DESARROLLO DE UNA GUÍA DE GESTIÓN DE RIESGOS DE TECNOLOGÍA INFORMÁTICA PARA ENTIDADES PÚBLICAS, A PARTIR DE LA METODOLOGIA COBIT Y LOS LINEAMIENTOS DEL GOBIERNO DE TI.

MONICA MERCADO
FABIOLA MEZA
GLADYS PICO
ERNESTO ROBLES
LOURDES SIERRA

TRABAJO INTEGRADOR PARA OPTAR AL TITULO DE ESPECIALISTA EN GERENCIA DE SISTEMAS DE INFORMACION

UNIVERSIDAD DEL NORTE EN CONVENIO CON LA UNIVERSIDAD TECNOLOGICA DE BOLIVAR

TUTOR

JORGE ENRIQUE GIL PEÑALOZA

CARTAGENA DE INDIAS D. T. Y C., 2006

TABLA DE CONTENIDO

INDICE DE GRAFICAS

INDICE DE TABLAS

INDICE DE FORMAS

INDICE DE ANEXOS

TEMA

Desarrollo de una Guía de Gestión de Riesgos de Tecnología Informática para Entidades Públicas, a partir de la metodología Cobit y los lineamientos del Gobierno de TI.

1. INTRODUCCIÓN

En nuestra opinión, el mayor grado de automatización de los procesos de negocio hace que las distintas áreas de una compañía se sostengan y apoyen cada vez más en los servicios de procesamiento de información.

Pensamos que a medida que las organizaciones se van transformando para competir en el mundo de la información, la capacidad para explotar sus activos intangibles se está haciendo más decisiva que su capacidad para gestionar sus activos físicos. La eficacia y eficiencia futuras de las compañías dependen cada vez en mayor grado del funcionamiento ininterrumpido de los sistemas de aplicación, ya que los mismos deben hacer posible dirigir y controlar el negocio mediante la distribución de la información en forma y tiempo tales que permitan a la Gerencia cumplir con sus responsabilidades.

Es aquí en donde nos atrevemos a afirmar que se hace importante el término de *gobernar correctamente los recursos de tecnologías de información*, también llamado por los expertos en el tema *Gobierno de TI*. Según nuestra investigación y experiencia, un correcto gobierno de TI hace posible el aprovechamiento al máximo de las capacidades que los sistemas de procesamiento de datos pueden brindar a una organización, esto se logra a través ciertas herramientas diseñadas especialmente para tal fin.

[1]Afirma la literatura especializada que el Gobierno de TI debe agregar valor al negocio a través del uso eficiente y eficaz de los recursos de tecnología de información, asegurar que no se realicen inversiones de TI en proyectos poco factibles desde el punto de vista técnico y económico, y garantizar la existencia de mecanismos de control adecuados.

Basados en lo anterior, preparamos este documento que describe una guía metodológica que incluye el estudio de las políticas de riesgo, funciones y responsabilidades de las diferentes áreas, y los procedimientos para, como parte también de la guía, medir, analizar, monitorear, controlar y administrar los riesgos relacionados con las TI existentes en la Gobernación de Bolívar, como lo son: Riesgos de Integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgos en la infraestructura y Riesgos de seguridad general, todo esto apoyado en estudios realizados en el año 2000 y una reciente auditoria de sistemas llevada a cabo en el año en curso.

La guía considera como herramienta de Gobierno de TI, a utilizar en cumplimiento de los fines del presente trabajo, la definición de los recursos de TI formulada por el modelo de control [2] COBIT, según se describe a continuación:

Datos	Objetos en su sentido más amplio (es decir, internos y externos), estructurados y no estructurados, gráficos, sonido, etc.
Sistemas de aplicación	Se entiende por tales los sistemas computadorizados de procesamiento de información, incluyendo los procesos manuales relacionados y las interfaces entre los mismos.
Tecnología	La tecnología abarca el hardware, los sistemas operativos, los sistemas de administración de bases de datos, las redes, los multimedios, etc.
Instalaciones	Recursos utilizados para alojar y dar soporte a los sistemas de información
Personas	Habilidades, aptitudes, conocimiento y productividad del personal para planificar, organizar, adquirir, entregar, brindar soporte y monitorear los sistemas y servicios de información

Fig. 1 Modelo de Control de COBIT

La norma COBIT muestra cuatro dominios básicos sobre los cuales trabajar y mediante los cuales se puede lograr un correcto y eficaz gobierno de TI, siempre y cuando se apliquen los controles y procedimientos necesarios para mantener la normalidad en cada uno de los aspectos que cubren los 4 dominios, estos dominios son: Planeación y Organización, Adquisición e Implementación, Entrega y Soporte y por ultimo Monitoreo e interactúan unos con otros mediante el diagrama siguiente:

Fig. 2 Estructura de Cobit

2. OBJETIVO GENERAL

Desarrollar una Guía de Gestión de Riesgos de Tecnología Informática utilizando la metodología Cobit y los lineamientos del Gobierno de TI, como herramienta de medición, eficiencia, efectividad y cumplimiento de los controles implementados en las entidades públicas.

3. OBJETIVOS ESPECIFICOS

- ✓ Establecer un procedimiento documentado para la definición del contexto organizacional y de administración del riesgo incluyendo el criterio de evaluación de los riesgos.
- ✓ Definir una metodología adecuada para la identificación de los escenarios, recursos informáticos y tecnología informática que posee la entidad pública.
- ✓ Definir el procedimiento para la Identificación y análisis de los riesgos asociados a cada uno de los escenarios en que se llevan a cabo procesos relacionados con recursos de TI en la entidad pública.
- ✓ Diseñar el modelo de evaluación con el fin de establecer las prioridades de la administración de riesgos.
- ✓ Diseñar la estructura con la cual se hará monitoreo y revisión al desempeño del sistema de administración y los cambios que podrían afectarlo.

4. ALCANCE

Se diseñará una Guía para la Gestión de Riesgos de TI para Entidades públicas con base en la metodología Cobit y los lineamientos del Gobierno de TI la cual contendrá:

- ✓ El procedimiento para establecer el contexto estratégico, organizacional y de administración del riesgo asociado a la TI.
- ✓ La metodología adecuada para la Identificación de los riesgos a través de qué, porqué y cómo las cosas pueden suceder.
- ✓ El procedimiento para el análisis de riesgos mediante la determinación de los controles existentes y los riesgos analizados en términos de consecuencia y probabilidad en el contexto de esos controles.
- ✓ El formato de evaluación de riesgos, comparando los niveles de riesgo estimados contra el criterio pre-establecido.
- ✓ El procedimiento para monitoreo y revisión del sistema de administración de riesgos asociados a TI y los cambios que podrían afectarlo.
- ✓ La metodología para el establecimiento de planes de comunicación al interior de la organización para el proceso de administración del riesgo.

La aplicación de la Guía de Gestión de Riesgos de TI se aplicará en sus dos primeras etapas en este documento. La última etapa de la guía corresponderá al planteamiento práctico del desarrollo de la Estructura para la Planeación Estratégica de Tecnología Informática, la aplicación del Gobierno de TI y la

metodología para la identificación de riesgos que se hará en la entidad pública Gobernación de Bolívar. Debido a que el tiempo no es suficiente para obtener los resultados finales de la aplicación de toda la guía, el entregable de esta investigación será el documento Guía de Gestión de Riesgos de TI para entidades públicas basado en la metodología Cobit y los lineamientos del Gobierno de TI, el cual contendrá la metodología para llevar a cabo un monitoreo y control de la tecnología informática alineándola con los objetivos del negocio y el ejemplo práctico de la aplicación de sus dos primeras etapas como modelo.

5. JUSTIFICACION

La administración del riesgo es un proceso interactivo de pasos bien definidos los cuales, si se toman de manera secuencial, soportan mejor la toma de decisiones contribuyendo a una mayor comprensión de los riesgos y sus impactos. El proceso de administración del riesgo puede ser aplicado a cualquier situación donde un resultado indeseado o inesperado pudiera ser significante o donde se identifiquen oportunidades[3].

Hoy en día las organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar, por tanto tienen una apreciación y entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección y control adecuado.

De acuerdo a la experiencia de los autores de este trabajo, en las entidades del gobierno se puede observar que no siempre se tiene la apreciación y entendimiento sobre los riesgos y controles del uso de la tecnología informática en los procesos diarios; por lo que no se dimensiona la criticidad que maneja cada escenario compuesto por TI.

Los autores tienen conocimiento, por investigaciones hechas, que algunas entidades públicas de la ciudad de Cartagena han realizado estudios sobre su plataforma tecnológica con el fin de evaluar o definir políticas y procedimientos que permitan establecer o ejercer controles en las actividades relacionadas con la administración de recursos informáticos. Esta preocupación surge a partir del incremento en el uso de sistemas de información como herramienta para el alcance de sus objetivos o metas.

A través de estos estudios, estas entidades públicas han podido identificar los riesgos en cada una de sus dependencias y a la vez han establecido controles para la minimización de los mismos.

Como resultado de estos estudios, se resalta la importancia de desarrollar una Guía de gestión de riesgos de TI, como herramienta para el monitoreo y control de las actividades de T.I., las cuales deberán estar alineadas con los objetivos del negocio.

En la actualidad las entidades públicas soportan muchos de sus procesos críticos y misionales sobre una plataforma de tecnología informática, la cual deberá brindar las garantías necesarias y confiables para operar en forma exitosa y eficiente. Pero ¿estas entidades públicas han contextualizado, dimensionado o sopesado los riesgos asociados a todos sus recursos informáticos y por ende a su activo más valioso, la información? La respuesta que los autores dan a este interrogante es, que existe la urgente necesidad que las instituciones públicas cuenten con una metodología, guía o modelo para la administración de los riesgos de tecnología informática relacionados con sus procesos.

Existen estándares que permiten que una organización identifique, analice y maneje los riesgos relacionados a sus recursos; así mismo que ejerza controles previos y de hechos, con el fin de minimizar los riesgos asociados a sus procesos.

El propósito de este trabajo, es la generación de una guía para las entidades públicas como herramienta de evaluación y seguimiento a los controles establecidos en sus procesos de tecnología informática y como procedimiento para la implementación de políticas de Gobierno de TI.

La creación de una Guía de gestión de riesgos de TI para entidades del estado a partir de la metodología Cobit y de los lineamientos del Gobierno de TI brindará los siguientes beneficios:

- ✓ Definir y establecer la responsabilidad de directivos y jefes en los procesos relacionados con TI.
- ✓ Enfocar los objetivos del negocio al logro de las metas y objetivos de la organización.
- ✓ Mantener el equilibrio entre el riesgo y el retorno de la TI y sus procesos.
- ✓ Proporcionar mejoras medibles en la efectividad y eficiencia de los procesos del negocio.
- ✓ Proveer la estructura que relaciona la información, los recursos y procesos de TI con los objetivos estratégicos de la organización.
- ✓ Integrar e institucionalizar las buenas prácticas sobre el desempeño de la TI para garantizar el soporte adecuado a los objetivos del negocio:

    - Planeación y Organización
    - Adquisición e implementación
    - Entrega y Soporte
    - Monitoreo

Por lo anterior, la Guía de gestión de riesgos de TI para entidades del estado, consideramos, será, con las debidas adaptaciones dependiendo de cada entidad en particular dado que en este trabajo se aplicó a la Gobernación de Bolívar, una herramienta con la que podrían contar las entidades públicas para fijar sus objetivos, dirigir sus procesos, planificar sus actividades, administrar sus riesgos, alcanzar sus beneficios y evaluar sus procesos. (Es conveniente comentar por que

la guía no aplicaría para entidades privadas o decir que por haberse aplicado en la Gobernación se atreven a decir que sería para las públicas aunque se podría extender con trabajos posteriores al sector privado)

6. MARCO TEORICO

6.1 Ámbito de aplicación

Los principios, normas y procedimientos de este manual deben ser conocidos y aplicados por todas las áreas y funcionarios de la entidad publica en cuestión, para lograr una gestión y control integral de los riesgos a los que está expuesta, en desarrollo de las distintas operaciones y actividades que como entidad del estado desarrolla apoyándose de los distintos recursos de TI que posee.

La gestión y control integral de los riesgos está enfocada hacia los siguientes puntos:

- Establecer el procedimiento para la definición del contexto estratégico, organizacional y de administración del riesgo asociado a la TI.

- Definir la metodología para la Identificación de los riesgos a través de qué, porqué y cómo las cosas pueden suceder.

- Definir el procedimiento para el análisis de riesgos mediante la determinación de los controles existentes y los riesgos analizados en términos de consecuencia y probabilidad en el contexto de esos controles.

- Diseñar el modelo de evaluación de riesgos, comparando los niveles de riesgo estimados contra el criterio pre-establecido.

- Establecer el procedimiento para dar tratamiento a los riesgos a través del monitoreo y desarrollo de un plan de manejo especifico para los mismos.

- Diseñar la estructura para el monitoreo y revisión del sistema de administración de riesgos asociados a TI y los cambios que podrían afectarlo.

Los puntos anteriores fueron pensados de tal forma que se pudiese cumplir con los 4 principios básicos de un Gobierno de TI[4], definidos por el Institute Governance IT:

- Alineación estratégica entre los objetivos de TI y los objetivos de negocio.
- La TI como impulsora del negocio y maximizadora de beneficios.
- Utilización responsable de los recursos de TI.
- Administración adecuada de los riesgos de TI.

6.2 Administración de riesgos[3]

La administración del riesgo es reconocida como una parte integral de las buenas prácticas de la administración. Es un proceso interactivo consistente de pasos, los cuales, cuando son realizados en secuencia, permiten un mejoramiento continuo en la toma de decisiones.

La administración del riesgo puede ser aplicada en muchos niveles en una organización. Puede ser aplicada en un nivel estratégico y en niveles operacionales. Podría ser incluso aplicada a proyectos específicos para asistir decisiones específicas o para manejar áreas de riesgo reconocido.[3]

Con cada ciclo, el criterio del riesgo puede ser fortalecido para lograr progresivamente mejores niveles de administración de riesgos.

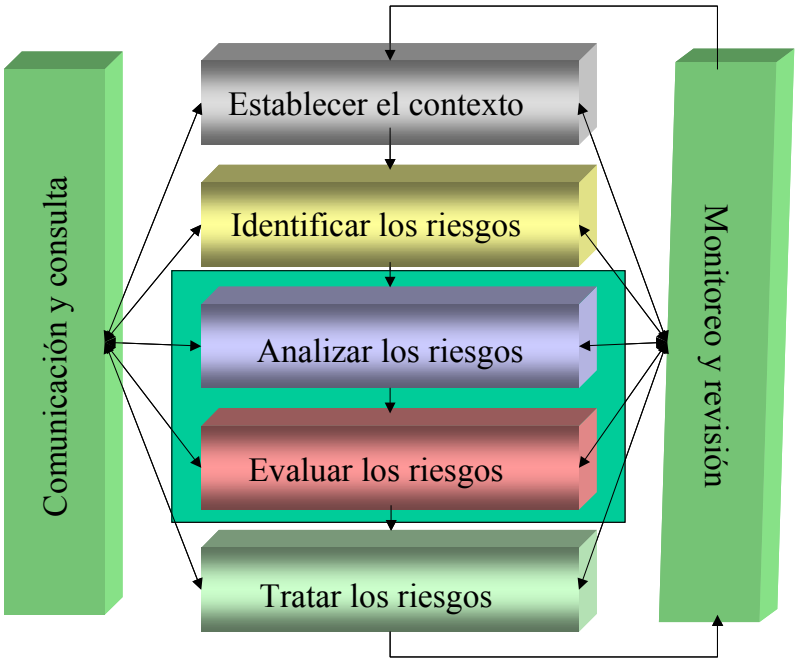


Fig. 3 Niveles de administración del riesgo

Por otra parte la Gerencia de las entidades del estado requieren de prácticas generalmente aplicables y aceptadas de control y gobierno de TI para medir en forma comparativa tanto su ambiente de TI existente, como su ambiente planeado.

6.2.1 Contexto de Administración del Riesgo y criterio de evaluación

En opinión de los autores de este documento, la administración de los riesgos de TI en las entidades públicas, se ha convertido en una herramienta importante para

atender situaciones donde un resultado no deseado o inesperado pueda ser convertido en algo significativo o permitan identificar oportunidades que satisfagan las necesidades de la organización. Hoy en día la mayoría de las organizaciones soportan sus procesos operativos en TI, esto ha generado un alto grado de dependencias de la tecnología informática, al tiempo que las organizaciones se ven en la necesidad de adquirir tecnología para implementar sistemas de información, incurriendo en altos costos y una elevada inversión por su adquisición, mantenimiento y seguridad. Otro de los factores importante en la administración de riesgo de TI, dentro de las organizaciones es la generación por parte del área de TI de objetivos concretos de control que contrarresten los ataques externos a los cuales es sometido frecuentemente.

Para el desarrollo del presente proyecto de la administración de riesgos de TI en las entidades publicas, emplearemos el modelo COBIT[2]; a partir de este generaremos nuestro modelo de gestión de riesgos asociados a TI, tomando como patrón el marco de referencia de COBIT.

La administración de riesgos implica una comprensión cabal de los objetivos estratégicos de la organización y de la vinculación de estos objetivos con los procesos críticos y las tareas particulares. La identificación, el análisis y la evaluación de los riesgos relacionados con el logro de los objetivos conforman la base para determinar cómo deben administrarse los mismos. La evaluación de riesgos no puede ser una actividad que se ejerce por única vez; por el contrario, requiere la implementación de un proceso activo para la continua evaluación del uso de recursos de sistemas de información o la aplicación de técnicas de mejora continúa de procesos.

Sobre la base del análisis de riesgos y dada la complejidad de los circuitos de procesamiento de información actuales, es necesario contar con un proceso de diseño y construcción de controles. Este proceso es necesariamente integral (extensivo a todas las áreas involucradas) y dinámico (en permanente evaluación y evolución). Por ello constituye una herramienta esencial del proceso operativo, debido a que integra y coordina los controles existentes en diferentes sectores de la organización para que sean eficaces, eficientes y económicos.

[5]La Dirección debe administrar los riesgos de la organización considerando los siguientes aspectos:

- ¬ Asegurar la transparencia respecto de los riesgos significativos y clarificar las políticas vinculadas con la aceptación y con la transferencia de riesgos.
- ¬ Considerar que una administración de riesgos transparente y pro-activa puede crear ventajas competitivas que pueden ser explotadas.
- ¬ Insistir en que la administración de riesgos debe estar integrada a las operaciones de la compañía, debe responder de manera rápida a los cambios en los riesgos del negocio y debe informar en forma oportuna a los niveles adecuados de administración según un esquema definido de escalamiento.

6.2.2 Riesgo Operacional y Gobernabilidad Corporativa

El riesgo operacional de una organización está directamente relacionado al nivel de desarrollo de la gobernabilidad corporativa.
Cuanto mayor sea el nivel de madurez de los procesos y servicios operacionales que dan soporte a los negocios de la organización, menor será su riesgo operacional.

De esta forma, se hace necesario analizar cada uno de los procesos y servicios de soporte, tales como recursos humanos, TI, telecomunicaciones, infraestructura y su nivel de madurez correspondiente, y asociarlos a los respectivos procesos de negocios para establecer el nivel de riesgo que cada proceso agrega.

Para cada proceso del área de negocios, la intersección con los procesos de soportes operacionales y administrativos, orientan el indicador de riesgo. Cada proceso de negocios se intercepta con procesos de soporte operacional diferentes, con nivel de madurez diferentes, resultando riesgos operacionales diferentes.

Por tanto, se hace necesario analizar el nivel de madurez de los procesos de soporte operacional que apoyan determinados negocios de forma específica y directa.

6.2.3 Riesgo Operacional y Dirección de TI

Con el desarrollo creciente de los servicios, dependientes de soluciones tecnológicas cada vez más complejas, observamos un cambio radical en el papel ejercido por el área de tecnología en el sector público. El área de TI no solo brinda soporte al negocio, sino que para muchas organizaciones hoy día, los sistemas y aplicaciones son el negocio.

El nivel de servicios de TI tiene una influencia directa en el resultado de éxito de las actividades llevadas a cabo en las instituciones públicas, a través de la reducción de costos administrativos y operacionales.

El nivel de servicios de TI está integrado a los procesos operacionales, con influencia directa en la validación del riesgo operacional, debiendo afectar decisivamente nivel operacional de la institución. Así, al hacer el análisis del riesgo operacional de la organización, deben destacarse las áreas como TI y telecomunicaciones, por la importancia en el resultado de la validación de riesgos de los procesos de negocios.

El análisis del nivel de dirección de TI se realiza a través de la depuración del nivel de madurez de los procesos y controles de TI. El nivel de madurez de los procesos, establece una relación directa con el nivel de riesgo que los procesos de TI agregan al riesgo de los procesos de negocios.

El mayor nivel de madurez debe buscarse en los procesos de TI que atienden a las actividades más críticas, dirigiendo de esta forma los esfuerzos para la mejoría del nivel de dirección y madurez de los procesos en cuestión.

Para identificar el nivel real del riesgo de TI en cada proceso es necesario descomponer estos procesos en elementos de TI y los riesgos inherentes. De esta forma tenemos que analizar el nivel de madurez de los procesos envueltos en las plataformas de hardware, software, telecomunicaciones, sistemas aplicados, datos referentes a un negocio determinado.

Se puede estimar el nivel de madurez de la organización si se compara con las definiciones presentadas en la siguiente tabla.

Nivel	Estado	Definición
0	No existe	La directiva (o el proceso) no está documentada y la organización, anteriormente, no ha tomado conciencia del riesgo de negocios asociado a esta administración de riesgos. Por lo tanto, no ha habido comunicados al respecto.
1	Ad hoc	Es evidente que algunos miembros de la organización han llegado a la conclusión de que la administración de riesgos tiene valor. No obstante, los esfuerzos de administración de riesgos se han llevado a cabo de un modo ad hoc. No hay directivas o procesos documentados y el proceso no se puede repetir por completo. En general, los proyectos de administración de riesgos parecen caóticos y sin coordinación; los resultados no se han medido ni auditado.
2	Repetible	Hay una toma de conciencia de la administración de riesgos en la organización. El proceso de administración de riesgos es repetible aunque inmaduro. El proceso no está totalmente documentado; no obstante, las actividades se realizan periódicamente y la organización está trabajando en establecer un proceso de administración de riesgos exhaustivo con la participación de los directivos. No hay cursos formales ni comunicados acerca de la administración de riesgos; la responsabilidad de la implementación está en manos de empleados individuales.
3	Proceso definido	La organización ha tomado una decisión formal de adoptar la administración de riesgos incondicionalmente con el fin de llevar a cabo su programa de seguridad de información. Se ha desarrollado un proceso de línea de base en el que se han definido los objetivos de forma clara con procesos

Nivel	Estado	Definición
		documentados para lograr y medir el éxito. Además, todo el personal dispone de algunos cursos de administración de riesgos rudimentaria. Finalmente, la organización está implementando de forma activa sus procesos de administración de riesgos documentados.
4	Administrado	Hay un conocimiento extendido de la administración de riesgos en todos los niveles de la organización. Los procedimientos de administración de riesgos existen, el proceso está bien definido, la comunicación de la toma de conciencia es muy amplia, hay disponibles cursos rigurosos y se han implementado algunas formas iniciales de medición para determinar la efectividad. Se han dedicado recursos suficientes al programa de administración de riesgos, muchas partes de la organización disfrutan de sus ventajas y el equipo de administración de riesgos de seguridad puede mejorar continuamente sus procesos y herramientas. Se utilizan herramientas de tecnología como ayuda para la administración de riesgos, pero la mayoría de los procedimientos, si no todos, de evaluación de riesgos, identificación de controles y análisis de costo-beneficios son manuales.
5	Optimizado	La organización ha dedicado recursos importantes a la administración de riesgos de seguridad y los miembros del personal miran al futuro intentando determinar los problemas y soluciones que habrá en los meses y años venideros. El proceso de administración de riesgos se ha comprendido bien y se ha automatizado considerablemente mediante el uso de herramientas (desarrolladas internamente o adquiridas a proveedores de software independientes). La causa principal de todos los problemas de seguridad se ha identificado y se han adoptado medidas adecuadas para minimizar el riesgo de repetición. El personal dispone de cursos en distintos niveles de experiencia.

Tabla No. 1 Niveles de madurez de la organización

6.2.4 Asignación de prioridades a riesgos

El proceso de asignación de riesgos incorpora el elemento de probabilidad a la declaración de repercusiones. Recuerde que una declaración de riesgo bien elaborada requiere tanto las repercusiones para la organización como la probabilidad de que se produzcan. El proceso de asignación de prioridades se puede considerar como el último paso en la "definición de los riesgos más importantes para la organización". Su resultado final es una lista de prioridades de riesgos que se utilizará como la información para el proceso de apoyo a la toma de decisiones.

