito empresarial relacionados con las TI son identificados en el reporte, incluyendo:

- 93% de los encuestados dijeron que las TI son de algo a muy importantes dentro de la estrategia corporativa – un incrementos del 6% respecto al 2005.
- Las TI están siempre presentes en la agenda del consejo directivo, de acuerdo a la opinión del 32% de los encuestados – en comparación con el 25% en el 2005.
- 18% de los encuestados dijeron que el departamento de TI siempre informa a la empresa acerca de oportunidades potenciales de negocio – sólo el 14% reportó lo mismo en el 2005.
- La conciencia del marco de trabajo Control de Objetivos de Información y Tecnología Relacionada (COBIT por sus siglas en inglés) para el gobierno de las TI sobrepasó el 50%, casi duplicándose desde el 2005.
- El uso de COBIT se duplicó (del 8 % en 2005 al 16%).

En el 2009, ISACA comisionó al "IT Alignment and Governance Research Institute" de la Universidad de Antwrep para que realice una investigación acerca del valor generado por Val IT y COBIT en las organizaciones.

La pregunta crucial de esta investigación fue: "**Cuál es la relación existente entre el desempeño de una organización y las prácticas de gobierno de IT basadas en Val IT 2.0 y COBIT 4.1**"

Para encontrar la respuesta, la investigación se realizó entre 538 empresas miembros de ISACA de todo el mundo que completaron un cuestionario de estado de implementación de 56 procesos de gobierno de IT y cuál es el desempeño frente a 20 objetivos de negocio y 18 objetivos de IT. La distribución geográfica de las empresas fue la siguiente:

1. 40% Norteamérica
2. 26% Asia
3. 19% Europa
4. 7% África
5. 5% Oceanía
6. 3% Latino América

Las empresas fueron agrupadas en 5 segmentos de industrias; a) Bancos, Servicios Financieros y Seguros, b) Gobierno, Servicios Públicos y Salud, c) Servicios Profesionales IT, Telecomunicaciones y Medios, d) Manufactura y Farmacéuticas y e) Comercio Minorista, Distribución y Transportes.

El perfil de las personas que contestaron fueron; 55% en áreas de negocio y 45% en áreas de IT.

Resultados principales:

Para concluir con los estudios investigados, presentamos a continuación un cuadro en el cual se menciona las últimas votaciones por internet, de personal que desea charlas sobre este tipo de metodologías dando como resultados los siguientes:

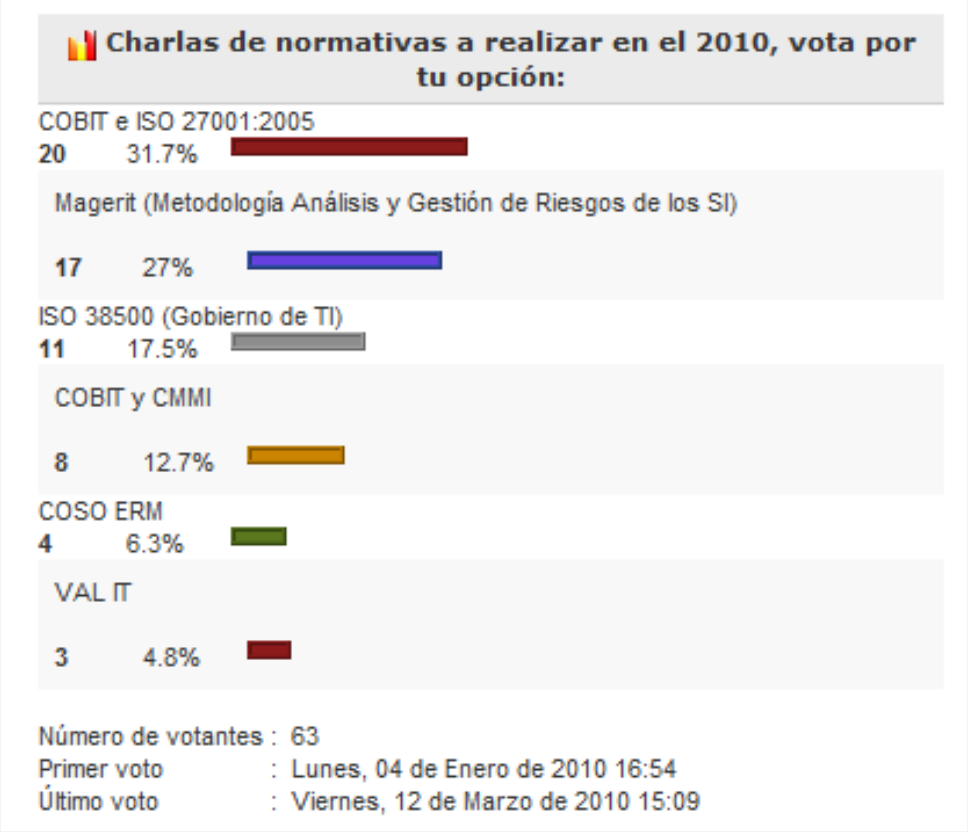


Fig. IV. 31. Resultados Encuesta

4.3 Análisis de metodologías seleccionadas

A continuación analizaremos más a fondo cada una de las metodologías escogidas para el estudio previo, el cual lo realizaremos mediantes matrices para cada una de las metodologías para de ello determinar lo mejor de los procesos y de esta manera iniciar el desarrollo de la metodología.

4.3.1 COBIT

Se divide en 4 Dominios y a su vez cada dominio en procesos, entonces por cada dominio se analizará y se determinará ventajas y desventajas del proceso.

Dominio: Planear y Organizar		
Procesos	**Ventajas**	**Desventajas**
PO1 Definir un Plan Estratégico de TI	Definir los objetivos de negocio y necesidades para las TI. Inventario de soluciones tecnológicas e infraestructura actual. Estudio de viabilidad oportuno. Existencia de evaluaciones de sistemas.	El plan estratégico solo define a largo plazo. Y si es a corto plazo este debe ser operacional
PO2 Definir la Arquitectura de Información	Incrementa la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.	Este proceso solo involucra a los factores aplicaciones y datos, siendo un factor importante también la tecnología.
PO3 Determinar la dirección tecnológica	Garantizar que la tecnología esté disponible y emergente en los casos que se aplique. Creación y mantenimiento de un plan de infraestructura tecnológica. Adecuación y evolución de la capacidad de la infraestructura actual.	El proceso no considera a las aplicaciones para poder determinar la tecnología.
PO4 Definir los procesos, organización y relaciones de TI	Supervisión y segregación de las obligaciones, roles y responsabilidades de la organización.	No integran un apartado para las prohibiciones de la organización.
PO5 Administrar la inversión en TI	Asegura el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio.	No toman medidas correctivas necesarias para brindar transparencia y responsabilidad dentro del costo total de la propiedad
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables.	Este proceso solo involucra al recurso personas, un factor q debe ser importante para comunicar seria también los proyectos desarrollados y por desarrollar.

PO7 Administración de recursos humanos	Maximiza las contribuciones del personal a los procesos de TI Satisface los requerimientos de negocio, a través de técnicas sólidas para administración de personal. Ayuda a cumplir la Eficiencia y la Efectividad del dominio.	
PO8 Asegurar el cumplimiento con los requerimientos Externos	Identificación y análisis de requisitos externos Considera leyes, regulaciones y contratos. Inspecciones regulares para cambios y mejoras. Seguridad y ergonomía Propiedad intelectual	No se aplica en riesgos informáticos (físicos y lógicos)
PO9 Evaluación de riesgos	Identifica y analiza el impacto de los riesgos, tomando medidas efectivas de costes para mitigar los riesgos. Considera el alcance: global o sistemas específicos. Realiza una evaluación de riesgos hasta la fecha. Toma medidas de riesgo cuantitativas y/o cualitativas. Muestra plan de acción de riesgos.	
PO10 Administración de proyectos	Organiza e identifica dando prioridad a los proyectos en línea junto al plan operacional. Considera**:** propiedad de proyectos; interrupción de tareas; distribución de responsabilidades; fase de aprobación; planes de seguridad de la calidad y métodos	No incluye una metodología para su aplicación. La organización debería adoptar y aplicar técnicas de gestión de proyectos para cada uno de los proyectos tomados.
PO11 Administración de calidad	Satisface los requerimientos del cliente. Realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización.	No incluye seguimiento de la calidad de los proyectos y las operaciones. No existe el control de una base en el que se pueda respaldarse para levar a cabo un correcto soporte técnico.

Tabla. IV. 2. Cobit – Dominio Planear y Organizar

Dominio: Adquirir e Implantar		
Procesos	**Ventajas**	**Desventajas**
AI1 Identificar soluciones automatizadas	Asegura la mejor aproximación para satisfacer los requisitos del usuario. Considera en el proceso estudios factibles, arquitectura de la información, la seguridad del coste-efectivo y aceptación de las facilidades y la tecnología	No involucra a los datos, ya que este es el activo más importante en la empresa.
AI2 Adquirir y mantener software aplicativo	Ayuda a cumplir la efectividad, eficiencia, integridad, conformidad, confiabilidad del dominio. Suministrar funciones automáticas que soporten de forma efectiva los procesos de negocio	Incluye obligatoriedad en la adquisición y mantenimiento del software.
AI3 Adquirir y mantener infraestructura tecnológica	Suministra las plataformas adecuadas para soportar las aplicaciones de negocios Asentamiento de la implantación de hardware y software Provisión de mantenimiento del hardware preventivo, y la instalación, seguridad y control de los sistemas software.	
AI4 Facilitar la operación y el uso	Asegura el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas. Realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento.	No involucra la producción de documentación de usuario, manuales de operación y material de entrenamiento.
AI5 Adquirir recursos de TI	Verifica y confirma que la solución sea adecuada para el propósito deseado. Realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas.	No se conoce si la organización está en capacidad de adquirir recursos.
AI6 Administrar cambios	Facilita un sistema de gestión que se suministre para el análisis, implementación y obtención de todos	

	los cambios solicitados para las infraestructuras existentes	

Tabla. IV. 3. Cobit – Dominio Adquirir e Implantar

Dominio: Entregar y Dar Soporte		
Procesos	**Ventajas**	**Desventajas**
Ds1 Definición de niveles de servicio	Asegura la alineación de los servicios claves de TI con la estrategia del negocio. Establece un entendimiento común del nivel de servicio requerido. Considera en su proceso: acuerdos formales, definición de responsabilidades, tiempos de respuesta y volúmenes, garantías de integridad y acuerdos no declarados.	La descripción de los servicios, como el nombre los llama, en si no involucra por niveles.
DS2 Administrar servicios de terceros	Asegura las reglas y las responsabilidades de terceras partes que estén definidas de forma clara y satisfagan los requisitos. Incluye medidas de control dirigidas en la inspección y monitorización de contratos existentes y procedimientos para su efectividad y conformidad con la política de la organización.	Existe obligatoriedad en el registro de información de este proceso. En una auditoria de riesgos informáticos, este proceso no es relevante.
DS3 Administrar desempeño y capacidad	Asegura que la capacidad adecuada está disponible y que se está haciendo un uso óptimo y mejor para encontrar las necesidades de cumplimiento requeridas. Contiene controles de gestión de capacidad y cumplimiento que coleccionen datos e informen en la gestión del trabajo.	En el proceso DS5 la administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.
DS4 Garantizar la Continuidad del Servicio	Hacer que los servicios de TI requeridos estén disponibles y asegurar un impacto de negocio mínimo en caso de una ruptura mayor. Facilita la posesión de un continuado y testeado plan de TI que esté en línea con la totalidad del plan continuo de negocio y con sus	No involucra parámetros para medir la continuidad de los servicios que presta la organización.

	requisitos de negocio relacionados.	
DS5 Garantizar la Seguridad de los Sistemas	Salvaguardar la información contra el uso no autorizado, descubrimiento o modificación, daño o pérdida. Facilita controles de acceso lógico que aseguren que el acceso a los sistemas, datos y programas está restringido a los usuarios autorizados.	La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad.
Ds6 Educación y entrenamiento de usuarios	Asegurar que los usuarios son eficientes en el uso de la tecnología y que son conscientes de los riesgos y responsabilidades en las que están involucrados. Incluye un entrenamiento comprensivo y un plan de desarrollo.	Debería haber una selección y clasificación de usuarios para el correcto entrenamiento de los mismos.
Ds7 Identificación y asignación de costos	Asegurar un correcto conocimiento de los costes atribuidos a los servicios de TI. Facilita un sistema de contabilidad de costes que asegure que dichos costes son registrados, calculados y localizados para el nivel de detalle requerido.	Para el ámbito relacionado a la auditoría de riesgos informáticos, no se inmiscuye a profundidad en el tema.
DS8 Apoyo y asistencia a los clientes de TI	Asegurar que cualquier problema experimentado por el usuario será resuelto apropiadamente. Facilita una fácil ayuda que suministre soporte de primer orden y consejo	Los problemas que se puedan presentar en los usuarios no son necesarios analizarlos como un punto aparte pues ya serán analizados en el proceso DS10 Administrar los problemas.
DS9 Administrar la configuración	Considerar todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y provee de un fundamento para una gestión de cambio firme. Facilita controles que identifiquen y registren todos los medios de TI y su localización física, y un programa regular de verificación que confirme dicha existencia.	Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso.
DS10 Administrar los problemas	Asegura que los problemas e incidentes serán resueltos, e investigando la causa para prevenir una nueva aparición de estos. Facilita un sistema de gestión de	La administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de

	problemas que registre y avance todos los incidentes.	problemas.
DS11 Administrar los datos	Asegura que los datos permanecen completos, correctos y válidos durante su introducción, actualización y almacenamiento. Facilita una combinación efectiva de aplicación y controles generales sobre las operaciones de TI.	Falta de detalle en la administración de datos que propone este proceso.
DS12 Administrar el ambiente físico	Provee de un medio físico apropiado que proteja el equipamiento de las TI y a las personas contra riesgos naturales y riesgos provocados por el hombre. Se cumple mediante una instalación de controles físicos apropiados que son revisados regularmente para su propia función	No menciona un plan a ejecutar mediante la auditoria.
DS13 Administrar las operaciones	Asegura que las funciones importantes soportadas de las TI son realizadas regularmente y de una forma ordenada. Se lo aplica mediante un planificador de actividades soportadas que es registrado y aclarado para el cumplimiento de todas las actividades.	Para realizar una administración de operaciones se requiere de una administración del procesamiento de datos y del mantenimiento del hardware. Como ya existe un proceso de administración de datos en uno de los dominios, este proceso incluye los mismos apartados.

Tabla. IV. 4. Cobit – Dominio Entregar y Dar Soporte

Dominio: Monitorear y Evaluar		
Procesos	**Ventajas**	**Desventajas**
M1 Monitoreo del Proceso	Garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas. Implementación de los sistemas soportados así como la aclaración del informe sobre los fundamentos regulares.	El proceso se lo aplica a todos los recursos del entorno a auditar, incluido al recurso humano.

M2 Evaluar lo adecuado del Control Interno	Asegura la realización de los objetivos de control internos establecidos para los procesos de las TI. Se lo verifica mediante una comisión de la administración para monitorizar controles internos, fijando su efectividad, e informando de ellos con bases regulares	Para una aplicación solo de riesgos informáticos, debería haber una clasificación de un control para lo físico y otro para lo lógico.
ME3 Garantizar el cumplimiento regulatorio	Incrementar la confianza y el cuidado entre la organización, los clientes, y los proveedores a terceros. Se lo comprueba por inspecciones de la seguridad independiente llevadas a cabo en intervalos regulares.	
ME4 Proporcionar gobierno de TI	Incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales.	Las tareas de esta actividad ya se mencionan, lo más importante en un proceso de otro dominio.

Tabla. IV. 5. Cobit – Dominio Monitorear y Evaluar

4.3.2 ISO 17799

Se divide en 10 Dominios de Control, entonces por cada dominio se analizará y se determinará ventajas y desventajas de las actividades que incluye el dominio.

ISO 17799		
Dominios de Control	**Ventajas**	**Desventajas**
Política de seguridad	Nos ayuda a mitigar los riesgos existentes en la organización a ser auditada. La Política en materia de seguridad implica a todo el personal involucrado en la seguridad de la información.	Por el personal que se involucra, no lo hacen fácil su aceptación.
Aspectos organizativos para la seguridad	Define y analiza las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información.	Limita a los empleados a desempeñar solo el trabajo asignado y que corresponda a su área.
	Define una clasificación de los activos relacionados con los sistemas	

Clasificación y control de activos.	de información. Verifica el correcto mantenimiento de un inventario actualizado que registra los datos, y proporciona a cada activo el nivel de protección adecuado a su criticidad en la organización. Asegura un nivel de protección adecuado a los activos de información. Mediante la información de activos se podrá determinar el trabajo y el tiempo que tomara el desarrollar la auditoria.	Se lo considera solo una parte general en la auditoria con una prioridad no muy alta. No presenta un modelo de clasificación de activos.
Seguridad ligada al personal.	Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios. Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento.	Este proceso se lo podría involucrar en la definición de la política de seguridad.
Seguridad física y del entorno.	Ayuda evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Evita la interrupción de las actividades de la organización	No incluye una previa administración del ambiente físico, para realizar una correcta detección de los riesgos.
Gestión de comunicaciones y operaciones.	Mantiene la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación. Asegura la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo. Evita daños a los activos e interrupciones de actividades de la organización. Previene la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.	Para esta gestión no incluye un plan de contingencia, aplicable a los factores que incluye este proceso.

	Garantizar la seguridad de las comunicaciones y de la operación de los sistemas críticos para el negocio.	
Control de accesos	Identifica actividades no autorizadas. Garantiza la seguridad de la información cuando se usan dispositivos de informática móvil y tele-trabajo. Se establecen controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc.	
Desarrollo y mantenimiento de sistemas	Evita pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevados a cabo de una forma segura. Ayuda a proteger la confidencialidad, autenticidad e integridad de la información.	Par el mantenimiento debe cumplir ciertas medidas mínimas de seguridad como control de acceso, perfiles de usuario, time-out, expiración de contraseñas, sesiones simultáneas, inyección de sql, etc.
Gestión de continuidad del negocio	Verifica la definición equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre. Los planes de contingencia deben ser probados y revisados periódicamente.	Se lo aplica de manera general para los procesos auditivos, pero para uno en exclusivo como el de auditar solo lo físico y lo lógico de la empresa, no se aplica totalmente en el análisis
Conformidad con la legislación	Identifica convenientemente la legislación aplicable a los sistemas de información corporativos integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento. Define un plan de auditoría interna y lo ejecuta convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.	

Tabla. IV. 6. Dominios de ISO 17799

4.3.3 MAGERIT

Esta metodología se especifica en 2 partes, la primera el Análisis y Gestión de Riesgos y la segunda la Planificación de los Riesgos, cada una incluye sus respectivas actividades, entonces se analizará y se determinará ventajas y desventajas de las actividades que incluye cada parte.

I. (AGR) Análisis y Gestión de Riesgos		
Actividades	**Ventajas**	**Desventajas**
Determinación de Objetivos, Estrategias y Políticas de Seguridad de los sistemas de Información.	Detecta si existen riesgos en los sistemas de información y buscar las estrategias y políticas más oportunas para cada caso.	No presenta un plan para el desarrollo de la misma actividad.
Establecimiento de la Planificación de la seguridad de los Sistemas de Información.	Presenta una planificación de la seguridad, con un proceso de identificación de los riesgos en los sistemas, la cual nos ayudará a desempeñar un buen trabajo el momento de actuar contra el riesgo detectado.	
Determinación de la organización de la seguridad de los Sistemas de Información.	Permite llevar un control minucioso de lo que sucede con los SI, de esta manera determinar cuál fue su causa y si se vuelva a presentar aplicar la solución correspondiente	
Implantación de Salvaguardas y otras medidas de seguridad de los Sistemas de Información.	En el caso de que no funcionaran las medidas de seguridad existentes, sería muy necesario implantar otras, que nos ayuden a proteger los SI.	No presenta un formato para crear medidas de seguridad para los sistemas de información.
Concentración de todos en la seguridad de los sistemas de información.	Se alerte a cada una de las personas que están en contacto con los sistemas de información.	Este proceso en vez de actividad será de considerarla más bien como sugerencia en la institución por parte de la persona encargada del departamento.
Seguimiento, Gestión de Configuración y de	Se desarrolla un seguimiento mediante un registro de cada uno de	Como ya se establece medidas de seguridad, se contradice a propiciar los

cambios de seguridad de los Sistemas de Información	los cambios que se desarrolla en los sistemas de información de la organización.	cambios de seguridad, ya que al establecer al inicio las reglas de juego, no habría porque haber cambios.
Reacción a cada evento, Registro de incidencias y recuperación de estados de seguridad	Llevar un registro de los sucesos e incidencias que se presentan en cada uno de los procesos en los que incluye la seguridad de los Sistemas de Información.	Actividad de relevancia, pero no limita sus registros por área de la organización.

Tabla. IV. 7. MAGERIT – Actividades AGR

II. Planificación de Gestión de Riesgos		
Planificación		
Actividades	**Ventajas**	**Desventajas**
Oportunidades de realización	Llevar un acuerdo entre la organización y el equipo auditor. Cuando ya se da por inicio a una actividad ya se tiene todo el respaldo necesario para dar por hecho el proceso de auditoría.	No se ve la necesidad de llevar a este acuerdo como una actividad de la metodología.
Definición de dominio y objetivos	Mediante la definición de objetivos nos permitirá seguir con el proceso hasta conseguir y cumplir los mismos.	
Planificación del proyecto	Con una planificación desarrolla al empezar con la auditoría, ayuda tanto al auditor como al equipo de trabajo colaborador de la institución a no desviar y continuar con el proceso de una manera ordenada y sistemática, por esta razón la actividad será escogida.	
Lanzamiento del proyecto	Lleva en cada uno de sus procesos la respectiva documentación. Comunica sobre la apertura de los proyectos al personal y/ usuarios que se involucran en cada uno de los proyectos de la organización	Esta actividad más es de formalismo, una tarea que no debe ser considerada como actividad, se la puede ejecutar en cualquier momento de un proceso.

Tabla. IV. 8. MAGERIT – Actividades Planificación de Gestión de riesgos – Planificación

II. Planificación de Gestión de Riesgos		
Análisis de riesgos		
Actividades	**Ventajas**	**Desventajas**
Recogida de información	Actividad de alta prioridad, consideramos que es la parte vital en la cual se inicia y se pone mucho empeño porque de esta manera se parte para comprobar si cumple o no con los objetivos y las labores que desarrolla la institución.	
Identificación y agrupación de ACTIVOS	Cuando ya damos inicio luego de una correcta recolección de información se presenta la identificación de los activos de la empresa, algo relevante para el proceso de auditoría, ya que nos permitirá determinar si coincide o no con los inventarios que la empresa nos proporciona para la realización d la auditora.	
Identificación y Evaluación de AMENAZAS	Identifica las amenazas a las que está expuesto el departamento para determinar la prioridad con la que se pueda presentar.	
Identificación y evaluación de VULNERABILIDADES	Identifica las características vulnerables que existe en el departamento así como también permite identificar rápidamente cual es el factor que está en peligro dentro del departamento.	
Identificación y valoración de IMPACTOS	Determina los impactos que ayudan a identificar el riesgo a ejecutarse, luego de la evaluación de las amenazas identificadas en la organización.	No menciona el proceso de priorizar a los riesgos identificados.
Evaluación del RIESGO	Se evalúa y se estudia a fondo el riesgo para corregir y aplicar y dar la solución optima.	Debería presentar por cada área una lista de recomendaciones, para ayudar al departamento a tomar decisiones.