Mediante la aplicación del proceso de administración de riesgos de seguridad, el nivel de probabilidad tiene la capacidad de incrementar la toma de conciencia de un riesgo a los máximos niveles de la organización o puede reducirla tanto que el riesgo se pueda aceptar sin más debate. La estimación de la probabilidad de riesgo requiere que el equipo de administración de riesgos de seguridad dedique mucho tiempo a evaluar exhaustivamente cada combinación de amenaza y vulnerabilidad de prioridad. Cada combinación se evalúa según los controles actuales para tener en cuenta la eficacia de dichos controles que pueda influir en la probabilidad de repercusiones para la organización. Este proceso puede resultar abrumador para organizaciones grandes y puede comprometer la decisión inicial de invertir en un programa de administración de riesgos formal. Para reducir el tiempo dedicado a la asignación de prioridades a los riesgos, el proceso se puede dividir en dos tareas:

- Proceso de nivel de resumen
- Proceso de nivel detallado.

En el proceso de nivel de resumen se genera una lista de riesgos con prioridades muy rápidamente. No obstante, el inconveniente es que se produce una lista que sólo contiene comparaciones de alto nivel entre los riesgos. Una larga lista de nivel de resumen de los riesgos en que cada uno se considere alto no proporciona suficientes indicaciones al equipo de administración de riesgos de seguridad ni le permite asignar prioridades a las estrategias de mitigación. En todo caso, los equipos pueden clasificar rápidamente los riesgos para identificar los riesgos altos y moderados, lo que permite que el equipo de administración de riesgos de seguridad centre sus esfuerzos sólo en los riesgos que parecen más importantes.

En el proceso de nivel detallado se elabora una lista con más detalle que permite diferenciar fácilmente los riesgos entre sí. La vista de riesgos detallada permite la clasificación apilada de los riesgos y también incluye una vista más detallada del posible efecto financiero derivado del riesgo.

Algunas organizaciones pueden optar por no elaborar una lista de riesgos de nivel de resumen. Si no se analiza, puede parecer que esta estrategia ahorra tiempo, pero no es así. Minimizar el número de riesgos en la lista de nivel detallado, en última instancia, hace que el proceso de evaluación de riesgos sea más eficaz. Un objetivo principal del proceso de administración de riesgos de seguridad es simplificar el proceso de evaluación de riesgos mediante el equilibrio entre la granularidad agregada al análisis de riesgos y el esfuerzo necesario para calcular el riesgo. Simultáneamente, intenta promover y conservar la claridad en relación con la lógica inherente para que los participantes dispongan de una comprensión clara de los riesgos para la organización.

Algunos riesgos pueden tener la misma clasificación en la lista de resumen y en la detallada; no obstante, las clasificaciones ofrecen suficiente información para determinar si el riesgo es importante para la organización y si debe pasar al proceso de apoyo a la toma de decisiones.

El objetivo final de la fase de evaluación de riesgos es definir los más importantes para la organización, todo lo contrario al proceso de apoyo a la toma de decisiones cuyo objetivo es determinar lo que se debe hacer para solucionar dichos riesgos.

6.2.4.1 Proceso de nivel de resumen

La lista de nivel de resumen utiliza la declaración de repercusiones generada durante el proceso de proceso de recopilación de datos. La lista de declaración de repercusiones es el primero de los dos elementos de información de la vista de resumen. El segundo elemento de información es la estimación de probabilidades que ha determinado el equipo de administración de riesgos de seguridad. En las siguientes tres tareas se proporciona información general acerca del proceso de asignación de prioridades de nivel de resumen:

- *Tarea 1: determinar el valor de las repercusiones a partir de las declaraciones de repercusiones elaboradas en el proceso de recopilación de datos.*
  La información de clase de activos y de exposición de activo obtenida en el proceso de recopilación de datos se debe resumir en un solo dato para determinar las repercusiones. Recuerde que las repercusiones son la combinación de la clase de activos y el alcance de exposición al activo. Puede utilizar una matriz para seleccionar el nivel por cada declaración de repercusiones.

		Referencia de clasificación de efecto		
Clase de activo	Alto	Efecto moderado	Efecto alto	Efecto alto
	Medio	Efecto bajo	Efecto moderado	Efecto alto
	Bajo	Efecto bajo	Efecto bajo	Efecto moderado
		Bajo	Medio	Alto
		Nivel de exposición		

Fig. 4 Clasificación de efecto sobre activos

- *Tarea 2: estimar la probabilidad de las repercusiones para la lista de nivel de resumen.*
  Utilice las mismas categorías de probabilidad descritas en el proceso de recopilación de datos. Las categorías de probabilidad se incluyen a continuación como referencia:

  - **Alta:** muy probable, previsión de uno o varios ataques en un año.
  - **Media:** probable, previsión de ataque una vez al menos en dos a tres años.
  - **Baja:** no probable, no se prevé ningún ataque en tres años.

- *Tarea 3: completar la lista de nivel de resumen mediante la combinación de los valores de repercusiones y de probabilidad por cada declaración de riesgo.*
  Según resulte adecuado para la entidad, el nivel de riesgo de una repercusión media combinada con una probabilidad media se puede definir como riesgo alto. Definir los niveles de riesgo independientemente del proceso de evaluación de riesgos proporciona las indicaciones necesarias para tomar esta decisión. Recuerde que la guía de administración de riesgos de seguridad es una herramienta para facilitar el desarrollo de un programa de administración de riesgos exhaustivo y coherente. Cada organización debe definir lo que significa riesgo alto para su propia empresa.
  Una matriz como la siguiente se puede utilizar para seleccionar la clasificación de riesgo de nivel de resumen.

		Clasificación de resumen de nivel de riesgo		
Efecto (de la tabla de efectos anterior)	Alto	Riesgo moderado	Riesgo alto	Riesgo alto
	Medio	Bajo alto	Riesgo moderado	Riesgo alto
	Bajo	Bajo alto	Bajo alto	Riesgo moderado
		Bajo	Medio	Riesgo
		Valor de probabilidad		

Fig. 5 Resumen de clasificación de efecto sobre activos

6.2.4.2 Proceso de nivel detallado

La elaboración de la lista de riesgos de nivel detallado es la última tarea del proceso de evaluación de riesgos. La lista detallada también constituye una de las tareas más importantes porque permite que la organización comprenda la lógica subyacente en los riesgos más importantes para la empresa. Después de completar el proceso de evaluación de riesgos, en ocasiones la simple notificación de un riesgo bien documentado a los participantes basta para desencadenar la acción.

La lista de riesgos detallada aprovecha muchos de los elementos de información de la lista de nivel de resumen; no obstante, la vista detallada requiere que el equipo de administración de riesgos de seguridad sea más específico en sus descripciones de repercusiones y de probabilidad. Por cada riesgo de nivel de resumen, compruebe que cada combinación de amenaza y vulnerabilidad no se repite en los riesgos. Normalmente es posible que los riesgos de nivel de resumen no se describan lo suficiente como para que se asocien a controles específicos del entorno; en este caso, no podrá estimar la probabilidad de que suceda de forma precisa.

La lista de riesgos de nivel detallado también requiere declaraciones específicas acerca de la efectividad del entorno de controles actual. Después de que el equipo de administración de riesgos de seguridad haya adquirido un conocimiento

detallado de las amenazas y vulnerabilidades que afectan a la organización, se puede iniciar el trabajo de conocer los detalles de los controles actuales. El entorno de controles actual determina la probabilidad de riesgos para la organización. Si el entorno de controles es suficiente, la probabilidad de un riesgo para la organización es baja. Si no lo es, se debe definir una estrategia de riesgos; por ejemplo, aceptar el riesgo o desarrollar una solución de mitigación.

El último elemento de la lista de riesgos de nivel detallado es una estimación de cada riesgo en términos cuantificables y monetarios. La selección de un valor monetario para el riesgo no se produce hasta que se ha empezado a trabajar en la lista de nivel detallado.

Teniendo en cuenta la anterior el proceso de nivel detallado se puede describir en cuatro fases que son:

- Determinar las repercusiones y la exposición.
- Identificar los controles actuales.
- Determinar la probabilidad de repercusiones.
- Determinar el nivel de riesgo detallado.

El resultado es una lista detallada de riesgos que afectan a la organización.

6.2.5 Enfoques de administración del riesgo[6]

Las organizaciones se han introducido en la administración de riesgos de seguridad debido a la necesidad de responder a una incidencia de seguridad relativamente pequeña. Por ejemplo, el equipo de un empleado se infecta con un virus y un responsable de la oficina convertido en experto informático debe averiguar cómo tiene que erradicar el virus sin destruir el equipo ni los datos que contiene. Independientemente de cuál sea la incidencia inicial, a medida que aparecen cada vez más problemas relacionados con la seguridad y comienzan a tener repercusiones en los negocios, muchas organizaciones sienten frustración al tener que responder a una crisis tras otra. Desean una alternativa a este enfoque reactivo, una alternativa que reduzca la probabilidad de que las incidencias de seguridad se produzcan en primer lugar. Las organizaciones que administran el riesgo de forma eficaz evolucionan a un enfoque más proactivo, pero, esto sólo constituye parte de la solución.

6.2.5.1 Enfoque reactivo

Cuando se produce una incidencia de seguridad, muchos profesionales de TI piensan que lo único para lo que tienen tiempo de hacer es contener la situación, averiguar qué ha sucedido y reparar los sistemas lo más rápidamente posible. Algunos pueden intentar identificar la causa principal, pero esto incluso puede parecer un lujo para los que tienen grandes restricciones de recursos. Aunque un

enfoque reactivo puede constituir una respuesta táctica eficaz a los riesgos de seguridad descubiertos y se han convertido en incidencias de seguridad, la imposición de un pequeño nivel de rigor al enfoque reactivo puede permitir que las organizaciones de cualquier tipo utilicen mejor sus recursos.

Fig. 6 Proceso de respuesta a incidencias

6.2.5.2 Enfoque proactivo[7]

La administración de riesgos de seguridad proactiva tiene numerosas ventajas con respecto a un enfoque reactivo. En vez de esperar a que suceda lo peor y, a continuación, llevar a cabo la respuesta, se minimiza la posibilidad de que pase lo peor antes de que se produzca. Se trazan planes para proteger los activos importantes de la organización mediante la implementación de controles que reduzcan el riesgo de que el software malintencionado, los piratas informáticos o un uso incorrecto accidental aprovechen las vulnerabilidades.

Evidentemente, las organizaciones no deben abandonar por completo la respuesta a incidencias. Un enfoque proactivo puede ayudar a las organizaciones a reducir

considerablemente el número de incidencias de seguridad que surjan en el futuro, pero no es probable que dichos problemas desaparezcan por completo. Por lo tanto, las organizaciones deben continuar mejorando sus procesos de respuesta a incidencias mientras desarrollan simultáneamente enfoques proactivos a largo plazo.

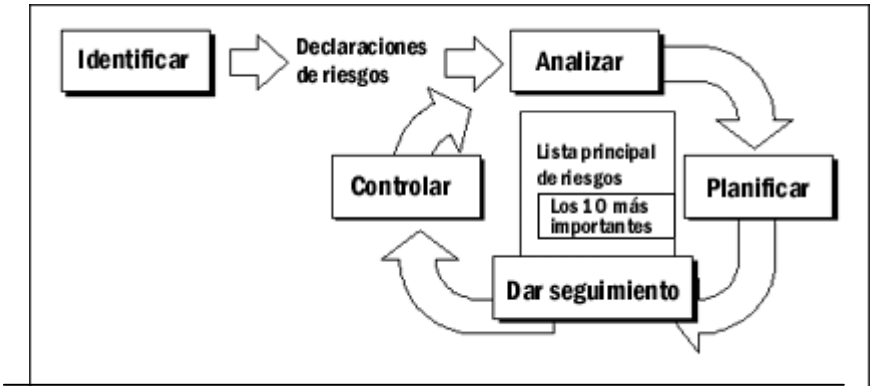


Fig. 7 Enfoque Proactivo

a. Identificar el riesgo

Proporciona las oportunidades, pistas e información que permiten al equipo plantear los riesgos mayores antes de que afecten adversamente a las operaciones y, por tanto, a la empresa.

En este paso, el equipo identifica los componentes del planteamiento del riesgo:
- Condición
- Consecuencias para las operaciones
- Consecuencias para la empresa
- Origen del riesgo
- Modo del error

Condición y consecuencias

Una manera intuitiva de analizar el futuro se basa en las frases del tipo "si ... entonces":: La condición es la parte del "si", mientras las consecuencias son expresadas con el "entonces". Por ejemplo, "si falla la única fuente de alimentación del servidor Web, entonces el sitio Web de la compañía no estará disponible".

Tenga en cuenta que entre la condición y las consecuencias puede haber una relación de muchos a muchos. Una sola condición puede causar numerosas consecuencias.

Es importante separar la consecuencia en dos partes durante la identificación: la consecuencia para las operaciones y la consecuencia para la empresa.

Consecuencias para la empresa podrían incluir el daño a la reputación de la compañía y los ingresos perdidos si el sitio se utilizaba para el comercio electrónico. Distinguir entre éstas es decisivo para una fase posterior del proceso, cuando el equipo clasifica los riesgos para garantizar que los más importantes reciban la atención que merecen, porque un riesgo puede tener muchas consecuencias para la operaciones, pero pocas para la empresa, o viceversa.

Origen del riesgo

Hay cuatro orígenes de riesgo principales en las operaciones de IT:

Las personas. Todo el mundo comete errores, por lo que incluso aunque la tecnología y los procesos del grupo no tengan errores, los errores humanos pueden ser un riesgo para la empresa.
El proceso. Los procesos con errores o mal documentados pueden ser un riesgo para la empresa incluso aunque se sigan a la perfección.
La tecnología. El personal de IT puede seguir perfectamente un proceso muy bien diseñado, pero producir errores para la empresa por problemas de hardware, software, etcétera.
Externos. Algunos factores quedan fuera del control del grupo de IT, pero pueden dañar la infraestructura y provocar fallos en la empresa. Entran en esta categoría los sucesos naturales, como terremotos e inundaciones, así como problemas generados externamente por el ser humano, como perturbaciones civiles, ataques de virus informáticos y cambios en las regulaciones gubernamentales.

Se trata de categorías amplias que, además, se superponen. Por ejemplo, si un empleado recién contratado es entrenado en software de copia de seguridad y semanas más tarde comete un error que provoca el fallo de la copia de seguridad, ¿la fuente de riesgo es la "gente" o el "proceso"? Si la compañía confía en una empresa de telecomunicaciones para el acceso a Internet y falla el hardware de ésta, ¿el error es "tecnológico" o "externo"?

Hay muchas maneras de decidir la categoría a la que corresponde un riesgo, pero es más importante definir una y mantenerla en lugar de perder tiempo buscando la forma "perfecta". Una opción consiste en preguntar si el grupo de IT tiene algún control sobre la causa del riesgo. Si no es así, el origen es externo. Esto definiría como "externo" un problema de hardware de una compañía de telecomunicación. En cuanto a los otros tres orígenes, ¿se habría producido el problema si hubiera sido diferente la persona, el proceso o la tecnología? Así se definiría el fallo del operador como "personal" si el empleado no prestó atención durante el entrenamiento u olvidó la lección, o de "proceso" si el entrenamiento fue incompleto o estuvo mal diseñado.

¿Por qué preocuparse por la fuente de riesgo? Porque afectará a la forma en que el equipo administrará el riesgo en los pasos posteriores del proceso. Por ejemplo, el equipo tratará de manera diferente la posibilidad de que los entrenados no

presten atención y la de que los materiales de entrenamiento sean de mala calidad.

Modo del error

Las operaciones pueden crear un fallo en la empresa de cuatro maneras diferentes:
Costo. La infraestructura puede funcionar adecuadamente, pero con un costo demasiado alto, produciendo una amortización de la inversión demasiado baja.
Agilidad. La infraestructura puede funcionar adecuadamente, pero carecer de la capacidad de cambiar con rapidez suficiente para atender a las necesidades de la empresa. Los problemas de capacidad son el caso más evidente. Por ejemplo, alguien puede tener una docena de servidores nuevos listos para dar servicio al incremento de necesidades de proceso, pero olvidó que los sistemas de refrigeración del centro de datos estaban ya al máximo de capacidad y la actualización de estos sistemas tardará un mes.
Rendimiento. La infraestructura puede no dar satisfacción a las expectativas de los usuarios bien porque éstas eran erróneas o porque el rendimiento de la infraestructura es incorrecto.
Seguridad. La infraestructura puede fallar a la empresa por no proporcionar protección suficiente a los datos y recursos o por tener una seguridad tan estricta que los usuarios legítimos no tienen acceso a los datos y recursos.

		Modo de error			
		Costo	Agilidad	Rendimiento	Seguridad
Origen del riesgo	Personas				
	Proceso				
	Tecnología				
	Externo				

Tabla No. 2 Identificación del origen del riesgo

b. Analizar el riesgo

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, el equipo agrega tres elementos más a las entradas de riesgo de la lista de riesgos principales: la probabilidad, impacto y exposición del riesgo. Estos elementos permiten al equipo categorizar los riesgos, lo que a su vez le permite dedicar más energía a la administración de los riesgos más importantes.

Probabilidad del riesgo

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo para las operaciones no plantea una amenaza a la empresa.
Asimismo, la probabilidad debe ser inferior al 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.
La probabilidad se puede entender también como la posibilidad de las consecuencia, porque si la condición se produce se supone que la probabilidad de la consecuencia será del 100%.

Impacto del riesgo
El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia.
La solución más efectiva es una consecuencia numérica. Decidir la manera de estimar las pérdidas no es un asunto trivial. La mejor solución es una escala numérica: cuanto mayor sea el número, mayor el impacto. Como regla general, la escala debería llegar al menos al tres para ofrecer una gama de valores de exposición. Sin embargo, tenga en cuenta que cuanto más alta sea la escala más tiempo se empleará en elegir exactamente el número correcto, sin que de ello se derive mucha precisión adicional.

Exposición al riesgo
La exposición es el resultado de multiplicar la probabilidad por el impacto. A veces, un riesgo de alta probabilidad tiene un bajo impacto y se puede ignorar sin problemas; otras veces, un riesgo de alto impacto tiene una baja probabilidad, por lo que también se puede ignorar. Los riesgos que tienen un alto nivel de probabilidad y de impacto son los que más necesidad tienen de administración, pues son los que producen los valores de exposición más elevados.
Al estimar la probabilidad y el impacto suele ser útil anotar su nivel de confianza. Por ejemplo, si un riesgo puede producir una pérdida de un millón de dólares, pero la confianza en la precisión de los datos es sólo del 20%, documéntelo así para que quienes analicen el riesgo puedan poner ese cálculo
en su perspectiva adecuada.

c. Planear la acción del riesgo

El paso de planeación convierte la información del riesgo en decisiones y acciones. Planear significa desarrollar acciones para los riesgos individuales, dando prioridad a las acciones relacionadas con cada riesgo y creando un plan integrado de la administración de riesgos.

Las tareas clave de este paso incluyen la definición de tres elementos más de riesgo: mitigaciones, desencadenadores y contingencias.

Mitigaciones

Las mitigaciones son los pasos que el equipo puede dar antes de que se produzca la condición y cada uno de los tres efectos sobre el riesgo:
Reducir. La reducción del riesgo minimiza la probabilidad del riesgo, su impacto o ambas cosas. Por ejemplo, la redundancia suele reducir el impacto del fallo. Cuando falla un componente no hay impacto porque el componente redundante sigue funcionando. Llevar un seguimiento de la duración esperada de un componente y sustituirlo antes de que se espere que falle reduce la probabilidad del fallo. Idealmente, un método de reducción reduce a cero la probabilidad o el impacto, aunque esto no es siempre posible.
Evitar. Evitar el riesgo previene que el equipo emprenda acciones que incrementen demasiado la exposición para justificar el beneficio. Un ejemplo sería una actualización de una aplicación poco importante y raramente utilizada en los 50.000 escritorios de una empresa. En la mayoría de los casos, el beneficio no justifica la exposición, por lo que IT, para evitar el riesgo, no actualiza la aplicación.
Transferir. Mientras que la estrategia de evitación elimina un riesgo, la estrategia de transferencia suele dejar el riesgo intacto, pero cambia la responsabilidad a otro grupo. Por ejemplo, una compañía con un sitio de comercio electrónico podría subcontratar a otra empresa la comprobación del crédito. Los riesgos siguen existiendo, pero pasan a ser responsabilidad de la empresa subcontratada. Sin embargo, si la empresa subcontratada es más capaz de encargarse de la comprobación del crédito, la transferencia de los riesgos sirve también para reducirlos.

Desencadenadores

Los desencadenadores indican al equipo que una condición va a producirse, o se ha producido, por lo que ha llegado el momento de poner en marcha el plan de contingencia.
En la definición de los elementos de riesgo puede resultar difícil distinguir entre consecuencias y desencadenadores. En una situación ideal, el desencadenador se produce antes que la consecuencia. Es útil pensar en ellos como indicadores luminosos que se encienden cuando todavía hay tiempo de evitar el peligro. Por ejemplo, si la condición es que el servidor se quede sin espacio en la unidad de disco duro, el desencadenador podría ser que el disco del servidor llegue al 95% de su capacidad y la tendencia sea ascendente.
En algunos casos, los desencadenadores pueden estar controlados por datos.

Por ejemplo, si la condición es que un servidor recién solicitado no llegue a tiempo para dar soporte al lanzamiento de una aplicación crítica para la misión, se puede poner un desencadenador en la fecha más reciente en la que el servidor podría llegar sin que se interfiera la seguridad.

Contingencias

Una contingencia es un paso que da el equipo si la condición se produce o el desencadenador llega a darse. El plan de contingencia documenta el conjunto de contingencias que utilizará el equipo al reaccionar ante una condición particular.
Siguiendo con el ejemplo anterior, si el servidor no llega a tiempo y el desencadenador se produce, una contingencia podría consistir en tomar prestado un servidor existente de un servicio menos importante.
Si la condición es que el servidor se quede sin espacio en la unidad de disco duro, se podría configurar un desencadenador que notifique a los operadores cuando sólo quede libre el 5% del disco. Una contingencia podría consistir en liberar espacio en el disco moviendo a otro servidor los archivos menos utilizados. Otra contingencia podría ser la de cerrar las aplicaciones no esenciales para que la que lo es no tenga competencia en el 5% de espacio restante en disco.

d. Realizar un seguimiento al riesgo

Durante la fase de seguimiento, el equipo recopila información acerca del modo en que cambian los riesgos; esta información sirve de base para las decisiones y acciones que se tomarán en el paso siguiente (control).

Este paso supervisa tres cambios principales:

Desencadenar valores. Si un desencadenador llega a producirse, habrá que ejecutar el plan de contingencia.
La condición, consecuencias, probabilidad e impacto del riesgo. Si cualquier de estos factores cambia (o se descubre que no es exacto), deberá ser evaluado de nuevo.
El progreso de un plan de mitigación. Si el plan va retrasado con respecto a lo programado o no produce el efecto deseado, deberá ser evaluado nuevamente.

Este paso supervisa los cambios anteriores en tres marcos de tiempo principales:

Constante. Muchos riesgos de las operaciones se pueden supervisar de manera constante, o al menos muchas veces cada día. Por ejemplo, unas herramientas pueden supervisar automáticamente cada varios segundos el uso de ancho de banda de un servidor Web.
Periódico. El equipo revisa periódicamente la lista de elementos superiores, para buscar cambios en los elementos más importantes. Esto suele producirse en las reuniones del equipo, la del consejo consultor de cambios, etcétera.
Específico. En algunos casos, alguien observa que parte de un riesgo ha cambiado.

e. Controlar los riesgos

El paso anterior (seguimiento) recopila información acerca de un riesgo y cuando cambia algo el paso de control ejecuta una reacción planeada a ese cambio:

- Si se ha cumplido un valor de desencadenador, ejecute entonces el plan de contingencia.
- Si un riesgo se ha vuelto irrelevante, retírelo entonces.
- Si la condición o la consecuencia ha cambiado, rehaga entonces el paso de identificación para evaluar de nuevo el elemento.
- Si ha cambiado la probabilidad o el impacto, vaya al paso de análisis para actualizarlo.
- Si ya no está en marcha el plan de mitigación, vaya entonces al paso de planeación para revisarlo.

Al principio este paso puede no parecer necesario, no resultando clara la distinción con el paso de seguimiento. En la práctica, la necesidad de actuar suele ser detectada por una herramienta o por personas que carecen de la responsabilidad, autoridad o experiencia que les permite reaccionar. El paso de control garantiza que sean las personas apropiadas las que reaccionen en el momento oportuno.
Por ejemplo:

Una herramienta automática podría supervisar constantemente el uso de ancho de banda de un servidor Web. Se ha definido un desencadenador según el cual si el uso da un salto del 10% en 10 minutos, la herramienta avisa a un operador con capacidad para ejecutar un plan de contingencia que asigne más ancho de banda al servidor. La detección del cambio forma parte del paso de seguimiento, el aviso al operador es la transición entre los pasos de seguimiento y de control, mientras que la acción del operador es el paso de control propiamente dicho.