Tabla. IV. 9. MAGERIT – Actividades Planificación de Gestión de riesgos –Análisis

II. Planificación de Gestión de Riesgos		
Gestión de Riesgos		
Actividades	**Ventajas**	**Desventajas**
Interpretación del Riesgo.	Realiza un estudio de cada uno de los riesgos identificados.	Consideramos que la actividad realiza el mismo trabajo que la actividad "Evaluación del Riesgo"
Identificación y estimación de funciones de salvaguarda.	Apoya las funciones de protección para cuando exista un riesgo e inmediatamente poder ejecutar este proceso y poder reparar el daño que este pueda producir.	
Selección de funciones de salvaguarda.	Realiza una selección de las más importantes y que puedan ser ejecutadas sin ninguna dificultad.	No incluye una selección por áreas en las que se divide la organización a ser auditada.
Cumplimiento de Objetivos.	Al final de la etapa esta actividad es muy significativa ya que se logrará determinar si existe o no el cumplimiento de los objetivos	Es una solución casi con baja prioridad, porque este proceso se lo lleva acabo al término de cada actividad de cada una de las fases.

Tabla. IV. 10. MAGERIT – Actividades Planificación de Gestión de riesgo – Gestión

II. Planificación de Gestión de Riesgos		
Selección de Salvaguardas		
Actividades	**Ventajas**	**Desventajas**
Identificación de mecanismos de seguridad	Permite identificar cada uno de los sistemas de seguridad que aplica la empresa.	Procesos redundantes. AGR ya menciona la necesidad de identificar medidas de seguridad.
Selección de mecanismos de seguridad	Realiza una selección de los mecanismos de seguridad identificados en el proceso anterior, más importantes y que puedan ser ejecutadas sin ninguna dificultad.	
Especificación de los mecanismos a implantar	Apoya las funciones y mecanismos de protección para cuando exista un riesgo e inmediatamente poder ejecutar este proceso y poder reparar el daño que este pueda producir.	
Planificación de la implantación	Desarrolla un plan para ejecutar el mecanismo de implantación especificado.	
	Luego de un proceso trabajoso de identificación, e implementación de mecanismos de seguridad se	Actividad casi con baja prioridad, porque este proceso se lo lleva acabo al

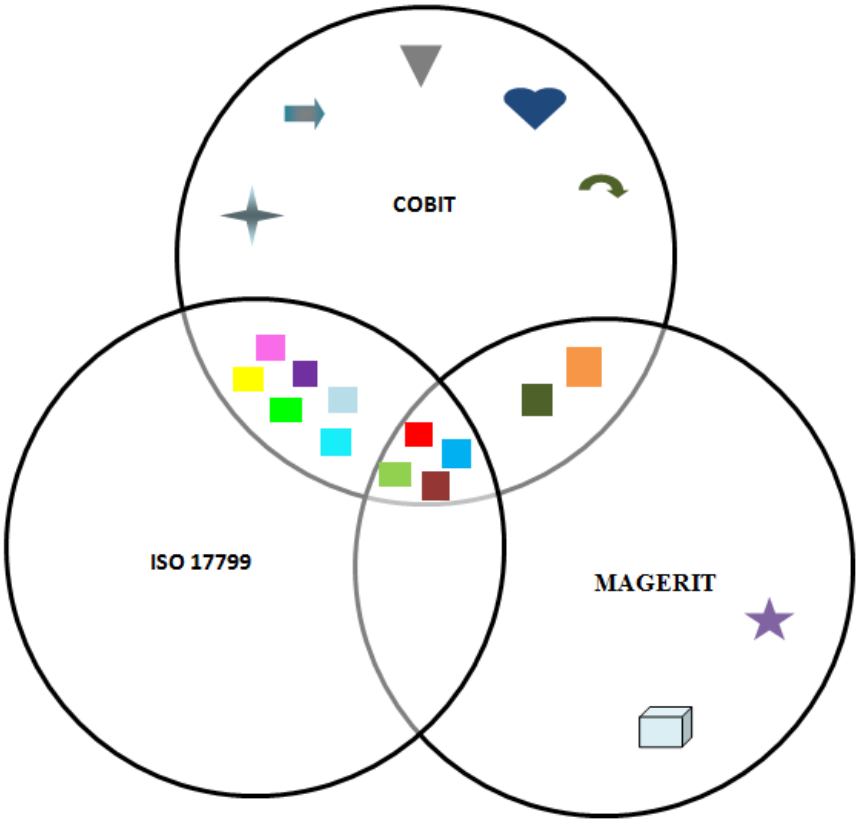
Integración de resultados	presentará los resultados y se determinará el nivel de cumplimiento de los objetivos y de las tareas que se desarrolla en el departamento.	término de cada actividad de cada una de las fases.

Tabla. IV. 11. MAGERIT – Actividades Planificación de Gestión de riesgos – Selección de Salvaguardas

4.4 Diseño y Definición de la Metodología

Luego de analizar los procesos de cada una de las metodologías hemos podido observar que algunos procesos de una metodología coinciden con procesos de otra pero que realizan una misma actividad, motivo por el cual se ha realizado una intersección, misma que se muestra el siguiente cuadro

En la tabla posterior se indica los procesos que coinciden y se define un proceso para nuestra metodología (MACORI).



MAGERIT

Determinación de Objetivos, Estrategias y Políticas de Seguridad de los sistemas de Información

Establecimiento de la Planificación de la seguridad de los Sistemas de Información

Implantación de Salvaguardas y otras medidas de seguridad de los Sistemas de Información

Reacción a cada evento, Registro de incidencias y recuperación de estados de seguridad

Definición de dominio y objetivos

Planificación del proyecto

Recogida de información

Identificación y agrupación de ACTIVOS

Identificación y Evaluación de AMENAZAS

Identificación y evaluación de VULNERABILIDADES

Identificación y valoración de IMPACTOS

Evaluación del RIESGO

Identificación y estimación de funciones de salvaguarda

Selección de funciones de salvaguarda

Cumplimiento de Objetivos

Integración de resultados

Fig. IV. 32. Diagrama de Venn de las Metodologías

COBIT	ISO 17799	MAGERIT	MACORI
Definir un Plan Estratégico de TI	Política de seguridad	• Determinación de Objetivos, Estrategias y Políticas de Seguridad de los sistemas de Información. • Definición de dominio y objetivos	Definir un plan, los objetivos y una política de seguridad.
Definir la Arquitectura de Información		Establecimiento de la Planificación de la seguridad de los Sistemas de Información	Planificación de la seguridad de los Sistemas de Información
• **Determinar la dirección tecnológica.** • **Adquirir y mantener infraestructura tecnológica.** • **Administrar cambios.**			Diseño y mantenimiento de un plan de infraestructura tecnológica.
Definir los procesos, organización y relaciones de TI	Aspectos organizativos para la seguridad.	Planificación del proyecto	Prestación y Organización de servicios
Administrar la inversión en TI.	Clasificación y control de activos.	Identificación y agrupación de ACTIVOS	Análisis y Control de Activos
Comunicar las Aspiraciones y la Dirección de la Gerencia			Comunicar las Aspiraciones y la Dirección de la Gerencia
Administración de recursos humanos.	Seguridad ligada al personal.		Control de Recursos Humanos

• **Evaluación de riesgos** • **Administrar el ambiente físico**	Seguridad física y del entorno.	• Identificación y Evaluación de AMENAZAS • Identificación y evaluación de VULNERABILIDADES • Identificación y valoración de IMPACTOS • Evaluación del RIESGO	Identificación y Evaluación del Riesgo
• **Administración de proyectos** • **Administración de calidad** • **Identificar soluciones automatizadas** • **Definición de niveles de servicio**			Gestionar la calidad de proyectos
Adquirir y mantener software aplicativo	Desarrollo y mantenimiento de sistemas.		Desarrollo y mantenimiento de sistemas.
• **Garantizar la Continuidad del Servicio**	• Gestión de continuidad del negocio.		Establecer planes de contingencia
• **Garantizar la Seguridad de los Sistemas**	• Control de accesos		Control de accesos
• **Administrar la configuración** • **Administrar los datos**	• Gestión de comunicaciones y operaciones.		Gestionar los datos, comunicaciones y operaciones
Educación y entrenamiento de usuarios			Capacitación a los usuarios
Administrar los problemas		• Identificación y estimación de funciones de salvaguarda.	

		• Selección de funciones de salvaguarda. • Implantación de Salvaguardas y otras medidas de seguridad de los Sistemas de Información. • Reacción a cada evento, Registro de incidencias y recuperación de estados de seguridad.	Identificación, selección e implementación de salvaguardas
Monitoreo del Proceso			Monitoreo del Proceso
Garantizar el cumplimiento regulatorio	Conformidad con la legislación		Garantizar el cumplimiento de las leyes
		Recogida de información.	Recogida de información.
		• Cumplimiento de Objetivos • Integración de resultados.	Conclusiones

Tabla. IV. 12. Definición de la metodología

4.4.1 Fases de la Metodología MACORI

MACORI (Metodología de Análisis y Control de Riesgos Informáticos) metodología organizada en cinco fases las mismas que se describen en el siguiente gráfico junto con las principales actividades.

MACORI

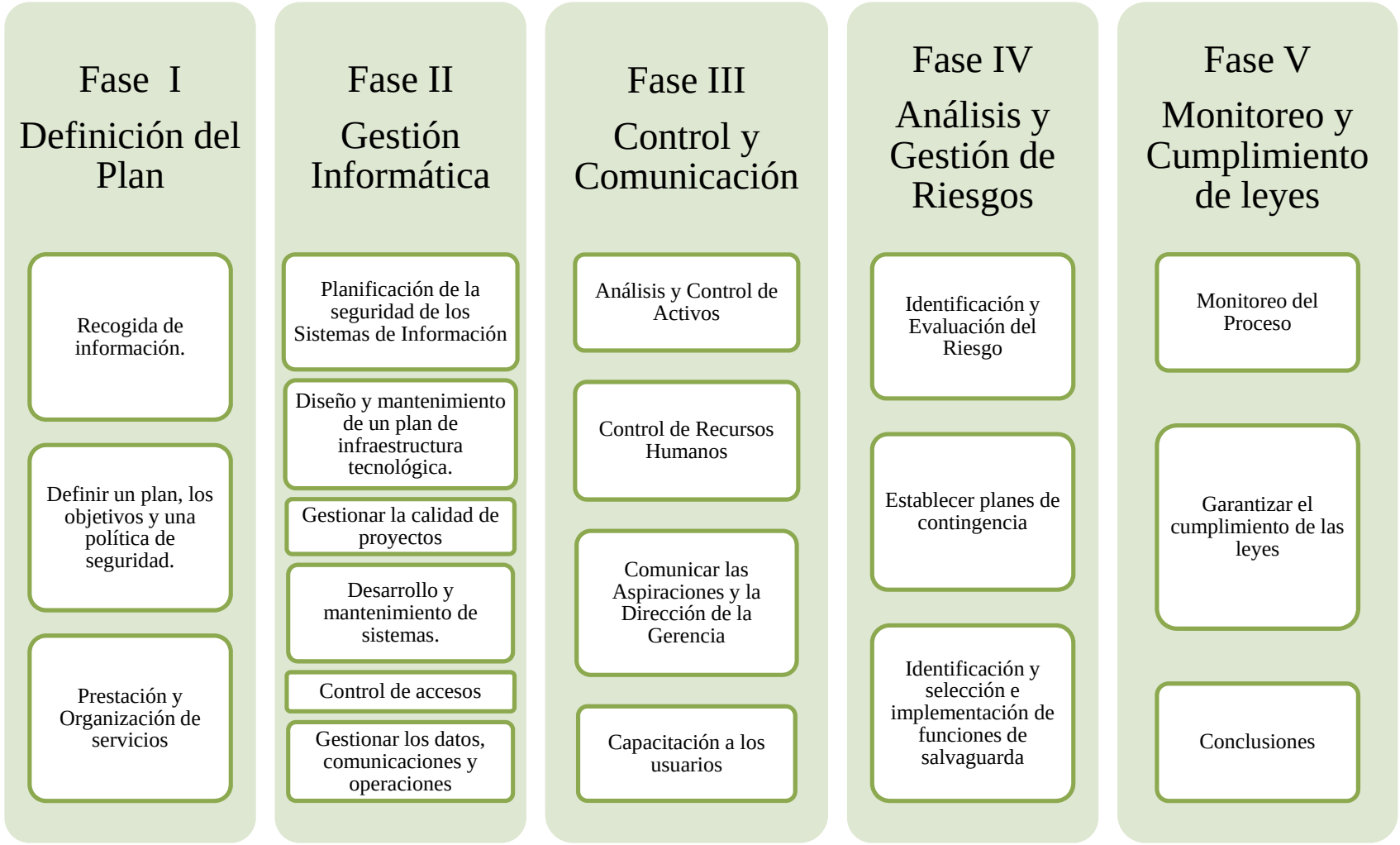


Fig. IV. 33. Fases de la metodología MACORI

El objetivo de cada una de las fases se describe a continuación:

Fase I: Definición del Plan

Crear un plan que defina, en cooperación con los interesados relevantes, como la tecnología de la información contribuirá a los objetivos de la empresa así como detallar la prestación y organización de servicios.

Fase II Gestión Informática

Dotar de la información necesaria en el más amplio nivel de detalle a los usuarios, empleados y jefes, de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red de la organización, así como la información que es procesada y almacenada en estos.

Fase III Control y Comunicación

Clasificar los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos. Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI.

Fase IV Análisis y Gestión de Riesgos

Desarrollar un plan de acción en base a la estrategia de Gestión de riesgos definida por la organización y los resultados del análisis de riegos realizados. Seleccionar e implantar salvaguardas para conocer, prevenir, impedir, reducir y controlar los riesgos identificados.

Fase V Monitoreo y Cumplimiento de leyes

Integrar los requerimientos de seguridad que deben cumplir todos los usuarios de la red bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos del departamento en cuanto al recurso humano, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

Definir indicadores de desempeño y comparar con las metas acordadas e iniciar las medidas correctivas necesarias.

En los siguientes apartados se pueden encontrar una descripción más detallada de las tareas a realizarse correspondientes a cada fase y actividad.

4.4.1.1 FASE I: DEFINICIÓN DEL PLAN

A. RECOGIDA DE INFORMACIÓN

Definir un conjunto de cuestionarios que permita hacer la toma de datos más eficaz, eficiente y homogénea. En la elaboración de los cuestionarios se deberá tener en cuenta tanto las necesidades de la información de la metodología como las adaptaciones particulares realizadas en ella.

Ejemplo de técnicas herramientas y métodos que pueden ser de utilidad para llevar a cabo esta actividad:

- ✓ Cuestionarios
- ✓ Guías para entrevistas
- ✓ Formularios para encuestas
- ✓ Modelos y formatos para los inventarios de cada área((HW, SW, consumibles, documentos, instalaciones, mobiliario y equipo, BD, sistemas)
- ✓ Instrumentos para la evaluación de sistemas
- ✓ Observación
- ✓ Experimentación
- ✓ Examen
- ✓ Inspección
- ✓ Confirmación
- ✓ Comprobación
- ✓ Revisión documental
- ✓ Matriz FODA

B. DEFINIR UN PLAN, LOS OBJETIVOS Y UNA POLÍTICA DE SEGURIDAD.

El trabajo que desarrolla esta actividad lleva en conjunto tres términos importantes:

1. Elaboración del Plan.- El plan será elaborado con el fin de definir las tareas que se tiene a responsabilidad el equipo auditor, en el plan se detallara la fase y la actividad con su fecha de inicio y de fin, de esta manera se obtendrá el tiempo que le llevará la auditoria.

2. Definición de Objetivos.- Se especificará los siguientes:

- **Objetivo general:** Fin global que se pretende alcanzar con el desarrollo de la Auditoría informática en el cual se plantean todos los aspectos que se pretende evaluar. Idea total de lo que se va a cubrir.
- **Objetivos particulares:** Fines individuales que se pretende alcanzar con el desarrollo de la auditoría informática, de un área, sistema o función en particular.
- **Objetivos específicos:** Determinación en forma detallada, de los fines que se pretenden alcanzar con la auditoría informática, señalando concretamente las áreas a evaluar y, específicamente, los sistemas, componentes o elementos concretos que deben ser evaluados.

3. Definición de la Política de Seguridad

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las Políticas de seguridad establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el por qué de ello. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas deben considerar los siguientes elementos:

- ✓ Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a

reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios.

- ✓ Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- ✓ Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- ✓ Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- ✓ Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- ✓ Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las Políticas deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

Algunos parámetros para establecer políticas de seguridad

Recomendamos algunos aspectos generales recomendados para la formulación de las mismas:

- ✓ Considere efectuar un ejercicio de análisis de riesgos informático, a través del cual valore sus activos, el cual le permitirá afinar las políticas de su organización.
- ✓ Involucre a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a la Política.
- ✓ Comunique a todo el personal involucrado en el desarrollo de las políticas, los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

- ✓ Recuerde que es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar los activos críticos de la funcionalidad de su área u organización.
- ✓ Desarrolle un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

C. PRESTACIÓN Y ORGANIZACIÓN DE SERVICIOS

Determinar cómo se encuentra organizado el departamento, con lleva la labor de indagar cuales son los servicios que presta la institución y en exclusividad el departamento en el cual se va a desarrollar el proceso auditivo, así como también averiguar cuál es el proceso que el departamento lleva a cabo para el registro de los mismos.

Crear y actualizar periódicamente la descripción de roles. Estas descripciones deben estar alineadas con la responsabilidad y la autoridad incluyendo definiciones de habilidades y experiencia necesarias en cada posición y que serán aplicables en el uso y evaluación del desempeño.

En esta actividad como en otras nos ayuda a verificar los requerimientos del usuario y el cumplimiento de los objetivos de la empresa y en este caso del departamento.

4.4.1.2 FASE II GESTIÓN INFORMÁTICA

A. PLANIFICACIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Los objetivos de esta actividad consisten en:

- ✓ Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
- ✓ Fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información.
- ✓ Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

Desarrollo de Aplicaciones:

- ✓ Planificar, coordinar y supervisar las actividades de análisis, diseño, desarrollo, mantenimiento y administración de aplicaciones que brinde nuevos servicios tecnológicos.
- ✓ Elaborar los términos de referencia para la estructuración de los proyectos en el área de desarrollo de aplicaciones.
- ✓ Probar la funcionalidad de las aplicaciones especializadas que se encuentran activas.

Para el desarrollo, mantenimiento o adquisición de software de aplicación el departamento debe disponer de un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas, que debe estar documentado y aprobado, y debe aplicarse en forma complementaria a las normas relativas a administración de proyectos.

Debe contemplar procedimientos detallados, mínimamente para:

- ✓ La formulación y documentación de requerimientos por parte de las áreas usuarias, ya sea para nuevos desarrollos, adquisiciones o cambios a los sistemas existentes, incluyendo la definición detallada de las necesidades que motivan el requerimiento y la especificación de los niveles de servicio esperados.
- ✓ El criterio para el establecimiento de prioridades entre los distintos requerimientos recibidos por el departamento.
- ✓ La aprobación por parte de los responsables de las áreas usuarias afectadas, de las especificaciones de diseño elaboradas.
- ✓ La participación de la unidad de auditoría interna durante el desarrollo.
- ✓ La utilización de estándares de diseño, programación y documentación.
- ✓ La realización de pruebas suficientes en las distintas etapas del desarrollo, conforme a un plan de pruebas y de control de calidad aprobado, en un ambiente específico representativo del ambiente operativo futuro y distinto del ámbito de producción.
- ✓ El control de las versiones del software por parte del área responsable de las tareas de desarrollo y mantenimiento de sistemas.
- ✓ La preparación de documentación de soporte para el usuario y el personal técnico.

- ✓ La contratación de servicios externos de desarrollo de sistemas debe estar justificada por escrito y autorizada por el responsable del departamento. El contrato debe estipular que el software, la documentación y demás ítems adquiridos se sometan a prueba y revisión antes de la aceptación por parte de la unidad y de las áreas usuarias.

Técnicas para asegurar el sistema

- ✓ Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.
- ✓ Vigilancia de red. Zona desmilitarizada
- ✓ Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

Seguridad de los sistemas de información y de datos

La seguridad de la información abarca muchas cosas, pero todas estas giran en torno a la información. Por ejemplo la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

Precisamente los riesgos es uno de los mayores problemas en la seguridad, ya que de TI debe de tener tres planos uno en el peor de los casos, otro un estado medio y un estado favorable. Ya que de esta manera se podrá mitigar el daño que se pueda provocar por que ya se tomaron medidas. No se puede decir que la seguridad teda un 100% de tranquilidad ya que cada día aparece un código nuevo o un ataque diferente, etc. pero tienes menos conflictos y un sistema en condiciones de producir.

Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

El termino Seguridad de Información, persiguen una misma finalidad al proteger la Confidencialidad, Integridad y Disponibilidad de la información; sin embargo, entre ellos

existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.

Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

Cabe mencionar que la seguridad es un proceso continuo de mejora por lo que las políticas y controles establecidos para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos.

Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal. .

Confidencialidad

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información.

Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La Alta disponibilidad sistemas objetivo debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque Denegación de servicio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

Sistemas informativos manuales

Para la información que se recaba en formatos no computarizados, la seguridad tendrá que aplicarse a sistemas de oficina ordinarios, a través de:

- ✓ Registros sobre la información y los documentos recibidos;
- ✓ El llenado correcto de los documentos y almacenarlos de forma segura;
- ✓ Conservar copias de documentos importantes de forma separada;
- ✓ Control del acceso a los documentos.

Sistemas informativos computarizados

Las medidas de seguridad tendrán que ser más complejas para los sistemas informativos computarizados, especialmente cuando se usen para producir o procesar el material electoral, para calcular el total de votos o los resultados de la elección. Se deberían realizar análisis de riesgo para determinar el método más efectivo para garantizar la seguridad de la información.

Las medidas de seguridad básicas que se podrían aplicar incluyen:

- ✓ Que los edificios en donde se encuentre el equipo de computación o de comunicaciones (instalaciones de microondas o cables ópticos), cuenten con una seguridad física adecuada, que incluya protección contra intervención humana o desastres naturales (inundación, incendio);

- ✓ Servicios de respaldo o de recuperación en caso de que el sistema falle, incluyendo suministro eléctrico, ligas de telecomunicaciones, equipo y programas de cómputo, así como métodos manuales que permitan obtener el mismo resultado en caso de que los sistemas de cómputo no reaccionen; también es de utilidad tomar algunas sencillas precauciones, como respaldar diariamente toda la información de los sistemas y almacenarla en otro lugar;
- ✓ Revisar de forma minuciosa todos los aspectos de los sistemas bajo condiciones de producción, antes de que sean introducidos;
- ✓ Establecer controles para acceder a los programas y a la información, para evitar que personas externas sin autorización accedan a ellos (para piratearlos), o que intenten manipular la configuración de los sistemas, los códigos de los programas o la información registrada;
- ✓ Garantizar que la capacitación del personal permita que puedan usar las computadoras y los programas que deberían usar, para que no se presenten pérdidas de datos o daños accidentales a los sistemas;
- ✓ Asegurar que todo el personal conozca las medidas de seguridad que deben aplicar.

B. DISEÑO Y MANTENIMIENTO DE UN PLAN DE INFRAESTRUCTURA TECNOLÓGICA.

El objetivo de esta tarea es: Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información; Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en los cuales éstos se apoyan; Definir los métodos de protección de información crítica.

Infraestructura Tecnológica y Soporte al Usuario

Para la infraestructura tecnología y el soporte al usuario incluye las siguientes tareas:

- ✓ Responsable de garantizar el óptimo funcionamiento de la infraestructura tecnológica y asegurar la disponibilidad de los equipos informáticos.

- ✓ Brindar soporte técnico, operativo y personalizado para la solución de problemas presentados a los clientes en hardware y software.
- ✓ Analizar y definir con otras áreas las necesidades de hardware que permitan optimizar las actividades realizadas por las mismas.
- ✓ Supervisar y administrar el correcto funcionamiento de los equipos y servicios informáticos.
- ✓ Coordinar la realización del mantenimiento preventivo y correctivo de equipos informáticos que se encuentren fuera de garantía.
- ✓ Investigar, evaluar y recomendar para la innovación y nuevos avances de hardware y herramientas al desarrollo tecnológico.
- ✓ Evaluar las ofertas presentadas para la adquisición de nuevo hardware basándose en la investigación de la nueva tecnología.

C. GESTIONAR LA CALIDAD DE PROYECTOS

La gestión de la calidad del proyecto es necesario aplicar en cada proyecto durante todas sus fases que lo conforman.

- ✓ Identificando cuáles estándares de calidad son relevantes al proyecto y determinando cómo satisfacerlos.
- ✓ Evaluando el desempeño total del proyecto sobre la base de sus actividades (¿cómo lo estamos haciendo?) para proveer la seguridad de que el proyecto satisfará dichos estándares de calidad.
- ✓ Monitoreando los resultados del proyecto sobre la base de sus entregables (¿cómo está lo que produjimos?) para determinar si cumple con los estándares de calidad e identificando la manera de eliminar causas de desempeño insatisfactorio.

La Gestión de Calidad de un proyecto, está formada por tres procesos que se encargan de definir todas las actividades para determinar las políticas, los objetivos y las responsabilidades relativos a la calidad, de modo que el proyecto satisfaga las necesidades por las cuales se realizará.

Los 3 procesos que abarca la Gestión de Calidad son:

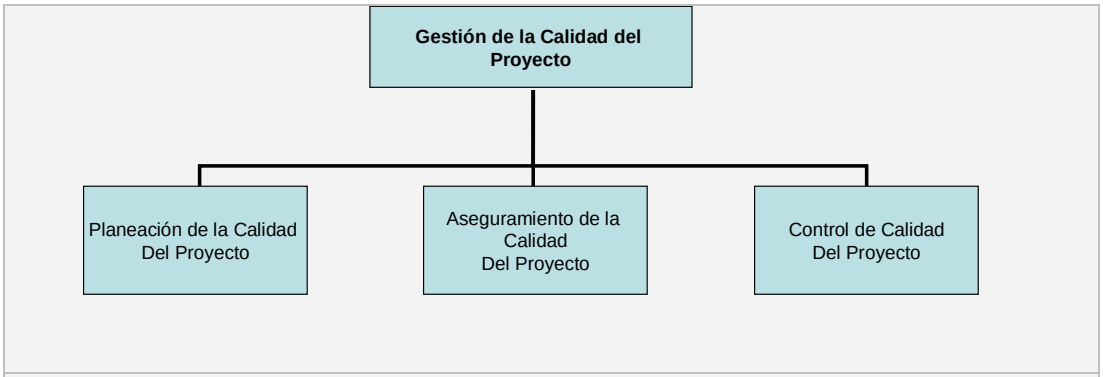


Fig. IV. 34. Gestión de la Calidad del Proyecto

Planeación de la calidad del proyecto.- El primer proceso de la gestión de calidad, la planificación, permite identificar que normas de calidad pueden ser aplicadas en el proyecto y determina como satisfacerlas. Incluye identificar los principales estándares de calidad en el proyecto y establecer la manera de satisfacerlos. A continuación se presenta un esquema gráfico de los insumos para la planeación de la calidad y las salidas generadas en el proceso.

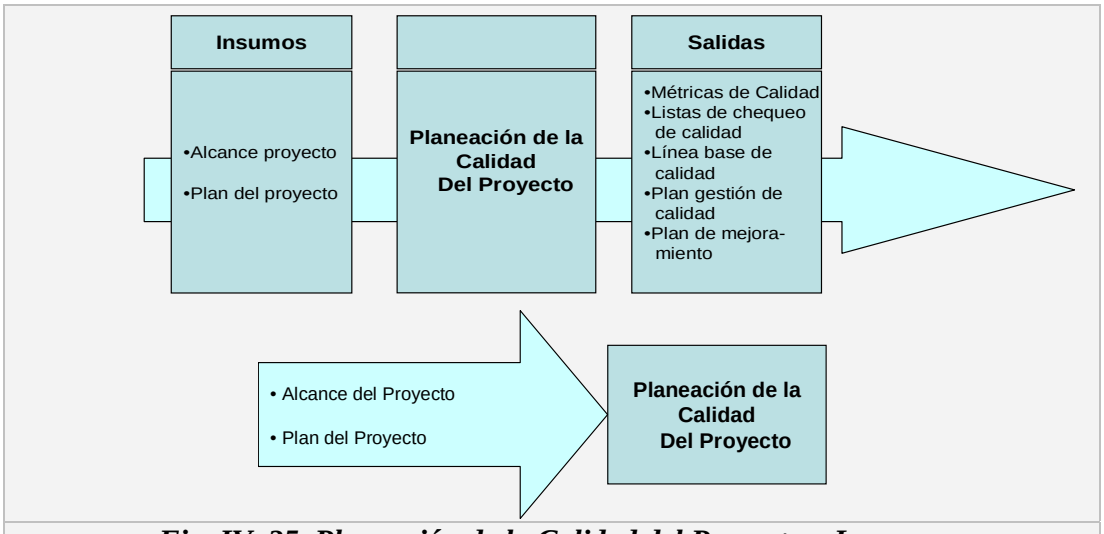


Fig. IV. 35. Planeación de la Calidad del Proyecto – Insumos

Alcance del Proyecto. El alcance es un insumo muy importante para la planeación de la calidad. Debe incluir los principales entregables del proyecto y los objetivos del mismo.

Plan del Proyecto. Provee todos los planes que sirvan para ejecutar, monitorear y controlar el proyecto, e incluye también los planes subsidiarios que proporcionan guía y dirección para la planeación de la calidad del proyecto.

Es importante también considerar otros insumos para la planeación de la calidad como los procesos organizacionales existentes (políticas de calidad de la Compañía y el Sistema de Gestión de Calidad) y los factores ambientales organizacionales como guías, estándares y regulaciones que puedan afectar el proyecto.

Técnicas para la planeación de la calidad

El proceso de planeación de la calidad debe considerar:

- ✓ Analizar el costo/beneficio sobre el costo de las actividades de calidad y el beneficio que producen en el desarrollo del proyecto y sus entregables.
- ✓ Comparar las prácticas de proyectos anteriores que generen ideas para mejorar y proveer un estándar por el cual medir su funcionamiento.
- ✓ Realizar experimentos como modelos o pilotos que permitan aumentar la calidad del producto final por diferentes acciones definidas como resultado del experimento.
- ✓ Total de costos en que se ha incurrido para alcanzar la calidad del producto y/o servicio.

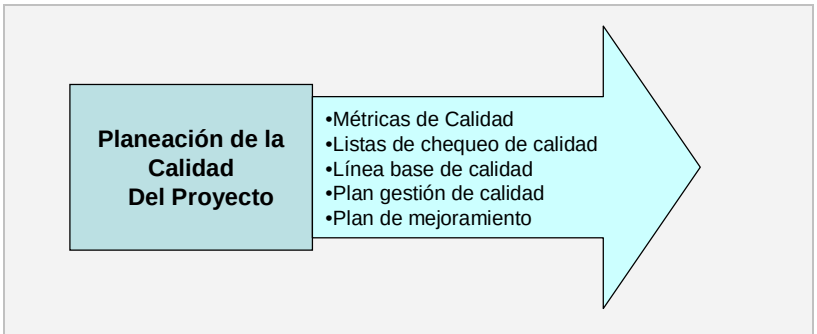


Fig. IV. 36. Planeación de la Calidad del Proyecto – Salidas

Métricas de calidad. Que describan específicamente cómo son las actividades y cómo son medidas por el proceso de control de la calidad.

Métricas de Calidad - Proceso XXXXX						
Descripción Actividad	Fecha Inicio	Fecha Finalización	Disponibilidad	Cobertura Pruebas		Evaluación Fallas
				Funcionales	Técnicas	
OBSERVACIONES: Realizado Por:						

Fig. IV. 37. Métricas de Calidad

Listas de chequeo de calidad. Que permitan verificar que se han realizado un conjunto de pasos necesarios para cumplir alguna actividad del proyecto.

Listas de Chequeo - Proceso XXXXX						
Objeto :						
DESCRIPCIÓN ACTIVIDAD	Composición Actividad			Actividad Cumplida		PROBLEMA PRESENTADO
	Paso 1	Paso 2	Paso N	SI	NO	
OBSERVACIONES: Realizado Por:				Revisado Por:		Aprobado Por:

Fig. IV. 38. Lista de chequeo

Línea base de calidad. Que registre los objetivos de calidad del proyecto.

Plan de gestión de calidad. Debe describir la forma como el equipo de la gerencia del proyecto implementará sus políticas de calidad. Es decir, describir la estructura

organizacional, responsabilidades, procedimientos, procesos, y recursos necesarios para implementar la gestión de la calidad.

Plan de mejoramiento. El mejoramiento de la calidad incluye tomar acciones para incrementar la eficacia y eficiencia del proyecto para proveer beneficios adicionales a los interesados del proyecto. El plan debe incluir el propósito, comienzo y fin del proceso, sus entradas y salidas, un diagrama de flujo de los procesos y guías de las actividades de mejoramiento.

Aseguramiento de la calidad del proyecto.- El aseguramiento de la calidad debe proveer la confianza de que el proyecto satisfará los estándares de calidad. El aseguramiento puede ser proporcionado al equipo del proyecto o a otros interesados que no estén activamente involucrados en el trabajo del proyecto. A continuación se presenta un esquema gráfico de los insumos para el aseguramiento de la calidad y las salidas generadas en el proceso.

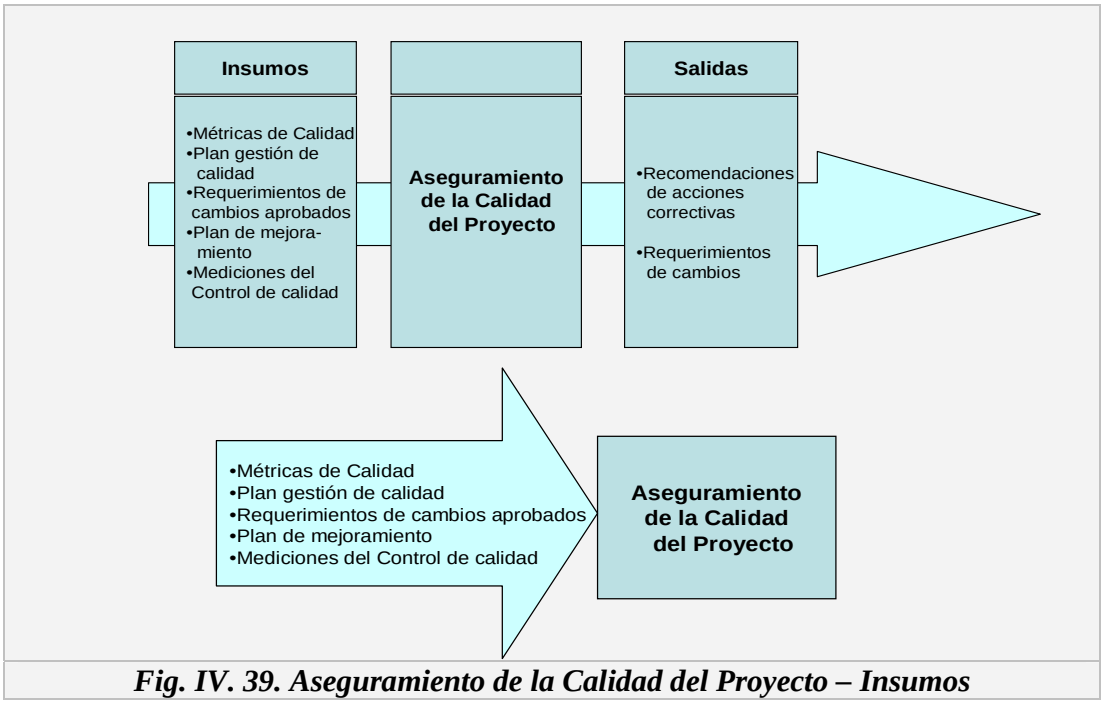


Fig. IV. 39. Aseguramiento de la Calidad del Proyecto – Insumos

Mediciones del control de calidad. Corresponde a los registros de las pruebas y mediciones del control de calidad para su comparación y análisis.

Mediciones de Control de Calidad											
OBJETIVO	INDICADOR	CUANTIFICADOR (INDICE)	META	PERIODO 1		PERIODO 2		PERIODO	
				Medición	Eficacia	Medición	Eficacia	Medición	Eficacia
Contribuír al mejoramiento continuo de la eficacia del sistema	Eficacia	Cambios implementados							
		# cambios implementados / # total cambios aprobados							
	Eficiencia	Porcentaje de indicadores cumplidos / total indicadores							
		Porcentaje entregables oportunos / total entregables							
	Calidad del servicio	Auditorías Internas de Calidad							

Fig. IV. 40. Mediciones de Control de Calidad

Requerimientos de cambios aprobados. Los cambios que tengan algún efecto sobre el plan de gestión de la calidad y que incluyan modificaciones a los métodos de trabajo, requerimientos y calidad del producto y/o servicio, alcance y cronograma del proyecto.

Es importante también considerar como insumos dentro del proceso de aseguramiento de la calidad del proyecto, la implementación de:

- ✓ Cambios
- ✓ Acciones correctivas
- ✓ Acciones preventivas
- ✓ Reparaciones a productos defectuosos.

Técnicas para el aseguramiento de la calidad

El aseguramiento de la calidad incluye revisiones, análisis y auditorias a las actividades del proyecto, con el fin de identificar las lecciones aprendidas que puedan mejorar el desempeño del proyecto.

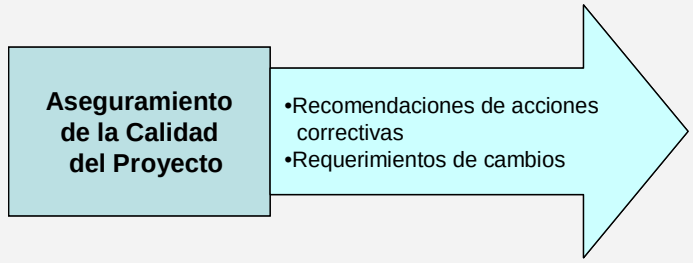


Fig. IV. 41. Técnicas para el aseguramiento de la calidad – Salidas

Recomendaciones de acciones correctivas. Resultado de actividades de aseguramiento de la calidad, como auditorias o análisis de procesos.

Requerimientos de cambios. Cambios que permitan incrementar la eficiencia y eficacia de las políticas, procesos y procedimientos dentro de la organización. Es importante también considerar como salidas dentro del proceso de aseguramiento de la calidad del proyecto las actualizaciones realizadas al plan del proyecto.

Control de calidad del proyecto

El tercer y último proceso, el control de Calidad, implica supervisar los resultados específicos del proyecto, para determinar si cumplen los estándares de calidad relevantes e identificar los modos de eliminar las causas de resultados insatisfactorios. En otras palabras, es la revisión de todas las técnicas aplicadas en el segundo proceso, para asegurar de que fueron bien implementadas. A continuación se presenta un esquema gráfico de los insumos para el control de calidad y las salidas generadas en el proceso.

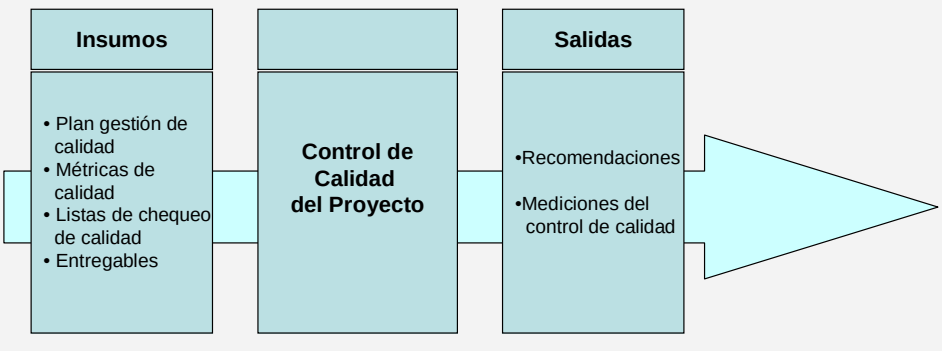


Fig. IV. 42. Control de Calidad del Proyecto

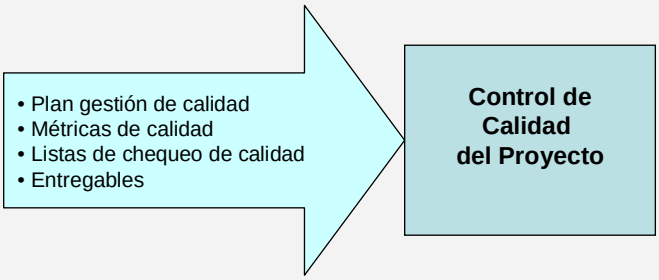


Fig. IV. 43. Control de Calidad del Proyecto – Insumos

Entregables. Proveen información sobre el resultado del proyecto.

Es importante también considerar como insumos dentro del proceso de control de calidad los cambios aprobados y los procesos organizacionales existentes que incluyan las políticas de calidad y el sistema de gestión de calidad.

Técnicas de control de calidad

Realizar actividades de inspección, revisión y/o auditorias incluye medir, examinar y probar las acciones a emprender para determinar si los resultados del producto y/o servicio están conforme a los requisitos.

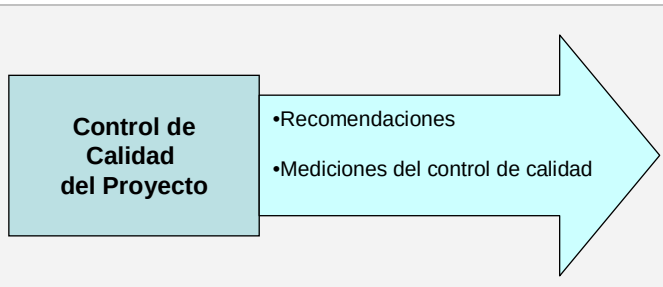


Fig. IV. 43. Control de Calidad del Proyecto – Salidas

Recomendaciones: Como resultado del control de calidad surgirán una serie de recomendaciones sobre:

- ✓ Requerimientos de cambios

- ✓ Acciones correctivas
- ✓ Acciones preventivas
- ✓ Reparaciones a productos defectuosos.

Es importante también considerar como salidas dentro del proceso de control de calidad del proyecto las actualizaciones al plan del proyecto y a las políticas de calidad.

Cada uno de los procesos están formados principalmente por entradas, herramientas, técnicas y salidas. Sin embargo es importante especificar que estos 3 procesos se relacionan entre sí. Básicamente, las salidas del proceso de Planificación de Calidad, sirven de entrada para los otros dos procesos. De igual modo, las salidas del proceso de Aseguramiento de Calidad sirven como entradas del último proceso.

La gestión de la calidad no solo implica gestionar la calidad del producto del proyecto sino también administrar la calidad de la gestión del proyecto como tal. Esto quiere decir que dentro de la gestión de calidad debemos ir mejorando continuamente el proceso de gestión de los proyectos en la organización reduciendo las actividades inútiles y que no agregan valor, permitiendo así un proceso más eficiente y efectivo.

D. DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

Abarca los siguientes puntos:

- ✓ Construir soluciones integrales (aplicaciones) a las necesidades de información de los usuarios.
- ✓ Usar las técnicas de construcción de sistemas de información orientadas netamente a la productividad del personal y a la satisfacción plena para el usuario.
- ✓ Construir equipos de trabajo con la participación del usuario y del personal técnico de acuerdo a metodologías establecidas.
- ✓ Mantener actualizado los sistemas de información de acorde a los cambios de especificaciones producidas en el medio interno y/o externo de la organización, teniendo presente la seguridad de la misma.

- ✓ Mantener comunicados a los usuarios y a sus colaboradores de los avances, atrazos y problemas que se presentan rutinariamente y cuando sea necesario a través de medios establecidos formalmente, como el uso de correo electrónico, mensajes relámpagos o flash.
- ✓ Mantener programas de capacitación para el personal técnico y usuarios.

El Servicio de Desarrollo y Mantenimiento de Sistemas realizará las siguientes actividades puntuales:

- ✓ Administrar el personal técnico, velar por su nivel y capacidad de servicio.
- ✓ Definir y mantener procedimientos operativos en las actividades de desarrollo y mantenimiento de sistemas de información de acuerdo a metodologías integradas, como las elaboradas por el Instituto Nacional de Estadística e Informática.
- ✓ Elaborar planes de trabajo/planes de sistemas, acorde a los objetivos de la organización en el uso de la informática y los servicios que presta.
- ✓ Elaborar y mantener estándares de desarrollo y mantenimiento de aplicaciones, que contemplen las normas de calidad internacional y mediante el uso de metodologías estándares.
- ✓ Evaluar el software orientado a la solución de las necesidades de los usuarios.
- ✓ Especificaciones de proceso y manejo de datos.
- ✓ Uso de Lenguajes de Programación apropiados a los problemas de estándares establecidos. Establecer el plan de prueba de sistemas de información.
- ✓ Realizar seguimientos a las actividades de desarrollo y mantenimiento.
- ✓ Elaborar rutas de operación de sistemas para uso interno y externo de los usuarios.
- ✓ Resolver problemas técnicos en el uso de software.

El recurso humano que está involucrado en esta actividad son:

Jefe de Proyecto Informático: Es la persona encargada de administrar un proyecto informático en todas sus etapas y el responsable de su éxito o fracaso.

Analista de Sistemas de Información: Encargado de la parte inicial del desarrollo de sistemas, efectuando el análisis del sistema de información a desarrollar en base a la información proporcionada por los usuarios que requieran dicha aplicación.

Analista - Programador: Es la persona que aprende de forma práctica las diferentes técnicas de análisis y diseño, y posteriormente trabaja independientemente en el desarrollo de sistemas informáticos, es decir, es una persona que realiza labores de análisis y también de programación.

Programador: Es la persona que usando herramientas de programación y en base al modelo presentado por el analista de sistemas realiza programas para diferentes usuarios.

E. CONTROL DE ACCESOS

Los objetivos que se quiere cumplir en esta actividad son:

- ✓ Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- ✓ Implementar seguridad en los accesos de usuarios por medio de técnicas de identificación y autenticación.
- ✓ Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.
- ✓ Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- ✓ Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- ✓ Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Realizar el control de acceso a la información significa seleccionar o filtrar los usuarios que pueden acceder a recursos informáticos. Los sistemas que permiten el acceso a todos los

usuarios y únicamente protegen de ataques de destrucción (denegación de servicios) no se pueden considerar control de accesos aunque si son parte de la seguridad y muchos autores los incluyen en este capítulo.

Es el servicio de seguridad que previene el uso de un recurso salvo en los casos y en la manera autorizados.

Es una función de seguridad esencial para proteger los datos y los tratamientos de posibles manipulaciones no autorizadas. Intervienen diversos componentes: identificación y autenticación de usuarios, autorización de derechos de acceso a distintos recursos del sistema, acceso a redes, sistemas, aplicaciones y datos, y el control y auditoría del acceso.

Su importancia es clave en el control de la seguridad. Por ello, los Criterios le dedican una amplia atención. Partiendo del análisis de las necesidades reales que tiene la Organización y sus componentes, se decidirán, aplicarán y verificarán los niveles de acceso de cada usuario.

Es pertinente mantener y revisar dichos niveles periódicamente, con el fin de evitar distorsiones en nuestro sistema, prestando especial atención a los accesos más privilegiados. El criterio de necesidad de uso es el que debe regir la asignación de dichos privilegios. Restricciones horarias, restricciones contra la copia, mantener un registro de eventos relativos al control de acceso, interrumpir la sesión automáticamente después de un período de tiempo sin que el usuario haya realizado ninguna acción, son otras posibles medidas encaminadas al control de accesos, que es una de las piedras angulares de la gestión de la seguridad.