6.3 Evaluación de Riesgos

[6]El proceso de administración de riesgos global consta de cuatro fases principales:

- *Evaluación de riesgos:* identificar y asignar prioridades a los riesgos para la empresa
- *Apoyo a la toma de decisiones:* identificar y evaluar las soluciones de control según un proceso definido de análisis de costo-beneficio.
- *Implementación de controles:* implementar y poner en funcionamiento las soluciones con el fin de reducir el riesgo para la empresa.
- *Medición de la efectividad del programa:* analizar la efectividad del proceso de administración de riesgos y comprobar que los controles proporcionan el nivel de protección previsto.

El proceso de administración de riesgos ilustra el modo en que un programa formal proporciona un método coherente de organización de recursos limitados para afrontar los riesgos en una organización. Las ventajas se aprecian mediante el desarrollo de un entorno de control asequible que afronte y mida el riesgo a un nivel aceptable.

La fase de evaluación de riesgos representa un proceso formal para identificar y asignar prioridades a los riesgos en la organización. El proceso de administración de riesgos de seguridad proporciona indicaciones detalladas acerca de cómo realizar las evaluaciones de riesgos y divide el proceso de la fase de evaluación de riesgos en los tres pasos siguientes:

1. Planeamiento
2. Recopilación de datos
3. Asignación de prioridades a riesgos

El resultado de la fase de evaluación de riesgos es una lista de prioridades de los riesgos que proporciona la información para la fase de apoyo a la toma de decisiones.

6.3.1 Metodología de Evaluación de Riesgos

6.3.1.1 Planeamiento

El paso de planeamiento es, indiscutiblemente, el más importante para garantizar la aceptación y el apoyo de los participantes a lo largo del proceso de evaluación de riesgos. La aceptación de los participantes es crucial porque el equipo de administración de riesgos de seguridad requiere una intervención activa del resto de los participantes. El apoyo también es fundamental porque los resultados de la evaluación pueden influir en las actividades de creación de presupuestos de los participantes si se precisan nuevos controles para reducir el riesgo. Las tareas principales del paso de planeamiento están enfocadas a alinear correctamente la fase de evaluación con los procesos de negocios, definir el ámbito de la evaluación de forma precisa y obtener la aceptación de los participantes.

En el paso de planeamiento también debe definir el ámbito de la evaluación de riesgos. En el sector de la seguridad de la información se utiliza el término evaluación de tantas formas que puede confundir a los participantes sin conocimientos técnicos. Por ejemplo, las evaluaciones de vulnerabilidades se llevan a cabo para identificar la configuración específica de tecnología o puntos débiles operativos. El término evaluación de cumplimiento se puede utilizar para comunicar una auditoria o una medición de los controles actuales según la directiva formal. El proceso de administración de riesgos de seguridad define la evaluación de riesgos como el proceso para identificar y asignar prioridades a los riesgos de seguridad de TI para la organización. Puede ajustar esta definición según resulte adecuado para su organización. Por ejemplo, algunos equipos de administración de riesgos de seguridad también pueden incluir la seguridad del personal en el ámbito de sus evaluaciones de riesgos.

Dado lo anterior los pasos a seguir en esta fase de planeamiento para la evaluación de riesgos serian:

- Definición del Ámbito.
- Aceptación de los participantes.

En esta fase de planeamiento encaja perfectamente lo que fue enunciado en el primer capitulo de esta guía en el cual se trabaja sobre la planeación estratégica de TI, mas que todo lo que concierne a definición del ámbito.

El segundo paso de esta fase se estaría cumpliendo en esta guía con lo expuesto en el capitulo anterior en el cual se hace referencia a la Herramienta de Gobierno de TI, COBIT, mas específicamente en los procesos llevados a cabo bajo el dominio Planificación y Organización (PO), y de forma mas detallada el proceso, Evaluación de Riesgos (PO9), mediante el cual se asegura el logro de los objetivos de TI y trata de responder a las amenazas hacia la provisión de servicios de TI, a través de *la participación de la propia organización en la identificación de riesgos de TI* y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos, tomando en cuenta aspectos como:

- Diferentes tipos de riesgos de TI (por ejemplo: tecnológicos, de seguridad, de continuidad, regulatorios, etc.)
- Alcance: global o de sistemas específicos
- Actualización de evaluación de riegos
- Metodología de evaluación de riesgos
- Medición de riesgos cualitativos y/o cuantitativos
- Plan de acción de riesgos

6.3.1.2 Recopilación de datos

Después del planeamiento, el siguiente paso consiste en recopilar la información relacionada con riesgos de los participantes de toda la organización; esta información también se utilizará en la fase de apoyo a la toma de decisiones.

Los elementos de datos principales recopilados durante el paso de recopilación de datos facilitados son:

- Activos Organizativos y Descripción de los activos
- Amenazas de seguridad y Vulnerabilidades
- Controles Propuestos

Teniendo en cuenta las tareas a realizar para la consecución de una eficaz recopilación de datos, hasta este punto de la guía se ha logrado cubrir el primer ítem/tarea de la recopilación de datos con lo expuesto en el segundo capitulo, *“Definir una metodología adecuada para la identificación de los escenarios,*

recursos informáticos y tecnología informática que posee la entidad pública", en el cual se hace una identificación y posterior descripción de activos/recursos de informática, al igual que también parte del tercer ítem/tarea con el desarrollo del anterior capitulo acerca de COBIT, en el cual se muestran una serie de controles plasmados en dicha norma para cierto tipo de riesgos y vulnerabilidades, por lo cual en este apartado se tratara el segundo ítem/tarea de la fase de recopilación de datos.

Amenazas de seguridad y Vulnerabilidades

La información acerca de las amenazas y vulnerabilidades proporciona la prueba técnica que se emplea para asignar prioridades a los riesgos en una empresa. Ésta es un área en la que resulta muy valiosa una investigación previa para ayudar a los responsables de negocios a detectar y comprender el riesgo en sus propios entornos.
Las repercusiones derivadas de una amenaza normalmente se definen con conceptos como confidencialidad, integridad y disponibilidad. Hacer referencia a estándares del sector resulta muy útil al investigar amenazas y vulnerabilidades.

En lo concerniente a riesgos puede resultar útil traducir las amenazas y vulnerabilidades en términos conocidos, Por ejemplo, ¿qué se intenta evitar? o ¿qué se teme que le suceda al activo? La mayoría de las repercusiones en la empresa se pueden clasificar en confidencialidad del activo, integridad o disponibilidad del activo para la realización de las actividades. Intente utilizar este enfoque si los participantes tienen dificultades para entender el significado de las amenazas para los activos organizativos. Un ejemplo habitual de una amenaza para la organización es un ataque a la integridad de los datos financieros. Después de haber articulado lo que intenta evitar, la siguiente tarea consiste en determinar el modo en que las amenazas se producen en la organización.

Una vulnerabilidad es un punto débil de un activo o grupo de activos que una amenaza puede atacar. De un modo simplificado, las vulnerabilidades proporcionan el mecanismo o el modo en que se pueden producir las amenazas. Como ejemplo, una vulnerabilidad habitual de los cosas es la ausencia de actualizaciones de seguridad.

Por cada amenaza identificada, tome en consideración la forma en cómo se podría producir la amenaza a través de ejemplos de propia ocurrencia. Cada amenaza puede tener varias vulnerabilidades, esto es normal y sirve de ayuda en las etapas posteriores de identificación de controles en la fase de apoyo a la toma de decisiones del proceso de administración de riesgos.

6.3.1.2.1 Relación de tipos

La relación que sigue clasifica los elementos dentro de un grupo determinado, con un nombre y una breve descripción de las características de este.

Es de anotar que la pertenencia de un elemento dentro de un grupo no es excluyente de su pertenencia a otro grupo; es decir, un elemento puede ser simultáneamente de varios tipos.

A. Servicios

Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requieren una serie de medios.

Los servicios aparecen como activos de un análisis de riesgos bien como servicios finales, prestados por la Organización a terceros; bien como servicios instrumentales, donde tanto los usuarios como los medios son propios; bien como servicios contratados, a otra organización que los proporciona con sus propios medios.
Así se encuentran servicios públicos prestados por la Administración para satisfacer necesidades de la colectividad; servicios empresariales prestados por empresas para satisfacer necesidades de sus clientes; servicios internos prestados por departamentos especializados dentro de la Organización, que son usados por otros departamentos u empleados de la misma, etcétera.

Al centrarse esta guía en la seguridad de las tecnologías de la información, es natural que aparezcan servicios de información, servicios de comunicaciones, servicios de seguridad, entre otros, sin ello ser un impedimento para encontrar otros servicios requeridos para el eficaz desempeño de la misión de la organización.

B. Datos/Información

Elementos de información que de forma singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo.

Los datos son el corazón que permite a una organización prestar sus servicios. Son en cierto sentido un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado en forma de bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

Es habitual que en un análisis de riesgos e impactos, el usuario se limite a valorar los datos, siendo los demás activos meros sirvientes que deben cuidar y proteger los datos que se les encomiendan.

Clasificación de Datos

La clasificación de datos es un procedimiento administrativo propio de cada organización o sector de actividad, que determina las condiciones de tratamiento de la información en función de la necesidad de preservar su confidencialidad.

- **Vitales**

Dícese de aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar aquellos que son imprescindibles para que la Organización supere una situación de emergencia, aquellos que permiten desempeñar o reconstruir las misiones críticas, aquellos sustancian la naturaleza legal o los derechos financieros de la Organización o sus usuarios.

- **Interés Comercial**

Dícese de aquellos que tienen valor para la prestación de los servicios propios de la organización.

- **Carácter Personal**

Dícese de cualquier información concerniente a personas físicas identificadas o identificables.
Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

- **Clasificados**

Dícese de aquellos sometidos a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es especialmente relevante. La tipificación de qué datos deben ser clasificados y cuales son las normas para su tratamiento, vienen determinadas por regulaciones sectoriales, por acuerdos entre organizaciones o por normativa interna.

C. Aplicaciones (Software)

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.
No preocupa en este apartado el denominado “código fuente” o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos.
Entran en esta clasificación todos los elementos de software, sin importar si fueron trabajados por la misma organización, o por alguna otra entidad sub-contratada bajo el servicio de software a la medida, así como también todo tipo de software de uso estándar como: navegadores, sistemas operativos, gestores de bases de datos, etcétera.

D. Equipos Informáticos (Hardware)

Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

- **Grandes equipos**

Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.

- **Equipos medios**

Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.

- **Informática personal**

Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.

- **Informática móvil**

Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.

- **Fácilmente reemplazable**

Son aquellos equipos que, en caso de avería temporal o definitiva pueden ser reemplazados pronta y económicamente.

- **De almacenamiento de datos**

Son aquellos equipos en los que los datos permanecen largo tiempo. En particular, se clasificarán de este tipo aquellos equipos que disponen de los datos localmente, a diferencia de aquellos que sólo manejan datos en tránsito.

- **Periféricos**

Dícese de impresoras, servidores de impresión, escáneres, dispositivos criptográficos, etcétera.

- **Soporte de la red**

Dícese de equipamiento necesario para transmitir datos: routers, módems, switches, firewalls, entre otros.

- **Redes de Comunicaciones**

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
Entran en este tipo redes como: red telefónica, RDSI (red digital, ISDN), X25 (red de datos), ADSL, punto a punto, red inalámbrica, satelital, red local (LAN), red metropolitana (MAN), Internet, red privada virtual (VPN).

- **Soportes de Información**

En este apartado se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
Se tienen que considerar todos los medios, ya sean electrónicos como: discos duros, disquetes, CD-ROM, dispositivos USB, DVD, cintas magnéticas, tarjetas de memoria; así como también los medios no electrónicos como podrían serlo: material impreso, cassete de video.

- **Equipamiento Auxiliar**

Hacen parte de este tipo otros equipos que sirven de soporte a los sistemas de información, sin estar estos directamente relacionados con datos, como lo son:

- Fuentes de alimentación
- Sistemas de alimentación ininterrumpida (UPS)
- Generadores eléctricos
- Aires acondicionados
- Cableado
- Suministros esenciales
- Mobiliario: armarios, etc.

E. Instalaciones

En este apartado entran los lugares donde se encuentran ubicados los sistemas de información y comunicaciones, como: edificios, y vehículos en los cuales se transporten recursos de TI vitales para el funcionamiento normal de las actividades de la entidad.

F. Personal

Pertenecen a este apartado las personas que están directamente relacionadas con los sistemas de información, como:

- Usuarios externos
- Usuarios internos
- Operadores
- Administradores de sistemas
- Administradores de comunicaciones
- Administradores de bases de datos
- Desarrolladores
- Subcontratas
- Proveedores

6.3.1.3 Asignación de prioridades

El paso de asignación de prioridades a riesgos es el primero de la fase que implica un elemento de subjetividad. La asignación de prioridades es subjetiva porque, después de todo, el proceso implica esencialmente la predicción del futuro. Debido a que el resultado de la evaluación de riesgos conduce a las inversiones en tecnología de la información (TI), el establecimiento de un proceso transparente con funciones y responsabilidades definidas resulta crucial para obtener la aceptación de los resultados y motivar que se emprendan acciones para mitigar los riesgos.

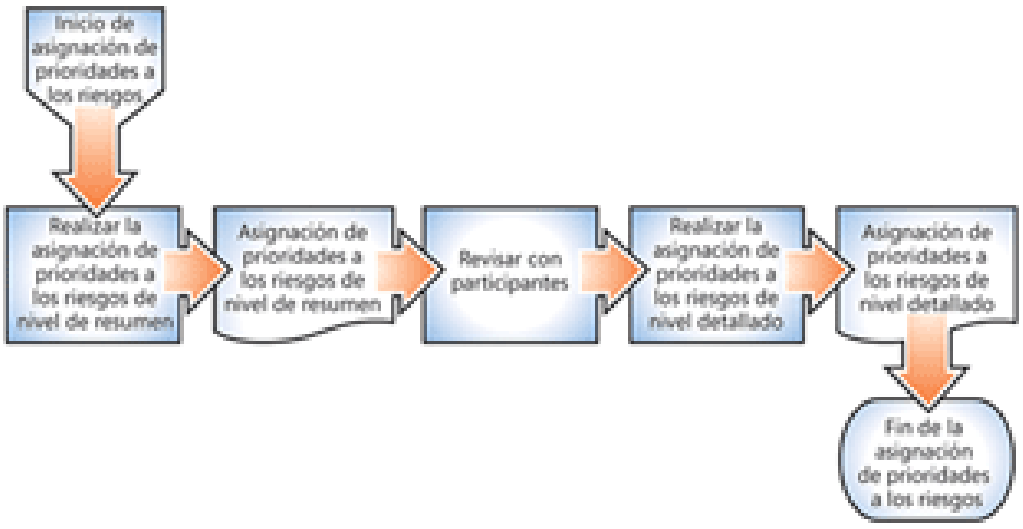


Fig. 8 Proceso de asignación de prioridades a riesgos

Este proceso puede resultar dispendioso para entidades muy grandes por lo que se recomienda dividir en dos tareas el proceso de asignación de prioridades: un proceso de nivel de resumen y otro de nivel detallado.

En el proceso de nivel de resumen se genera una lista de riesgos con prioridades muy rápidamente, similar a los procedimientos de selección que se utilizan en las habitaciones de urgencias hospitalarias para garantizar que se ofrece ayuda a los pacientes que más la necesitan en primer lugar. No obstante, el inconveniente es que se produce una lista que sólo contiene comparaciones de alto nivel entre los riesgos. Una larga lista de nivel de resumen de los riesgos en que cada uno se considere alto no proporciona suficientes indicaciones al equipo de evaluación de riesgos de seguridad ni le permite asignar prioridades a las estrategias de mitigación. En todo caso, los equipos pueden clasificar rápidamente los riesgos para identificar los riesgos altos y moderados, lo que permite que el equipo de evaluación de riesgos de seguridad centre sus esfuerzos sólo en los riesgos que parecen más importantes.
En el proceso de nivel detallado se elabora una lista con más detalle que permite diferenciar fácilmente los riesgos entre sí. La vista de riesgos detallada permite la clasificación apilada de los riesgos y también incluye una vista más detallada del posible efecto financiero derivado del riesgo.

Algunos riesgos pueden tener la misma clasificación en la lista de resumen y en la detallada; no obstante, las clasificaciones ofrecen suficiente información para determinar si el riesgo es importante para la organización y si debe pasar al proceso de apoyo a la toma de decisiones.

El objetivo final de la fase de evaluación de riesgos es definir los riesgos más importantes para la organización.

6.3.1.3 .1 Asignación de prioridades a riesgos de nivel de resumen

A continuación se detalla el proceso de elaboración de las listas de riesgos de nivel de resumen:

Determinar el nivel de las repercusiones

La información de clase de activos y de exposición de activo obtenida en el proceso de recopilación de datos se debe resumir en un solo dato para determinar las repercusiones. Las repercusiones son la combinación de la clase de activos y el alcance de exposición al activo. Se utiliza la figura No. 4, vista en el ítem 6.2.4.1, para seleccionar el nivel por cada declaración de repercusiones.

Estimar la probabilidad de nivel de resumen

Se utilizan las mismas categorías de probabilidad descritas en el proceso de recopilación de datos. Las categorías de probabilidad se incluyen a continuación como referencia:

- Alta: muy probable, previsión de uno o varios ataques en un año.
- Media: probable, previsión de ataque una vez al menos en dos a tres años.
- Baja: no probable, no se prevé ningún ataque en tres años.

Completar la lista de nivel de resumen

Después de que el equipo de evaluación de riesgos estime la probabilidad, se utiliza la figura No. 5, vista en el ítem 6.2.4.1, para seleccionar la clasificación de riesgo de nivel de resumen.

Como revisión, en la siguiente figura se representan todas las columnas de la lista de nivel de resumen:

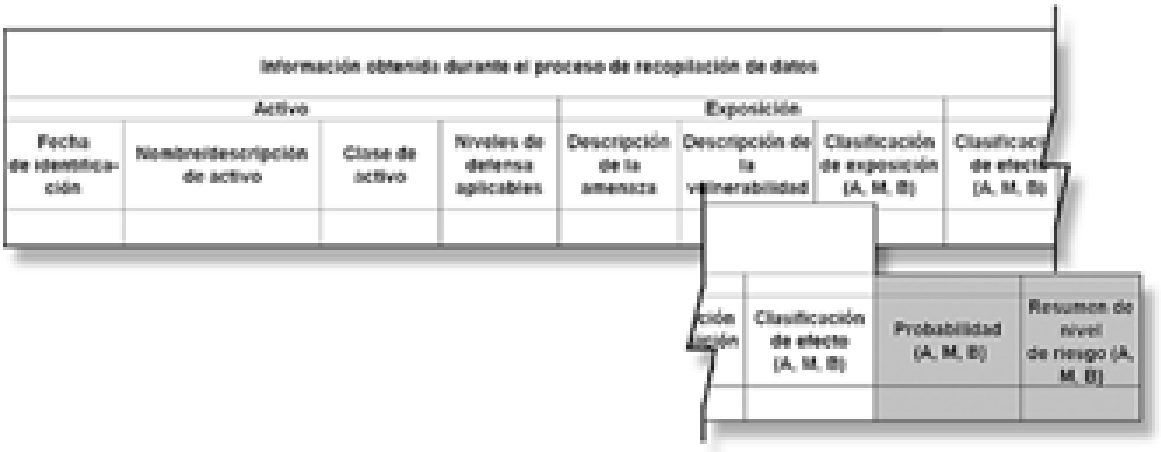


Fig. 9 Lista de nivel resumen

La siguiente tarea del proceso de asignación de prioridades es la revisión de los resultados de resumen con los participantes en el proceso de evaluación de riesgos. Se utilizaran los siguientes criterios al seleccionar los riesgos que se incluirán en el proceso de asignación de prioridades de nivel detallado:

Riesgos de nivel alto: los riesgos clasificados como altos se deben incluir en la lista detallada. Cada riesgo alto debe tener una resolución después del proceso de apoyo a la toma de decisiones; por ejemplo, aceptar el riesgo o desarrollar una solución de mitigación.

Riesgos dudosos: cree el análisis de asignación de prioridades detallado para riesgos moderados que requieren una resolución. En algunas organizaciones se pueden llegar a incluir todos los riesgos moderados en la lista detallada.

Riesgos controvertidos: si un riesgo es nuevo, no se ha comprendido bien o los participantes tienen distintos puntos de vista, cree el análisis detallado para que los participantes tengan un conocimiento más preciso del riesgo.

6.3.1.3 .2 Asignación de prioridades a riesgos de nivel detallado

La elaboración de la lista de riesgos de nivel detallado es la última tarea del proceso de evaluación de riesgos. La lista detallada también constituye una de las tareas más importantes porque permite que la organización comprenda la lógica subyacente en los riesgos más importantes para la entidad.

A continuación se describe el proceso de asignación de prioridades a riesgos de nivel detallado:

Determinar las repercusiones y la exposición

En primer lugar incorpore la clase de activos de la tabla de resumen en la plantilla detallada. A continuación, seleccione la exposición del activo. Tenga en cuenta que la clasificación de exposición de la plantilla detallada contiene granularidad adicional en comparación con el nivel de resumen. La clasificación de exposición de la plantilla detallada es un valor de 1 a 5. Recuerde que la clasificación de exposición define el alcance de los daños en el activo. Utilice las siguientes plantillas como guía para determinar la clasificación de exposición adecuada para su organización. Debido a que cada valor de las cifras de exposición puede afectar al nivel de repercusiones en el activo, inserte el mayor de los valores después de haber asignado las cifras. La primera cifra de exposición ayuda a cuantificar el alcance de las repercusiones de un ataque a la confidencialidad o integridad de los activos de negocios. La segunda cifra ayuda a cuantificar las repercusiones en la disponibilidad de los activos.

Clasificación de exposición	Confidencialidad o integridad de activo
5	Daños graves o totales al activo; por ejemplo, son visibles externamente y afectan a la rentabilidad o al éxito de la empresa.
4	Daños graves, pero no totales, al activo; por ejemplo, afectan a la rentabilidad o al éxito de la empresa; pueden ser visibles externamente.
3	Pérdida o daños moderados; por ejemplo, afectan a las prácticas de negocios internas, se produce un aumento de los costos operativos o se reducen los ingresos.
2	Daños o pérdida moderados; por ejemplo, afectan a las prácticas de negocios internas; no se puede medir un aumento de los costos.
1	Cambios menores en el activo o ningún cambio

Fig. 10 Nivel de exposición de activos

Después de tener en cuenta el alcance de los daños producidos por posibles ataques a la confidencialidad y la integridad, utilice la siguiente figura para

determinar el nivel de repercusiones debido a la ausencia de disponibilidad del activo. Seleccione el valor más alto como el nivel de exposición de ambas tablas.

Clasificación de exposición	Disponibilidad	Descripción
5	Detención del trabajo	Importantes costos de soporte técnico o compromisos de negocios cancelados.
4	Interrupción del trabajo	Aumento cuantificable de los costos de soporte técnico o retraso en los compromisos de negocios.
3	Retrasos en el trabajo	Efecto apreciable en los costos de soporte técnico y en la productividad. No se producen consecuencias en la empresa que se puedan medir.
2	Distracción en el trabajo	No se puede medir el efecto, pequeños aumentos en los costos de soporte técnico o de infraestructura.
1	Absorbidos por las operaciones de negocios normales	Sin impacto cuantificable en los costos de soporte técnico, productividad o compromisos de negocios.

Fig. 11 Nivel de repercusiones

Identificar los controles actuales

En los cálculos de probabilidad detallada también se evalúa una clasificación de efectividad de los controles; no obstante, la documentación de los controles aplicables facilita la comunicación de los elementos de riesgo. Puede resultar útil organizar las descripciones de los controles en categorías conocidas de grupos de controles de administración, operaciones o técnicos.

Determinar la probabilidad de repercusiones

La clasificación de probabilidad consta de dos valores. El primer valor determina la probabilidad de la vulnerabilidad existente en el entorno según los atributos de la misma y al ataque posible. El segundo valor determina la probabilidad de la vulnerabilidad existente en función de la efectividad de los controles actuales. Cada valor se representa mediante un intervalo de 1 a 5. Utilice las figuras No. 12 y 13 como orientación para determinar la probabilidad de cada repercusión en la organización. A continuación, la clasificación de probabilidad se multiplicará por la clasificación de efecto para determinar la clasificación de riesgo relativo.

En la figura No. 12 se incluyen estos atributos de vulnerabilidad:

- **Población de piratas informáticos**: la probabilidad de ataque normalmente aumenta a medida que se incrementa el tamaño y el nivel de conocimientos técnicos de la población de piratas informáticos.

- **Acceso remoto y local:** la probabilidad normalmente aumenta si una vulnerabilidad se puede aprovechar de forma remota.

- **Visibilidad de vulnerabilidad:** la probabilidad normalmente aumenta si una vulnerabilidad es conocida y está disponible de forma pública.

- **Automatización de ataque:** la probabilidad normalmente aumenta si un ataque se puede programar para buscar automáticamente vulnerabilidades en entornos grandes.

Definiciones de probabilidad para vulnerabilidades
Alta
Población grande de piratas informáticos: "script-kiddie"(jóvenes intrusos)/aficionados
Se puede ejecutar remotamente
Se necesitan privilegios anónimos
Método de aprovechamiento publicado externamente
Automatizado
"5" si se aplica **alguna**
Media
Población media de piratas informáticos: expertos/especialistas
No se puede ejecutar remotamente
Se necesitan privilegios de nivel de usuario
Método de aprovechamiento no público
No automatizado
"3" si se aplica **alguna**
Baja
Población pequeña de piratas informáticos: conocimientos privilegiados
No se puede ejecutar remotamente
Se necesitan privilegios de nivel de administrador
Método de aprovechamiento no público
No automatizado
"1" si se aplica **alguna**

Fig. 12 Probabilidades para vulnerabilidades

Seleccione la clasificación adecuada en la siguiente figura.

La clasificación de probabilidad consta de DOS partes:

Suma de vulnerabilidades:	
Atributos de exposición (seleccione uno de los anteriores)	
alta	**5**
media	**3**
baja	**1**
valor de probabilidad (1, 3 o 5)	

Fig. 13 Clasificación de probabilidades

Determinar el nivel de riesgo detallado

En la siguiente figura se muestra el resumen de nivel detallado para identificar el nivel de cada riesgo identificado. Aunque la evaluación de riesgos en un nivel detallado pueda parecer complicada, se puede hacer referencia a la lógica subyacente en cada tarea de la clasificación de riesgos mediante las figuras anteriores. Esta posibilidad de realizar el seguimiento de cada tarea en la declaración de riesgo proporciona un valor significativo cuando se ayuda a los participantes en la evaluación de riesgos, a comprender los detalles subyacentes del proceso de evaluación de riesgos.

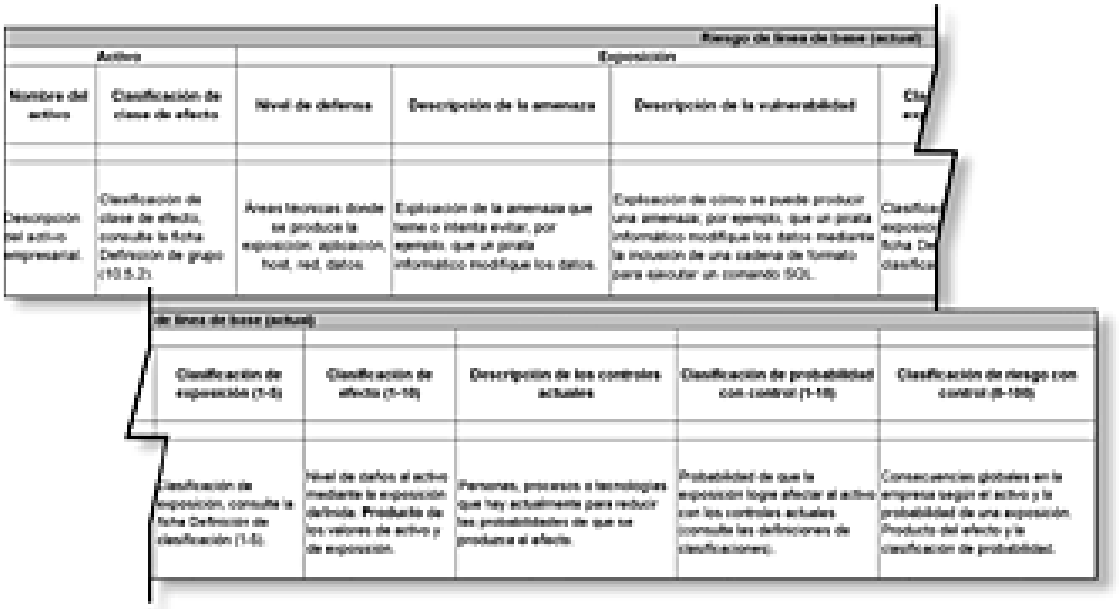


Fig. 14 Resumen de nivel de riesgo

6.4 COBIT[8]

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI. Los principios fundamentales de COBIT son: Los requerimientos de la información del negocio, recursos de tecnología de informática y los procesos de tecnología de informática.

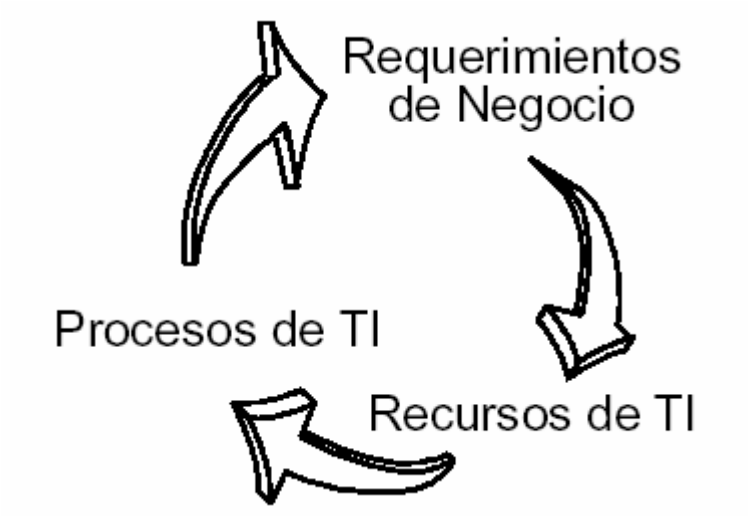


Fig. 15 Principios fundamentales de COBIT

Los aspectos de seguridad identificados por COBIT son: la confidencialidad, integridad y disponibilidad como elementos claves.

Confidencialidad: se refiera a la protección de información sensible contra divulgación no autorizada.

Efectividad*:* La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.

Eficiencia*:* Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).

Integridad: Se refiera a la precisión y suficiencia de información así como a su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento: De las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.

Confiabilidad: Proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con las responsabilidades de los reportes financieros y de cumplimiento normativo.

Los recursos de TI identificados en COBIT son: los datos, aplicaciones, tecnología, instalaciones y personal pueden explicarse/ definirse como se muestra a continuación:

Datos: Los elementos de datos en su mas amplio sentido (externos, internos), estructurados y no estructurados, gráficos etc.

Aplicaciones: Se entiende como sistema de aplicación la suma de procedimientos manuales y programados.

Tecnología: La tecnología cubre Hardware, Software, Sistemas Operativos, Sistemas de Administración de Bases de Datos, Redes y Multimedia etc.

***Instalaciones*:** Recursos para alojar y dar soporte a los sistemas de información.

Personal: Habilidades del personal conocimientos, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

El marco de referencia de COBIT esta constituido por Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. Existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos. Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas.

El concepto de ciclo de vida cuenta típicamente con requerimientos de control diferentes a los de actividades discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con “cortes” naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.

El marco referencial conceptual puede ser enfocado desde los principios fundamentales de COBIT: Los requerimientos de la información del negocio, recursos de tecnología de informática y los procesos de tecnología de informática. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente.

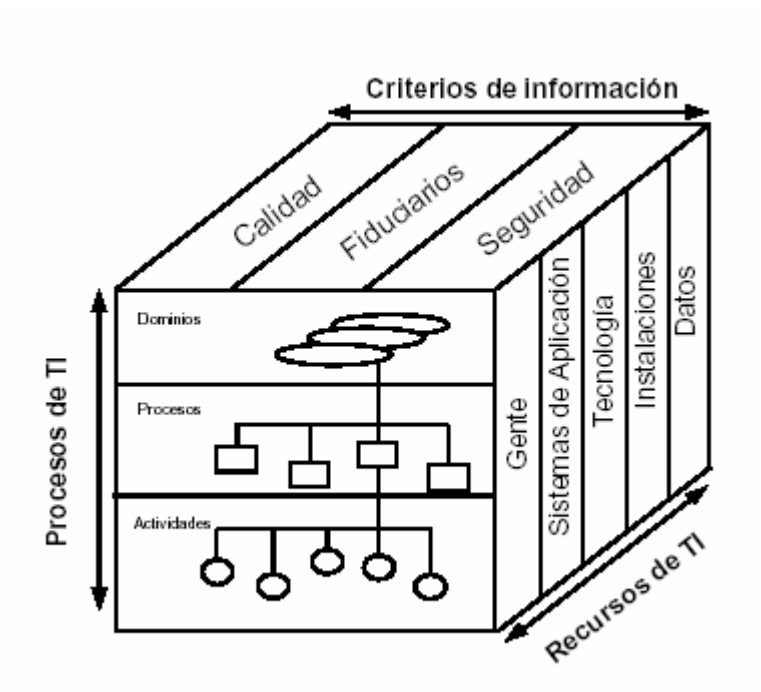


Fig. 16 Marco referencial de COBIT

El marco de referencial de COBIT ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de TI particular, cuyo logro es posible a través de un establecimiento de controles, para el cual deben considerarse controles aplicables potenciales. Los Objetivos de Control de TI han sido organizados por proceso/actividad, como se muestra a continuación:

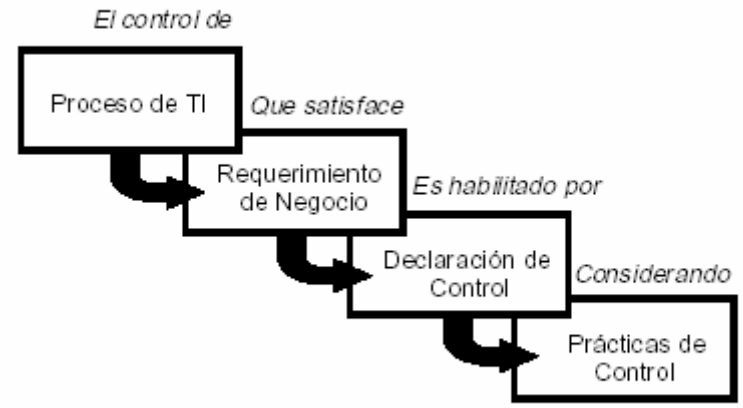


Fig. 17 Proceso de TI según COBIT

COBIT es la herramienta más completa que existe para administrar y operar a un nivel superior los estándares de tecnología para la administración de sistemas de información lo cual brinda a la alta gerencia la posibilidad de medir la efectividad,

eficiencia, confidencialidad, integridad, y disponibilidad de sus recursos de TI a través de una política clara y de buenas practicas de control de TI.

Esta herramienta permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio. COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de organizaciones, a nivel mundial.

El objetivo de COBIT es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

Por lo tanto, COBIT esta orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con tecnología de información y con tecnologías relacionadas.

El objetivo principal del proyecto COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

6.4.1 La estructura de COBIT

Se define a partir de una premisa simple y pragmática: *"Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".*

COBIT se divide en tres (3) niveles: Dominios, Procesos y Actividades

- **Dominios:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.
- **Actividades:** Acciones requeridas para lograr un resultado medible.

Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI.

El proceso de análisis en el área de TI se desarrolla utilizando los 34 procesos del COBIT (ver Anexo 1).

El análisis de riesgo de cada uno de los procesos de COBIT, así como los respectivos objetivos del control deberán dirigir los puntos de mejoría, generando acciones y proyectos para la mitigación de los riesgos de TI.

6.4.1.1 Dominio Planeación y Organización (PO)

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas

PO1 Definición de un plan Estratégico

Objetivo: Lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.
- El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
- Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI
- Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos

***Requerimientos de negocios*:**

Establecer un equilibrio entre la misión de la entidad pública y la utilización de las tecnologías de información que le permitan garantizar el logro de los objetivos propuestos.

Se hace posible:

Implementar políticas que normatizen la aplicación de actividades que promuevan el uso de los sistemas de información como mecanismo para la ejecución de los procesos.

Se toma en consideración:

Leyes y normas establecidas por los organismos de control
Los organismos y entidades del estado están regidos por entes reguladores y de control, encargados de generar las leyes y decretos que rigen los procesos dados en cada una de ellas. Estas leyes y decretos constituyen la misión de las empresas del estado. Las leyes deben ser aplicadas por la gerencia de cada una de las entidades, para el desarrollo y la implementación de planes a largo y corto plazo que satisfagan las metas de la organización.

Objetivos de negocio y necesidades de TI
La gerencia será la encargada de establecer los procesos y procedimientos de la organización y determinar qué, cómo, quien y cuando se realizan las actividades que garanticen el cumplimiento de las políticas y normas establecidas, asegurando la eficiente ejecución de estas actividades.

Inventario de soluciones tecnológicas e infraestructura actual
Dentro de la estructura organizacional la gerencia de la función de planeación de los sistemas de información, deberá realizar los planes y programas necesarios para la realización de estas actividades.

Evaluación de sistemas existentes
La gerencia de planeación de los servicios de información será la encargada de evaluar los sistemas tecnológicos y determinar objetivamente el estado de los mismos, para suministrar a la alta gerencia la información necesaria para la toma de decisiones que contribuyan al mejoramiento y efectividad de los sistemas de información de la entidad.

Cambios organizacionales
En las entidades del estado la alta gerencia debe promover planes y programas que garanticen el sostenimiento de los procesos misionales a pesar de los cambios administrativos dados por ley.

PO2 Definición de la Arquitectura de Información

Objetivo: Satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

- La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
- El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.
- La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

***Requerimientos de negocio*:**

Organizar de la mejor manera los sistemas de información

Se hace posible a través de:

La creación y mantenimiento de un modelo de información de negocios y asegurando que se definan sistemas apropiados para optimizar la utilización de esta información.

Se toma en consideración:

Documentación
Con base en políticas establecidas y asignadas por los organismos de control, los cuales periódicamente requieren el envío y reporte de los datos producto de los procesos realizados de acuerdo a la misión de la organización estatal. La gerencia de servicios de información debe brindar a la entidad herramientas que ayuden al responsable de emitir el reporte de los datos llevar a cabo sus tareas de manera oportuna y eficiente. Se debe desarrollar y actualizar una arquitectura de información con todos los datos manejados en el interior y por fuera de la entidad.

Diccionario de datos
La gerencia de información debe crear y mantener actualizado sin cambiar su estructura, el diccionario de datos con la información que maneja la organización.

Reglas de sintaxis de datos
Deberá establecerse un marco de referencia de Clasificación general relativa a la ubicación de datos en clases de información (por ejemplo, categorías de seguridad), así como a la asignación de propiedad. Las reglas de acceso para las clases deberán definirse apropiadamente.

Propiedad de la información y clasificación de seguridad
Desarrollar planes de contingencia que nos garanticen en una escala superior la seguridad de la información manejada dentro de la organización.

PO3 Determinación de la dirección tecnológica

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.
- El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

Requerimientos de negocios:

Aprovechar la tecnología disponible en la organización.

Se hace posible a través de:

La creación y mantenimiento de un plan de infraestructura tecnológica.

Se toma en consideración:

Planeación de la infraestructura tecnológica

Debe ser función de la gerencia de sistemas de información, en las entidades públicas velar por el cumplimiento y aplicación de las políticas y normas que promuevan y apoyen la utilización de los sistemas de información creando y actualizando planes y programas de infraestructura de acuerdo a los objetivos establecidos en el largo y corto plazo.

Monitoreo de desarrollos tecnológicos

Se debe realizar por parte de la gerencia de sistema de información un monitoreo continuo de las tendencias futuras y condiciones regulatorias que puedan tenerse en cuenta durante el desarrollo de las actividades para la toma de decisiones.

Contingencia en la infraestructura tecnológica

El plan de infraestructura tecnológica deberá ser evaluado teniendo en cuenta los aspectos de contingencia como: redundancia, resistencia, capacidad de adecuación y evolución de infraestructura.

Planes de adquisición de hardware y software

Se debe realizar planes para la adquisición de hardware y software que estén acordes con las necesidades establecidas e identificadas en el plan de infraestructura tecnológica.

Estándares de tecnología

Estandarizar a través de normas la arquitectura tecnológica con base al plan de infraestructura tecnológica, liderado por el área de TI y apoyado por la alta gerencia.

PO4 Definición de la organización y de las relaciones de TI

Objetivo: Prestación de servicios de TI

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- El comité de dirección el cual se encargara de vigilar la función de servicios de información y sus actividades.
- Propiedad, custodia, la Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente
- Segregación de funciones, con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.
- Los roles y responsabilidades, la gerencia deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas
- La descripción de puestos, deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
- Los niveles de asignación de personal, deberán hacerse evaluaciones de requerimientos regularmente para asegurar para asegurar una asignación de personal adecuada en el presente y en el futuro.
- El personal clave, la gerencia deberá definir e identificar al personal clave de tecnología de información.

Requerimientos de negocios:

Prestación de los servicios de TI. Establecimiento de la estructura organizacional.

Se hace posible a través de:

De la organización estructurada eficientemente con tareas y responsabilidades definidas y relacionadas

Se toma en consideración:

Comité de planeación o dirección de la función de servicios de información
La alta gerencia de la organización deberá crear un comité para la vigilancia del funcionamiento del servicio de información y sus actividades. Deberán participar funcionarios de la dirección general, coordinadores y funcionarios capacitados en tecnología de información. Este comité deberá reunirse de manera periódica e informar por medio de actas a la dirección general.

Ubicación de los servicios de información en la organización
La alta gerencia deberá ubicar al área de sistemas dentro de la estructura organizacional general y deberá asegurar la existencia de autoridad, actitud crítica e independencia por parte del departamento usuario con un grado tal que sea posible garantizar soluciones de tecnología de información efectivas y progreso suficiente al implementarlas, así como establecer una relación directa con la alta Gerencia para incrementar la capacidad de previsión, la comprensión y las habilidades para identificar y resolver problemas de tecnología de información..

Revisión de Logros Organizacionales
Revisar periódicamente que la estructura organizacional cumpla continuamente con los objetivos y en caso de cambios se adapte a estos.

Funciones y Responsabilidades
La Gerencia deberá asegurar que todo el personal en la organización conozca sus funciones y responsabilidades en relación con los sistemas de información. Todo el personal deberá contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas. Todos deberán estar conscientes de que tienen una cierta responsabilidad con respecto a la seguridad y al control interno. Consecuentemente, deberán organizarse y emprenderse campañas regulares para aumentar la conciencia y la disciplina.

Responsabilidad de la Seguridad, calidad y propiedad de la información.
La Gerencia deberá asignar formalmente la responsabilidad de la seguridad de la calidad de la información al área de sistemas y garantizar que existan los controles y planes de contingencia necesarios para salvaguardar la información. Así mismo deberá asegurar que todos los activos de información cuenten con un propietario asignado que se responsabilice de las decisiones de acuerdo a las funciones realizadas. Al mismo tiempo la gerencia debe asignar un administrador de la seguridad de la información que maneje los niveles de acceso para los diferentes usuarios.

Supervisión y Segregación de Funciones

La alta gerencia deberá implementar prácticas de supervisión en el área de sistemas para que las funciones y responsabilidades sean llevadas a cabo apropiadamente, al mismo tiempo deberá crear una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico.

La Gerencia deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones:

- Uso de sistemas de información;
- Entrada de datos;
- Operación de cómputo;
- Administración de redes;
- Administración de sistemas;
- Desarrollo y mantenimiento de sistemas
- Administración de cambios
- Administración de seguridad;
- Auditoria de seguridad necesaria para el puesto y ser adecuadas para su utilización en evaluaciones de desempeño.

Asignación de Personal para Tecnología de Información

El área de sistemas deberá estar dotada por un número suficiente de personal competente en tecnología de información. Esta asignación deberá ser evaluada mínimo cada año o cuando se presenten cambios organizacionales, en el. Ambiente operacional o de tecnología de información. Cada uno de los integrantes del área de sistemas deberá tener claramente la responsabilidad de acuerdo al perfil que cumpla dentro del área y de las habilidades con que cuente la persona, también se deberán definir e identificar al personal clave de la organización.

Relaciones

La Gerencia de la función de servicios de información deberá llevar a cabo las acciones necesarias para establecer y mantener una coordinación, una comunicación y un enlace óptimo entre la función de servicios de información y demás elementos interesados dentro y fuera de la función de servicios de información (usuarios, proveedores, oficiales de seguridad, Gerentes).

PO5 Manejo de la inversión

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando 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, teniendo en cuenta:

- Las alternativas de financiamiento, se deberán investigar diferentes alternativas de financiamiento.
- El control del gasto real, se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información
- La justificación de costos y beneficios, deberá establecerse un control gerencial que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costos. Los beneficios derivados de las actividades de TI deberán ser analizados en forma similar.

Requerimientos de negocios:

Asegurar dentro del presupuesto inicial de la entidad, los recursos financieros para el desarrollo de proyectos de tecnología de información

Se hace posible a través de:

Presupuesto inicial aprobado con asignación especificas a proyectos de TI.

Se toma en consideración:

Alternativas de financiamiento
Contar con el presupuesto aprobado para financiar la ejecución de los planes a largo y corto plazo de tecnología de información dentro de la organización.

Monitoreo y justificación de costo - beneficio
Se deben establecer mecanismos para verificar que los planes ejecutados se cumplan de acuerdo a los tiempos establecidos y a los costos presupuestados.
Se deben analizar los beneficios derivados de la ejecución e implementación de los proyectos de tecnología de información.

PO6 Comunicación de la dirección y aspiraciones de la gerencia

Objetivo: 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. Toma en cuenta:

- Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá

ser establecido por la Alta Gerencia y promoverse a través del ejemplo.
- Las directrices tecnológicas
- El cumplimiento, la Gerencia deberá también asegurar y monitorear la duración de la implementación de sus políticas.
- El compromiso con la calidad, la Gerencia de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.
- Las políticas de seguridad y control interno, la alta gerencia deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

Requerimientos del Negocio:

Dar a conocer los principios organizacionales para generar sentido de pertenencia entre los integrantes de la entidad.

Se hace posible a través de:

Políticas y normas establecidas y difundidas en toda la organización.

Se toma en consideración:

Código de ética y conducta
La gerencia debe fomentar dentro de la cultura organizacional, la generación de los valores éticos, integridad, filosofía y estilo operativo en cuanto a las herramientas y programas de TI implementados en la organización. Además de asumir la responsabilidad completa de la formulación, el desarrollo, la documentación, la promulgación y el control de políticas que cumplan las directrices planteadas.

Las políticas organizacionales deben ser cumplidas en todos los niveles de la organización. Destinando recursos para la implementación de la misma. Las políticas deberán ser ajustadas regularmente para adecuarse a las condiciones cambiantes y podrán ser replanteadas o transformadas en su totalidad.

La gerencia deberá crear el manual de funciones y procedimientos y velar por el cumplimiento de las políticas y estándares contenidos en el, además asegurar la compresión por parte del personal las mismas.

Políticas sobre el marco de referencia para la seguridad y el control interno
Se deberá desarrollar y mantener una política de seguridad de alto nivel al igual que una filosofía de calidad y una política de control interno, las cuales especifiquen el propósito y los objetivos de la organización, la estructura gerencial, la definición y asignación de responsabilidades para su implementación en todos los niveles, al igual que la definición de acciones disciplinarias asociadas con las políticas de seguridad y de control interno y la filosofía de calidad.

Derecho propiedad intelectual
La gerencia deberá implementar una política en cuanto a los desarrollos de software dentro o fuera de la organización.

PO7 Administración de recursos humanos

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

- El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
- Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera
- La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
- La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

Requerimientos de negocios:

Aprovechar al máximo el potencial del personal que realiza las operaciones de TI en la empresa.

Se hace posible a través de:

Manuales y técnicas bien definidas y un eficiente manejo y control del personal

Tomando en consideración:

Reclutamiento del personal

La gerencia de la entidad estatal, de acuerdo a las leyes y políticas de la contratación publica, deberá escoger a los funcionarios que desempeñaran las funciones de la empresa teniendo en cuenta su perfil, grado de conocimiento, la experiencia y habilidades en la realización de las actividades propias del cargo.

Entrenamiento del personal

La gerencia deberá establecer políticas claras para que los empleados reciban la capacitación necesaria al momento de posesionarse en cualquier cargo y debe velar por el mantenimiento de los manuales de funciones actualizados según las normas y políticas vigentes, para que sirva como una herramienta de trabajo al empleado en la ejecución de sus labores y par que el desempeño normal de la organización no se vea afectado.

Evaluación de Desempeño de los Empleados

La gerencia de acuerdo a los formatos establecidos por la ley, deberá distribuir entre sus funcionarios coordinadores los formatos para la evaluación de desempeño del personal a su cargo para que se realice la respectiva evaluación por parte del área de personal.