Además, se adoptarán medidas excepcionales para los equipos portátiles y el acceso de terceras personas.

F. GESTIONAR LOS DATOS, COMUNICACIONES Y OPERACIONES

La meta a cumplir en esta actividad es:

- ✓ Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones
- ✓ Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

La unidad de informática, o personal de la misma dedicado o asignado en el área de programación o planificación y desarrollo de sistemas, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para el departamento a ser auditado.

La aceptación del software se hará efectiva por los jefes del departamento, previo análisis y pruebas efectuadas por el personal de informática.

Se verificará la utilización de software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.

El software diseñado localmente o llámese de otra manera desarrolladas por programadores internos, deberán ser analizados y aprobados, por el gestor de seguridad, antes de su implementación.

Verificar la tarea de los programadores el realizar pruebas de validación de entradas, en cuanto a:

- ✓ Valores fuera de rango.
- ✓ Caracteres inválidos, en los campos de datos.
- ✓ Datos incompletos.
- ✓ Datos con longitud excedente o valor fuera de rango.
- ✓ Datos no autorizados o inconsistentes.
- ✓ Procedimientos operativos de validación de errores
- ✓ Procedimientos operativos para validación de caracteres.
- ✓ Procedimientos operativos para validación de la integridad de los datos.

- ✓ Procedimientos operativos para validación e integridad de las salidas.

Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

Comprobar la existencia de la documentación de cada uno de los sistemas desarrollados en el departamento.

Verificar que se adquiera software únicamente de fuentes confiables y en caso contrario, este se adquirirá en código fuente.

Los servidores, al igual que las estaciones de trabajo, deberán tener instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la institución, deberán ser etiquetados de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.

Deberá ser llevado un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

4.4.1.3 FASE III CONTROL Y COMUNICACIÓN

A. ANÁLISIS Y CONTROL DE ACTIVOS

Los objetivos a cumplir en esta actividad son:

- ✓ Garantizar que los activos de información reciban un apropiado nivel de protección.
- ✓ Designar a los propietarios de la información existente en el Organismo.
- ✓ Clasificar la información para señalar su sensibilidad y criticidad.
- ✓ Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación

Es preciso realizar y mantener un inventario de los activos a proteger, identificando a sus propietarios y documentando en el caso de activos de información los usuarios a los que se autoriza el acceso, especialmente en el caso de ficheros con datos de carácter personal.

El activo esencial: información (datos)

- ✓ Los servicios
- ✓ Las aplicaciones informáticas *(software)*
- ✓ Los equipos informáticos *(hardware)*
- ✓ Los soportes de información
- ✓ El equipamiento auxiliar
- ✓ Las redes de comunicaciones
- ✓ Las instalaciones
- ✓ Las personas

Capa 1: El entorno: activos que se precisan para garantizar las siguientes capas

- ✓ Equipamiento y suministros: energía, climatización, comunicaciones
- ✓ Personal: de dirección, de operación, de desarrollo, etc.
- ✓ Otros: edificios, mobiliario, etc.

Capa 2: El sistema de información propiamente dicho

- ✓ Equipos informáticos *(hardware)*
- ✓ Aplicaciones *(software)*
- ✓ Comunicaciones
- ✓ Soportes de información: discos, cintas, etc.

Capa 3: La información

- ✓ Datos
- ✓ Meta-datos: estructuras, índices, claves de cifrado, etc.

Capa 4: Las funciones de la Organización, que justifican la existencia del sistema de información y le dan finalidad

- ✓ Objetivos y misión
- ✓ Bienes y servicios producidos

Capa 5: Otros activos

- ✓ Credibilidad o buena imagen
- ✓ Conocimiento acumulado
- ✓ Independencia de criterio o actuación
- ✓ Intimidad de las personas
- ✓ Integridad física de las personas

B. CONTROL DE RECURSOS HUMANOS

Lo que se pretende con esta actividad es:

- ✓ Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y manejo no autorizado de la información
- ✓ Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal, incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
- ✓ Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

- ✓ Establecer Acuerdos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- ✓ Establecer las herramientas necesarias para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Como fácilmente puede apreciarse, el esfuerzo humano resulta vital para el funcionamiento de cualquier organización; si el elemento humano está dispuesto a proporcionar su esfuerzo, la organización marchará; en caso contrario, se detendrá. De aquí a que toda organización debe prestar primordial atención a su personal.

No hay duda de que muchos trabajadores por lo general están insatisfechos con su empleo actual o con el clima organizacional imperante en un momento determinado y eso se ha convertido en una preocupación para muchos gerentes. Tomando en consideración los cambios que ocurren en la fuerza de trabajo, estos problemas se volverán más importantes con el paso del tiempo.

Todos los gerentes deben actuar como personas claves en el uso de técnicas y conceptos de administración de personal para mejorar la productividad y el desempeño en el trabajo. Pero aquí nos detenemos para hacernos una pregunta: *¿Pueden las técnicas de administración de recursos humanos impactar realmente en los resultados de una compañía?* La respuesta es un "SI". En el caso de una organización, la productividad es el problema al que se enfrenta y el personal es una parte decisiva de la solución. Las técnicas de la administración de personal, aplicadas tanto por los departamentos de administración de personal como por los gerentes de línea, ya han tenido un gran impacto en la productividad y el desempeño.

Aun cuando los activos financieros, de equipamiento y de planta son recursos necesarios para la organización, los empleados – el recurso humano – tienen una importancia sumamente considerable. Los recursos humanos proporcionan la chispa creativa en cualquier organización. La gente se encarga de diseñar y producir los bienes y servicios, de

controlar la calidad, de distribuir los productos, de asignar los recursos financieros, y de establecer los objetivos y estrategias para la organización. Sin gente eficiente es imposible que una organización logre sus objetivos. El trabajo del gerente de recursos humanos es influir en esta relación entre una organización y sus empleados.

C. COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA

Los objetivos que se desea cumplir con esta actividad son:

- ✓ Definir y comunicar las políticas
- ✓ Implementar programa de comunicación continua
- ✓ Asegura la concienciación y el entendimiento de los riesgos del negocio
- ✓ Debe garantizar l cumplimiento de leyes y reglamentos relevantes.

Lo que se pretende en esta actividad es satisfacer los requerimientos de negocio para que la información precisa y oportuna sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades se enfoquen en proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de trabajo de control de TI.

D. CAPACITACIÓN A LOS USUARIOS

Los analistas de sistemas se involucran en un proceso educacional con los usuarios que es llamado capacitación. A lo largo del ciclo de vida de desarrollo de sistemas los usuarios han estado involucrados, por lo que ahora el analista debe poseer una valoración adecuada de los usuarios que deben ser capacitados. Tal como hemos visto, los centros de información mantienen instructores propios.

En la implementación de grandes proyectos, el analista estafa frecuentemente analizando la capacitación en vez de estar personalmente involucrado en él. Uno de los valores más preciados que puede dar el analista a cualquier situación de capacitación es la capacidad de ver el sistema desde el punto de vista del usuario. El analista nunca debe olvidar qué es el enfrentar un nuevo sistema. Estos recuerdos pueden ayudar a que el analista empatase con los usuarios y facilite su capacitación.

El analista tiene cuatro lineamientos principales para ajustar una capacitación. Son:

1. Establecimiento de objetivos mensurables.
2. Uso de métodos de capacitación adecuados.
3. Selección de lugares de capacitación adecuados.
4. Empleo de materiales de capacitación comprensibles.

En la figura 21.16 se proporciona un resumen de consideración para los objetivos, métodos, lugares y materiales de capacitación.

Elementos	Factores Relevantes
Objetivos de la capacitación. Métodos de capacitación.	Dependen de los requerimientos del trabajo del usuario. Dependen del trabajo del usuario, personalidad conocimientos y experiencias; use una combinación de pláticas, demostraciones, práctica y estudio.
Sitios de capacitación	Depende de los objetivos de la capacitación, costo, disponibilidad; sitios gratis de vendedor con equipo operable; instalación en casa; instalaciones rentadas
Materiales de capacitación	Depende de las necesidades del usuario; manuales de operación, casos, prototipos de equipo y salida; tutoriales en línea.

Tabla. IV. 13. Capacitación a los Usuarios

4.4.1.4 FASE IV ANÁLISIS Y GESTIÓN DE RIESGOS

A. IDENTIFICACIÓN Y EVALUACIÓN DEL RIESGO

Los objetivos planteados para esta actividad son:

- ✓ Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

- ✓ Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
- ✓ Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.
- ✓ Implementar medidas para proteger la información manejada por el personal en las oficinas en el marco normal de sus labores habituales.
- ✓ Proporcionar protección proporcional a los riesgos identificados.

Análisis de riesgo informático

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: *"lo que no está permitido debe estar prohibido"* y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

3. Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

1. Construir un perfil de las amenazas que esté basado en los activos de la organización.

2. Identificación de los activos de la organización.

3. Identificar las amenazas de cada uno de los activos listados.

4. Conocer las prácticas actuales de seguridad

5. Identificar las vulnerabilidades de la organización.

   - ✓ Recursos humanos
   - ✓ Recursos técnicos
   - ✓ Recursos financieros

6. Identificar los requerimientos de seguridad de la organización.

7. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.

8. Detección de los componentes claves

9. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:

- ✓ Riesgo para los activos críticos
- ✓ Medidas de riesgos
- ✓ Estrategias de protección
- ✓ Planes para reducir los riesgos.

B. ESTABLECER PLANES DE CONTINGENCIA

Los objetivos a cumplir en esta actividad son:

- ✓ Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
- ✓ Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- ✓ Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias.

Un plan de contingencia el conjunto de procedimientos alternativos a la operativa normal de cada empresa, cuya finalidad es la de permitir el funcionamiento de ésta, aún cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización.

El Plan de Contingencia Informático (o Plan de Contingencia Institucional) implica un análisis de los posibles riesgos a cuales pueden estar expuestos nuestros equipos de cómputo y sistemas de información. Corresponde aplicar al Centro de Informática y

Telecomunicaciones, aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

El Plan de Contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre.

La información como uno de los activos más importantes de la Organización, es el fundamento más importante de este Plan de Contingencia.

La orientación principal de un plan de contingencia es la continuidad de las operaciones de la empresa, no sólo de sus sistemas de información.

Su elaboración la podemos dividir en cuatro etapas:

a. Evaluación.

b. Planificación.

c. Pruebas de viabilidad.

d. Ejecución.

e. Recuperación.

Las tres primeras hacen referencia al componente preventivo y las últimas a la ejecución del plan una vez ocurrido el siniestro.

Cada etapa está dividida a su vez en subetapas que se detallan y explican en siguientes entregas.

Evaluación:

1. Constitución del grupo de desarrollo del plan.

Este grupo debe estar liderado por un responsable del plan y formado por los líderes de las áreas que se desean cubrir con dicho plan. Su elaboración ha de desarrollarse con la continua supervisión por parte de la dirección ya que durante la elaboración y/o ejecución de éste, deberán comprometerse recursos y aprobarse procedimientos especiales que requieran un nivel de autorización superior.

2. Identificación de las funciones críticas.

Esta subfase consiste en identificar aquellos elementos de nuestra empresa o funciones que puedan ser críticos ante cualquier eventualidad o desastre y jerarquizarlos por orden de importancia dentro de la organización.

3. Definición y documentación de los posibles escenarios con los que podemos encontrarnos para cada elemento o función crítica.

Puede tratarse de problemas en el hardware, software de base, de telecomunicaciones, software de aplicación propio o provisto por terceros, etc. También deben incluirse en esta categoría los siniestros provocados por incendios, una utilización indebida de medios magnéticos de resguardo o back up o cualquier otro daño de origen físico que pudiera provocar la pérdida masiva de información. También incluimos en este apartado todos aquellos problemas asociados con la carencia de fuentes de energía y de telecomunicaciones.

4. Análisis del impacto del desastre en cada función crítica.

Consiste en realizar un análisis del impacto de cada problema sobre cada una de las funciones críticas de la organización, teniendo en cuenta las siguientes prioridades:

- ✓ Evitar pérdidas de vida.
- ✓ Satisfacer las necesidades básicas.
- ✓ Reanudar las operaciones lo antes posible.
- ✓ Proteger el medio ambiente.

- ✓ Lograr las conexiones con los principales clientes y proveedores.
- ✓ Mantener la confianza en la empresa.

Una correcta cuantificación del impacto económico de cada problema ayudará a una correcta selección de la solución alternativa.

5. Definición de los niveles mínimos de servicio.

Se trata de definir los mínimos niveles de servicio aceptables para cada problema que se pueda plantear. Es importante que dicho nivel se consensúe con cada uno de los responsables de las áreas que puedan verse afectadas.

6. Identificación de las alternativas de solución.

En esta subfase deberán identificarse las soluciones alternativas para cada uno de los problemas previsibles. Para ello se puede considerar:

- ✓ Implementar procesos manuales.
- ✓ Contratar las tareas críticas con terceros.
- ✓ Diferir la tarea crítica por un tiempo determinado.
- ✓ Otra medida que permita continuar las operaciones.

7. Evaluación de la relación coste/beneficio de cada alternativa.

De cada alternativa identificada en el punto anterior y sobre la base del impacto económico de cada problema, deberá determinarse la mejor solución desde el punto de vista coste/beneficio para cada proceso crítico y su tiempo de elaboración con un nivel de servicio que satisfaga el nivel mínimo.

Planificación:

1. Documentación del plan de contingencia.

Es necesario documentar el plan, cuyo contenido mínimo será:

- ✓ Objetivo del plan.
- ✓ Modo de ejecución.
- ✓ Tiempo de duración.
- ✓ Costes estimados.
- ✓ Recursos necesarios.
- ✓ Evento a partir del cual se pondrá en marcha el plan.
- ✓ Personas encargadas de llevar a cabo el plan y sus respectivas responsabilidades.

2. Validación del plan de contingencia.

Es necesario que el plan sea validado por los responsables de las áreas involucradas. De igual manera hay que tener en cuenta las posibles consecuencias jurídicas que pudiesen derivarse de las actuaciones contempladas en él.

Pruebas de Viabilidad:

1. Definir y documentar las pruebas del plan

Es necesario definir las pruebas del plan y el personal y recursos necesarios para su realización. Una correcta documentación ayudará a la hora de realizar las pruebas.

2. Obtener los recursos necesarios para las pruebas

Deben obtenerse los recursos para las pruebas, ya sean recursos físicos o mano de obra para realizarlas.

3. Ejecutar las pruebas y documentarlas

Consiste en realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles.

La capacitación del equipo de contingencia y su participación en pruebas son fundamentales para poner en evidencia posibles carencias del plan.

Es necesario documentar las pruebas para su aprobación por parte de las áreas implicadas.

4. Actualizar el plan de contingencia de acuerdo a los resultados obtenidos en las pruebas.

Será necesario realimentar el plan de acuerdo a los resultados obtenidos en las pruebas.

Hay que tener en cuenta que el plan de contingencia general o de continuidad de operaciones de la empresa contiene los planes de contingencia específicos para cada problema definido. Los distintos planes deben integrarse en un todo, considerando las posibles relaciones mutuas.

Ejecución:

En esta fase hay que tener muy presente que el plan no busca resolver la causa del problema, sino asegurar la continuidad de las tareas críticas de la empresa.

Recuperación:

Los datos afectados por el siniestro que pudiesen haber quedado desactualizados o corruptos, deben corregirse usando los procedimientos ya definidos.

En general, la reiniciación del proceso normal no implica la cancelación del alternativo, salvo que deban utilizarse los mismos recursos. Si esto no es así, durante cierto tiempo, los procesos deberían ejecutarse en paralelo para asegurar que la reiniciación de la operación normal es correcta y, ante cualquier defecto, continuar con el de contingencia.

Una vez finalizado el plan, es conveniente elaborar un informe final con los resultados de su ejecución cuyas conclusiones pueden servir para mejorar éste ante futuras nuevas eventualidades.

C. IDENTIFICACIÓN, SELECCIÓN E IMPLEMENTACIÓN DE SALVAGUARDAS

Los objetivos de esta actividad son:

- ✓ Identificar los mecanismos de salvaguarda asociadas a cada activo, intentando obtener información del coste del mantenimiento de tales salvaguardas.

- ✓ Identificar y agrupar las amenazas

Un mecanismo de salvaguarda es un procedimiento o dispositivo, físico o lógico que reduce el riesgo.

Una amenaza es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos

Selección de salvaguardas

a. Establecer una política de la Organización al respecto: directrices generales de quién es responsable de cada cosa
b. Establecer una norma: objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada
c. Establecer unos procedimientos: instrucciones paso a paso de qué hay que hacer
d. Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas
e. Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto

Para aquellos riesgos cuya mitigación requiere la implantación de nuevas salvaguardas se definen las nuevas salvaguardas a implantar, teniendo en cuenta:

- ✓ Capacidad de la Salvaguarda para mitigar el riesgo correspondiente y otros riesgos afines.
- ✓ Experiencia existente en la organización para la implantación de dichas salvaguardas.
- ✓ Relaciones entre salvaguardas, Por ejemplo posibilidad de adquirir módulos adicionales de productos de seguridad ya implantados en la sociedad.
- ✓ Dificultad y coste para implantar y mantener cada salvaguarda teniendo en cuenta el entorno y las circunstancias de la sociedad.

4.4.1.5 FASE V MONITOREO Y CUMPLIMIENTO DE LEYES

A. MONITOREO DEL PROCESO

Se deben definir indicadores de desempeño para monitorear la gestión y las excepciones de las actividades de TI.

La unidad de TI debe presentar informes periódicos de gestión a la dirección de la organización para que esta supervise el cumplimiento de los objetivos planteados.

Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

Se deberá efectuar una copia automática de los archivos y se conducirá o enviara hacia otra terminal o servidor, evitando que se guarde la copia localmente donde se produce.

B. GARANTIZAR EL CUMPLIMIENTO DE LAS LEYES

Los objetivos a cumplir en esta actividad son:

- ✓ Cumplir con las disposiciones legales, normativas y contractuales a fin de evitar sanciones administrativas y legales al Organismo y/o al empleado.
- ✓ Garantizar que los sistemas cumplan con las Políticas y estándares de seguridad del Organismo.
- ✓ Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de las Políticas y estándares de seguridad, sobre las plataformas tecnológicas y los sistemas de información.
- ✓ Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
- ✓ Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.
- ✓ Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

C. CONCLUSIONES

CAPÍTULO V

5. AUDITORÍA INFORMÁTICA

5.1 FASE I: DEFINICIÓN DEL PLAN

5.1.1 Recogida de información

El inicio de esta primera etapa corresponde a la recogida de la información la misma que se llevará a cabo mediante cuestionarios – encuestas que se realizo en el departamento de informática, los mismos que están archivados en los anexos de la presente aplicación **(Ver anexo 1)**

Para la elaboración de los mencionados cuestionarios se tomo en cuenta las necesidades de la información, así como las adaptaciones realizadas en ella.

En lo referente a las técnicas empleadas se considero factible realizar guías para la entrevista, y se procedió a la práctica con la colaboración de entrevistado el Ing. Silvio Hidalgo y el equipo de trabajo del departamento de informática.

I20La información que se recabo gracias al equipo de trabajo, es información realizada en cada uno de los formatos que la institución maneja, así como es inventarios de las áreas físicas (HW, equipo) y lógicas (BD, sistemas, SW) del departamento. **(Ver anexo 2)**

Como punto primordial de la información del departamento informático, está en mencionar los objetivos del mismo los cuales nos ayudaran para la verificación del cumplimiento de ellos en la aplicación de las actividades propuestas en el departamento, mismas q se encuentran mencionadas en el **anexo 3**Así como también se detalla las funciones del departamento en el **anexo 4**

Para que la información que se recopila sea veraz se realizo una eficiente y detallada revisión documental y de equipo, confirmando los datos recibidos.

5.1.2 Definir un plan, los objetivos y una política de seguridad.

El trabajo que desarrolla esta actividad lleva en conjunto tres términos importantes:

1. **Elaboración del Plan**.- El plan será elaborado con el fin de definir las tareas que se tiene a responsabilidad el equipo auditor, en el plan se detallara la fase y la actividad con su fecha de inicio y de fin, de esta manera se obtendrá el tiempo que le llevará la auditoria.

Fase	Actividad	Auditora Responsable	Inicio	Fin
Definición del Plan	Recogida de información.	Geomayra Paredes - Mayra Vega		
	Definir un plan, los objetivos y una política de seguridad.	Geomayra Paredes		
	Prestación y Organización de servicios.	Mayra Vega		
Gestión Informática	Planificación de la seguridad de los Sistemas de Información	Geomayra Paredes - Mayra Vega		
	Diseño y mantenimiento de un plan de infraestructura tecnológica.	Geomayra Paredes - Mayra Vega		
	Gestionar la calidad de proyectos	Geomayra Paredes		
	Desarrollo y mantenimiento de sistemas.	Mayra Vega		

	Control de accesos	Mayra Vega
	Gestionar los datos, comunicaciones y operaciones	Geomayra Paredes
Control y Comunicación	Análisis y Control de Activos	Mayra Vega
	Control de Recursos Humanos	Mayra Vega
	Comunicar las Aspiraciones y la Dirección de la Gerencia	Geomayra Paredes
	Capacitación a los usuarios	Geomayra Paredes
Análisis y Gestión de Riesgos	Identificación y Evaluación del Riesgo	Geomayra Paredes
	Establecer planes de contingencia	Geomayra Paredes
	Identificación y selección e implementación de funciones de salvaguarda	Geomayra Paredes - Mayra Vega
Monitoreo y Cumplimiento de leyes	Monitoreo del Proceso	Geomayra Paredes - Mayra Vega
	Garantizar el cumplimiento de las leyes	Geomayra Paredes - Mayra Vega
	Conclusiones	Geomayra Paredes - Mayra Vega

Tabla. V. 14. Planificación del Desarrollo de la Auditoria

Perfiles Técnicos:

- Especialista en hardware y software.
- Experto organizador y coordinador.
- Especialista en software de comunicaciones y redes.
- Especialista en diseño de redes.
- Experto en optimización de métodos y medios de comunicación con el computador y los usuarios.
- Especialista en mantenimiento de infraestructura de redes.
- Conocimiento de normas y estándares para la auditoría interna.
- Políticas organizacionales sobre la información y las tecnologías de la información.
- Conocimientos de la organización respecto a la ética, estructura organizacional, tipo de supervisión existente, historia de la organización, cambios recientes en la administración, operaciones o sistemas, la industria o ambiente competitivo en la cual se desempeña la organización, aspectos legales.

Definición de Objetivos

Se especificará los siguientes:

Objetivo general:

- Desarrollar la Auditoría de Riesgos Informáticos Físicos y Lógicos en el Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura aplicando la metodología desarrollada llamada MACORI

Objetivos particulares:

- Efectuar la Definición del Plan, La Gestión Informática, El Control y Comunicación, El Análisis y Gestión de Riesgos y, El Monitoreo y Cumplimiento de leyes, fases de la metodología desarrollada a aplicarse en el Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura.