Responsabilidad Con los Bienes del Estado
La gerencia debe establecer políticas claras en cuanto a la utilización de los bines del estado, dándolas a conocer a sus funcionarios para que no atenten contra el detrimento publico y establecer medidas disciplinarias cuando se viole alguna de ellas.

Cambios de Puesto y Despidos
La Gerencia deberá asegurar que se tomen acciones oportunas y apropiadas con respecto a cambios de puesto y despidos, de tal manera que los controles internos y la seguridad no se vea perjudicados por estos eventos.

PO8 Asegurar el cumplimiento con los requerimientos Externos

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales
Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

- Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.
- Leyes, regulaciones y contratos

- Revisiones regulares en cuanto a cambios
- Búsqueda de asistencia legal y modificaciones
- Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- Privacidad
- Propiedad intelectual
- Flujo de datos externos y criptografía

***Requerimientos de negocios*:**

Cumplir con las obligaciones legales que se presenten por situaciones internas y externas de la organización.

Se hace posible a través de:

La identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, y llevando a cabo las medidas apropiadas para cumplir con ellos.

Tomando en consideración:

Revisión de Requerimientos Externos

La organización deberá establecer y mantener procedimientos para la revisión de requerimientos externos y para la coordinación de estas actividades. Deberán revisarse continuamente los requerimientos legales, políticas y leyes o cualquier otro requerimiento externo relacionado con las prácticas y controles de tecnología de información. La Gerencia deberá también evaluar el impacto de cualquier relación externa en las necesidades generales de información de la organización, incluyendo la determinación del grado al cual las estrategias del área de TI debe soportar o cumplir con los requerimientos de terceros. La Gerencia deberá asegurar que se establezcan contratos formales para determinar acuerdos entre proveedores y terceros, sobre procesos de comunicación, así como sobre estándares de mensajes de transacción, seguridad y almacenamiento de datos. Cuando se realicen operaciones de intercambio en Internet, la gerencia deberá imponer adecuados controles para asegurar el cumplimiento de leyes locales y costumbres en un ámbito mundial.

Prácticas y Procedimientos para el Cumplimiento de Requerimientos Externos

Deberán asegurar que se lleven a cabo oportunamente las acciones correctivas apropiadas para garantizar el cumplimiento de los requerimientos externos. Además, deberán establecerse y mantenerse procedimientos adecuados que aseguren el cumplimiento continuo. A este respecto la Gerencia deberá solicitar apoyo al departamento jurídico de la entidad si fuere necesario.

Cumplimiento de Seguridad y Ergonomía

La Gerencia deberá asegurar el cumplimiento de los estándares ergonómicos y de seguridad en el ambiente de trabajo de los usuarios y el personal del área de TI

Propiedad intelectual y flujos de datos

La Gerencia deberá asegurar el cumplimiento de las regulaciones sobre privacidad o confidencialidad, propiedad intelectual, flujo de datos externos y criptografía aplicables a las prácticas de tecnología de información de la organización.

Cumplimiento con los Contratos de Seguros

La Gerencia deberá asegurar la identificación y el continuo cumplimiento de los requerimientos de los contratos de seguros.

PO9 Evaluación de riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI

Para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.
- Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.
- Actualización de evaluación de riesgos
- Metodología de evaluación de riesgos
- Medición de riesgos cualitativos y/o cuantitativos
- Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
- Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

***Requerimientos de negocios*:**

Responder a las amenazas relacionadas con la operación de TI, contribuyendo al logro de los objetivos del área de TI.

Se hace posible a través de:

La participación de la organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos para mejorar la toma de decisiones.

Tomando en consideración:

Evaluación de riesgos del negocio
La Gerencia deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información relevantes para el logro de los objetivos del negocio, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos utilizando los resultados de auditorias, inspecciones e incidentes identificados.

Enfoque de Evaluación de Riesgos
La Gerencia deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

Identificación de Riesgos
La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.

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

PO10 Administración de proyectos

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión
Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como

la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

- El involucramiento de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
- Presupuestos de costos y horas hombre
- Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
- Plan de administración de riesgos para eliminar o minimizar los riesgos.
- Planes de prueba, entrenamiento, revisión post-implementación.

PO11 Administración de calidad

Objetivo: Satisfacer los requerimientos del cliente

Para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

- Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.
- Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorias, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.
- Metodologías del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
- Documentación de pruebas de sistemas y programas
- Revisiones y reportes de aseguramiento de calidad

6.4.1.2 Dominio Adquisición e Implementación (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

AI1 Identificación de Soluciones Automatizadas

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
- Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.
- Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
- Seguridad con relación de costo-beneficio favorable para controlar que los costos no excedan los beneficios.
- Pistas de auditoria para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensitivos (ej. Identificación de usuarios contra divulgación o mal uso)
- Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
- Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología especifica a ser proporcionada.

AI2 Adquisición y mantenimiento del software aplicativo

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- Requerimientos de archivo, entrada, proceso y salida.
- Interfase usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
- Personalización de paquetes
- Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
- Controles de aplicación y requerimientos funcionales
- Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

AI3 Adquisición y mantenimiento de la infraestructura tecnológica

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
- Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
- Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

AI4 Desarrollo y mantenimiento de procedimientos

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

- Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
- Manuales de Operaciones y controles, de manera que estén en permanente actualización.
- Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

AI5 Instalación y aceptación de los sistemas

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
- Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
- Acreditación de manera que la Gerencia de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

- Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera mas económica.

AI6 Administración de los cambios

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual y toma en consideración:

- Identificación de cambios tanto internos como por parte de proveedores
- Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
- Evaluación del impacto que provocaran los cambios.
- Autorización de cambios
- Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.
- Distribución de software, estableciendo medidas de control especificas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

6.4.1.3 Dominio Entrega de Servicios y Soporte (DS)

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Ds1 Definición de niveles de servicio

Objetivo: Establecer una comprensión común del nivel de servicio requerido

Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

- Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por

servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

- Definición de las responsabilidades de los usuarios y de la función de servicios de información
- Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
- Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.
- Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su costo.
- Garantías de integridad
- Convenios de confidencialidad
- Implementación de un programa de mejoramiento del servicio.

Ds2 Administración de servicios prestados por terceros

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos

Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

- Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
- Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.
- Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
- Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

Ds3 Administración de desempeño y capacidad

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.

Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

- Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información
- Monitoreo y reporte de los recursos de tecnología de información
- Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
- Administración de capacidad estableciendo un proceso de planeación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño
- Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

Ds4 Asegurar el Servicio Continuo

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- Planificación de Severidad
- Plan Documentado
- Procedimientos Alternativos
- Respaldo y Recuperación
- Pruebas y entrenamiento sistemático y singulares

Ds5 Garantizar la seguridad de sistemas

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso
- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario

- Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas
- Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
- Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
- Utilización de Firewalls si existe una conexión con Internet u otras redes públicas en la organización

Ds6 Educación y entrenamiento de usuarios

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados

Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- Curriculum de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
- Campañas de concientización, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento
- Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información

Ds7 Identificación y asignación de costos

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI

Para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

- Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios
- Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de computo y aseguren el trato justo de los departamentos usuarios y sus necesidades
- Tarifas definiendo e implementando procedimientos de costeo de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía

Ds8 Apoyo y asistencia a los clientes de TI

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente

Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

- Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda
- Monitoreo de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas
- Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias

Ds9 Administración de la configuración

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios

Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

- Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición
- Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración
- Chequeo de software no autorizado revisando periódicamente las computadoras personales de la organización
- Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas

Ds10 Administración de Problemas

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

Ds11 Administración de Datos

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

Ds12 Administración de las instalaciones

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

Ds13 Administración de la operación

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

6.4.1.4 Dominio Monitoreo (M)

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los

requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

M1 Monitoreo del Proceso

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.
Para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

Se debe tener en consideración:

La dirección de sistemas debe impulsar la definición de indicadores del desempeño relevantes, el informe sistemático y oportuno del desempeño, y la acción inmediata en caso de desviaciones.

A través de esta tarea de monitoreo se asegura el logro de los objetivos establecidos para los procesos de TI, esto se hace posible a través de la definición por parte de la gerencia de reportes e indicadores de desempeño gerenciales, la implementación de sistemas de soporte así como la atención regular a los reportes emitidos, tomando en consideración:

- Indicadores clave de desempeño
- Factores críticos de éxito
- Evaluación de la satisfacción de los servicios prestados
- Reportes gerenciales

Esta tarea de monitoreo de procesos se puede llevar a cabo bajo la aplicación de los objetivos de control plasmados en COBIT

- *Recolección de Datos de Monitoreo:* Para los procesos de tecnología de información y de control interno, la dirección de sistemas deberá asegurar que se definan indicadores de desempeño relevantes (ej. comparaciones externas) tanto para actividades internas como las proporcionadas por terceros y que se recolecten datos para la creación de reportes relevantes de desempeño y reportes de excepción relacionados con estos indicadores.

- *Evaluación de Desempeño:* Los servicios a ser proporcionados por la función de servicios de información deberán ser medidos (indicadores clave de desempeño y/o factores críticos de éxito) y comparados con los niveles objetivo. Las evaluaciones a la función de servicios de información deberán ser desarrolladas en forma continua.

- *Evaluación de la Satisfacción de los Servicios Prestados:* A intervalos regulares, la dirección de sistemas deberá efectuar mediciones de la satisfacción de los clientes con respecto a los servicios proporcionados por la función de servicios de información, con la intención de identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento.

- *Reportes Gerenciales:* Deberán proporcionarse reportes gerenciales para ser revisados por la alta gerencia en cuanto al avance de la organización hacia las metas identificadas. Con base en la revisión, la Gerencia deberá iniciar y controlar las acciones pertinentes.

M2 Evaluar lo adecuado del Control Interno

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.
Para ello la gerencia es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

Se debe tener en consideración:

Mediante esta evaluación se hace posible asegurar el logro de los objetivos de control interno establecidos para los procesos de TI a través del compromiso de la dirección de sistemas de monitorear los controles internos, evaluar su efectividad y emitir reportes sobre ellos en forma regular, tomando en consideración aspectos como:

- Monitoreo permanente de control interno
- Comparación con mejores prácticas
- Reportes de errores y excepciones
- Auto evaluaciones
- Reportes gerenciales

Hay objetivos de control aplicables a esta tarea de evaluación del control interno, para el correcto y eficaz monitoreo del sistema de administración de riesgos, entre estos se encuentran:

- *Monitoreo de Control Interno:* La Gerencia deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

- *Operación Oportuna de Controles Internos:* La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la dirección de sistemas.

- *Reporte sobre el Nivel de Control Interno:* La Dirección de sistemas deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas para asegurar la efectividad continua de su sistema de control interno. Deberán llevarse a cabo acciones para identificar qué información es requerida a un nivel particular de toma de decisiones.

- *Seguridad de Operación y Aseguramiento de Control Interno:* La garantía de seguridad operacional y el aseguramiento de control interno deberán ser establecidos a través de una "auto auditoria" o de una auditoria independiente para examinar si la seguridad y los controles internos se encuentran operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos. Las actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

M3 Obtención de Aseguramiento Independiente

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

Como esta guía esta orientada hacía entidades públicas, éste proceso se ha tratado generalizadamente porque esta dirigido a organizaciones enfocadas a negocios, sin embargo no se desconoce que en casos especiales puede tener aplicabilidad en el ámbito gubernamental.

M4 Proveer Auditoria Independiente

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorias independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoria, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta auditoria deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoria.

Se debe tener en consideración:

Con el cumplimiento de este proceso se logra incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas, a través de auditorias independientes desarrolladas en intervalos regulares, tomando en consideración aspectos como:

- Independencia de auditoria
- Involucramiento proactivo de auditoria
- Ejecución de auditorias por parte de personal calificado
- Aclaración de resultados y recomendaciones
- Actividades de seguimiento

Para el cumplimiento de este proceso se hace necesaria la aplicación de ciertos objetivos de control, con el fin de llevar a cabo y de manera eficaz el proceso de monitoreo del sistema de administración de riesgos, los objetivos de control aplicables a este proceso son los siguientes:

- *Estatutos de Auditoria:* La alta gerencia de la organización deberá establecer los estatutos para la función de auditoria. Este documento deberá establecer la responsabilidad, autoridad y obligaciones de la función de auditoria. Asimismo este documento deberá ser revisado periódicamente para asegurar que se mantengan la independencia, autoridad y responsabilidad de la función de auditoria.

- *Independencia:* El auditor deberá ser independiente del auditado tanto en actitud como en apariencia (real y percibida). Los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado, y en la medida de lo posible, deberá también ser independiente de la propia empresa. De esta manera, la función de auditoria deberá ser suficientemente independiente del área auditada para concluir una auditoria en forma objetiva.

- *Ética y Estándares Profesionales:* La función de auditoria deberá asegurar el cumplimiento de los códigos aplicables de ética profesional (ej. Código de Ética de la *Information Systems Audit and Control Association*) y estándares de auditoría (ej. Estándares de la *Information Systems Audit and Control Association*) en todo lo que lleve a cabo. El debido cuidado profesional deberá observarse en todos los aspectos del trabajo de auditoria, incluyendo el respeto de estándares aplicables sobre auditoria y tecnología de información.

- Competencia: La dirección de sistemas deberá asegurar que los auditores responsables de las revisiones de las actividades de la función de servicios de información de la organización, sean técnicamente competentes y cuentan en forma general con las habilidades y conocimientos necesarios para desempeñar dichas revisiones en forma efectiva, eficiente y económica. La dirección de sistemas deberá asegurar que el personal asignado a tareas de auditoria de sistemas de información, mantiene su nivel de competencia técnica mediante un programa adecuado de educación profesional continua.

- *Planeación:* La dirección de sistemas deberá establecer un plan de auditoria para garantizar que se obtenga un aseguramiento regular e independiente con respecto a la efectividad, eficiencia y economía de la seguridad y de los procedimientos de control interno, así como de la habilidad de la dirección de sistemas para controlar las actividades de la función de servicios de información. Dentro de este plan la dirección de sistemas deberá determinar las prioridades relacionadas con la obtención de aseguramiento independiente. Los auditores deberán planear el trabajo de auditoria para alcanzar los objetivos de auditoria y cumplir con los estándares profesionales correspondientes.

- *Ejecución del Trabajo de Auditoria:* Las auditorias deberán ser supervisadas apropiadamente para proporcionar certeza de que los objetivos de auditoria están siendo alcanzados y que los estándares profesionales de auditoria que sean aplicables están siendo observados. Los auditores deberán asegurarse de obtener evidencia suficiente, confiable, relevante y útil para alcanzar los objetivos de auditoria de forma efectiva. Los hallazgos y conclusiones de auditoria deben estar

soportadas por un análisis apropiado y una correcta interpretación de esta evidencia.

- *Reporte:* La función de auditoria de la organización deberá proporcionar un reporte en un formato adecuado, para todo el personal interesado una vez concluida su revisión. El reporte de auditoria deberá mostrar los objetivos de la auditoria, el período de cobertura y la naturaleza y extensión de trabajo de auditoria realizado. El reporte deberá identificar a la Organización, los destinatarios del informe y cualquier restricción en su circulación. El reporte de auditoria deberá también mostrar los hallazgos, conclusiones y recomendaciones relacionadas con el trabajo de auditoria llevado a cabo, así como cualquier salvedad o comentario que el auditor tenga con respecto a la auditoria.

- *Actividades de Seguimiento:* La resolución acerca de los comentarios sobre la auditoria depende de la dirección de sistemas. Los auditores deberán solicitar y evaluar información pertinente sobre hallazgos, conclusiones y recomendaciones previos para determinar si las acciones apropiadas han sido implementadas de manera oportuna.

6.5 GOBIERNO DE TI[9]

El Gobierno de TI (GTI), es el marco de derecho otorgado para la toma de decisiones y la definición de responsabilidades para impulsar comportamientos adecuados en el uso de TI.

Dentro de las características del Gobierno de TI, se encuentran las siguientes:

1. Es responsabilidad de ejecutivos y socios.
2. Enfocado en el logro de las metas y objetivos de la organización.
3. Preocupado por la adición de valor a la organización.
4. Mantiene el equilibrio entre el riesgo y el retorno de la TI y sus procesos.
5. Proporciona mejoras medibles en la efectividad y eficiencia de los procesos del negocio.
6. Provee la estructura que relaciona la información, los recursos y procesos de TI con los objetivos estratégicos de la organización.
7. Integra e institucionaliza las buenas prácticas sobre el desempeño de la TI para garantizar el soporte adecuado a los objetivos del negocio

    - ✓ Planeación y Organización
    - ✓ Adquisición e implementación
    - ✓ Entrega y Soporte
    - ✓ Monitoreo

Para evaluar la efectividad de un GTI se valora la efectividad en la obtención de cuatro importantes objetivos:

- ✓ Uso Costo-Efectivo de la TI
- ✓ Uso efectivo de TI para el área financiera
- ✓ Uso efectivo de TI para el crecimiento
- ✓ Uso efectivo de TI para adquirir flexibilidad de negocios

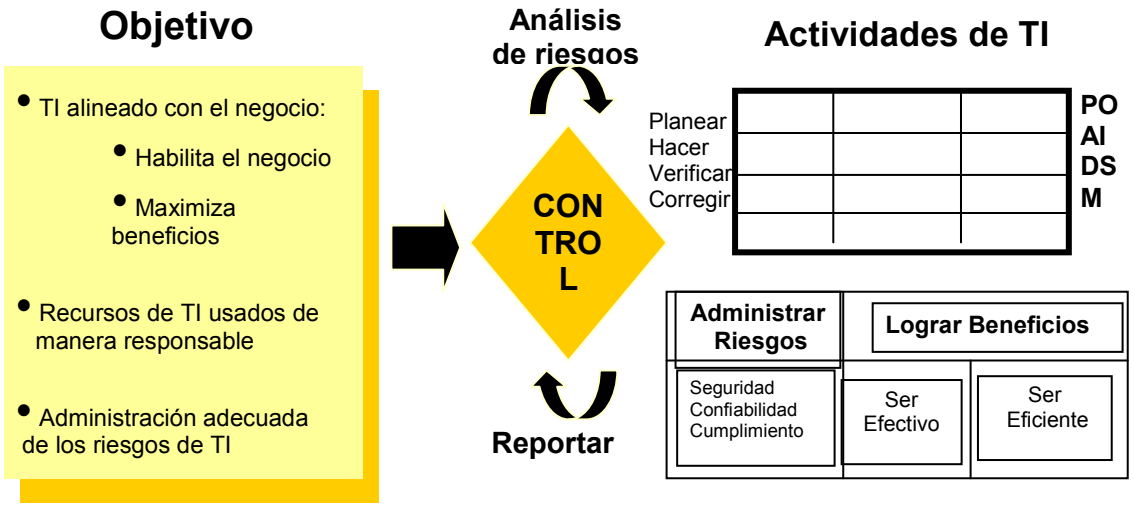


Fig. 18 Gobierno de TI

El GTI comprende 5 dominios críticos, que son:

- Principios de TI: Decisiones de alto nivel acerca del papel estratégico de la TI en el negocio.
- Arquitectura de TI: Un conjunto integrado de decisiones técnicas para guiar a la organización en la satisfacción de sus necesidades.
- Infraestructura de TI: Provee la base para las capacidades de TI, se crea cuando se conocen con precisión las necesidades y usos que tendrá en la compañía.
- Aplicativos para necesidades de negocio: Aplicativos comprados o desarrollados que satisfacen los requerimientos de negocios.
- Priorización e inversiones: Decisiones acerca de cuánto y en qué invertir en TI, incluyendo la justificación para aprobación de proyectos.

Y presenta 6 Arquetipos de gobierno para la toma de decisiones:

- Monarquía de negocio: La constituye un ejecutivo Senior o un grupo de ellos, a veces incluyendo el CIO.
- Monarquía de TI: Un ejecutivo o grupo de ejecutivos de TI.
- Federal: Ejecutivo de alto nivel y un grupo de ejecutivos de las divisiones operativas (puede incluir a TI).

- Duopolio de TI: Decisión de dos partes que involucra ejecutivos de TI y ejecutivos de negocios.
- Feudal: Líderes de unidades de negocios o procesos, toman decisiones aisladas del entorno basados solamente en necesidades propias.
- Anarquía: Cada usuario individual o grupo pequeño toma sus decisiones

Lo anterior, se lleva a una matriz que permite analizar donde se están tomando las decisiones de TI en la organización, según el enfoque:

Decision / Archetype	IT principles	IT architecture	IT infra-structure strategies	Business application needs	IT investment
Business Monarchy	X				X
IT Monarchy		X	X		
Federal				X	
Duopoly					
Feudal					
Anarchy					

Researcher interpretation of UPS governance arrangements based on interviews with senior executives on the firm's IT steering committee.

Fig. 19 Matriz de análisis

ENFOQUE CENTRALIZADO DE GTI

Se basa en una fuerte estandarización de sus procesos, lo que les permite lograr un comportamiento adecuado en el uso de TI, eficiencia en costos y uso de recursos. Sus esfuerzos se orientan a obtener rentabilidad.

ENFOQUE DESCENTRALIZADO DE GTI

Consiste en manejar responsabilidades localmente en sus áreas. Quieren mantener autonomía en sus unidades de negocios y evitar obstáculos a la creatividad y la innovación. De manera consistente a lo anterior requieren algunos mecanismos de GTI con frecuencia relacionados con la prioridad de las inversiones y el manejo de riesgos. Sus esfuerzos se orientan al crecimiento del ingreso y la innovación.

ENFOQUE HÍBRIDO DE GTI

Consiste en balancear el contraste entre Gobierno para rentabilidad y Gobierno para crecimiento del ingreso y la innovación.

Estas compañías enfocan sus esfuerzos en utilizar servicios compartidos para obtener receptividad en sus clientes o economías de escala ó ambas. Sus principios de TI enfatizan en la reutilización de procesos, sistemas, tecnologías y módulos de datos. Las empresas líderes en utilización de sus activos generalmente manejan las decisiones en Duopolios y Gobiernos de tipo Federal.

Las compañías pueden usar el marco de Gobierno de TI para ayudar a diseñar las estructuras y procesos que aumenten los beneficios estratégicos del uso de TI.

Para aplicar efectivamente el Gobierno de TI, se recomienda los siguientes cuatro pasos:

- ✓ Primero: Identificar las necesidades de sinergia y autonomía de la compañía.

  Es conveniente que la valoración de la importancia de este aspecto sea muy realista y que permita también la autonomía que sea conveniente a los objetivos estratégicos de la compañía.

- ✓ Segundo: Establecer el papel de la Estructura de la organización.

  La estructura de la organización puede ser centralizada, descentralizada ó mixta. La estructura mixta combina las dos primeras formas y puede llegar a ser compleja y limitar su efectividad.
  Estableciendo prioridades en la organización para la autonomía y sinergia las compañías se pueden crear diseños organizacionales e incentivar a esos sistemas a cumplir con dichas prioridades. Las compañías pueden iniciar el diseño de su GTI .

- ✓ Tercero: Identificar los comportamientos deseables para TI que caen fuera del alcance de la Estructura organizacional

  Identificar cuáles comportamientos organizacionales hay que reforzar, identificar cuales comportamientos adicionales debe promover para conseguir sus objetivos de sinergia y autonomía.

- ✓ Cuarto: Diseñar el Gobierno de TI.

  Una vez los objetivos de GTI están claros las compañías pueden diseñar su GTI, definiendo sus acuerdos de gobierno y especificando los mecanismos que implementarán esos acuerdos.

6.5.1 Apoyo a la toma de decisiones basado en Gobierno de TI

El proceso de apoyo a la toma de decisiones incluye un análisis de costo-beneficio formal con funciones y responsabilidades definidas en los límites organizativos. El análisis de costo-beneficio proporciona una estructura coherente y exhaustiva para identificar, determinar el alcance y seleccionar la solución más eficaz y asequible para reducir el riesgo a un nivel aceptable. De forma similar al proceso de evaluación de riesgos, el análisis de costo-beneficio requiere definiciones de función estrictas para que funcione de forma eficaz. Asimismo, antes de efectuar el análisis de costo-beneficio, el equipo de administración de riesgos de seguridad debe garantizar que todos los participantes, incluido el patrocinador ejecutivo, han reconocido y aceptado el proceso.

Cada entidad fija sus propios objetivos de negocios y busca cumplirlos a través de un conjunto de medidas organizacionales que reflejan la cultura de la organización. Muchas empresas muestran sus estilos de gobernabilidad basados en cómo TI se relaciona con las unidades de negocios, la relación de estas unidades con la estructura corporativa y qué tan ampliamente es compartido el proceso de toma de decisiones dentro y entre las organizaciones.