Objetivos específicos:

Se menciona de acuerdo a cada una de las fases:

Fase 1

- Recopilar la información.
- Definir y/o Elaborar un plan de actividades y una política de seguridad respectivamente.
- Determinar la Prestación y Organización de servicios en el departamento

Fase 2

- Indagar como se encuentra la planificación de la seguridad de los Sistemas a de Información
- Investigar cómo está el diseño y cómo realizan el mantenimiento de la infraestructura tecnológica.
- Averiguar cómo realizan la gestión de la calidad de proyectos

- Inquirir los procesos a seguir para el desarrollo y mantenimiento de sistemas.
- Investigar la manera cómo se lleva a cabo el control de accesos
- Determinar el proceso a seguir para la gestión de los datos, comunicaciones y operaciones

Fase 3

- Comprobar cómo se lleva a cabo el Análisis y Control de Activos
- Determinar el Control de Recursos Humanos
- Comprobar si se comunicar las Aspiraciones y la Dirección de la Gerencia
- Investigar cual es el proceso de la Capacitación a los usuarios

Fase4

- Indagar la existencia de un proceso de Identificación y Evaluación del Riesgo
- Averiguar si existen y si lo aplican los planes de contingencia en el departamento
- Identificar y seleccionar la implementación de funciones de salvaguarda

Fase 5

- Comprobar si existe la realización de Monitoreo del Proceso en el Departamento
- Investigar si el departamento garantiza el cumplimiento de las leyes
- Emitir los resultados de la auditoria de cada una de las fases de la metodología MACORI mediante las conclusiones respectivas de una de las actividades de la fase V

5.1.3 Prestación y Organización de servicios

Se determinó que la organización del departamento está acorde con la labor que desempeña, y los servicios que presta se detallan a continuación:

- ✓ Planificar, organizar, dirigir y controlar las areas de administración de redes, telecomunicaciones, servicios informáticos y soporte técnico.
- ✓ Auditar diariamente toda la información que ingresa al sistema y solucionar cualquier inconveniente que por deficiencia eléctrica u otras circunstancias haga que se esté afectando nuestro optimo servicio,
- ✓ Establecer panes anuales de capacitación del personal técnico, en las diferentes aéreas.
- ✓ Definir, actualizar y ejecutar un Plan estratégico Operativo, Informático que satisfaga en forma actualizada las necesidades latentes.
- ✓ Preparar los presupuestos para la adquisición con características y especificaciones técnicas que hagan que los software y servicios informáticos sean excelentes.
- ✓ Diseñar y controlar la ejecución de los proyectos informáticos, con capacidad para cubrir las necesidades actuales y las que puedan darse en un futuro inmediato.
- ✓ Mantener actualizado el manual de Procedimientos Informáticos y difundirlo con eficacia.

Servicios Informáticos

- ✓ Administra los sistemas informáticos como el SATJE y el Sistema de Pensiones Alimenticias.
- ✓ Administra, monitorea, actualiza el Portal Web y sus bases de datos.
- ✓ Analiza, diseña y actualiza los módulos del Sistema Automático de Tramitación Judicial Ecuatoriano (SATJE) y realiza auditoria de sus resultados.
- ✓ Diseña e implementa nuevos sistemas informáticos, utilizando tecnologías de punta como Multicapa (Windows-Linux), etc.

- ✓ Administra y controla el desarrollo de programas informáticos, vigila su uso, aplicación y proyección.
- ✓ Establece y ejecuta procedimientos de seguridad y control en los servidores de bases de datos web y sistemas corporativos.

Administración de Redes y Telecomunicaciones

- ✓ Del antecedente expuesto y para su cumplimiento Administra las Redes Informáticas y de Telecomunicaciones.
- ✓ Determina las políticas de seguridad en los servidores, redes locales y de área extendida.
- ✓ Administra el servidor de archivos, servidor web intranet y extranet, servidor de comunicaciones.
- ✓ Mantiene actualizado el inventario del equipo activo y pasivo de las redes locales y de área extendida.
- ✓ Supervisa los sistemas integrados de telefonía IP y de telecomunicaciones.

En esta actividad como en otras nos ayuda a verificar los requerimientos del usuario y el cumplimiento de los objetivos de la empresa y en este caso del departamento.

5.2 FASE II GESTIÓN INFORMÁTICA

5.2.1 Planificación de la seguridad de los Sistemas de Información

Matriz de actividades que se desarrolla en el Áreas del departamento

Valoración	
0	No participa
1	Poca Participación
2	Participación Parcial
3	Participación Moderada
4	Participación Total

Departamento de Informática

Áreas / Actividades	PLANIFICACIÓN					Total
	Análisis	Diseño	Desarrollo	Mantenimiento	Administración de Aplicaciones	
Jefatura	4	4	3	3	4	**18**
Desarrollo y Programación	4	3	2	1	3	**13**
Redes	3	2	2	1	3	**11**
Soporte Técnico	1	0	0	1	2	**4**
Total	**12**	**9**	**7**	**6**	**12**	

Tabla. V. 15. Planificación

Para el trabajo de planificación de las actividades de análisis, diseño, desarrollo, mantenimiento y administración de aplicaciones las áreas que participan en este proceso de planificación es el área de jefatura con una participación total en cada una de las actividades, así como también en un 75%, participa el área de desarrollo y programación. Para este proceso de planificación se encuentra con una participación parcial el área de redes del departamento y a su vez el área de soporte técnico también inmiscuido con un 25% de participación en la planificación del desarrollo de aplicaciones.

Mediante la matriz también se puede interpretar la participación por actividades, así tenemos que en el proceso de Análisis y Administración de Aplicaciones las áreas del departamento tienen una participación moderada en el proceso de planificación, a su vez en el proceso de Diseño, las áreas participan en un 50% en colaboración a la planificación y en las actividades de Desarrollo y Mantenimiento las áreas colaboran parcialmente en la planificación del desarrollo de aplicaciones

Áreas / Actividades	COORDINACIÓN					Total
	Análisis	Diseño	Desarrollo	Mantenimiento	Administración de Aplicaciones	
Jefatura	3	4	4	2	3	**16**
Desarrollo y Programación	3	3	4	3	3	**16**
Redes	2	2	2	2	2	**10**
Soporte Técnico	0	0	0	0	0	**0**
Total	**8**	**9**	**10**	**7**	**8**	

Tabla. V. 16. Coordinación

En el trabajo de Coordinación de las actividades de análisis, diseño, desarrollo, mantenimiento y administración de aplicaciones las áreas que participan en este proceso de Coordinación es el área de jefatura y el área de desarrollo y programación con una participación moderada en cada una de las actividades. El área de Redes coordina con la aplicación con una participación parcial, y el área de soporte técnico se excluye de esta actividad ya que no participa de la misma.

A través de la matriz también se puede interpretar la participación por actividades, así tenemos, que en el proceso de Análisis Diseño Mantenimiento y Administración de Aplicaciones las áreas del departamento tienen una participación parcial en el proceso de coordinación, a su vez en el proceso de Desarrollo, las áreas participan en un 75% coordinando las actividades.

Áreas / Actividades	SUPERVISIÓN					Total
	Análisis	Diseño	Desarrollo	Mantenimiento	Administración de Aplicaciones	
Jefatura	3	3	4	2	4	**16**
Desarrollo y Programación	3	3	3	4	4	**17**
Redes	3	2	2	4	4	**15**
Soporte Técnico	1	0	0	4	4	**9**
Total	**10**	**8**	**9**	**14**	**16**	

Tabla. V. 17. Supervisión

Análisis.- En la supervisión de las actividades de análisis, diseño, desarrollo, mantenimiento y administración de aplicaciones las áreas que participan en este proceso de supervisión es el área de jefatura, el área de desarrollo y programación y el área de redes con una participación moderada en cada una de las actividades. El área de soporte técnico participa en la supervisión con una participación parcial.

A través de la matriz también se puede interpretar la participación por actividades, así tenemos, que en el proceso de Mantenimiento y Administración de Aplicaciones las áreas del departamento tienen una participación total en el proceso de supervisión, a su vez en el proceso de Análisis, las áreas participan en un 75% coordinando las actividades y en las actividades de Diseño y Desarrollo las áreas participan parcialmente en las actividades de supervisión.

La planificación, la coordinación y la supervisión de las actividades de análisis, diseño, desarrollo, mantenimiento y administración de aplicaciones esta a la responsabilidad del

Ing. Silvio Hidalgo, Analista II quien participa como responsable del área de desarrollo y programación, del departamento de la Dirección Provincial de Pichincha.

Las actividades que él realiza son:

- Administra las bases de datos del sistema automático SATJE.
- Desarrolla las aplicaciones para el sistema SATJE y administra las aplicaciones realizadas para la web.
- Controla el mantenimiento del sistema automático
- Controla el buen funcionamiento de los servidores de réplica, producción, aplicaciones.

Funcionalidad de las aplicaciones que se encuentran activas en el departamento

Para probar la funcionalidad de las aplicaciones especializadas que se encuentran activas en el departamento se consideró los siguientes parámetros, con su respectiva valoración.

Valoración	
0	Funcionalidad Nula
1	Funcionalidad Parcial
2	Funcionalidad Completa

Características / **Módulos**	**MÓDULO DE**											**TOTAL**
	Sorteos Primera Instancia	**Sorteos Segunda Instancia y Corte Suprema**	**Trámite judicial**	**Digitación**	**Administración**	**Ventanillas**	**Casilleros**	**Recepción de Escritos**	**Estadísticas**	**Pagadurías de los Juzgados de la Niñez y Adolescencia**	**Sistema de Control de Mantenimiento y Reparación de Equipos**	
Multiplataforma	0	0	0	0	0	0	0	0	0	0	0	**0**
Portable	2	2	2	2	2	2	2	2	2	2	2	**22**

Multiusuario	0	0	2	0	2	2	0	0	0	0	0	**6**
Diseño Amigable	2	2	2	2	2	2	2	2	2	2	2	**22**
Usabilidad	2	2	2	2	2	2	2	2	2	2	2	**22**
Cumple los requisitos	2	2	2	2	2	2	2	2	2	2	2	**22**
Rápido	2	2	2	2	2	2	2	2	2	2	2	**22**
Fácil de usar	2	2	2	2	2	2	2	2	2	2	2	**22**
Personalizado	2	2	2	2	2	2	2	2	2	2	2	**22**
Diseño intuitivo	2	2	2	2	2	2	2	2	2	2	2	**22**
Integración con Internet	0	0	0	0	0	0	0	0	0	0	0	**0**
TOTAL	**16**	**16**	**16**	**16**	**18**	**18**	**16**	**16**	**16**	**16**	**16**	

Tabla. V. 18. Funcionalidad de los Módulos

Análisis.- En el proceso de prueba de la funcionalidad de las aplicaciones activas en el departamento se puede concluir que en ninguno de los módulos se aplica la característica de ser multiplataforma y que tengan integración con internet, pero a su vez todos cuentan con las características de ser: portables, de contar con un diseño amigable e intuitivo, de cumplir los requisitos de ser fáciles de usar, de ser rápidos y personalizados.

Los módulos que se encuentran activos en el departamento cumplen en un alto porcentaje las características de la funcionalidad de las aplicaciones así tenemos a l módulo de Trámite judicial, Administración y Ventanillas cumplen la funcionalidad de las aplicaciones en un 80% y los módulos de Sorteos Primera Instancia, Sorteos Segunda Instancia y Corte Suprema, Digitación, Casilleros, Recepción de Escritos, Estadísticas, Pagadurías de los Juzgados de la Niñez y Adolescencia y el Sistema de Control de Mantenimiento y Reparación de Equipos, cumplen las características de la funcionalidad de las aplicaciones en un 70%.

El departamento de informática para el desarrollo, mantenimiento o adquisición de software de aplicación el departamento no dispone de un procedimiento o metodología para

las actividades de desarrollo, mantenimiento o adquisición de sistemas, pero si realizan la documentación y se aplica en forma complementaria a las normas relativas de la administración de proyectos.

La persona que controla la documentación de los nuevos desarrollos y adquisiciones de SW para el departamento es el Ing. Diego Larco, responsable del Área de Jefatura.

En el departamento si existe un criterio para el establecimiento de prioridades entre los distintos requerimientos recibidos por el departamento y este se despacha de acuerdo a como se van presentando diariamente.

Durante el desarrollo de las aplicaciones que elaboran en el departamento si existe el proceso de realización de pruebas suficientes en las distintas etapas del desarrollo, conforme a un plan de pruebas y de control de calidad aprobado, en un ambiente específico representativo del ambiente operativo futuro y distinto del ámbito de producción, este proceso se responsabiliza al Área de Desarrollo y Programación con la coordinación de la Ing. Mirian Yepez. De la misma manera se realiza el control de las versiones del software por parte del área responsable de las tareas de desarrollo y mantenimiento de sistemas.

El departamento también realiza la actividad de capacitar a los usuarios y al personal técnico y la persona responsable quien desarrolla la aplicación capacita al personal de capacitación y también al personal de mantenimiento y luego las personas de capacitación capacitan a los usuarios del sistema.

El departamento en lo que tiene que ver con contratación de servicios externos de desarrollo de sistemas no realiza adquisiciones ya que en el departamento realiza todo.
En lo que se refiere a seguridad de la información del sistema, el departamento codifica la información mediante la técnica de Criptografía, así como también se menciono por parte del entrevistado que si existe vigilancia de la red.

Seguridad de los sistemas de información y de datos

Valoración	
0	No Aplican
1	Aplican Parcialmente

2	Lo aplican totalmente

	Aplicaciones Software	Infraestructura de la red	Datos e Información manual	TOTAL
Confidencialidad	2	2	2	**6**
Integridad	2	2	1	**5**
Disponibilidad	2	1	1	**4**
TOTAL	**6**	**5**	**4**	

Tabla. V. 19. Seguridad de los sistemas

Análisis.- Las disposiciones para la seguridad deberían enfocarse en garantizar la disponibilidad, la precisión, la integridad y cuando sea necesario, la confianza en la información. Entre más complejo sea el sistema de información que se use, más complejas tendrán que ser las medidas para protegerlo, por ello se opto por determinar cómo se lleva a cabo la seguridad de los sistemas de información en el departamento de informática. Llegando a determinar que las aplicaciones de software aplican en un 100% la confidencialidad la integridad y la disponibilidad. En lo que tiene q ver a la infraestructura de la red también aplica los conceptos de seguridad, aunque el de la disponibilidad lo aplica parcialmente y en los datos e información de forma manual se aplica parcialmente las consideraciones de la seguridad de los sistemas de información.

De acuerdo a las características se concluye q la confidencialidad es un aspecto que se cumple y se aplica totalmente en cada uno de los sistemas de información desarrollados en el departamento de informática.

Sistemas informativos manuales

El registro de la información que lo recopila de forma manual lo realizan mediante Scripts, con un correcto almacenamiento y realizando los respectivos respaldos mediante almacenamiento robótico

5.2.2 Diseño y mantenimiento de un plan de infraestructura tecnológica.

Seguridades Físicas y Lógicas

Seguridad Física

La instalación de toma eléctrica está en correctas condiciones, no presentan daños, éstas están ubicadas estratégicamente para ser de utilidad en el departamento.

El cableado eléctrico está perfectamente en buen estado, éste no se encuentra pelado o presenta averías. El control de ingreso a los laboratorios se da de buena manera es decir solo podrán ingresar el personal autorizado. El control de la existencia de equipos se da por la Ing. Marcelo Guerra y el encargado de cada departamento en el caso de los equipos y dispositivos de las redes que se encuentran en el departamento.

Cabe mencionar que hasta la fecha todos los equipos están completos y no se han reportado robos o daños por parte del personal de trabajo.

Seguridad Lógica

En cuanto al acceso a los sistemas con los que cuenta el departamento de informática de la dirección provincial del consejo de la judicatura – Pichincha estos están seguros mediante control de acceso el cual se realiza en el dominio mediante el Active Directory, y al sistema mediante el propio módulo de ingreso por usuario. Para el manejo del sistema automático se toma en cuenta que el usuario esté solamente en una sola judicatura, sea único usuario y el password sea personalizado y encriptado. La tecnología protectora para mantener los sistemas de información del departamento es el antivirus Kaspersky que cuenta con todas las protecciones.

Matriz de Seguridades Físicas y Lógicas

Valoración	
0	Depreciable
1	Casi probable
2	Probable
3	Frecuentemente

Seguridades Físicas				
Impacto / Amenazas	**Incendios**	**Robos**	**Daños**	**Total**
Instalación tomas eléctricas	0	0	0	**0**
Cableado eléctrico	1	0	1	**2**
Ingresos al centro de cómputo	1	2	1	**4**
Total	**2**	**2**	**2**	

Tabla. V. 20.Seguridades Físicas

Análisis.- La seguridad física que aplica el departamento presenta que es depreciable que se aplique la amenaza de incendios, robos y daños al impacto de la instalación de tomas eléctricas.

Presente q por el cableado eléctrico existe la probabilidad que se presente los impactos mencionados, así como también existe la probabilidad que se aplique estas amenazas al impacto del cableado eléctrico. Y por el factor de ingresos al centro de cómputo es casi probablemente que se aplique los incendios, robos y daños en el departamento de informática.

Seguridades Lógicas						
Impacto / Amenazas	**Sabotaje**	**Errores**	**Robo de identidad**	**Transacciones no utilizadas**	**Perdidas de información**	**Total**
Acceso a sistemas	0	0	0	0	0	**0**
Acceso a paginas prohibidas	0	0	0	0	0	**0**
Virus	1	1	1	1	2	**6**
Total	**1**	**1**	**1**	**1**	**2**	

Tabla. V. 21. Seguridades Lógicas

Análisis.- Para la seguridad lógica que aplica el departamento el porcentaje es depreciable cuando para que se aplique las amenazas de sabotaje, errores, robo de identidad, transacciones no utilizadas y perdidas de información, mientras que la causa para que el impacto de los virus causa efecto esta casi probablemente que se aplique en la amenaza de la perdida de información.

En la infraestructura tecnológica del departamento, El Ing. Diego Larco, se encarga de ver que exista toda la infraestructura adecuada para que cada usuario se desempeñe bien en su área de trabajo. Existe el personal dedicado al área de soporte técnico y por la demanda que se da, las demás áreas colaboran con soporte técnico.

Infraestructura de red

Dispone de cableado de red, sus equipos están conectados entre sí y cada uno actúa de forma dependiente. Las canaletas de cableado de red y cableado eléctrico se encuentran un poco desorganizadas por lo que no ofrecen una excelente protección.

Las tomas de luz son ya de hace un gran tiempo y éstas están en buenas condiciones con protecciones y adecuadas instalaciones, ubicadas en sitios claves del centro de cómputo, es decir que éstos están bien distribuidos. Su conexión es a Tierra y sus cables de los equipos están organizados por lo que es muy difícil provocar algún daño en los mismos.

En el departamento de informática se cuenta con equipos de red, para la distribución de internet y de los servicios que presta los mismos que permiten la interconexión entre computadores. Todas las redes q son controladas por el departamento se adjunto en el **anexo 5**

Matriz de infraestructura de las Redes

Valoración	
0	No existe (0%)
1	Malo (33%)
2	Bueno (67%)
3	Excelente (100%)

Infraestructura / Estados	Organización	Condiciones	Distribución	Conectividad	Protección	Total
Cableado de red	3	3	3	3	3	**15**
Canaletas de cableado de red	2	2	2	2	2	**10**
Canaletas de cableados eléctrico	3	3	3	3	3	**15**
Toma de luz	3	3	3	3	3	**15**
Conexión a tierra	3	3	3	3	3	**15**
Topología de red	3	3	3	3	3	**15**
Dispositivos de red	3	3	3	3	3	**15**
Cableado de equipos de computo	2	3	1	2	2	**11**
Total	**21**	**22**	**21**	**22**	**22**	

Tabla. V. 22. Infraestructura de Red

Análisis.- En cuanto al cableado de Red, canaletas de cableados eléctrico, toma de luz, conexión a tierra, topología y dispositivos de red, éstas se encuentran en un excelente estado es decir equivale a un 100%, refiriéndose a su organización, condiciones, distribución conectividad y protección lo que refleja la existencia de la infraestructura de red implementada. En lo que tiene que ver a las canaletas de cableado de red determinamos que es bueno el estado de estos en la red que equivale a un 67%, también nos damos cuenta que el cableado de los equipos de computo se encuentran en un estado bueno calificándole con un 70%.

Inventario de hardware y software

Valoración	
0	No existe
1	Incompletos
2	Completos

Equipos / Características	Cantidad	Marca	Parámetro Existencia del Inventario()
Monitor	47	5 LENOVO 12 ACER 17” 20 HEWLETT. P 6 COMPAQ 2 CLEARTEK 1 SAMSUNG 1 IBM	2
CPU	45	5 LENOVO 15 ACER 20 HEWLETT 5 COMPAQ	2
Mouse	45	12 HEWLETT. P 11 COMPAQ	2
Teclado	43	19 HEWLETT P 2 HP-COMPAQ 5 LENOVO 12 HACER 5 COMPAQ	2
Touch Screem	1	TIPO KIOSCO	2
UPS	12	CDP	2
Parlante	6	4 COMPAQ 2 ALTEC	2
Scanner	1	HEWLETT P	2
Impresora	18	11 EPSON 5 XEROX 2 LEXMARK	2
Memory Flash	2	2 IMCP 1 GB	2
Laptop	1	TOSHIBA	2
Dvd Externo	6	6 LG	2
Floppy USB	7	7 MPF82E	2
Proyector	1	INFOCUS LP600	2
Sistema de Multiplexación	2	2 LG	2
Fotocopiadora	1	CANON	2
Teléfono digital	7	ALCATEL	2

Tabla. V. 23. Inventario de Hardware

Análisis.- Actualmente se encuentran todos los equipos mencionados en la matriz, determinado de esta manera que no existe ninguna alteración a pesar de la des actualización que existe en el inventario porque es un archivo que tienen del año anterior. Cabe recalcar que el mismo se encuentra de una forma ordenada todos y cada uno de los equipos que pertenecen a la institución, hasta los que se encuentran dados de baja como lo mencionan en el documento de inventario.

En cuanto al inventario de software también se puede determinar la existencia de paquetes de Ofimática como: Office 2003/2007, Kaspersky y dentro de los Sistemas Operativos que se encuentran en las maquinas son XP y Windows Server 2003 en los servidores de la red del centro de computo, en cuanto a los sistemas que usan en la institución a parte de los mencionados como módulos anteriormente poseen de un portal web, información que se le detalla en el **anexo 6**

La existencia de los equipos utilizados para cada una de las redes auditadas así como también del equipo en funcionamiento que se encuentra en la institución es completa, es decir que todo cuando se maneja en el inventario se encuentra correctamente registrado y llevado de una forma correcta de parte de la persona encargada del inventario de los equipos del departamento.

Refiriéndonos al software, las dependencias en las cuales se encuentra implementadas las diferentes redes estudiadas en esta auditoría disponen de los paquetes de ofimática, antivirus, sistemas operativos de acuerdo a los requerimientos y limitaciones de los usuarios.

Necesidades de hardware

Valoración	
0	No existe lo necesario
1	Existe lo necesario
2	Existe más de lo necesario

Necesidades de HW		
Necesidades de una red / Usuarios	**Departamento de Informática**	**Usuario Final**
Estaciones de trabajo	1	1
Servidores	1	1
Tarjeta de interfaz de red	2	1
Cableado	2	1
Equipo de conectividad	2	1
Equipos de oficina (Impresoras, papel etc.)	1	0

Tabla. V. 24. Necesidades de Hardware

Durante el proceso auditivo se pudo constatar que en si necesidades de hardware no tiene, aunque de parte de los usuarios si existe una alta demanda de personas q se quejan por el mal estado en el que se encuentran las impresoras de sus oficinas.

Al interpretar el cuadro también observamos que en el departamento de informática si existe lo necesario y hasta mas, en los casos de equipo de conectividad, cableado y tarjetas de interfaz, mientras que en los lugares de trabajo de los usuarios existe lo necesario en las infraestructura de red, aunque hay faltante en lo que respecta al equipo de oficina, como se daba a conocer anteriormente.

Administración de los equipos y servicios informáticos

La coordinación de la realización del mantenimiento preventivo y correctivo de equipos informáticos se encuentra a cargo de la Ing. Betty Sisa, Ing. Gina Paladines e Ing. Edgar Baldion que a su vez son quienes evalúan y dan recomendaciones para la innovación de los nuevos avances de hardware y herramientas al desarrollo tecnológico del departamento y por ende de la institución.

El proceso para llevar a cabo el correcto mantenimiento preventivo y correctivo de los equipos, se realiza previa a la coordinación del equipo mencionado, a través de contratos con las empresas que realizan mantenimiento de equipos de acuerdo a las marcas de los equipos.