Los mecanismos de Gobernabilidad de TI, como *Comités, Acuerdos de niveles de servicios, Charge-backs* y otros, proveen el significado que permitirán al estilo de gobernabilidad de TI entregar resultados concretos. Estos mecanismos permiten maximizar el valor de la empresa mediante la estandarización, los acuerdos claros y disciplinas financieras.

Armonizar estos factores es clave para la implementación de un proceso de gobernabilidad de TI. Es además importante evitar las siguientes situaciones, que normalmente frenan los intentos de mejorar la gobernabilidad de TI:

- **Participación inadecuada de la gerencia de negocios:** Los gerentes de TI deben presentar un plan realista con las fortalezas de la gobernabilidad, que pueda demostrar su vínculo para mejorar el negocio, o la Administración alta de negocios, podría calificar el proceso de Gobernabilidad de TI, como una “Actividad” mas de TI y relegar en la prioridad y soporte que esta requiere.

- **Falta de objetivos bien articulados:** Sin objetivos claros, muchas personas involucradas en el proceso de gobernabilidad de TI, van a cuestionar su participación, pensando en “¿que hay en esto para mi?” y fallar en entender la gobernabilidad de TI como un medio para alcanzar los objetivos de negocios.

- **Falta de procesos de Gobernabilidad claramente definidos:** Deben existir procesos claros y prácticos de Gobernabilidad de TI, que reconozcan el estilo de toma de decisiones, cultura y practicas de la empresa e identificar pasos de acción, roles, responsabilidades y entregables finales e intermedios.

El proceso es la clave, diseñar la gobernabilidad como un conjunto de procesos de inicio-a-fin para definir roles y responsabilidades y crear un mecanismo de gobernabilidad accionable, adaptado a su estilo de toma de decisiones y cultura administrativa.

Se hace necesario, teniendo en cuenta el proceso de Gobierno de TI, definir o tener claro la clase de estructura organizativa a nivel de toma de decisiones que se esta manejando en la entidad, es decir en donde se están tomando las decisiones correspondientes a los cinco (5) dominios críticos que se presentan en el gobierno de TI, esto se hace posible a través de la aplicación de la matriz de la figura No. 19 en la que se relacionan los seis (6) arquetipos con los cinco (5) dominios antes mencionados.

Decisión / Arquetipo	Principios de TI	Arquitectura de TI	Infraestructura de TI	Aplicativos para necesidades de Negocio	Priorización e Inversiones
Monarquía de Negocio					
Monarquía de TI					
Federal					
Duopolio					
Feudal					
Anarquía					

Durante la fase de apoyo a la toma de decisiones, el equipo de administración de riesgos de seguridad debe determinar cómo afrontar los riesgos clave del modo más eficaz y asequible. El resultado final serán planes claros para controlar, aceptar, transferir o evitar cada uno de los riesgos principales identificados en el proceso de evaluación de riesgos. Los seis pasos de la fase de apoyo a la toma de decisiones son:

1. *Definir los requisitos funcionales:* Los requisitos de seguridad funcionales son declaraciones que describen los controles necesarios para mitigar el riesgo. El término "funcional" es importante: los controles se deben describir según las funciones deseadas en oposición a las tecnologías especificadas. Pueden ser

posibles soluciones técnicas alternativas y cualquier resolución es aceptable si cumple los requisitos de seguridad funcionales. El equipo de administración de riesgos de seguridad es el encargado de definir los requisitos funcionales, el primer resultado del proceso del análisis de costo-beneficio. Para identificar correctamente los posibles controles, el equipo de administración de riesgos de seguridad tiene que definir lo que los controles deben realizar para reducir el riesgo para la empresa. Aunque el equipo conserva la responsabilidad, es muy recomendable la colaboración con el responsable de la solución de mitigación.

2. *Seleccionar las soluciones de control:* En el siguiente paso de esta fase corresponde a los responsables de mitigación elaborar una lista de nuevos posibles controles para cada riesgo que cumplan los requisitos funcionales del mismo. En muchas organizaciones, los miembros del grupo de seguridad de información podrán colaborar mediante la identificación de una serie de posibles controles para cada riesgo identificado y caracterizado durante la fase anterior. Las organizaciones que no dispongan de suficientes especialistas internos para este fin pueden complementar la labor de los responsables de mitigación con consultores.

3. *Revisar las soluciones según los requisitos:* El equipo de administración de riesgos de seguridad debe aprobar la solución de control para garantizar que el control cumple los requisitos funcionales definidos. Otra ventaja de la colaboración en los procesos de costo-beneficio reside en la capacidad de anticipar las comprobaciones y los balances inherentes al proceso; por ejemplo, si el responsable de mitigación está incluido en la definición de requisitos de seguridad, normalmente la solución cumplirá los requisitos.

4. *Estimar la reducción del nivel de riesgo que cada control proporciona:* Después de que el equipo de administración de riesgos de seguridad apruebe la mitigación posible, debe volver a calcular la reducción de riesgo global para la empresa. La cantidad de reducción de riesgo se comparará con el costo de la solución de mitigación. Éste es el primer paso en el que el importe económico puede proporcionar valor al análisis de costo-beneficio. La experiencia demuestra que la reducción de riesgo normalmente se estima ampliando la probabilidad del efecto a la empresa. Recuerde que cada clasificación de probabilidad (alta, media o baja) tiene un intervalo de tiempo previsto en el que es probable que se produzca el ataque.

5. *Estimar los costos de cada solución:* En la siguiente tarea de esta fase corresponde al responsable de mitigación estimar el costo relativo de cada control propuesto. El equipo de ingeniería de TI debe poder determinar el modo de implementar cada control y proporcionar estimaciones razonablemente precisas acerca de lo que costará la adquisición, la implementación y el mantenimiento de cada uno. Debido a que el proceso de administración de riesgos de seguridad que estamos siguiendo implica un proceso de administración de riesgos híbrido, no es necesario calcular los costos precisos, basta con unas estimaciones. Durante el análisis de costo-beneficio, se

compararán los valores y los costos relativos de cada control en vez de las cifras financieras absolutas. Cuando el equipo cree estas estimaciones, debe tener en cuenta todos los gastos directos e indirectos que puedan estar asociados a un control.

6. *Seleccionar la estrategia de mitigación de riesgos:* El último paso en el análisis de costo-beneficio consiste en comparar el nivel de riesgo después de la solución de mitigación con el costo de dicha solución. Tanto el riesgo como el costo contienen valores subjetivos que son difíciles de cuantificar en términos financieros exactos. Utilice los valores cualitativos como una prueba razonable de comparación. Evite la tentación de descartar los costos intangibles si se produce el riesgo. Pregunte al responsable del activo qué sucedería si el riesgo se produjera. Pida al responsable que documente su respuesta para evaluar la importancia de la solución de mitigación. Esta táctica puede ser tan persuasiva como una comparación aritmética de valores cuantitativos.

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones de tipo gerencial, no técnico, condicionadas por diversos factores:

- La gravedad del impacto y/o del riesgo
- Las obligaciones a las que por ley esté sometida la Organización
- Las obligaciones a las que por reglamentos sectoriales esté sometida la Organización
- Las obligaciones a las que por contrato esté sometida la Organización

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- Imagen pública de cara a la Sociedad
- Política interna: relaciones con los propios empleados, tales como capacidad de contratar al Personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.
- Relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, ...
- Relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
- Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad
- Acceso a sellos o calificaciones reconocidas de seguridad

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si:

1. **Es crítico** en el sentido de que requiere atención urgente
2. **Es grave** en el sentido de que requiere atención
3. **Es apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento
4. **Es asumible** en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación.

Las razones que pueden llevar a esta aceptación son:

- Cuando el impacto residual es despreciable
- Cuando el riesgo residual es despreciable
- Cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

Esta calificación tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

6.6 PLANEACION ESTRATEGICA DE TECNOLOGIA INFORMATICA (PETI/PESI)

La incorporación de TI es uno de los temas principales que concierne hoy en día a altos ejecutivos y organizaciones, por ello la necesidad de TI para generar una ventaja competitiva se hace evidente, esto ha producido una creciente demanda en el desarrollo de los sistemas de información (SI) y los componentes tecnológicos, para soportar las actividades de una empresa/organización/negocio.

Sin embargo, es una realidad que el riesgo de las organizaciones también se ha incrementado. La administración de los recursos, consolidación e integración de los recursos de TI se ha vuelto una tarea compleja, este se ha identificado como un proceso lleno de amenazas y cuellos de botella.

De manera errónea, el desarrollo de TI es visto por los expertos en el área como un conjunto de procesos de diseño individuales (antiguamente). Las aplicaciones son construidas para satisfacer metas a corto plazo o problemas inmediatos. No se establece claramente una estrategia de TI, un plan o curso, y tampoco se considera la visión global de los recursos con que cuenta la organización.

La TI se desarrolla de manera espontánea, en respuesta a las necesidades urgentes del negocio, lo que produce islas de TI a lo largo y ancho de todas las

áreas funcionales (baches), que no crecen coherentemente hacia una arquitectura integrada de sistemas, tecnología e información.
Juntado a todo esto, las tendencias de desarrollo de TI se han caracterizado por su esfuerzo en automatizar el "desorden". Muy poco esfuerzo es puesto en especificar las estrategias de negocios y construir un modelo de la organización, como precursores en la especificación de los requerimientos de TI. Estas disciplinas coexisten de manera separada en la práctica.

La PETI (Planeación Estratégica de Tecnología de Información) es ampliamente reconocida como una herramienta para ordenar los esfuerzos de incorporación de TI. Establece las políticas requeridas para controlar la adquisición, el uso y la administración de los recursos de TI. Integra la perspectiva de negocios/organizacional con el enfoque de TI, estableciendo un desarrollo informático que responde a las necesidades de la organización y contribuye al éxito de la empresa. Su desarrollo está relacionado con la creación de un plan de transformación, que va del estado actual en que se encuentra la organización, a su estado final esperado de automatización, esto, en concordancia con la estrategia de negocios y con el propósito de crear una ventaja competitiva.

La PETI consiste en un proceso de planeación dinámico, en el que las estrategias sufren una continua adaptación, innovación y cambio, que se refleja en los elementos funcionales que componen toda la organización.

6.6.1 Perspectiva General

Se presenta una metodología de PETI, correspondiente a la categoría de metodologías integrales, que consta de quince (15) módulos agrupados en cuatro (4) fases. Este paradigma está concebido, en concordancia con el modelo conceptual, a través de una visión estratégica de negocios/organizacional y una visión estratégica de TI. La metodología integra ambas visiones en una única final.

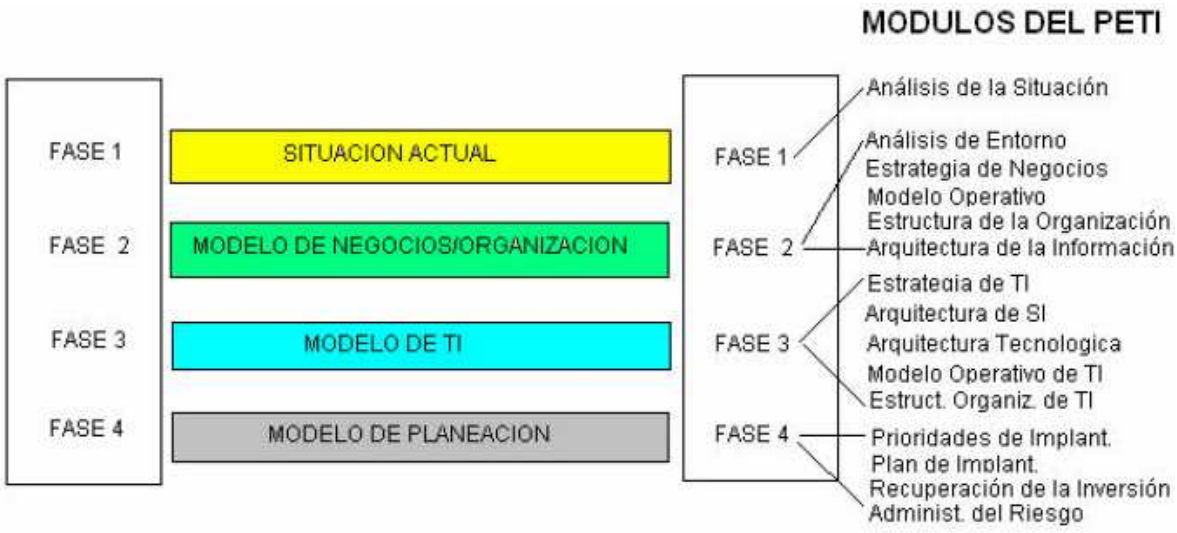


Fig. 20 Estructura PETI

Todo el proceso comienza con un análisis de la situación actual en la **fase I**, que produce el modelo funcional imperante en la empresa. En este paso se evalúa de manera general el entendimiento de la estrategia de negocios, la eficiencia de los procesos operativos y la aceptación de TI en la organización.

La fase II, relacionada con la creación de un modelo de la organización, inicia con un análisis del entorno y el establecimiento de la estrategia de negocios (el proceso de planeación se basa en una transformación de dichas estrategias). Continúa con el diseño en detalle de los modelos operativos, que van a producir en parte los requerimientos de TI necesarios para mejorar la eficiencia y la productividad de la empresa (esta aproximación es soportada por una reingeniería de procesos o una automatización incremental, que se concentran en identificar deficiencias operativas, con el propósito de rediseñarlas o modificarlas, y automatizarlas).

Posteriormente, se construye la estructura de la organización, que especifica puestos, perfiles, habilidades, etcétera, necesarios para administrar la empresa. La fase termina con la construcción de una arquitectura de información, que identifica las necesidades globales de información de la empresa. El modelo es descrito con la utilización de términos y conceptos de negocio / organización, independientemente del soporte computacional y jerga informática.

La fase III trata del desarrollo de un modelo de TI. En su primer módulo, tiene como objetivo la transformación de las estrategias de negocios en una estrategia de TI. Sigue con la construcción de la arquitectura de sistemas, que establece un marco para la especificación de las aplicaciones y la integración de la información. Luego se definen los elementos clave y las características esenciales de la arquitectura tecnológica (hardware y comunicaciones), que establece la plataforma en la que los sistemas van a funcionar. Continúa con el diseño en detalle de los modelos operativos de TI, que describen el funcionamiento del área informática.
Finaliza con la definición sobre la estructura de la organización de TI, necesaria para administrar los requerimientos informáticos.

La fase IV se concentra en la elaboración de un modelo de planeación. Primero se establecen las prioridades para la implantación de la TI y los procesos operativos. Luego se define un plan de implantación, que determina el orden de desarrollo de los proyectos de negocios / organización y de TI. Continúa con un estudio de la recuperación de la inversión, a través de un análisis costo / beneficio. Todo el proceso finaliza con un estudio de administración del riesgo, que se encarga de reconocer la existencia de amenazas que puedan poner en peligro el éxito del PETI.

6.6.1.1 Fase I PETI, Situación Actual

Todo el proceso comienza con un análisis de la situación actual en la fase I, que produce el modelo funcional imperante en la empresa. Involucra un examen y

estudio del estado actual de la empresa. Produce como resultado el modelo funcional en el que opera la organización. El propósito es entender apropiadamente la posición de la empresa, sus problemas y madurez tecnológica.

Esta fase cuenta con un solo módulo: análisis de la situación actual, que se divide en dos pasos. El primero trata sobre la identificación del alcance competitivo de la organización. Establece las características principales que influyen en la estrategia de negocios, y describe el comportamiento global de la empresa.

El segundo paso está relacionado con una evaluación de las condiciones actuales de la empresa. Dicha revisión debe incluir la evaluación de tres aspectos fundamentales: estrategias de negocios, modelo operativo y TI. Este esfuerzo se encarga de desarrollar el entendimiento de alto nivel de la situación actual de la empresa.

El paso relacionado con la estrategia de negocios, se enfoca a la revisión del conocimiento actual sobre la organización en planeación estratégica. No debe confundirse con el establecimiento de las estrategias. De hecho está relacionado con el entendimiento de alto nivel sobre la estrategia de la organización; la difusión a ejecutivos altos y medios, y la manera como éstos se involucra con el plan estratégico de la organización. El modelo operativo consiste en una revisión y el estudio de las condiciones en que se encuentran las áreas funcionales. Los procesos y las actividades deben ser identificados, evaluados y asociados con la información requerida por cada área. Los datos deben ser obtenidos con base en la observación, así como a través de entrevistas con ejecutivos y usuarios clave.

El propósito es determinar la situación del entorno en la organización, identificar problemas y establecer las necesidades de información dentro y fuera de la función informática. El análisis debe concentrarse en el entendimiento de la operación, sin necesidad de considerar la estructura de la organización.

El modelo operativo consiste en una revisión y el estudio de las condiciones en que se encuentran las áreas funcionales. Los procesos y las actividades deben ser identificados, evaluados y asociados con la información requerida por cada área. Los datos deben ser obtenidos con base en la observación, así como a través de entrevistas con ejecutivos y usuarios clave. El propósito es determinar la situación del entorno en la organización, identificar problemas y establecer las necesidades de información dentro y fuera de la función informática. El análisis debe concentrarse en el entendimiento de la operación, sin necesidad de considerar la estructura de la organización.

El paso de TI trata con la evaluación de:

1. Las capacidades del portafolio de aplicaciones de software e infraestructura técnica (hardware y comunicaciones), identificando debilidades y deficiencias tecnológicas.

2. La conformación de la estructura de la organización de TI (recursos humanos), que consiste en el examen de la capacidad de los recursos humanos y la conformación de la estructura de puestos del personal y
3. El análisis financiero, relacionado con la inversión histórica y actual en TI, y el retorno de la inversión esperada. Este punto busca inspeccionar los estándares de inversión de la empresa y compararlos ("benchmarketing") con los estándares de inversión del mercado, justificando la situación informática actual.

Es importante notar que esta reseña no debe ser demasiado detallada y es conveniente llevarla a cabo en un tiempo corto. El detalle del modelo deberá ser alcanzado en las fases subsecuentes.

6.6.1.2 Fase II PETI, Modelo de Negocios/Organización

En esta fase la metodología está relacionada con la creación de un modelo de negocios/organización, que representa la piedra fundamental del proceso de planeación de TI. Se concentra en el entendimiento del entorno y el establecimiento de la estrategia de negocios, que determina la construcción del modelo operativo, la estructura de la organización y la arquitectura de información.

El análisis del entorno identifica las condiciones del ambiente, que influyen sobre la empresa. El objetivo es evaluar fuerzas, debilidades, oportunidades y riesgos del sector. Las fuerzas y debilidades involucran la investigación del mercado doméstico, la carga financiera, productos, mercados, administración, estructura, cultura y recursos financieros de la empresa. En este análisis se debe buscar una comparación ("benchmarking") con el estado de las empresas relacionadas. El análisis de oportunidades y los riesgos, están relacionados con el estudio de consumidores, competidores y políticas del ambiente externo, como alianzas estratégicas, poder adquisitivo, costos de abastecimiento, etcétera. Estos aspectos pueden estar presentes ahora y/o pueden presentarse también en el futuro, influyendo sobre la estrategia de negocios, la operación administrativa y los sistemas de la organización.

La estrategia de negocios se divide en: estrategia organizacional, competencias fundamentales y estrategia competitiva. La estrategia de negocios es un proceso que tiene que ver con la identificación de la visión, misión, objetivos, metas, estrategias y factores críticos de éxito (FCEs). Su definición se establece a través de una interrelación, entre los elementos que unos con otros componen las estrategias, las entidades externas y el entorno de la organización. Las competencias fundamentales están relacionadas con las fortalezas de una organización. La estrategia competitiva establece que el éxito de una empresa radica en satisfacer las necesidades de un cliente, ofreciéndole un valor agregado. Involucra cualidades de servicio, precio, confianza, imagen, etcétera, que hacen que un producto sea identificado como único y diferente. En este paso la influencia de la TI es determinante. Puede dar un valor agregado a servicios, productos y competencia, cambiando la manera como los negocios son llevados a cabo.

Algunas de las estrategias competitivas más comunes se basan en el establecimiento de una diferenciación, bajos costos, enfoque específico e innovación.

El modelo operativo se enfoca en el análisis y la reestructuración del funcionamiento de la empresa. Es un paso fundamental como precursor en la identificación de requerimientos de TI. Su naturaleza de diseño varía, de reestructuraciones radicales o reingeniería de procesos, a escenarios con un crecimiento gradual llamado modelado incremental. Es una perspectiva menos drástica, que intenta mejorar lo que ya existe.

Nótese que un proceso es un conjunto parcialmente ordenado de pasos, que intentan alcanzar los objetivos dados, en concordancia con el planteamiento de la estrategia de negocios. El proceso de refinamiento es diferente de otros estudios, en los que se construye una estructura jerárquica compuesta sólo de objetivos y sub-objetivos.

6.6.1.3 Fase III PETI, Modelo de TI

La tercera fase está relacionada con la creación de un modelo de TI, que defina los lineamientos, controle las interfaces y establezca la integración de los componentes tecnológicos. El propósito es identificar soluciones de TI para establecer una ventaja estratégica y competitiva, así como el soporte operacional correspondiente.

La estrategia de TI está relacionada con los esfuerzos de diseño e implantación de TI, para soportar las estrategias de negocio de una empresa, en este caso de una entidad pública. Determina los lineamientos informáticos que deberán cumplir software, hardware y comunicaciones, para formar parte de la arquitectura informática, explícitamente, es un conjunto de lineamientos estratégicos, establecidos para relacionar el desarrollo del modelo de TI con la dirección estratégica del negocio y el comportamiento de la organización, permitiendo a la entidad alcanzar una ventaja estratégica y competitiva.

Tiene que ver con la identificación, formulación, entendimiento y refinamientos del propósito, política y dirección tecnológica de la organización. La importancia del proceso de definición de la estrategia de TI, está en transformar la estrategia de negocios en lineamientos de TI.

Por ejemplo, supongamos que las estrategias de una empresa pretenden desarrollar un alto grado de descentralización en la autoridad de sus ejecutivos en el mundo, debido a la dispersión geográfica de sus áreas funcionales. La estrategia de TI podría incorporar tecnología que soporte: diseño de bases de datos distribuidas, sistemas de información soportados por modelos de datos sofisticados, sistemas de información ejecutiva orientados a diferentes niveles de mando, entre otros.

Un aspecto importante de la correspondencia entre las estrategias, es que la TI es desarrollada como parte integral de la organización. El proceso de transformación requiere la interacción de ejecutivos de negocios con expertos en TI, esto permite a los ejecutivos revisar si los planteamientos estratégicos de TI son afines con la estrategia de negocios, y determinar su capacidad en la producción de los resultados esperados en corto o largo plazo.

La arquitectura de sistemas de información determina el portafolio de aplicaciones necesario para sostener las estrategias, operación y estructura de la organización es fundamental en el proceso de planeación, ya que: 1) Determina la visión global de los recursos de información, definiendo su alcance y asegurando su integración con los otros sistemas de información. 2) Establece el orden de desarrollo de los sistemas, en base a su precedencia natural. 3) Clarifica la relación que existe entre las aplicaciones y las necesidades de información de las áreas funcionales. Su construcción se basa en el establecimiento de las relaciones que existen entre las clases de, que integren la dinámica propuesta por las estrategias de negocios, pueden ser utilizadas para establecer la interrelación entre las aplicaciones.

La arquitectura de TI se compone de sistemas de información desarrollados para soportar las actividades funcionales tradicionales de operación, monitoreo/control, planeación y toma de decisiones. Estas aplicaciones se utilizan para reducir costos de operación, mejorar la calidad y la eficiencia del trabajo, y darle a la organización la oportunidad de competir. En general no tienen ninguna relación con proveedores, consumidores y con el mundo externo.

La planeación exige buscar y seleccionar, entre diversas alternativas, las aplicaciones que mejor se adapten a las necesidades de la empresa, es por eso que una vez establecida la arquitectura de sistemas, es necesario evaluar las características funcionales y los costos de las aplicaciones existentes en el mercado, esto se lleva a cabo considerando los lineamientos establecidos en la estrategia de TI que deben cumplir los proveedores.

También es importante establecer tiempos y costos de desarrollo, en caso de que no exista un proveedor que cumpla con las características requeridas; los costos sean elevados, o que la aplicación sea innovadora.

Una vez definida la arquitectura de sistemas, el siguiente paso involucra la especificación de los elementos clave y las características esenciales de la arquitectura tecnológica, que incluye la especificación de computadoras, impresoras, redes de computadoras, puertos, etcétera.

En este módulo se establecen los componentes tecnológicos; el lugar donde los sistemas y procesos van a correr; las características de almacenamiento de datos; la ubicación de los usuarios, y la manera como van a estar conectados. Esta tarea se lleva a cabo considerando como antecedente la arquitectura de SI y el modelado de la organización.