5.2.3 Gestionar la calidad de proyectos

El proceso de gestión de calidad incluye 3 importantes procesos, para q la gestión sea aplicada y verificada de la mejor manera. Además en lo que se refiere a la Evaluación del desempeño total del proyecto, si lo aplican y cada jefe de área es el responsable, dependiendo del proyecto que realicen.

Normas y/o Estándares	Que satisface
IEEE Std 610 – 1991	Define la calidad del software como ”el grado con el que un sistema, componente o proceso cumple los requerimientos especificados y las necesidades o expectativas del cliente o usuario”
Norma ISO 9001:2000	Especifica los requisitos para un sistema de gestión de calidad, al menos permite identificar más fácilmente los principales hitos afectados por las pruebas que deben satisfacer, y por ende aquellas actividades o tareas que deben ser cuidadas meticulosamente.
IEEE 1012	Que el control de calidad de software sea realizado por un equipo experto e independiente al grupo de desarrollo, trabajando paralelamente junto con este durante el ciclo de vida de desarrollo pero gestionando de forma autónoma, garantizando así su independencia.

Tabla. V. 25. Normas y Estándares

1. Planeación de la calidad del Proyecto

La gestión de la calidad del proyecto se lo aplica en cada proyecto durante todas sus fases que lo conforman. Los estándares más relevantes para la ejecución de los proyectos del departamento se presentan en la siguiente tabla, así como también se menciona las partes del proyecto que se satisface:

Valorización del primer proceso de la gestión de calidad

Para la planeación de la calidad del proyecto involucra los procesos de insumos, técnicas y salidas para lo cual se elaboro un cuadro por medio del cual se evaluará si las actividades son aplicadas en el proyecto.

Valoración	
0	No se aplica (0%)
1	Poca Aplicación (25%)
2	Se aplica Parcialmente (50%)
3	Aplicación Moderada (75%)
4	Se Aplica Totalmente (100%)

Planeación de la Calidad del Proyecto				
Actividades / **Para el proyecto**		**¿Considerado en el proyecto?**	**¿Ayuda al cumplimiento de los objetivos del proyecto?**	**Total**
Insumos				
Alcance del Proyecto		4	4	8
Plan del Proyecto		4	4	8
Técnicas para la planeación de la calidad	Analizar el costo/beneficio que producen en el desarrollo del proyecto y sus entregables.	3	4	7
	Comparar con proyectos anteriores que generen ideas para mejorar y proveer un estándar por el cual medir su funcionamiento.	4	4	8
	Realizar experimentos que permitan aumentar la calidad del producto final.	2	3	5
	Total de costos en que se ha incurrido para alcanzar la calidad del producto y/o servicio.	3	3	6
Total		20	22	
Salidas				

Métricas de calidad.	1	3	7
Listas de chequeo de calidad.	2	3	5
Plan de gestión de calidad.	3	3	6
Línea base de calidad.	2	3	5
Plan de mejoramiento.	2	4	6
Total	10	16	

Tabla. V. 26. Planeación de la calidad del proyecto.

Análisis

En el primer proceso de aplicación en los insumos concluimos que todas y cada una de las actividades son consideradas en los proyectos con una aplicación moderada. Aunque para estas actividades los miembros de la gestión de proyectos mencionaron y se evaluó que con una aplicación total ayudaría al cumplimiento de los objetivos del proyecto.

Mencionando detalladamente los insumos, se evaluó y se concluye que para los proyectos con un 100% lo aplican en lo que se refiere a: al alcance del proyecto; elaboración de un plan de proyecto, así como también en la aplicación de las siguientes técnicas: El análisis del costo y beneficio que produce el desarrollo del proyecto y la Comparación con proyectos anteriores.

En cambio en el factor del Total de costos y la realización de experimentos que permitan aumentar la calidad del producto final lo aplican en un 75 % a los proyectos q desarrolla el departamento.

Para las salidas que genera la planeación de la calidad del proyecto se puede determinar que en el departamento las salidas son consideradas parcialmente en el proyecto mientras que los gestores piensan que con una aplicación moderada se lograría el cumplimiento de los objetivos del proyecto. En cambio en forma detallada los parámetros de salidas se concluye que las Métricas de calidad son aplicadas de forma total en la planeación de la calidad de los proyectos. Mientras que las listas de chequeo de calidad, El Plan de gestión de calidad, La Línea base de calidad Y el Plan de mejoramiento lo aplican en un 75% a los proyectos, para medir la calidad de los mismos.

2. Aseguramiento de la calidad del proyecto

El aseguramiento debe ser proporcionado al equipo del proyecto o a otros interesados que no estén activamente involucrados en el trabajo del proyecto. Para la verificación de las tareas que involucra este proceso se elaboro la siguiente matriz y se la evaluó de la siguiente manera:

Valoración	
0	No se aplica (0%)
1	Poca Aplicación (25%)
2	Se aplica Parcialmente (50%)
3	Aplicación Moderada (75%)
4	Se Aplica Totalmente (100%)

Aseguramiento de la calidad del proyecto			
Actividades / **Para el proyecto**	**¿Considerado en el proyecto?**	**¿Ayuda al cumplimiento de los**	**Total**
Insumos			
Métricas de Calidad	4	4	8
Plan de Gestión de calidad	2	3	5
Requerimientos de cambios aprobados	2	3	5
Plan de mejoramiento	3	3	6
Mediciones de Control de Calidad	2	3	5
Técnicas para el aseguramiento de calidad			
Revisiones, análisis y auditorias a las actividades del proyecto	2	3	5
Total	15	19	

Salidas			
Recomendaciones de acciones correctivas	1	3	4
Requerimientos de cambios	2	3	5
Total	3	6	

Tabla. V. 27.Asegutamiento de la calidad del proyecto.

Análisis

Para el aseguramiento de la calidad se tomó en cuenta los insumos los cuales se evaluó y se determina que lo consideran en el proyecto con una aplicación moderada. Además el equipo de trabajo alude que de la misma manera con una aplicación moderada ayudará al cumplimento de los objetivos del proyecto.

Detallando por actividades los insumos, se evaluó y se concluye que para los proyectos con un 100% lo aplican las métricas de calidad. Mientras que en las actividades de Plan de Gestión de calidad, Requerimientos de cambios aprobados, Plan de mejoramiento, Mediciones de Control de Calidad y las Revisiones, análisis y auditorias a las actividades del proyecto se aplican de manera moderada en el aseguramiento de la calidad de los proyectos.

Para las salidas se determina que el grupo de trabajo considera a estos aspectos con una aplicación baja en la aplicación de los proyectos, y concluyen que con una aplicación moderada de estas actividades si se ayudaría al cumplimiento de los objetivos del proyecto. Detallando cada uno de los aspectos de las salidas se concluye que para los Requerimientos de cambios y Recomendaciones de acciones correctivas se aplica parcialmente en la calidad del proyecto.

3. Control de calidad del proyecto

El control de Calidad, implica la supervisión de los resultados específicos del proyecto para determinar si cumplen los estándares de calidad relevantes e identificar los modos de eliminar las causas de resultados insatisfactorios, para ello se elaboró la siguiente matriz

para poder evaluar cada uno de los aspectos que se considera para el control de calidad de los proyectos que desarrollan en el departamento de informática.

Valoración	
0	No se aplica (0%)
1	Poca Aplicación (25%)
2	Se aplica Parcialmente (50%)
3	Aplicación Moderada (75%)
4	Se Aplica Totalmente (100%)

Control de calidad del proyecto			
Actividades / **Para el proyecto**	**¿Considerado en el proyecto?**	**¿Ayuda al cumplimiento de los objetivos del**	**Total**
Insumos			
Plan de Gestión de calidad	3	4	7
Métricas de Calidad	3	4	7
Listas de chequeo de calidad	2	3	5
Entregables	3	3	6
Técnicas para el control de calidad			
Actividades de inspección, revisión y/o auditorias	2	3	5
Total	**13**	**17**	
Salidas			
Recomendaciones	2	2	4
Mediciones del control de calidad	1	1	2
Total	**3**	**3**	

Tabla. V. 28. Control de calidad del proyecto.

Análisis

El tercer y último proceso, el control de Calidad en el cual se procede a la revisión de todas las técnicas aplicadas en el segundo proceso, para asegurar de que fueron bien

implementadas, de lo cual se obtuvo que: los insumos de este control de calidad son considerados en un 75% y este equipo cree que de igual manera ayuda al cumplimiento de los objetivos del proyecto.

Detallando por actividades los insumos, se evaluó y se concluye que para los proyectos con un 100% lo aplican las Métricas de Calidad y el Plan de Gestión de calidad, mientras que las listas de chequeo de calidad, Entregables y Actividades de inspección, revisión y/o auditorias son aplicadas en un 75%.

Cabe mencionar que en esta última actividad incluye medir, examinar y probar las acciones a emprender para determinar si los resultados del producto y/o servicio están conforme a los requisitos.

Para las salidas se determina que el grupo de trabajo considera a estos aspectos con una en un 50% en la aplicación de los proyectos, y concluyen que de la misma manera no están de acuerdo en que estos aspectos les ayudarían a cumplir los objetivos del proyecto. Detallando cada uno de los aspectos de las salidas se concluye que las mediciones del control de calidad se aplican parcialmente en el proyecto y las Recomendaciones se aplican en un 25% en la calidad del proyecto.

5.2.4 Desarrollo y mantenimiento de sistemas.

En la actividad del Desarrollo de los sistemas que elabora el departamento, involucra la construcción de estas aplicaciones de acuerdo a las necesidades de los usuarios dependiendo las áreas que integran el departamento, las cuales vamos a detallar en el siguiente cuadro:

Valoración	
0	Ninguna gestión (0%)
1	Poca Gestión (35%)
2	Gestión Parcial (70%)
3	Gestión Total (100%)

Necesidades / Áreas	Jefatura	Desarrollo y Programación	Redes	Soporte Técnico	Total
Inventario actualizado	1	0	2	1	4
Que los procesos judiciales sean inmediatamente designados.	3	3	1	1	8
Problemas con los usuarios que van a utilizar el software.	3	2	2	3	10
No empleo de la metodología para el desarrollo de software.	2	1	1	1	5
Existe una alta demanda de equipos que necesitan asistencia técnica	3	1	2	3	9
Suspensión de las labores de los sistemas, por problemas de la red.	3	1	2	3	9
Total	15	6	10	12	

Tabla. V. 29. Desarrollo y Mantenimiento de sistemas.

Análisis

El departamento dividido en sus 4 áreas, desempeñan varias actividades y entre ella la que más sobresale es la de desarrollo, para la cual se tomo las tareas q conlleva para el cumplimiento de la misma, así como las necesidades que se presenta en el departamento, y la valorización que le da cada una de las áreas a estas necesidades. Entonces los datos obtenidos en la matriz presenta q existe poca gestión de parte de cada una de las áreas, hacia las necesidades de: llevar un inventario actualizado y algo muy importante el uso de una metodología para el desarrollo de los sistemas.

Así como también, cabe recalcar, que el departamento con su jefe a la cabeza es quien ayuda en una gestión total a resolver inmediatamente las necesidades presentadas. Las Áreas de Soporte técnico y de Redes también están al apoyo de la soluciones ya que en el departamento se exteriorizan mas en necesidades q inmiscuyen directamente a esta área.

Como nos daremos cuenta también el trabajo del área de desarrollo y programación es de poca gestión, por el factor q mencionamos anteriormente.

La comunicación con el equipo de trabajo se lo realiza mediante las necesidades de los usuarios, y la persona encargada de la designación y conformación de los grupos de trabajos es el jefe del departamento. Para observar y tener conocimiento de cada uno de los proyectos vigentes, para lo cual planifican y ejecutan reuniones semanales o mensuales para tratar asuntos de avances de proyectos, atrasos y problemas que se presentan rutinariamente puede ser con todo el equipo informático para saber qué es lo que están haciendo y como van, o puede ser las reuniones solo entre el equipos de cada área.

Algunas de las técnicas que usa el departamento durante la construcción de los sistemas de información son:

- Preparación del Entorno de Generación y Construcción.
- Generación del Código de los componentes y Procedimientos.
- Ejecución de las Pruebas Unitarias.
- Ejecución de las Pruebas de Integración
- Ejecución de las Pruebas del Sistema.
- Elaboración de los Manuales de Usuario.
- Definición de la Formación de Usuarios Finales.
- Construcción de los Componentes y Procedimientos de Migración y Carga Inicial de Datos.
- Aprobación del Sistema de Información.

Los programas de capacitación lo lleven a cabo al termino del proyecto, la persona responsable del proyecto es la encargada de capacitar el personal de capacitación, y este tendrá la responsabilidad de capacitar a los usuarios y personal técnico de cada uno de los sistemas que se implementa en el departamento.

En el departamento si elaboran planes de trabajo para cada uno de los proyectos a desarrollar así como también para cada una de las funciones que se planifica en el

departamento. De la misma manera para el proceso del desarrollo de los sistemas, los programadores mantienen estándares de desarrollo y usan lenguajes de programación apropiados para cada uno de los proyectos.

La persona encargada de la correcta ejecución de los proyectos realiza seguimientos en las actividades tanto de desarrollo como en las de mantenimiento.

5.2.5 Control de accesos

El acceso no autorizado a los sistemas de información, bases de datos y servicios de información lo controlan mediante permisos de acceso a responsabilidad del Administrador de la bases de datos.

La seguridad entre redes es controlada. No llevan un registro de los eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas. Aunque son solucionados por parte del área de soporte técnico.

El jefe responsable del Área de Redes es la persona encargada de concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

La Protección no es solo un trabajo del departamento de Informática. La Protección comienza en la Dirección de la Compañía y se extiende a toda la empresa. Con el desarrollo de esta actividad queremos verificar la seguridad de la empresa y lograr responder a estas preguntas:

1. **¿Cómo llegará a tener la seguridad que precisa en su empresa?**
2. **¿Qué pasos sigue su compañía para alcanzarla?**
3. **¿Ante caídas -o destrucción- de sus sistemas: La institución podría continuar?**

Este Test debería ser aplicado continuamente por**:** Directivos y Ejecutivos de la Empresa, Gestores de Negocios, y Profesionales de Informática. Pero como aplicativo y proceso auditivo consideramos y lo tomamos en cuenta para poder sacar conclusiones sobre el control de accesos que lleva a cabo el departamento.

La Seguridad, ó si lo prefiere llamar "Ciberseguridad", en la empresa con sus sistemas informáticos conectados a Internet es más importante de lo que "pensamos y apreciamos" y **debe de comenzar en la cúspide de la Dirección de la Empresa y descender a todas las áreas y departamentos que integran la organización.** Aunque en estos momentos piense lo contrario, **también las personas que inspeccionan y operan el negocio** necesitan concienciarse y preocuparse por la seguridad tanto como su Dirección de Informática, la Administración de su Red, o sus vigilantes.

1. Mi compañía, sus directivos y gestores consideran la seguridad informática como responsabilidad de...

- [x] Del departamento de Informática.
- [ ] La Dirección y Gerencia de la Empresa.
- [ ] Todos los Directivos.
- [ ] Todos los Empleados.
- [ ] Todos los indicados en las opciones anteriores.

2. Mi compañía tiene escrito un plan de seguridad y procesos de auditoría ...

- [ ] Si están establecidos.
- [ ] Si están establecidos y se han desarrollado de acuerdo con los objetivos del negocio.
- [x] Están desarrollándose.
- [ ] No tenemos ni plan de seguridad, ni procesos de auditoría. Por ahora, no nos hemos planteado su desarrollo.

3. Mi compañía periódicamente y formalmente evalúa el estado de la información sobre seguridad.

- [x] Si. Se toma tiempo y esfuerzo para revisarla y asignar las acciones que se precisen según el plan establecido.

☐ No. Pero ya se ha iniciado un plan de evaluación.

☐ No. Actualmente no tenemos ningún plan previsto para realizar su evaluación.

4. Mi compañía tiene establecida una arquitectura de seguridad de los sistemas informáticos.

☉ Si. Disponemos de diagramas que detallan todo lo que necesita ser securizado y como debe securizarse.

☐ No. No tenemos definida la arquitectura, pero ya ha comenzado a desarrollarse.

☐ No. No disponemos de arquitectura, ni está previsto crear los diagramas.

5. Mi compañía facilita permanentemente, de forma ágil y controlada, formación en seguridad informática para todos los empleados.

☐ Si. Ofrecemos formación en seguridad informática a toda la organización.

☉ Si. Además de la formación, los asistentes practican con las reglas de seguridad informática establecidas.

☐ Si. Además de la formación y prácticas con las reglas, ***solicitamos*** a los asistentes que se esfuercen en descubrir si pueden ser infringidas.

☐ No. Pero tenemos previsto llevar a cabo un programa de formación.

☐ No. No tenemos formación, ni reglas sobre seguridad informática.

6a. Para controlar el acceso a los activos de información mi compañía usa.

☐ VPNs para controlar el acceso a la red.

☐ Cortafuegos para controlar el acceso a la red.

☉ Cortafuegos y VPNs.

☐ No utilizamos ni VPNs ni Cortafuegos.

6b. Para controlar el acceso mi compañía usa.

- [ ] "Passwords" para el control de acceso a la red.
- [ ] "Passwords" para el control de acceso a la red y sistemas individuales.
- [x] "Passwords" para el control de acceso a la red, sistemas individuales y aplicaciones.
- [ ] "Passwords" para el control de acceso a la red, sistemas individuales, aplicaciones y ficheros.
- [ ] Autenticación Biométrica para controlar el acceso en uno ó más de los niveles anteriores.
- [ ] Mi compañía no hace control de acceso en ningún nivel.

7a. Mi compañía verifica el software para virus, gusanos, caballos de Troya y software no autorizado o pirateado.

- [x] Cada semana.
- [ ] Cada mes.
- [ ] Ocasionalmente.
- [ ] Nunca.

7b. Mi compañía hace copias de seguridad del software y datos.

- [x] Diariamente.
- [ ] Semanalmente.
- [ ] Mensualmente.
- [ ] Ocasionalmente.
- [ ] Nunca.

7c. Mi compañía actualiza y aplica las correcciones (parches) del software.

- [ ] Tan pronto como las actualizaciones y correcciones están disponibles.

◉ Regularmente en intervalos que están definidos.

○ Ocasionalmente.

○ No tenemos costumbre de actualizar o aplicar correcciones en el software que utilizamos.

8. Mi compañía usa herramientas de monitorización del sistema y la red.

○ Si. Tenemos instaladas estas herramientas.

○ Si. Tenemos estas herramientas instaladas y periódicamente examinamos los resultados que producen.

◉ Si. Tenemos estas herramientas instaladas, periódicamente examinamos los resultados que producen, e investigamos cualquier cosa que consideramos sospechosa.

○ No. No tenemos estas herramientas.

9. Mi compañía protege el acceso físico a las instalaciones de los sistemas informáticos.

◉ Si. Mi compañía protege los sistemas y servidores de red en un local cerrado con llave.

○ Si. Mi compañía limita el acceso físico mediante tarjetas de identificación electrónica.

○ Si. Mi compañía limita el acceso físico mediante identificación biométrica.

○ No. En mi compañía no está limitado el acceso físico a los sistemas.

10. Mi compañía tiene un plan de recuperación de desastres que permite la continuidad del negocio.

○ Si. Mi compañía tiene un plan.

○ Si. Mi compañía tiene un plan que ha sido probado recientemente.

◉ No. Mi compañía no tiene un plan

○ No. Pero se ha comenzado a desarrollar uno.

Comentarios sobre la Evaluación y Recomendaciones: Según las respuestas dadas en el Test se obtuvo una evaluación porcentual. La puntuación obtenida permitirá conocer el estado general de la Seguridad que brinda el departamento.

Valoración	
F - FALLA GRAVEMENTE	**0 y 59 puntos**
D - ES MUY POBRE	**60 y 69 puntos**
C - SOLO BASICA	**70 y 79 puntos**
B - ACEPTABLE	**80 y 89 puntos**
A - BUENA	**90 y 100 puntos**

Resultados

LA SEGURIDAD ES MUY POBRE Su empresa ha obtenido 'D'. El departamento obtuvo una puntación de 64, por tanto se concluye q el servicio de seguridad q ofrece el departamento está asumiendo riesgos muy altos.

Su red, datos, operaciones y credibilidad están en alto riesgo. Son muy vulnerables a: hurto, paradas de funcionamiento o destrucción.

Necesita preguntarse seriamente por la inversión requerida para mitigar los riesgos más importantes. Deben tomar conciencia que empresas y ciudadanos de un amplio conjunto de países trabajan y se esfuerzan en desarrollar la Sociedad de la Información y hacer un Ciberespacio Seguro. Conseguirlo es una nueva clase de Defensa Civil, pues depende de todos. Pero en la actualidad, según la puntuación obtenida en el test, su compañía no forma parte de este grupo. El resultado es que además su organización también puede poner a otros en serios riesgos.

Mientras sus sistemas informáticos permanezcan tan vulnerables existen grandes posibilidades de que un hacker pueda hacer uso de sus sistemas para interrumpir Internet o servicios vitales conectados a la misma.

De alta prioridad a la solución de las importantes deficiencias en seguridad de sus sistemas informáticos. Si en su organización no dispone de recursos internos para superar esta situación, le recomendamos que los solicite externamente.

5.2.6 Gestionar los datos, comunicaciones y operaciones

La unidad de informática, o personal de la misma dedicado o asignado en el área de programación o planificación y desarrollo de sistemas, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para el departamento a ser auditado.

La aceptación del software se hará efectiva por los jefes del departamento, previo análisis y pruebas efectuadas por el personal de informática.

Se verificará la utilización de software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.

El software diseñado localmente o llámese de otra manera desarrolladas por programadores internos, deberán ser analizados y aprobados, por el gestor de seguridad, antes de su implementación.

Verificar la tarea de los programadores el realizar pruebas de validación de entradas, en cuanto a las actividades mencionadas en la tabla a ser valorizada.

Los valores que se considera en la tabla valorización, son datos en porcentajes que representan en q valor es aplicado las actividades del programador durante el desarrollo de los sistemas informáticos.

Valoración	
1	Bajo (25%)
2	Medio (50%)
3	Parcialmente (75%)
4	En su totalidad (100%)

Tareas del Programador Actividades a desarrollar	Validación de Entradas y Salidas			Total
	Antes	Durante	Después	
Valores fuera de rango	2	3	4	9
Caracteres inválidos, en los campos de datos	3	3	4	10
Datos incompletos.	2	4	4	10
Datos con longitud excedente o valor fuera de rango	1	4	3	8
Datos no autorizados o inconsistentes.	2	4	4	10
Procedimientos operativos de validación de errores	1	2	3	6
Procedimientos operativos para validación de caracteres.	1	3	3	7
Procedimientos operativos para validación de la integridad de los datos.	3	3	3	9
Procedimientos operativos para validación e integridad de las salidas.	2	2	4	8
Total	17	28	32	

Tabla. V. 30. Actividades del Programador.

Análisis

El trabajo de los programadores, según la tabla nos damos cuenta que los programadores toman más en cuenta las actividades ya después de terminada la tarea. En cambio por actividades individuales, se presenta q los Procedimientos operativos de validación de errores y los Procedimientos operativos para validación de caracteres. Lo aplican en un 50%, mientras q el resto de actividades lo llevan a la práctica con un promedio alto de 75%.

5.3 FASE III CONTROL Y COMUNICACIÓN

5.3.1 Análisis y Control de Activos

Los archivos en el departamento si son protegidos, ya que todas las personas con nombramiento que trabajan en el departamento son los responsables o de tener a su cargo los activos que se encuentran en él. Pero no lo tienen de una forma organizada, simplemente a cada personal se le asigna un determinado activo y se le asigna la responsabilidad de proteger el mismo.