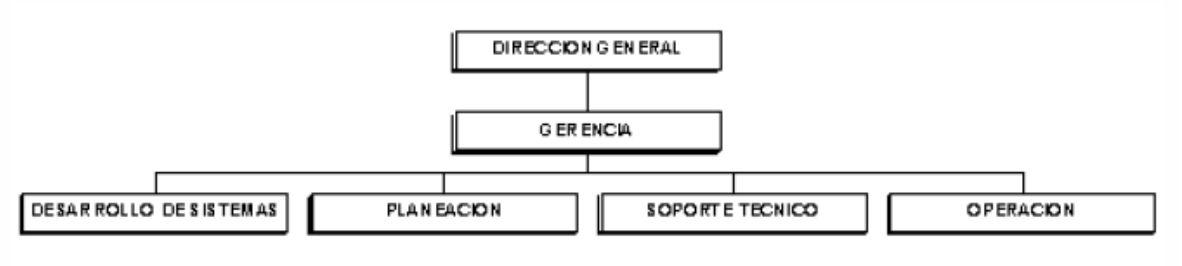
Ambos permiten establecer el detalle de las necesidades de hardware y redes de comunicaciones.

Al igual que en el módulo anterior, es necesario buscar y seleccionar la infraestructura tecnológica que mejor se adapte a las necesidades de la empresa y establecer sus costos.
Esto se lleva a cabo, considerando los lineamientos establecidos en la estrategia de TI que deben cumplir los proveedores.

La estructura de la organización informática determina los aspectos de la administración de los recursos humanos en TI (organización, perfiles, entrenamiento, etcétera) y la conformación de la estructura de puestos del personal informático. Su finalidad es sustentar la función de TI, en la medida que la organización incorpora hardware, software y comunicaciones, así como en la conformación de la estructura de la organización.

El personal de un área de informática es variado: involucra expertos en análisis, así como el diseño de sistemas y comunicaciones, entre otros. Las funciones que realizan comprenden el establecimiento de estándares, la comunicación con los usuarios, el diseño de bases de datos, el desarrollo de diccionarios de datos, el desarrollo del PETI, la capacitación y el desarrollo de documentación, entre otros.

Este podría ser un ejemplo de una estructura de organización informática en una entidad



6.6.1.4 Fase IV PETI, Modelo de Planeación

La cuarta y última fase se vincula con la creación de un modelo de planeación, relacionado con la identificación de proyectos que muestren cómo los recursos van a ser incorporados en la organización. Se concentra en el establecimiento de sus prioridades, la creación de un plan, un estudio del retorno de la inversión y un análisis del riesgo.

El establecimiento de las prioridades es un método que permite colocar, en el orden debido de implantación, los procesos automatizables del modelo operativo y los traducidos en sistemas de información, esto en términos del potencial de ganancia y la probabilidad de éxito.

El plan de implantación determina la secuencia de proyectos que contribuyen a la creación de la PETI, dando una estimación del tiempo de duración. Cada proyecto especifica los pasos intermedios y la sincronización de todas las actividades para alcanzar los objetivos. La secuencia de implantación está determinada por el orden establecido en el módulo anterior. Los sistemas de información prioritarios serán aquellos que brinden mayor beneficio a la empresa y que, por orden natural, deban ser implantados primero

Las técnicas de planeación son variadas, se pueden utilizar diagramas para establecer la secuencia y estimar los tiempos de duración de los proyectos, el calendario puede ser representado a través de una diagrama o grafica de barras horizontales, su tarea principal es formalizar las fechas de inicio y fin de un proyecto, así como establecer puntos de control para la supervisión del plan de implantación.

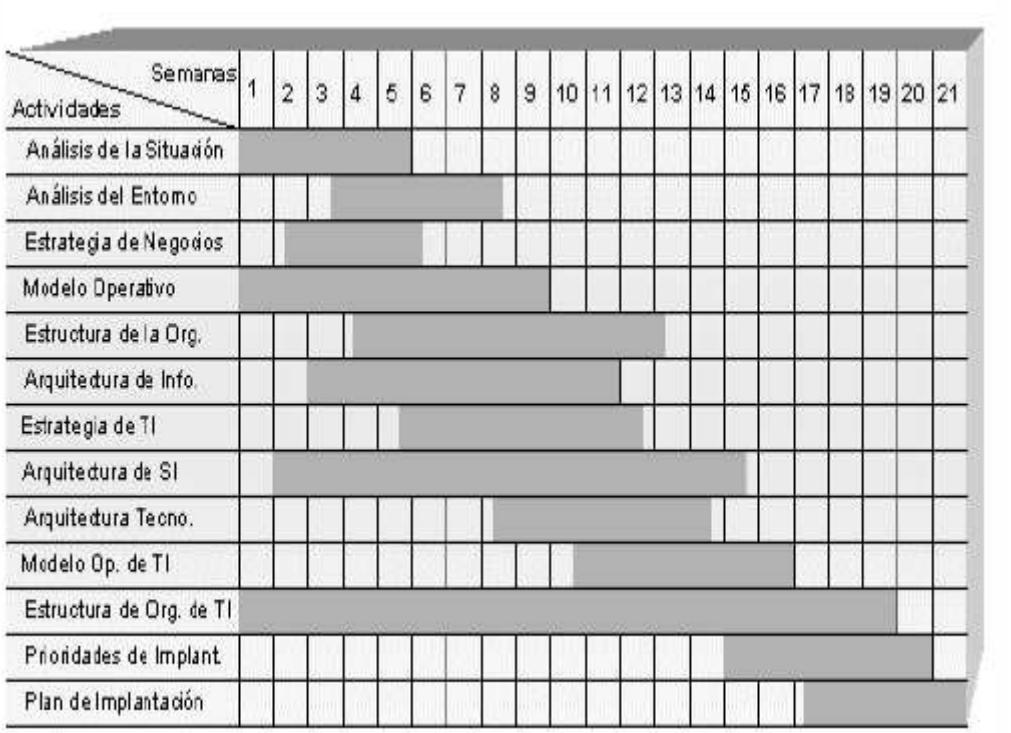


Fig. 21 Diagrama de barras horizontales

El retorno de la inversión es un estudio de viabilidad de la PETI, basado en un análisis costo/beneficio.

Un costo es un desembolso de recursos para la organización, asociado con la implementación de tecnología de información, un modelo operativo o la incorporación de recursos humanos. Generalmente es representado en términos

monetarios. Los costos de un proyecto de desarrollo de sistemas pueden estimarse con bastante precisión, teniendo una especificación de los tiempos y los recursos humanos necesarios. En particular, los costos de hardware y software son fáciles de obtener a través de entrevistas con los proveedores.

Un beneficio es una mejora o contribución para la organización. Obviamente está asociado con la implementación de tecnología de información, el modelo operativo o la incorporación de recursos humanos. Tradicionalmente son clasificados como tangibles o intangibles. En ambos casos, un valor monetario está asociado con ellos, desgraciadamente no siempre es fácil convertir los beneficios en dinero.

La administración del riesgo se encarga de reconocer la existencia de amenazas, determinando sus orígenes y consecuencias. Además trata de aplicar factores de modificación para contrarrestar situaciones adversas. Las estrategias para administrar el riesgo dependen, principalmente, de la naturaleza del riesgo y las variables asociadas que influyen en el rango de opciones de una empresa.

Los cuatro métodos principales para combatir el riesgo, son:

- ✓ **Reducción:** Apoyada en acciones para la eliminación o disminución del riesgo.
- ✓ **Protección:** Relacionada con elementos físicos para la eliminación o reducción del riesgo.
- ✓ **Transferencia:** Orientada a la delegación de responsabilidades a terceros.
- ✓ **Financiamiento**: Sustentado en la adopción de métodos para el control de inversiones

Por último, se debe tener en cuenta que el resultado de un plan estratégico no es simplemente producir un documento, sin embargo dicho documento debe existir, en si el resultado de un plan estratégico de TI, es desarrollar un entendimiento explícito y compartido de la misión y los objetivos del Área de Sistemas de la Organización, en cuanto a las actividades soportadas en TI y a las TI se refiere.

6.7 CONTROL INTERNO

El control interno es la adopción de una serie de medidas que se establecen en las empresas, con el propósito de contar con instrumentos tendientes a salvaguardar la integridad de los bienes institucionales y así ayudar a la administración y cumplimiento correcto de las actividades y operaciones de las empresas

Entre los beneficios del Control Interno se destacan:

- Proteger y salvaguardar los bienes de la empresa y a su personal.
- Prevenir y en su caso, descubrir la presencia de fraudes, robos y acciones dolosas.

- Obtener la información contable, financiera y administrativa de manera confiable y oportuna.
- Promover el desarrollo correcto de las funciones, operaciones y actividades de la empresa.

Y particularmente para la Guía de Gestión de Riesgos de TI para Entidades Públicas, el Control Interno tiene objetivos claramente definidos, como son:

- ✓ Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa.
- ✓ Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.
- ✓ Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.
- ✓ Implementar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.
- ✓ Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.

El Análisis de Riesgo, comprende la identificación de los componentes que hacen parte del escenario en que se esta evaluando y de los riesgos asociados a cada uno de estos componentes, para ello se debe tener en cuenta lo siguiente:

Componentes que hacen parte de la entidad:

- ✓ Datos
- ✓ Sistemas de aplicación
- ✓ Tecnología
- ✓ Instalaciones
- ✓ Recurso humano

Amenazas a las que están expuestos los componentes:

- ✓ Fraude y robo
- ✓ Acceso ilegal
- ✓ Perdida de información
- ✓ Errores y omisiones
- ✓ Sistemas no disponibles
- ✓ Desastres y sabotaje

Una vez se han definido los componentes y las amenazas, es necesario establecer la categorización del riesgo o factor del riesgo; para ello se utilizará la Técnica Delphi[10], la cual consiste en una "votación" comparando cada componente o amenaza frente a los otros.

6.7.1 Metodología para evaluar controles en ambientes de procesamiento de datos según la Técnica Delphi.

Se realiza con la participación de algunos expertos que tienen un profundo conocimiento del proceso que se está evaluando. La participación de estas personas en el equipo de trabajo asegura que el resultado final de la clasificación del riesgo pueda ser implementado rápidamente.

6.7.1.1. Descripción de la metodología

Definición de componentes y amenazas

Previo a toda evaluación de Auditoria de Sistemas, es necesario determinar cuáles son los escenarios de riesgo (puntos de atención) y cuáles son las amenazas a que están expuestos cada uno de ellos.

6.7.1.1.1.Componentes

Recurso Humano
Comprende a todas las personas vinculadas a la organización (ya sean internas o externas) con capacidad de acceder al sistema de procesamiento electrónico de datos.

Datos
Son los archivos de información que están contenidos en las unidades de disco, de cinta y otros dispositivos de almacenamiento.

Software
El software es el soporte lógico tanto aplicativo como ambiental para Mainframe y microcomputadores. También incluye documentación, logs y formas de papelería, entre otros.

Hardware
Es la plataforma computacional conformada por los equipos centrales y de comunicaciones, terminales financieras, administrativas y además por los microcomputadores, entre otros.

Instalaciones Físicas

Se refiere a los sitios o lugares donde se realiza el procesamiento electrónico de datos, así como aquellos en donde se almacena la información.

6.7.1.1.2.Amenazas

Fraude y Robo

Robo de datos u otros activos utilizando procedimientos manuales o automatizados, incluye fraudes o robos mediante la operación (manipulación) de los equipos de la organización.

Acceso Ilegal

Incluye el acceso no autorizado a datos confidenciales, bases de datos, redes, programas de computador, documentos importantes, entre otros.

Pérdida de Información

Abarca aspectos tales como pérdida, desvío o el no procesamiento de mensajes; Errores en recuperación de información, documentación incompleta; virus, entre otros.

Errores y omisiones

Se refiere a errores en la preparación, autorización, procesamiento y salidas de información; toma errada de decisiones; multas o sanciones.

Sistema no disponible

Incluye fallas en los equipos de procesamiento electrónico de información, caídas de línea, entre otros. Suspensión temporal o permanente de los servicios de PED.

Desastre y Sabotaje

Se refiere a desastres físicos incluyendo incendios, inundaciones, azocada, terremoto y sabotaje, entre otros.

6.7.1.1.3.DEFINICION DEL FACTOR DE RIESGO

Una vez se han definido los componentes y las amenazas, es necesario establecer la categorización del riesgo. Así, a través de la Técnica Delfhi[10], es necesario realizar una "votación" comparando cada componente o amenaza frente a los otros.

A continuación se muestran unos posibles resultados obtenidos:

CALIFICACION DE COMPONENTES

24,0	**Recursos Humanos**	**Recursos Humanos**			
17,0	**Datos**	6 0	**Datos**		
9,0	**Software**	6 0	5 1	**Software**	
6,0	**Hardware**	6 0	6 0	4 2	**Hardware**
4,0	**Instalac. Físicas**	6 0	6 0	4 2	4 2 **Instalac. Físicas**

Como se puede observar, el orden de importancia está registrado en la siguiente lista:

Recurso humano = 24

Datos = 17

Software = 9

Hardware = 6

Instalaciones físicas = 4

CALIFICACION DE AMENAZAS

18,0	Acceso Ilegal	Acceso Ilegal				
28,0	Fraude y Robo	0 6	Fraude y Robo			
15,0	Pérdida de Información	4 2	6 0	Pérdida de Información		
14,0	Errores y Omisiones	4 2	6 0	3 3	Errores y Omisiones	
12,0	Sistema no Disponible	4 2	4 2	4 2	4 2	Sistema no Disponible
3,0	Desastre y Sabotaje	6 0	6 0	6 0	5 1	4 Desastre y 2 Sabotaje

Una vez finalizada la evaluación de las amenazas, la siguiente es la lista de prioridades:

Fraude = 28

Acceso ilegal = 18

Pérdida de información = 15

Errores y omisiones = 14

Sistema no disponible = 12

Desastres y sabotaje = 3

Con las calificaciones de los componentes y las amenazas, se construye la siguiente matriz de ponderación del riesgo:

		AMENAZAS						
		FRAUDE Y ROBO (28)	ACCESO ILEGAL (18)	PERDIDA DE INFORM (15)	ERRORES Y OMISION (14)	SISTEMA NO DISP. (12)	DESASTRE Y SABOTAJE (3)	
COMPNTES	RECURSO HUMANO (24)	12.44%	8.00%	6.67%	6.22%	5.33%	1.33%	
	DATOS (17)	8.81%	5.67%	4.72%	4.41%	3.78%	0.94%	
	SOFTWARE (9)	4.67%	3.00%	2.50%	2.33%	2.00%	0.50%	
	HARDWARE (6)	3.11%	2.00%	1.67%	1.56%	1.33%	0.33%	
	INST. FISICAS(4)	2.07%	1.33%	1.11%	1.04%	0.89%	0.22%	
	TOTAL	31.11%	20.00%	16.67%	15.56%	13.33%	3.33%	100.00%

ALTO RIESGO	> 5.0%
MEDIANO RIESGO	entre 1.33% y 5.0%
BAJO RIESGO	< 1.33%

6.7.1.1.4 CUBRIMIENTO DEL CONTROL

Una vez definido el factor de riesgo, es imperioso medir el cubrimiento del control. Para llevar a cabo esta evaluación es necesario realizar las siguientes actividades.

6.7.1.1.4.1. EVIDENCIAR LOS CONTROLES EXISTENTES

Como producto de las labores de comprobación, verificación, investigación, indagación, análisis y observación se debe obtener una

lista de controles existentes; así mismo, el auditor debe incluir (si es procedente) unos controles adicionales que a su juicio deberían ser implantados.

6.7.1.1.4.2. CLASIFICAR Y CALIFICAR LOS CONTROLES

El auditor debe identificar a que "celda"[11] pertenece cada uno de los controles que recopiló. Adicionalmente debe calificar cada uno de los controles utilizando la siguiente tabla:

CRITERIO	PUNTAJE
El control no aplica	N
El control es redundante	R
El control es efectivo, es clave y no se cumple o no se conoce	1
El control es efectivo, no es clave y no se cumple o no se conoce	2
El control no es efectivo y se cumple	3
El control es efectivo, no es clave y se cumple	4
El control es efectivo, es clave y se cumple	5

Así las cosas, el porcentaje de cubrimiento del control para cada celda está dado por la siguiente fórmula:

$$\% \text{ DE CUBRIMIENTO} = \frac{\Sigma \text{ PC}}{((TE + TS - TN)*5)}$$

Donde, PC = Calificación de la efectividad de cada control (Existente o Sugerido)

TE = Total controles existentes

TS = Total controles sugeridos

TN = Total Controles que no aplican o son redundantes

6.7.1.1.4.3. DETERMINAR EL GRADO DE RIESGO

El grado de riesgo asociado a cada celda está determinado por la siguiente operación:

% DE RIESGO = (1 – C)

Dónde, C = % de cubrimiento del control.

De acuerdo con el porcentaje obtenido, el nivel de riesgo se puede clasificar de la siguiente manera:

%		SIGNIFICADO
0.00	9.99	Los controles son adecuados
10.00	39.99	Los controles son suficientes
40.00	59.99	El control es débil
60.00	79.99	El control es deficiente
80.00	100.00	El control no opera

6.7.1.1.4.4. DETERMINAR EL NIVEL PONDERADO DE RIESGO

El nivel ponderado de riesgo de cada una de las celdas está determinado por la siguiente fórmula.

NPR = Σ (RA * FR)

Dónde, NPR = Nivel ponderado de riesgo

RA = % de riesgo asociado a cada celda

FR = Factor de riesgo de acuerdo con la tabla de ponderación

7. GUIA PROPUESTA DE GESTION DE RIESGOS DE TECNOLOGIA INFORMATICA PARA ENTIDADES PÚBLICAS

El modelo propuesto de Guía de Gestión de Riesgos de Tecnología Informática para Entidades Públicas presenta cinco fases, las cuales se desarrollarán en este capitulo.

La primera fase presenta la definición del contexto organizacional de la entidad pública con el fin de establecer la conformación del área de tecnología informática y la funcionalidad de ésta en el desarrollo de las actividades cotidianas.

La segunda fase permite identificar los escenarios, recursos y tecnología informática con que cuenta la entidad.

La tercera fase identifica, a partir de la información de las fases anteriores, los riesgos asociados a cada uno de los componentes identificados y realiza un análisis o valoración de los mismos.

La cuarta fase aplica el modelo de evaluación de riesgos recomendado para la entidad pública.

La última fase realiza el monitoreo y revisión del resultado obtenido en la fase anterior, con miras al establecimiento de controles que permitan minimizar esos riesgos de manera que no afecten el contexto organizacional.

Durante el desarrollo de la guía de gestión de riesgos de TI, se deberá ir estructurando y documentando, de no existir en la entidad pública, la política organizacional de comunicación que permita gestionar los riesgos de Tecnología Informática como parte integral del proceso de planeamiento y administración de la cultura general de la organización.

El plan de comunicación deberá contener los lineamientos sobre:

- Establecer un equipo que comprenda personal de alta dirección para ser responsable por las comunicaciones internas acerca de la gestión de riesgos de TI al interior de la entidad pública;
- Procurar la toma de conciencia de los funcionarios públicos acerca de la administración de riesgos de TI;
- Comunicación / diálogo en toda la entidad acerca de administración de riesgos y la política de la organización sobre los riesgos del negocio;
- Asegurar niveles apropiados de reconocimiento, recompensas y sanciones;
- Establecer procesos de administración de desempeño.

(Ver diagrama de la guía)

7.1 Establecimiento del procedimiento para la definición del contexto organizacional y de administración del riesgo incluyendo el criterio de evaluación de los riesgos.

Fig. 22 Componentes para la definición del contexto organizacional

Para la aplicación de la guía de gestión de riesgos de tecnología informática en entidades públicas, se requiere tener definido el direccionamiento y la planeación estratégica de la organización, lo cual permitirá obtener la Planeación estratégica de TI que deberá alinearse con los objetivos de la organización.

7.1.1 Planeación Estratégica de Tecnología Informática - PETI

Para realizar la Planeación estratégica de la entidad se debe utilizar la estructura contenida en la forma F01 la cual esta orientada a:

- Identificar los componentes de tecnología informática de la entidad pública

- Establecer un plan estratégico para el área de informática que por su transversalidad en la organización involucra a todas las demás áreas de la compañía.

ESTRUCTURA PARA LA PLANEACION ESTRATEGICA DE TI - PETI

1. Establecer el Direccionamiento Estratégico de TI
    - 1.1 Valores
    - 1.2 Misión
    - 1.3 Visión

2. Diagnóstico Estratégico de TI

    2.1 Análisis y diagnóstico de la Estructura Organizacional
    - 2.1 Estructura
    - 2.2 Personal
    - 2.3 Funciones
    - 2.4 Contexto
    - 2.5 Procesos

    2.2 Análisis y Diagnostico de TI
    - 2.1 Descripción de Aplicaciones Existentes
    - 2.2 Descripción del Entorno Informático
    - 2.3 Diagnóstico del Desarrollo Informático

    2.3 Construcción de la Matriz DOFA
    - 2.3.1 Fortalezas
    - 2.3.2 Debilidades
    - 2.3.3 Oportunidades
    - 2.3.4 Amenazas
    - 2.3.5 Matriz ponderada

    2.4 Identificación de Necesidades y Descripción de los Sistemas de Información
    - 2.4.1 Necesidades de Informática
    - 2.4.2 Modelo Conceptual de Datos
        - 2.4.2.1 Entidades
        - 2.4.2.2 Agrupación de Entidades
        - 2.4.2.3 Modelo de Datos

    - 2.4.3 Especificaciones de los Sistemas de Información

    2.5 Definiciones Estratégicas
    - 2.5.1 Objetivos estratégicos de TI
    - 2.5.2 Estrategias de TI

    2.6 Definición y Descripción del escenario propuesto
    - 2.6.1 Estructuras Organizativa
        - 2.6.1.1 Funciones y Responsabilidades de Gestiones de la Informática
        - 2.6.1.2 Procedimientos de Gestiones de la Información

    - 2.6.2 Soporte Físico, Lógico y Comunicaciones
        - 2.6.2.1 Soporte Físico
        - 2.6.2.2 Soporte Lógico

2.6.2.3 Redes Y comunicaciones

2.6.3 Políticas, Métodos y Normas

2.7 Planes de Acción
2.7.1 Plan de Actividades
2.7.2 Plan de Recursos
2.7.3 Plan de Información

Forma F01

La aplicación de la anterior estructura permitirá establecer cual es la posición actual de la organización con respecto al uso de la tecnología informática para el desarrollo de sus estrategias de negocio.

De igual forma en esta primera etapa de la guía se aplicará el Gobierno de TI con el fin de establecer como se toman las decisiones en la organización con respecto al manejo de TI y como afecta esto el alcance de los objetivos de la organización.

7.1.2 Gobierno de TI - GTI

La aplicabilidad del Gobierno de TI permitirá determinar donde se están tomando las decisiones de inversión en TI al interior de la organización y para ello se aplicarán los siguientes pasos:

Primer paso:

Para evaluar la efectividad de un GTI se valora la efectividad en la obtención de cuatro importantes objetivos dando respuesta a las siguientes preguntas:

¿Que tan importantes son los siguientes resultados para su GTI, en una escala de 1 a 5?

¿Cuál es la influencia del GTI en su negocio en una escala de 1 a 5?

Objetivos:

- Uso Costo-Efectivo de la TI
- Uso efectivo de TI para el área financiera
- Uso efectivo de TI para el crecimiento
- Uso efectivo de TI para adquirir flexibilidad de negocios

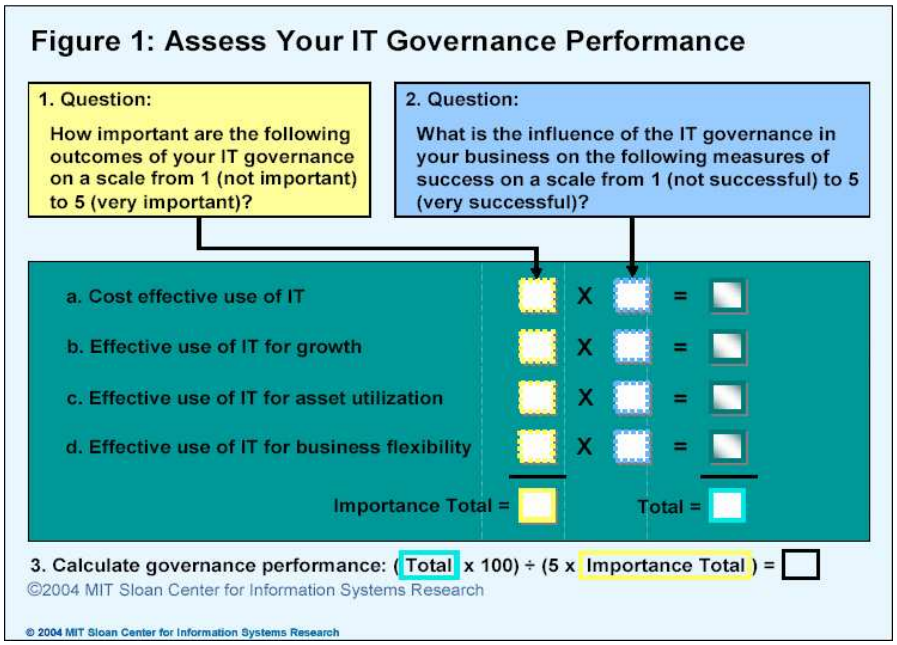


Fig. 23 Evaluando el Gobierno de TI

Se toma como modelo la Figura No. 23 y se utiliza para ello la forma F02 que permite totalizar la puntuación asignada y *determinar el nivel de desempeño* con respecto a los estándares que existen en el mundo, siendo la puntuación de mejor desempeño financiero aquellas que obtienen un puntaje superior a 74 puntos.