Los activos que llevan un control son:

- ✓ Información(Datos)
- ✓ Las aplicaciones informáticas(SW)
- ✓ Los equipos informáticos(HW)
- ✓ Las redes de comunicaciones
- ✓ Las instalaciones

La información no se encuentra clasificada por capas como las detalladas como tarea de esta actividad, ya que los jefes generalmente son responsables de este tipo de activos independientemente de lo que sean software ó hardware.

5.3.2 Control de Recursos Humanos

La presencia de errores humanos como: comisión de ilícitos, (encargo no permitido legal ni moralmente) uso inadecuado de instalaciones y manejo no autorizado de la información en el departamento se da con frecuencia cuando el Jefe del Departamento sale de vacaciones o con permiso médico, que en este caso queda alguien en su cargo, por lo que la persona que tenga nombramiento es la más adecuada o caso contrario son todos los del Departamento quienes se responsabilizan de las funciones del departamento en forma rotativa

La principal responsabilidad que tienen el personal en el departamento es de cumplir con las obligaciones y tareas asignadas a todos y cada uno del personal que conforman el

departamento de informática, dependiendo del área en que se encuentre, aunque como en el departamento son un equipo y cuando hay mas tareas a realizar en algún departamento, el personal también se une para cumplir dicho propósito y de esta manera quedar alto el Departamento.

Para llevar a cabo los objetivos como departamento, si existen acuerdos de confidencialidad entre el personal del departamento, prácticamente entre todos los que conforman el departamento de Informática, trabajan como equipo, ellos tienen estrategias para manejar de la mejor manera el funcionamiento del departamento.

El departamento garantiza el cumplimiento de las funciones del mismo llevando a cabo semanalmente reuniones de trabajo, para lo cual todos deben tener avances de sus proyectos o novedades y de acuerdo a lo que se diga, la situación y el proyecto se toma las medidas pertinentes.

5.3.3 Comunicar las Aspiraciones y la Dirección de la Gerencia

El equipo de trabajo en las reuniones que tienen semanalmente, comunica las aspiraciones al área de jefatura, para de esta manera llevar siempre la comunicación entre el personal y las personas responsables de los proyectos, de las áreas y del departamento.

5.3.4 Capacitación a los usuarios

La capacitación a los usuarios se lleva a cabo por parte de la persona que desarrolla el sistema, quien a su vez es la responsable de capacitar al personal de capacitación para que ellos se encarguen de transmitir esta información por medio de una capacitación a los usuarios de los sistemas, las cuales serán elaboradas previas a una planificación.

5.4 FASE IV ANÁLISIS Y GESTIÓN DE RIESGOS

5.4.1 Identificación y Evaluación del Riesgo

ID	Descripción del Riesgo	Categoría	Consecuencia
R1	Problemas con los usuarios que van a utilizar el software(70)	Técnico	Acumulación de trabajo

R2	El software no satisface con todas las necesidades previstas por el usuario(40)	Proyecto	Pérdida de tiempo y recursos
R3	Resistencia al uso del software por parte de los usuarios(20)	Negocio	Perdida de recursos al construir un SW que no va a ser usado.
R4	Pérdida de los respaldos durante el desarrollo de software(35)	Negocio	Retraso del proyecto. Información compartida
R5	Pérdida de la documentación de los software desarrollados(12)	Proyecto	Información compartida
R6	Suspensión de las labores de los sistemas, por problemas de la red(75)	Negocio	Retraso en las actividades de la organización
R7	Existe una alta demanda de equipos que necesitan asistencia técnica(80)	Técnico	Perdida de recursos
R8	Pérdida de información almacenada manualmente(5)	Negocio	Información irreal
R9	El soporte Técnico no se proporciona a tiempo(40)	Técnico	Paralización de actividades
R10	El proyecto entregable, no cumple las expectativas del usuario final(20)	Proyecto	Inconformidad con el producto final
R11	No empleo de la metodología para el desarrollo de software(80)	Proyecto	Descoordinación del software
R12	No existe comunicación en el equipo de trabajo(25)	Proyecto	Aumento en los costos. Retraso en la entrega.
R13	No utilizar un mismo estándar de desarrollo(5)	Proyecto	Incomprensión en la reimplantación del proyecto
R14	No realizar el control de acceso al departamento(15)	Negocio	Ingreso de intrusos que pueden sustraer información y/o equipos.

R15	Ingreso a los sistemas sin autentificarse(3)	Negocio	Sustracción de información
R16	Mala administración de los medios de almacenamiento(35)	Negocio	Pérdida de tiempo en buscar una determinada información.
R17	No actualizar el inventario(40)	Negocio	No existe un control de activos. Perdida de equipos
R18	Falta de responsabilidad por parte del personal del departamento(15)	Negocio	Desorganización e incumplimiento de funciones.
R19	Compartir las claves de acceso(15)	Negocio	Acceso a información confidencial.
R20	Incumplimiento de leyes(5)	Negocio	Problemas legales

Tabla. V.31 .Identificación y Evaluación del Riesgo.

CRITERIOS DE VALORACIÓN DE LA PROBABILIDAD

Rango de Probabilidad	Descripción	Valor
1% - 33%	Baja	1
33% - 66%	Media	2
67% - 99%	Alta	3

Tabla. V.32. Criterios de la Valoración de la Probabilidad.

CRITERIOS DE VALORACIÓN DEL IMPACTO

Impacto	Retraso	Impacto Técnico	Impacto en Costo	Valor

Bajo	1 semana	Seguro impacto en el desarrollo del proyecto	< 1 %	1
Moderado	2 semanas	Moderado efecto en el desarrollo del proyecto	< 7 %	2
Alto	1 mes	Severo efecto en el desarrollo del proyecto	< 15 %	3
Crítico	> 1 semanas	Proyecto no puede ser culminado	> 20 %	4

Tabla. V.33. Criterios de la Valoración del Impacto

CRITERIOS DE VALORACIÓN DE LA EXPOSICIÓN AL RIESGO

Exposición	**Valor**	**Color**
Baja	1 o 2	Verde
Media	3 o 4	Amarillo
Alta	Mayor a 6	Rojo

Impacto / Probabilidad	**Bajo=1**	**Moderado=2**	**Alto=3**	**Crítico=4**
Alta	3	6	9	12
Media	2	4	6	8
Bajo	1	2	3	4

Tabla. V.34. Criterios de la Valoración de la Exposición al riesgo

ID	**PROBABILIDAD**			**IMPACTO**		**EXPOSICIÓN**	
	%	**Valor**	**Probabilidad**	**Valor**	**Impacto**	**Valor**	**Exposición**
R1	70	3	Alta	1	Bajo	2	Media
R2	40	2	Media	2	Moderado	4	Media

R3	20	1	Baja	1	Bajo	1	Baja
R4	35	2	Media	2	Moderado	4	Media
R5	12	1	Baja	2	Moderado	2	Baja
R6	75	3	Alta	3	Alto	9	Alta
R7	80	3	Alta	4	Crítico	12	Alta
R8	5	1	Baja	1	Bajo	1	Baja
R9	40	2	Media	3	Alto	6	Alta
R10	20	1	Baja	3	Alto	3	Medio
R11	80	3	Alta	3	Alto	9	Alta
R12	25	1	Baja	1	Bajo	1	Baja
R13	5	1	Baja	1	Bajo	1	Baja
R14	15	1	Baja	1	Bajo	1	Baja
R15	3	1	Baja	1	Bajo	1	Baja
R16	35	3	Alta	1	Bajo	3	Medio
R17	40	2	Media	3	Alto	6	Alta
R18	15	1	Baja	2	Moderado	2	Baja
R19	15	1	Baja	2	Moderado	2	Baja
R20	5	1	Baja	1	Bajo	1	Baja

Tabla. V.35. Valorización de Riesgos.

Estudiando todos y cada uno de los riesgos que se presentan en el departamento en cada una de las tareas se concluye que los riesgos de: Suspensión de las labores de los sistemas, por problemas de la red; Existe una alta demanda de equipos que necesitan asistencia técnica; El soporte Técnico no se proporciona a tiempo; No empleo de la metodología para el desarrollo de software; No actualizar el inventario, **son los de alta exposición** a que pueda llevarse a efecto en interrumpiendo a cumplir los objetivos del departamento.

5.5 FASE V MONITOREO Y CUMPLIMIENTO DE LEYES

5.5.1 Monitoreo del Proceso

Fecha	Variables	Cumple satisfactoriamente
01/12/2010	Organización de las actividades del departamento	SI
03/12/2010	Seguridad de los Sistemas de Información	SI
05/12/2010	Infraestructura tecnológica	SI
06/12/2010	Calidad de proyectos	SI
07/12/2010	Desarrollo y mantenimiento de sistemas	SI
09/12/2010	Control de accesos	SI
11/12/2010	Comunicaciones y operaciones de los datos.	SI
12/12/2010	Control de Activos	SI
13/12/2010	Control de recursos humanos	SI
15/12/2010	Comunicar las aspiraciones y la dirección de la gerencia	SI
17/12/2010	Capacitación a los usuarios	SI
18/12/2010	Identificación y Evaluación de los Riesgos del Departamento	**SI**
18/12/2010	Garantizar el cumplimiento de las leyes	**SI**

5.5.2 Garantizar el cumplimiento de las leyes

Las funciones que desarrollan el departamento y cada personal que labora en el mismo están cumpliendo y garantizando que se encuentre dentro del reglamento y desempeñando muy bien el trabajo que cada miembro del equipo de trabajo del departamento.

5.5.3 Conclusiones

- ✓ Se desarrollo la Auditoria de Riesgos Informáticos Físicos y Lógicos en el Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura, aplicando satisfactoriamente la metodología MACORI por cada actividad de cada una de las fases, llegando a evaluar y a identificar cada uno de los riesgos.

- ✓ En la primera Fase "Definición del Plan", se desarrollo la correcta Recopilación de la información, para lo cual se llevo a cabo entrevistas y encuestas aplicadas al personal del departamento, en la Elaboración del Plan de actividades se lo elaboro estableciendo actividades para cada persona del equipo de trabajo y en la prestación de servicios se identifico cada una de las funciones del departamento.

- ✓ Para la Fase 2 **"**La Gestión Informática", se logro identificar como se encuentra la planificación de la seguridad de los Sistemas de Información desarrollando cuadros y evaluando en la planificación, la coordinación y la supervisión de las actividades que se desarrollan en las áreas de los departamentos para cada uno de los sistemas de información.

- ✓ Se investigo como se desarrollan y se lleva a cabo el mantenimiento de la infraestructura dividiéndolo en seguridades físicas concluyendo que hasta la fecha todos los equipos están completos y no se han reportado robos o daños por parte del personal de trabajo. Para la seguridad lógica el personal lleva un control de acceso el cual se realiza en el dominio mediante el Active Directory, y para los sistemas mediante el propio módulo de ingreso por usuario.

- ✓ El proceso de gestión de calidad de proyectos se verifico, se evaluó y se determino que la Evaluación del desempeño total del proyecto, se realiza por cada jefe del área, ya que es quien se responsabiliza de la actividad dependiendo del proyecto que realicen.

- ✓ Para la actividad del servicio de gestión de seguridad, el servicio de seguridad q ofrece el departamento está asumiendo riesgos muy altos. La red, datos, operaciones y credibilidad están en alto riesgo. Son muy vulnerables a: hurto, paradas de funcionamiento o destrucción.

- ✓ En la Fase 3 **"**El Control y Comunicación" se comprobó que la información no se encuentra clasificada por capas y no esta detalladas, ya que los jefes generalmente son responsables de este tipo de activos independientemente de lo que sean software ó hardware.

- ✓ El departamento garantiza el cumplimiento de las funciones del mismo llevando a cabo semanalmente reuniones de trabajo, para lo cual todos deben tener avances de sus proyectos o novedades y de acuerdo a lo que se diga, la situación y el proyecto se toma las medidas pertinentes.

- ✓ El equipo de trabajo en las reuniones que tienen semanalmente, comunica las aspiraciones al área de jefatura, para de esta manera llevar siempre la comunicación entre el personal y las personas responsables de los proyectos, de las áreas y del departamento.

- ✓ La capacitación a los usuarios se lleva a cabo por parte de la persona que desarrolla el sistema, quien a su vez es la responsable de capacitar al personal de capacitación para que ellos se encarguen de transmitir esta información por medio de una capacitación a los usuarios de los sistemas, las cuales serán elaboradas previas a una planificación.

- ✓ Para la Fase4 **"**El Análisis y Gestión de Riesgos" se llevo a cabo la identificación de los riesgos que se presentan en el departamento auditado, d los cuales se concluye que el riesgo Suspensión de las labores de los sistemas, por problemas de la red; Existe una alta demanda de equipos que necesitan asistencia técnica; El soporte Técnico no se proporciona a tiempo; No empleo de la metodología para el desarrollo de software y el No actualizar el inventario, son riesgos de alta

exposición que pueda llevarse a efecto llegando a interrumpir el cumplimiento de los objetivos del departamento.

- ✓ En la Fase 5 **"**El Monitoreo y Cumplimiento de leyes" se determino que si se lleva a cabo un el Monitoreo del Proceso en el Departamento y se investigo que si se llevo a cabo el cumplimiento de las leyes.

5.6 COMPROBACIÓN DE LA HIPOTESIS

Hipótesis - Planteada

El desarrollo y la aplicación de la metodológica para la auditoria de riesgos informáticos (físicos y lógicos) basados en varias herramientas y metodologías de auditoría informática; proporcionará resultados eficientes para el departamento de informática de la organización auditada.

Demostración de la Hipótesis

Para la comprobación de la hipótesis anteriormente citada se presenta a continuación los resultados obtenidos del estudio y análisis que proyectaron a través de la auditoría realizada anteriormente en el departamento (resultados que se puede observar en **el anexo 7**), en comparación con la metodología desarrollada (apartado que se puede observar en la Tabla 12 y Figura 32 y 33) y con la aplicación de la MACORI valorizamos con la siguiente tabla, de esta manera demostraremos cuan eficiente resulto la aplicación de la metodología en el departamento de Informática.

Valorización MACORI			
Excelente	**Muy Buena**	**Buena**	**Malo**
4	**3**	**2**	**1**

Parámetro 1 (P1=Definición del Plan)

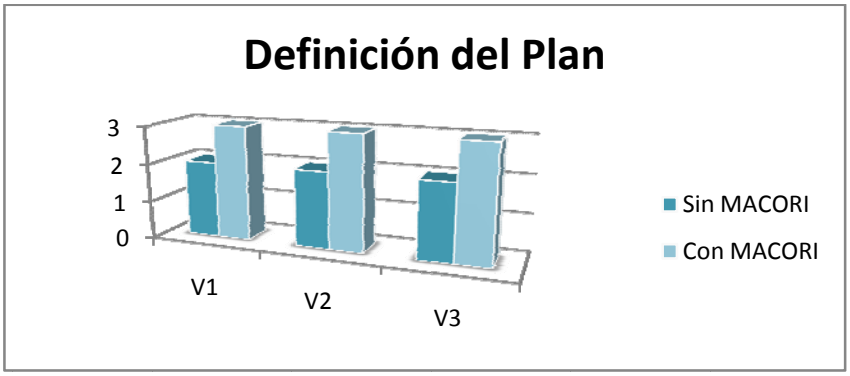
Variables:

V1= Recogida de información

V2= Cumplimiento de objetivos y de una política de seguridad.

V3= Prestación y Organización de Servicios

Parámetro 1		
Variables	**Sin la aplicación de la metodología MACORI**	**Con la aplicación de la metodología MACORI**
Variable 1 (V1)	3	4
Variable 1 (V2)	2	3
Variable 1 (V3)	2	3
Total P1	**7**	**10**



En el parámetro definición del plan, realizamos un análisis de la información (ver tabla 2, 4, 6, 7, 8 y 9) que se logro recabar para cada una de las variables en la auditoría realizada previamente en la institución, con una valorización que se da con la aplicación de MACORI se concluye que en este apartado la eficiencia se aplica en un 83% mientras que sin la aplicación de la metodología en un 58%.

Parámetro 2 (P2= Gestión Informática)

Variables:

V1= Seguridad de los Sistemas de Información.

V2= Infraestructura tecnológica.

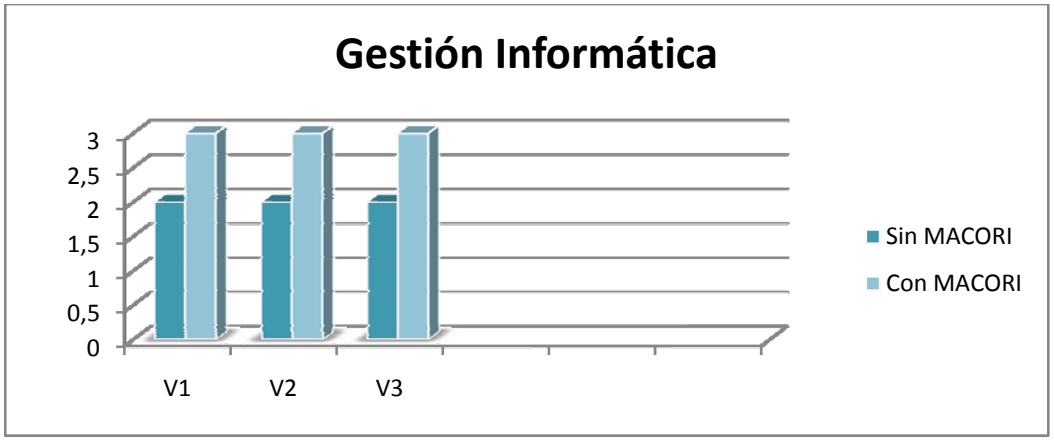
V3= Calidad de proyectos.

V4= Desarrollo y mantenimiento de sistemas.

V5= Control de accesos.

V6= Comunicaciones y operaciones de los datos.

Parámetro 2		
Variables	**Sin la aplicación de la metodología MACORI**	**Con la aplicación de la metodología MACORI**
Variable 1 (V1)	2	4
Variable 2 (V2)	2	4
Variable 3 (V3)	1	4
Variable 4 (V4)	4	4
Variable 5 (V5)	2	3
Variable 6 (V6)	2	3
Total P2	**13**	**22**



Para el parámetro Gestión Informática se realizó un análisis de la información (ver tabla 2, 4, 6, 7, 8 y 9) que se logro recabar para cada una de las variables en la auditoría realizada previamente en la institución, con una valorización que se da con la aplicación de

MACORI se concluye que en este apartado la eficiencia se aplica en un 91% mientras que sin la aplicación de la metodología en un 54%.

Parámetro (P3= Control y Comunicación)

Variables:

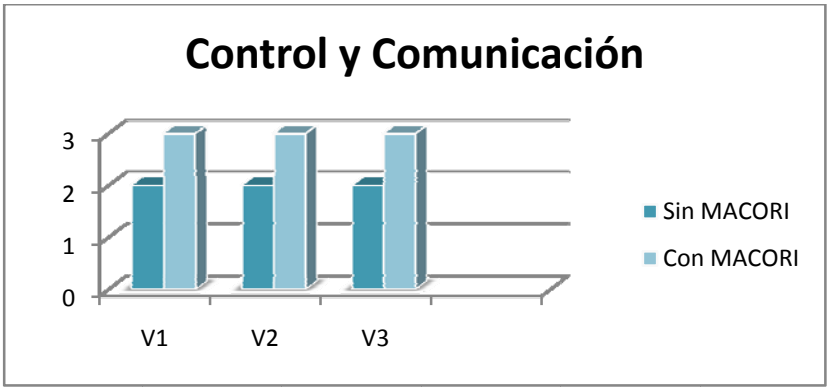
V1 = Análisis y Control de Activos

V2 = Control de recursos humanos

V3 = Comunicar las aspiraciones y la dirección de la gerencia

V4 = Capacitación a los usuarios

Parámetro 3		
Variables	**Sin la aplicación de la metodología MACORI**	**Con la aplicación de la metodología MACORI**
Variable 1 (V1)	3	3
Variable 2 (V2)	3	3
Variable 3 (V3)	1	4
Variable 4 (V4)	1	3
Total P3	**8**	**13**



Para el parámetro Control y Comunicación se realizó un análisis de la información (ver tabla 2 y 4) que se logro recabar para cada una de las variables en la auditoría realizada

previamente en la institución, con una valorización que se da con la aplicación de MACORI se concluye que en este apartado la eficiencia se aplica en un 81% mientras que sin la aplicación de la metodología en un 50%.

Parámetro 4 (P4= Análisis y Gestión de Riesgos)

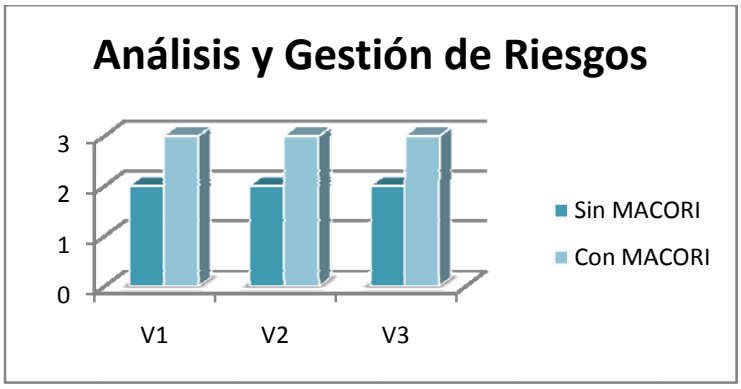
Variables:

V1 = Identificación y Evaluación del Riesgo

V2 = Establecer planes de contingencia

V3 = Identificación, selección e implementación de salvaguardas

Parámetro 4		
Variables	**Sin la aplicación de la metodología MACORI**	**Con la aplicación de la metodología MACORI**
Variable 1 (V1)	3	4
Variable 2 (V2)	3	3
Variable 3 (V3)	3	3
Total P4	**9**	**10**



En el parámetro Análisis y Gestión de Riesgos, realizamos un análisis de la información (ver tabla 2, 7, 9 y 10) que se logro recabar para cada una de las variables en la auditoría realizada previamente en la institución, con una valorización que se da con la aplicación de MACORI se concluye que en este apartado la eficiencia se aplica en un 83% mientras que sin la aplicación de la metodología en un 75%.

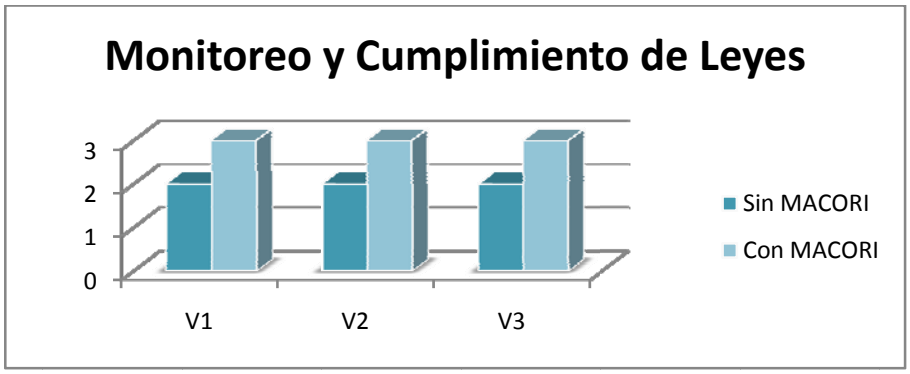
Parámetro 5 (P5= Monitoreo y Cumplimiento de Leyes)

Variables: V1=Monitoreo del Proceso

V2=Garantizar el cumplimiento de las leyes

V3=Conclusiones

Parámetro 5		
Variables	**Sin la aplicación de la metodología MACORI**	**Con la aplicación de la metodología MACORI**
Variable 1 (V1)	2	3
Variable 2 (V2)	2	3
Variable 3 (V3)	2	3
Total P5	**6**	**9**



En el parámetro Monitoreo y Cumplimiento de Leyes, realizamos un análisis de la información (ver tabla 5, 6, y 11) que se logro recabar para cada una de las variables en la auditoría realizada previamente en la institución, con una valorización que se da con la

En aplicación de MACORI se concluye que en este apartado la eficiencia se aplica en un 75% mientras que sin la aplicación de la metodología en un 50%.

Parámetros	Variables	Sin MACORI	Con MACORI	Promedio Sin MACORI	Promedio Con MACORI
Definición del Plan	**V1= Recogida de información**	**3**	**4**		
	V2= Cumplimiento de objetivos y de una política de seguridad.	**2**	**3**		
	V3= Prestación y Organización de Servicios	**2**	**3**		
		7	**10**	**58%**	**83%**
Gestión Informática	**V1= Seguridad de los Sistemas de Información**	**2**	**4**		
	V2= Infraestructura tecnológica	**2**	**4**		
	V3= Calidad de proyectos	**1**	**4**		
	V4= Desarrollo y mantenimiento de sistemas	**4**	**4**		
	V5= Control de accesos	**2**	**3**		
	V6= Comunicaciones y operaciones de los datos.	**2**	**3**		
		13	**22**	**54%**	**91%**
Control y Comunicación	**V1 = Análisis y Control de Activos**	**3**	**3**		
	V2 = Control de recursos humanos	**3**	**3**		
	V3 = Comunicar las aspiraciones y la dirección de la gerencia	**1**	**4**		
	V4 = Capacitación a los usuarios	**1**	**3**		
		8	**13**	**50%**	**81%**

P4= Análisis y Gestión de Riesgos	**V1 = Identificación y Evaluación del Riesgo**	**3**	**4**		
	V2 = Establecer planes de contingencia	**3**	**3**		
	V3 = Identificación, selección e implementación de salvaguardas	**3**	**3**		
		9	**10**	**75%**	**83%**
Monitoreo y Cumplimiento de Leyes	**V1=Monitoreo del Proceso**	**2**	**3**		
	V2=Garantizar el cumplimiento de las leyes	**2**	**3**		
	V3=Conclusiones	**2**	**3**		
		6	**9**	**50%**	**75%**

Totales de los parámetros que se obtuvo sin la aplicación de la metodología

$$\sum \boldsymbol{Parametros} = \%\boldsymbol{P1} + \%\boldsymbol{P2} + \%\boldsymbol{P3} + \%\boldsymbol{P4} + \%\boldsymbol{P5}$$

$$\sum \boldsymbol{Parametros} = \mathbf{58\%} + \mathbf{54\%} + \mathbf{50\%} + \mathbf{75\%} + \mathbf{50\%}$$

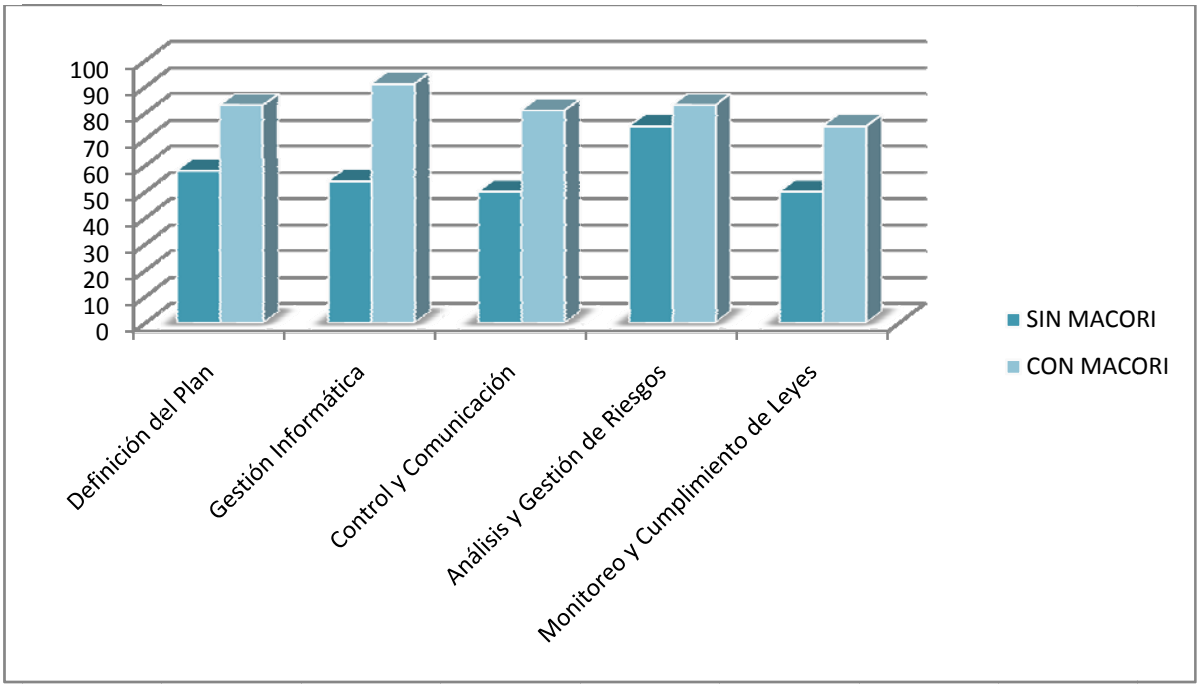
$$\sum \boldsymbol{Parametros} = \mathbf{57,4\%}$$

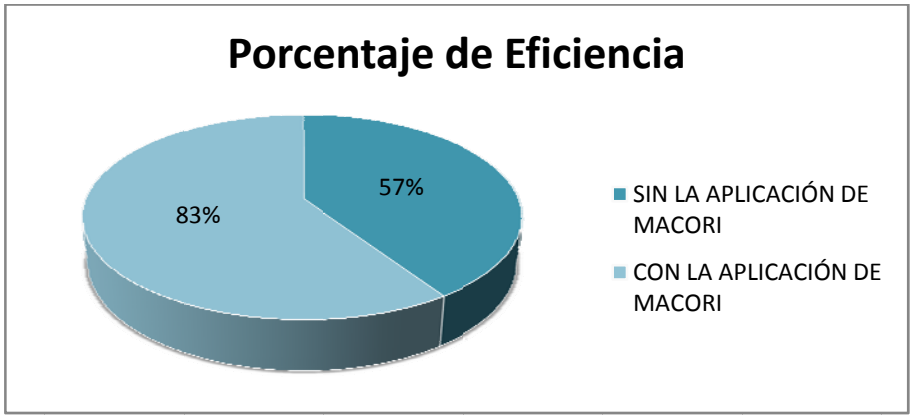
Totales de los parámetros que se obtuvo con la aplicación de MACORI

$$\sum \boldsymbol{Parametros} = \%\boldsymbol{P1} + \%\boldsymbol{P2} + \%\boldsymbol{P3} + \%\boldsymbol{P4} + \%\boldsymbol{P5}$$

$$\sum \boldsymbol{Parametros} = \mathbf{83\%} + \mathbf{91\%} + \mathbf{81\%} + \mathbf{83\%} + \mathbf{75\%}$$

$$\sum \boldsymbol{Parametros} = \mathbf{82,6\%}$$





Conclusión

Luego de un trabajo de análisis desarrollo y aplicación de metodologías, se llevo a cabo la comprobación de cuan eficiente llego a ser en la puesta en práctica en el Departamento de Informática, proporcionando como resultados que llego a ser más eficiente en un 25.2% la Metodología MACORI, en comparación a resultados obtenidos en base resultados de la auditoría realizada previamente en el departamento.

CONCLUSIONES

- ✓ Previo a un estudio y análisis de metodologías, se desarrollo una metodología para la auditoria de riesgos informáticos, la cual nos ayudo a la identificación de riesgos físicos y lógicos del Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura.
- ✓ Se estudió recursos herramientas, estándares, normas involucradas en auditoría informática y en riesgos informáticos, se acoplo conceptos y se determino las mejores prácticas y se procedió a recabar lo más relevante de cada recurso estudiado, para el respectivo análisis.
- ✓ Luego de la selección de las herramientas consideradas como mejores prácticas tales como: COBIT, ISO 17799 y MAGERIT, se procedió a un análisis minucioso de cada herramienta, estudiando cada una de las actividades de cada metodología y llegando a concluir que Cobit se enfoca mas a la administración y regulación de las actividades de la organización, inmiscuyendo siempre al gobierno TI, mientras que ISO 17799 se orienta mas al trabajo de seguridad de la infraestructura tecnológica y Magerit dirige cada actividad en la identificación y gestión de los riesgos que se pueden presentar en la empresa.
- ✓ Se desarrolló MACORI una metodológica de Auditoría de Riesgos Informáticos (físicos y lógicos) tomando las etapas más importantes de las herramientas analizadas, integrando un procedimiento completo que involucra el trabajo de la administración de la seguridad y la gestión de los problemas identificados.
- ✓ La puesta en práctica de MACORI del Departamento de Informática de la Empresa se procedió auditar mediante cada una de las fases de la metodología, llegando a determinar el cumplimiento en algunas fases y la inobservancia en otras actividades resultados que se presento al concluir la auditoria.
- ✓ Los resultados de la auditoría realizada en el departamento de informática, mediante la metodología MACORI resulto ser más eficiente en un 25% en comparación a resultados obtenidos en otra auditoria , resultados que se proporciono mediante un informe detallado por cada una de las fases, al jefe del departamento como ayuda para que los riesgos identificados sean solucionados.

RECOMENDACIONES

- ✓ Para un estudio a profundidad se recomienda que para el desarrollo del estudio y análisis de metodologías existentes, se tome en consideración ,técnicas y herramientas de comparación avanzadas, que sea para aplicar las empresas de nuestro medio.

- ✓ Que la metodología desarrollada debe ser utilizada exclusivamente para realizar auditorías de riesgos en el área informática ya que contiene actividades que puede ser aplicada en organizaciones de nuestro medio.

- ✓ Por las ventajas que nos brinda la metodología MACORI se recomienda a las instituciones públicas y privadas, aplicarla en sus áreas informáticas, para determinar los riesgos por los que puede estar atravesando los equipos informáticos.

RESUMEN

Se desarrollo una metodología para la auditoría de riesgos informáticos (físicos y lógicos) con el objetivo de evaluar la eficacia y eficiencia que presenta el Departamento de Informática de la Dirección Provincial del Consejo de la Judicatura de la Provincia de Pichincha.

Para la elaboración de la metodología, se realizó un análisis previo de las metodologías ITIL, COBIT, ISO 17799, CRMR y MARGERIT, de las cuales se considero los procesos más importantes y que estén acorde a las necesidades de la empresa, realizando para ello cuadros comparativos con cada una de las fases que incluye estas metodologías, llegando así a estructurar 5 fases las cuales conforman la Metodología llamada MACORI (Metodología de Análisis y Control de Riesgos Informáticos).

La auditoria de riesgos informáticos (físicos y lógicos) se llevo a cabo cumpliendo cada una de las fases de la metodología MACORI, para ello se realizó entrevistas y encuestas al personal del departamento, así como también se ejecutó la técnica de observación, para constatar el funcionamiento tanto del equipo informático físico como lógico.

La metodología desarrollada puede ser utilizada exclusivamente para realizar auditorías de riesgos en el área informática y contiene actividades que puede ser aplicada en organizaciones de nuestro medio.

Los resultados de la auditoría realizada en el departamento de informática, mediante la metodología MACORI resulto ser más eficiente en un 25% en comparación a resultados obtenidos en otra auditoria , resultados que se proporciono mediante un informe detallado por cada una de las fases, al jefe del departamento como ayuda para que los riesgos identificados sean solucionados.

La aplicación de la metodología MACORI ayuda a la correcta evaluación de los riesgos que se presentan en el departamento del Consejo de la Judicatura de la Provincia de Pichincha, superando las fortalezas y oportunidades como institución.

Por las ventajas que nos brinda la metodología MACORI se recomienda a las instituciones públicas y privadas, aplicarla en sus áreas informáticas, para determinar los riesgos por los que puede estar atravesando los equipos informáticos.

SUMMARY

A methodology for informatics risk(physical and logical) auditory was developed to evaluate the efficacy and efficiency of the Informatics Departament of the Province Directorship of the Judiciary Council of Pichincha Province. Fort he methodology elaboration a previous analysis of the methodologies ITIL, COBIT, ISO 17799, CRMR and MAGERIT was carried out of which the most important processes were considered making sure they agree whit the Enterprise needs. Comparative charts were form the methodology called MACORI(Informatics Risk Control and Analysis Metodology). The informatics risk auditory (physical and logical) was carried out accomplishing each phase of the MACORI methodology; for this interviews and questionnaires were made to the department personnel; the observation technique was also carried out to assess the functioning of both the informatics physical and logical equipment. The developed methodology can be exclusively used to carry out auditory of risks in the informatics area and contains activities which can be applied in the organizations of our environment. From the auditory results at the informatics departamento the MACORI methodology proved to be more efficent by a 25% as compared to the results of another auditory; these results were provided through a detailed report for each phase to the departamento head as a help for the risk solution. The MACORI methodology application helps the correct evaluation of the risks at the Judiciary Council Department of the Pichincha Province, overcoming strengths and opportunities as an institution.

Because of its advantages the MACORI methodology is recommended to the public and prívate institution so that they could apply it informatics areas to determine the risks of the informatics equipament.

ABREVIATURAS	
CMM	Modelo de Capacidad y Madurez.
ISO 17799	(International Organization for Standardization) estándar para la seguridad de la información.
MAGERIT	La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas.
IBM-PC	International Business Machines Personal Compute
FREE BSD	Sistema operativo UNIX de libre distribución.
NET BSD	NetBSD es un sistema operativo de la familia Unix.
IEC950	Comisión Electrotécnica Internacional (Especificación Técnica, Protocolos De Ensayo, Homologación De Marcas Y Modelos, Reparación, Mantenimiento Y Condiciones A Cumplir Por Las Empresas Proveedoras).
ISACA.-	Asociación para la Auditoría y Control de Sistemas de Información
ITGI.-	Instituto de Administración de las Tecnologías de la Información
ITSEC.-	Criterios de la evaluación de seguridad de la tecnología de información
COSO.-	Organizaciones Patrocinadoras de la Comisión Treadway
ISO 9001.-	Organización Internacional para la Estandarización y especifica los requisitos para un buen sistema de gestión de la calidad
PRINCE2	Método de gestión de proyectos que cubre la administración, control y organización de un proyecto
UK	
OGC	
TICs.-	Tecnologías de la información y la comunicación
UNE 71502.-	Norma específica los requisitos para establecer, implantar, documentar y evaluar un SGS

BS 7799.-	Estándar de seguridad de información de facto, creada por British Standards Institution (BSI) como un conjunto de controles de seguridad y de metodologías para su correcta aplicación.
UNE-ISO UNE-EN-ISO	Es una norma ISO tomada por CEN y convertida en norma EN-ISO
IEC 17799	Comisión Electrotécnica Internacional estándar para la seguridad de la información
LPI.-	Ley de Propiedad Intelectual
LSSI.-	Ley de Servicios de la Sociedad de Información y Comercio Electrónico
SGI	
SAP.-	Sistema informático diseñado para gestionar de manera más eficiente los recursos y procesos de producción de bienes y servicios al interior de una organización
IEEE STD 610 – 1991	Institute of Electrical and Electronics Engineers Staff
NORMA ISO 9001:2000	Especificaciones técnicas y desarrollo de la certificación de gestión de la calidad
IEEE 1012	Standard for Software Verification and Validation

GLOSARIO

Amenazas.- Cualquier acción o evento que puede ocasionar consecuencias adversas

Análisis de impacto al negocio.- Evaluar los resultados y las consecuencias de la inestabilidad.

Ataques.- Tipos y naturaleza de inestabilidad en la seguridad

Autenticación.- Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

Autorización: Lo que se permite cuando se ha otorgado acceso

Backup.- En tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

Benchmarking.- Es el proceso continuo de medir productos, servicios y prácticas contra los competidores o aquellas compañías reconocidas como líderes en la industria

Biométrica.-Estudio de los métodos automáticos para la identificación de personas basados en características físicas o conductuales.

Boot.-En informática, la secuencia de arranque, (boot o booting en inglés) es el proceso que inicia el sistema operativo cuando el usuario enciende una computadora.

Bugs.- es el resultado de un fallo o deficiencia durante el proceso de creación de programas de ordenador o computadora (software).

Control de Acceso.- Limitar el acceso autorizado solo a entidades autenticadas

Checklist.- El término monitoreo de red describe el uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla vía correo electrónico, beeper u otras alarmas.

Euro método.-La dinámica de la vida moderna provoca continuos cambios en las actividades comerciales de todos los tipos de organizaciones (incluyendo las administraciones públicas). Para hacer frente a estos cambios se precisan sistemas de información cada vez más potentes y flexibles.

Estrategia.- los pasos que se requieren para alcanzar un objetivo

Exposiciones.- Áreas que son vulnerables a un impacto por parte de una amenaza

Gobierno.- proporcionar control y dirección a las actividades

Hacking.-Gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats").

Identificación.- Verificación de una persona o cosa; reconocimiento.

Impacto.- Los resultados y consecuencias de que se materialice un riesgo

Integridad.- La corrección de los datos que presenta una base de datos.

Knowledge.-1.Hechos, o datos de información adquiridos por una persona a través de la experiencia o la educación, la comprensión teórica o práctica de un tema u objeto de la realidad.

Lógica difusa.-La lógica difusa o lógica heurística se basa en lo relativo de lo observado. Este tipo de lógica toma dos valores aleatorios, pero contextualizados y referidos entre sí.

Métrica.-Es la medida que permite caracterizar un sistema de información o software.

Monitoreo.- Medición de actividades de seguridad

Normas.- Establecer los límites permisibles de acciones y procesos para cumplir con las políticas

Outsourcing.-El término outsourcing, aunque no específico del área de sistemas, refleja el uso de agentes externos para ejecutar una o más actividades organizadas.

Plan de contingencia.-es un tipo de plan preventivo, predictivo y reactivo.

Políticas.- declaración de alto nivel sobre la intención y la dirección de la gerencia

Políticas de seguridad.-Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.
Riesgo.- La explotación de una vulnerabilidad por parte de una amenaza

Sabotaje.- Daño o deterioro que para perjudicar a los patronos hacen los usuarios en la maquinaria o productos.
Salvaguarda.-Protección, defensa, garantía.

Sarbanes Oxley.-La Ley Sarbanes Oxley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

StakeHolders.- Se puede definir como cualquier persona o entidad que es afectada por las actividades de una organización; por ejemplo, los trabajadores de esa organización, sus accionistas, las asociaciones de vecinos, sindicatos, organizaciones civiles y gubernamentales, etc.

Usabilidad.-Es la facilidad con que las personas pueden utilizar una herramienta particular o cualquier otro objeto fabricado por humanos con el fin de alcanzar un objetivo concreto.

Vulnerabilidades.- Deficiencias que pueden ser explotadas por amenazas

BIBLIOGRAFIA WEB

1. Análisis y Gestión de Riesgos

http://www.willydev.net/descargas/willydev_gerenciaderiesgosfactorcriticodeexito.pdf

http://e-articles.info/t/i/1619/l/es/

http://www.eumed.net/libros/2009c/605/PLAN%20DE%20CONTINGENCIA%20INFORMATICO%20Y%20SEGURIDAD%20DE%20INFORMACION%20PRESENTACION.htm

http://www.mailxmail.com/curso-gestion-riesgos-sistemas-informacion/identificacion-mecanismos-salvaguarda-amenazas

http://inspeccionumvi11.iespana.es/ind12213.pdf

http://www.darfe.es/CMS/

15/09/10

2. Auditoria

http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

http://www.utpl.edu.ec/ecc/wiki/index.php/Auditoria_Inform%C3%A1tica#Datos_Generales:_7

05/06/10

3. Catástrofes

http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm

05/06/10

4. Cobit

http://www.monografias.com/trabajos38/cobit/cobit.shtml

http://msaffirio.wordpress.com/2007/03/03/la-cobit-y-la-organizacion-del-area-informatica/

http://www.isaca-bogota.net/Metodologias/COBIT/COBIT4.0_Castellano.pdf

http://www.dspace.espol.edu.ec/bitstream/123456789/5300/2/COBIT.ppt

08/07/10

5. Control y Comunicación

http://www.scribd.com/doc/6538499/Analisis-y-Control-Del-Activo-Fijo?secret_password=&autodown=pdf

http://pdf.rincondelvago.com/control-de-rrhh.html

http://www.elprisma.com/apuntes/administracion_de_empresas/controldepersonal/

http://www.aladi.org/biblioteca/08_CapacitacionUsuarios.html

http://www.sicht.ucv.ve:8080/biblioteca/software/taller/ponencias/UNIANDES.pdf

http://www.bibliociencias.cu/gsdl/collect/bdref/index/assoc/HASH0131.dir/doc.pdf

http://www.monografias.com/trabajos29/importancia-capacitacion/importancia-capacitacion.shtml

10/08/10

6. Gestión Informática

http://alarcos.inf-cr.uclm.es/per/fruiz/cur/mso/comple/Cobit.pdf

https://www.mdgsi.upv.es/mis/datoscursospdf/librotemario.pdf

http://www.recursosnorenovables.gov.ec/es/el-ministerio/341-direccion-de-gestion-tecnologica.html

http://www.recursosnorenovables.gov.ec/es/el-ministerio/385-gestion-tecnologico-procesos.html

http://www.slideshare.net/lecastillox/adquirir-implementar-cobit4

http://www.slideshare.net/elsy123/plan-de-gestion-de-uso-de-tic-2384735

http://www.monografias.com/trabajos11/conge/conge.shtml

http://www.icesi.edu.co/blogs/gerenciaproyectosti/2008/09/19/gestion-de-la-calidad/

http://www.slideshare.net/rfsolano/gestion-de-la-calidad-del-proyecto-547726

http://red2007-cursoaci.nireblog.com/post/2007/03/03/servicio-de-desarrollo-y-mantenimiento-de-los-sistemas

http://www.csae.map.es/csi/metrica3/evs.pdf

http://www.wikilearning.com/tutorial/control_de_accesos-introduccion/3394-1

05/08/10

7. Itil

http://www.osiatis.es/formacion/formacion_itil.php

ISO 17799

http://www.mvausa.com/Colombia/Presentaciones/INTRODUCCION_ISO_17799.pdf

http://es.wikipedia.org/wiki/ISO/IEC_17799

03/08/10

8. Magerit

http://es.wikipedia.org/wiki/Magerit

http://www.um.es/giisw/oficial/cMagerit.htm

03/08/10

9. Metodología

http://www.monografias.com/trabajos31/metodologia-itil/metodologia-itil.shtml

http://www.taringa.net/posts/downloads/2996453/Software-d-Auditoria-Informatica,-Planeacion-y-Riesgos-de-TI.html

http://revistas.mes.edu.cu/eduniv/02-Libros-por-ISBN/959-16-0500/0455-Metodologia-para-Auditorias-de-Informacion-Investigacion-UPR.pdf

05/06/10

10. Organización de la Seguridad Informática

http://www.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica?autodown=pdf

http://auditoriasistemas.com/auditoria-informatica/seguridad-informatica/

17/03/2010

11. Políticas de seguridad

http://www.segu-info.com.ar/politicas/

http://www.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica

http://auditoriasistemas.com/auditoria-informatica/politicas-de-seguridad/

http://www.unal.edu.co/seguridad/documentos/guia_para_elaborar_politicas_v1_0.pdf

17/03/2010

12. Riesgo

http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf

http://www.basc-costarica.com/documentos/riesgosinformatica.pdf

http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf

http://www.basc-costarica.com/documentos/riesgosinformatica.pdf

08/07/10

13. Seguridad de la información

http://www.mvausa.com/Colombia/Presentaciones/INTRODUCCION_ISO_17799.pdf

17/03/2010

14. Unidad informática

http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm

17/03/2010

ANEXOS