	¿Que tan importantes son los siguientes resultados para su GTI, en una escala de 1 a 5?	¿Cuál es la influencia del GTI en su negocio en una escala de 1 a 5	**TOTAL**
Uso Costo-Efectivo de la TI			
Uso efectivo de TI para el área financiera			
Uso efectivo de TI para el crecimiento			
Uso efectivo de TI para adquirir flexibilidad de negocios			
Total Importancia:		**Total:**	
Calculo Desempeno del GTI :		**(Total x 100)/(5xTotal importancia)=CGTI**	

Forma F02

Segundo paso

Determinar quién debe tomar y ser considerado responsable de cada área de decisiones. Para ayudar a la entidad a definir estos roles elaboramos la matriz de la Tabla No. 3.

DOMINIOS DE GTI	PREGUNTAS	RESPUESTAS
Principios de TI	¿Cómo los principios del negocio se trasfieren sobre los principios de TI para guiar la toma de decisiones en TI?	
	¿Cuál es el papel de TI en el negocio?	
	¿Cuál es el desempeño deseable en TI?	
	¿Cómo será fundada TI?	
Arquitectura de TI	¿Cuáles son los procesos principales de la empresa?¿Cómo están relacionados?	
	¿Cuál información dirige los procesos principales?¿Cómo debe ser integrada esta información?	
	¿Cuáles capacidades técnicas deben ser estandarizadas en toda la empresa para soportar la eficiencia en TI y facilitar la estandarización e integración?	
	¿Cuáles actividades deben ser estandarizadas en toda la empresa para facilitar la integración de datos?	
	¿Qué preferencias tecnológicas guiarán el acercamiento de la empresa a proyectos de TI?	
Infraestructura de TI	¿Cuáles servicios de infraestructura son mas críticos para que la empresa logre sus objetivos estratégicos?	
	¿Cuáles servicios de infraestructura deben ser implementados en toda la empresa y cuáles son los requerimientos para implementar ese servicio?	

	¿Cómo deberían ser valorados los servicios de infraestructura?	
	¿Cuáles son los planes para mantener actualizada la tecnología que se utiliza?	
	¿Cuáles servicios de infraestructura pueden ser contratados en Outsourcing?	
Aplicaciones de Necesidades de negocios	¿Cuáles son las oportunidades de mercado para nuevas aplicaciones de negocios?	
	¿Cómo están diseñados los experimentos estratégicos para medir el éxito?	
	¿Cómo pueden ser resueltas las necesidades de negocios con la arquitectura estándar? ¿Cuándo una necesidad de negocio justifica una excepción del estándar?	
	¿Quién responderá por los resultados y por implementar los cambios necesarios para asegurar la obtención de valor?	
Priorización e Inversiones en TI	¿Cuáles cambios o mejoras son mas importantes para la empresa?	
	¿Cuál es la distribución actual del portafolio de TI ? ¿Es este portafolio consistente con los objetivos estratégicos de la empresa?	
	¿Cuál es la importancia relativa de las inversiones de TI en la empresa? Las inversiones actuales en TI reflejan su importancia relativa?	
	¿Cuál es el correcto balance entre las prioridades para los proyectos de modo que se consiga un balance entre estandarización e innovación?	

Tabla No. 3 Matriz de toma de decisiones y definición de responsables de GTI

Tercer paso

Definir las entradas en la matriz de GTI en la cual se establece de donde surgen las necesidades de inversión de TI o donde nacen las propuestas de desarrollo de TI, teniendo en cuenta los arquetipos de gobierno y los dominios.

Dominio/ Arquetipo	Principos de TI	Arquitectura de TI	Estrategias de Infraestrc de TI	Necesidades de aplicativos para el negocio	Inversiones en TI
Monarquía de Negocios					
Monarquía de TI					
Federal					
Duopolio de TI					
Feudal					
Anarquía					
Desconocido					

Tabla No. 4 Matriz de entradas de GTI

Cuarto paso

Definir en las salidas en la matriz de GTI, es decir, donde se toman las decisiones con respecto a las entradas definidas en la tabla anterior.

Dominio/ Arquetipo	Principos de TI	Arquitectura de TI	Estrategias de Infraestrc de TI	Necesidades de aplicativos para el negocio	Inversiones en TI
Monarquía de Negocios					
Monarquía de TI					
Federal					
Duopolio de TI					
Feudal					
Anarquía					
Desconocido					

Tabla No. 5 Matriz de salida de GTI

Una vez se establece la toma de decisiones en la matriz de GTI se puede observar que tipo de gobierno se esta aplicando en la entidad y clasificarlo según la siguiente tabla:

Quinto paso

Según el esquema de la matriz de toma de decisiones se establece si el GTI que opera en la entidad es de enfoque centralizado o descentralizado. (Ver Anexo 2)

Más

Dominio/ Arquetipo	Principios de TI	Arquitectura de TI	Estrategias de Infraestructura	Necesidades de aplicaciones de negocios	Inversiones en TI
Monarquía de Negocios					
Monarquía de TI					
Federal					
Duopolio de TI					
Feudal					
Anarquía					
Desconocido					

Centralizado

Tabla No. 6 Matriz de GTI

Y se analiza según la siguiente tabla:

Menos

Elemento estratégico.	Beneficios	Utilización de Activos	Crecimiento
Mecanismos clave de GTI	- Manejo a través de toda la organización. - Arquitectura de procesos. - Presupuesto aprobado. - Hacer seguimiento del valor aportado al negocio por TI.	- Buenas relaciones entre los gerentes de Negocios y de TI. - Equipos de trabajo operativos incluyen un miembro de TI. - Liderazgo de TI en los organismos de toma de decisiones.	- Presupuesto aprobado y manejo de riesgos. - Responsabilidad local - Portal u otros recursos corporativos.
Infraestructura de TI	Capas de Servicios compartidos administrados centralizadamente	Servicios compartidos coordinados centralizadamente	Capacidad local personalizada con pocos servicios compartidos requeridos.
Gobierno	Más centralizado. Monarquías y Federal	Mixto Federal y Duopolios	Menos centralizado. Acuerdos Feudales, énfasis en manejo de riesgos.

Tabla No. 7 Enfoques de GTI

Una vez se tiene identificado y definido el contexto organizacional se procede a establecer el criterio de evaluación según los enfoques propuestos.

7.1.3 Criterio de evaluación[7]

La entidad pública debe establecer a partir de las teorías expuestas el criterio de evaluación del riesgo que utilizará en el proceso de evaluación del riesgo que contempla esta guía. (Ver Anexo 3)

Se recomienda a la entidad el uso del enfoque Proactivo, el cual funciona según la figura No. 7 del ítem 6.2.5.2.

7.2 Metodología para la identificación de los escenarios, recursos informáticos y tecnología informática que posee la entidad pública.

La entidad pública deberá aplicar el primer paso de la metodología Delphi[10] para la identificación de los escenarios (puntos de atención) en que se llevan a cabo procesos de tecnología informática;

Esta metodología maneja una clasificación general de escenarios y riesgos asociados a cada uno de estos escenarios, que sirve de modelo para que a partir de ella se definan cuales serán los escenarios que se evaluaran.

Para el registro de cada uno de los escenarios identificados deberá utilizarse la forma F03, la cual contiene la plantilla de recopilación de datos que permite a la entidad clasificar sus activos informáticos:

Plantilla de recopilación de datos

Identifique los activos que su grupo debe desarrollar, administrar, dar soporte o mantener.

Nombre del activo	Clasificación del activo (repercusión alta, media o baja en la empresa)
1.	

Complete la información siguiente por cada activo:

Nivel de defensa	Temores o riesgos que se intentan evitar: (Amenazas)	Cómo puede suceder: (Vulnerabilidades)	Nivel de exposición (A, M, B)	**Descripciones de los controles actuales**	Probabilidad (A, M, B)	**Preocupaciones de control, nuevos controles posibles**
Físico						
Aplicación						
Host						
Red						
Datos						

Forma F03

En la primera parte de la plantilla se debe registrar el nombre del activo teniendo en cuenta la categorización de componentes que ofrece la metodología de evaluación de C.I.

Luego se clasifica el activo de acuerdo a la repercusión que este tenga dentro de la entidad (Alta, Media o Baja).

Posteriormente, en la segunda parte, se debe completar toda la información asociada a ese activo, es decir, indicar a que tipo de amenaza esta expuesto ese componente para lo cual también se utilizara la categorización de amenazas que ofrece la metodología de evaluación de C.I.

En la columna siguiente se debe registrar la vulnerabilidad que posee el activo y su nivel de exposición, teniendo en cuenta los niveles existentes para ello según lo visto en la figura No. 4.

Seguidamente se deberá registrar en la siguiente columna los controles que operan actualmente con el fin de reducir el nivel de exposición y se procederá a registrar el nivel de probabilidad del riesgo, según lo visto en la figura No. 5.

Por último, se deberá registrar la funcionalidad de los controles o las sugerencias y recomendaciones para la implementación de nuevos controles.

Se deberá crear una forma por cada componente o recurso identificado, posteriormente se consolidara la información de todas las formas F03 en la forma F04 registrándose en forma resumida y conforme se solicita la información de la forma F03.

Información obtenida durante el proceso de recopilación de datos							
Activo				Exposición			
Fecha de identificación	Nombre/descripción de activo	Clase de activo	Niveles de defensa aplicables	Descripción de la amenaza	Descripción de la vulnerabilidad	Clasificación de exposición (A, M, B)	Clasificación de efecto (A, M, B)

Forma F04

7.3 Definición del procedimiento para la identificación y análisis de los riesgos asociados a cada uno de los escenarios en que se llevan a cabo procesos relacionados con recursos de TI en la entidad pública.

El procedimiento que se utilizará para la identificación y análisis de los riesgos asociados a cada uno de los escenarios es la Metodología Delphi[10] la cual hace parte de la Evaluación de Control Interno.

La metodología Delphi permite tratar por independiente cada uno de los aspectos a evaluar y se hace necesario que la entidad haya identificado en la fase anterior

de la guía los escenarios, componentes, recursos y tecnología informática sobre los que realizará el análisis de riesgos.

Esta fase de la guía se divide en tres fases a su vez, que son:

- Conformación del equipo interdisciplinario
- Calificación de componentes y amenazas
- Construcción de la matriz de Impacto

7.3.1 Conformación del equipo interdisciplinario

La entidad deberá conformar un grupo interdisciplinario de profesionales de cada una de las áreas críticas de la entidad donde la tecnología informática soporte procesos misionales con el fin de proceder a realizar una votación comparando cada entre si los escenarios.

Este grupo interdisciplinario debe propender porque en el proceso de votación prevalecerá el criterio de la organización para el cumplimiento de sus estrategias de negocio, es decir, se debe votar teniendo en cuenta que de acuerdo al resultado final se asignaran las prioridades de atención a cada escenario.

7.3.2 Calificación de componentes y amenazas

La calificación de componentes y amenazas consiste en comparar a través de una matriz inversa a los escenarios entre si con el fin de establecer la importancia que para la entidad representa ese escenario por mayoría de votos.

El número de votos se registra en cada casilla de acuerdo al escenario que se evalúa frente al otro escenario siguiendo el modelo que sigue:

CALIFICACION DE COMPONENTES

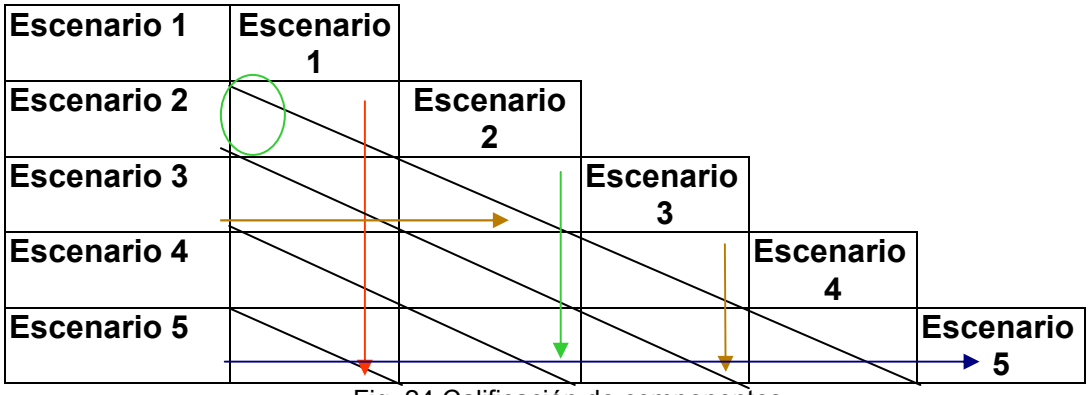


Fig. 24 Calificación de componentes

La dirección de las flechas indica el orden para sumar los valores obtenidos en la votación. Los totales que se obtengan de la votación por cada uno de los escenarios permitirán establecer el orden de importancia o prioridad de atención en riesgos de cada uno de los escenarios.

De igual forma se aplica el mismo procedimiento para las amenazas identificadas en la fase anterior de la guía.

CALIFICACION DE AMENAZAS ASOCIADAS A CADA UNO DE LOS COMPONENTES

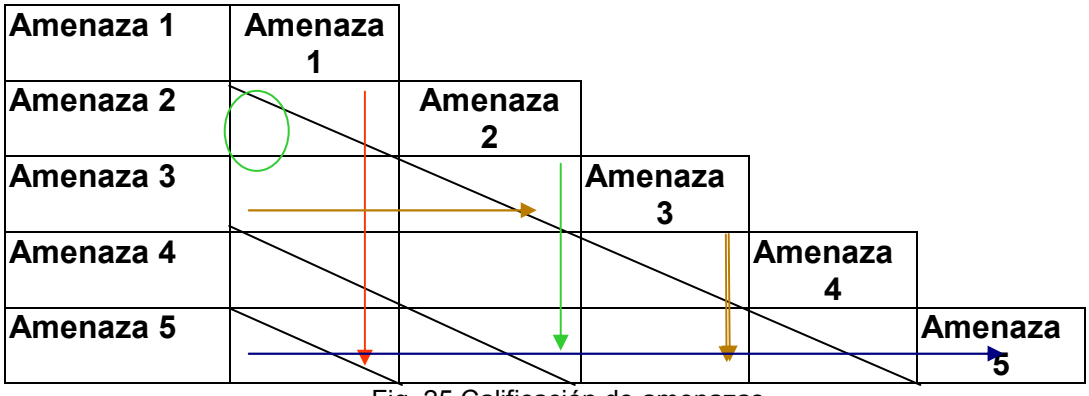


Fig. 25 Calificación de amenazas

Al igual que en la calificación de componentes, en esta votación también se obtienen totales los cuales mostrarán el orden de prioridad de las amenazas con respecto a los escenarios según el criterio del equipo que realiza la votación.

7.3.3 Construcción de la matriz de Impacto

Una vez se tiene establecido el orden prioritario de escenarios y amenazas de acuerdo a la votación obtenida, estos valores se llevan a una matriz de impacto a través de la cual se definirá el nivel de riesgo que tiene cada uno de los escenarios con respecto a las amenazas en un mismo plano. Para ello se debe utilizar el siguiente modelo: (Ver Anexo 4)

	Amenaza 1	Amenaza 2	Amenaza 3	Amenaza 4	Amenaza 5	Amenaza 6
Escenario 1	%					
Escenario 2						
Escenario 3						
Escenario 4						
Escenario 5						
TOTALES						

Fig. 26 Matriz de ponderación del riesgo

Aplicando la siguiente formula para hallar el porcentaje de cada celda.

$$PHV = \Sigma PH \times \Sigma PV \qquad PCA = PC \times PA \qquad \mathbf{\% = (PCA/PHV)x100}$$

Donde,

ΣPH: sumatoria de los pesos horizontales
ΣPV: sumatoria de los pesos verticales

PC: Peso del componente
PA: Peso de la amenaza

Cada celda de la matriz se llena con el valor porcentual resultante de aplicar la anterior formula y representa el grado de riesgo a que esta expuesto cada componente frente a ese riesgo.

Una vez se llenan todas las celdas, se establece el nivel de riesgo de acuerdo a rangos que se definen a partir de los valores mínimos y máximos obtenidos, es decir, se establecen 3 rangos de atención: Bajo, Medio y Alto.

Las celdas que clasifiquen en el rango más alto corresponden a los componentes que se encuentran expuestos a mayor riesgo y demandan una atención en un corto plazo.

7.3.4 Evaluación de controles existentes

Todas aquellas celdas que califiquen dentro del rango mas alto de riesgo se listaran en orden descendente y se procederá a listar los controles existentes para minimizar cada uno de los riesgos identificados.

La calificación de cada uno de estos controles se hará de acuerdo a los criterios que expone para ello la Metodología Delphi[10].

7.4 Diseño del modelo de evaluación con el fin de establecer las prioridades de la administración de riesgos.

7.4.1 Evaluación de riesgos del negocio

Los directivos de las áreas que conforman a la Entidad pública deberán establecer un marco de referencia para la evaluación de riesgos a partir de la identificación de aquellos riesgos que ponen en peligro el alcance de los objetivos del negocio.

Para la identificación de los riesgos globales que afectan a la entidad pública, se podrán apoyar en resultados de auditorias realizadas, incidentes presentados con anterioridad e inspecciones hechas por entidades de control donde se hayan hecho observaciones del tipo que afecten el logro de los objetivos del negocio.

7.4.2 Enfoque de evaluación de riesgos

El enfoque de evaluación de riesgos propuesto, tal como se planteo en el capitulo anterior, corresponde al enfoque proactivo: Identificación de riesgos, Análisis de riesgos, Planificación de acciones, seguimiento y control.

7.4.3 Identificación de riesgos

El Estándar Australiano AS/AZN4360:1999 presenta una plantilla para la identificación de los riesgos donde se consignan las fuentes de riesgo y las áreas de impacto dentro de la organización.

Fuentes de Riesgo	Areas de Impacto				
	*	*	*	*	*
Relaciones comerciales y legales					
Económicas					
Comportamiento humano					
Eventos naturales					
Circunstancias políticas					
Aspectos tecnológicos/técnicos					
Actividades y controles gerenciales					
Actividades individuales					

Tabla No. 8 Plantilla de identificación de fuentes de riesgo y áreas de impacto

En las columnas se colocaran las áreas de impacto según la siguiente lista, siempre y cuando apliquen a la entidad:

A	Base de activos y recursos de la organización, incluyendo al personal.
B	Ingresos y derechos
C	Costos de las actividades, tanto directos como indirectos.
D	Gente
E	Comunidad
F	Desempeño
G	Cronograma y programa de actividades
H	El ambiente
I	Intangibles tales como la reputación, gestos de buena voluntad, calidad de vida.
J	Comportamiento organizacional.

Forma F05

Las entradas de la tabla pueden realizarse con marcas para mostrar donde ocurren los riesgos, o con notas descriptivas más detalladas.

Se deben identificar los activos de negocios que estén en este ámbito para llevar a cabo los debates acerca de los riesgos. Esto incluye activos intangibles como la reputación de la empresa e información digital y activos tangibles como la infraestructura física.

También se deberán identificar o confirmar los o el responsable del activo. Se deberá documentar los responsables de activos específicos durante los debates de riesgos facilitados. Esta información puede resultar útil durante el proceso de asignación de prioridades para confirmar la información y comunicar los riesgos directamente a los responsables de activos.

Como ayuda para clasificar los activos, se pueden agrupar en escenarios de negocios. Seguidamente, se deberá documentar los activos específicos en cada escenario conforme se indica en la Forma F03.

Una vez identificados los activos, la segunda responsabilidad del equipo de la evaluación de riesgos, consiste en clasificar cada activo en lo que se refiere al efecto posible en la organización.

El anterior procedimiento corresponde a lo realizado en la Fase II de esta guía.

7.4.4 Asignación de prioridades

Primeramente se realizara el proceso de asignación de prioridades a riesgos en el nivel resumen y posteriormente se hará a nivel detallado. (Ver Anexo 5)

A nivel resumen:

Se toma la información de los activos y de exposición de activos obtenida en el paso anterior (Identificación de riesgos); la cual se resume en un solo dato para determinar las repercusiones.

Las repercusiones se obtienen a partir de la combinación de la clase de activos y el alcance de exposición de estos activos, y una vez obtenidas las repercusiones, se procede a categorizar según las tres referencias que existen: Alto, medio o bajo.

Los datos de este primer paso de la asignación de prioridades a nivel resumen se obtienen de la Fase II de la guía.

La Forma 04 de la Fase II de la guía, representa las columnas de la lista de nivel de resumen.

Se utiliza la columna de fecha de identificación por si se registran datos de revisiones anteriores.

Para finalizar el proceso de asignación de prioridades a riesgos de nivel resumen, se utilizaran los siguientes criterios para cada uno de los riesgos registrados en la forma 04. Lo que servirá como base para la priorización de nivel detallado:

- ✓ Riesgos de nivel alto
- ✓ Riesgos dudosos
- ✓ Riesgos controvertidos

A nivel detallado:

Se deberá tomar la lista de los activos del negocio, tal como se hizo en la Fase II de la guía y seleccionar la exposición del activo de acuerdo a lo expuesto en la figura No. 10.

La clasificación de exposición define el alcance de los daños en el activo; para determinar el alcance de los daños producidos por posibles ataques a la confidencialidad o integridad de activo se utilizará lo expuesto en la figura No. 11 para determinar el nivel de repercusiones debido a la ausencia de disponibilidad del activo.

Es importante en este momento identificar los controles actuales que de una u otra forma operan o se encuentran instalados en los escenarios donde se encuentran los activos relacionados en las formas.

Para la clasificación y evaluación de la efectividad de los controles se deberá utilizar el procedimiento expuesto en la Metodología de Evaluación de Control Interno, Delphi.

7.5 Diseño de la estructura con la cual se hará monitoreo y revisión al desempeño del sistema de administración y los cambios que podrían afectarlo.

Esta última fase de la guía, describe las actividades que se deben realizar para el seguimiento y mejoramiento de lo desarrollado en las fases anteriores, sometiéndolas a una continua revisión y aplicando los ajustes y correcciones necesarios a los métodos y técnicas utilizadas.

Para la realización del monitoreo y revisión de los riegos, se recomienda utilizar el modelo que Cobit presenta para el desarrollo de estas actividades, dentro de los cuales se empleara la técnica indicadores de calidad, diagramas de causa y efecto, formatos de evaluación y la metodología Delphi.

La evaluación regular de los procesos dentro de la organización permitirá la verificación de la calidad y efectividad de los controles utilizados para eliminar los riesgos asociados con el logro de los objetivos de la organización.

Para ello se deben realizar dos acciones como son:

- El Monitoreo de Procesos
- La Evaluación del Control Interno de la organización

7.5.1 Monitoreo de Procesos

El Monitoreo del Proceso asegura el logro de los objetivos establecidos para los procesos de TI, esto se hace posible a través de la definición por parte de la gerencia de reportes e indicadores de desempeño gerenciales, la implementación de sistemas de soporte así como la atención regular a los reportes emitidos, tomando en consideración:

- Indicadores claves de desempeño
- Evaluación de la satisfacción de los servicios prestados
- Reportes gerenciales

7.5.1.1 Indicadores claves de desempeño

Los indicadores proporcionaran información sobre los objetivos del negocio, a partir de los cuales los directivos podrán apoyarse para la toma de decisiones.

Es importante que los indicadores no controlen la actividad pasada solamente. Los indicadores deben reflejar los resultados muy puntuales de los objetivos, pero también deberán informar sobre el avance para alcanzar esos objetivos.

Para la definición de los indicadores se debe tener en cuenta lo siguiente:

- ✓ Elementos críticos
  - Componentes: ¿Qué cosas deben ocurrir como resultado para considerar que se ha tenido éxito en el logro del objetivo?
  - Factor: ¿Qué cosas vitales debe realizar la dependencia o entidad para lograr resultados?

  Por cada elemento crítico de éxito se debe crear un indicador que contenga: nombre, forma de medición y unidad de medida. Se deberá establecer una meta/objetivo alcanzable para ese indicador.

- ✓ Los niveles de alcance para indicadores en una entidad pública son:

- Impacto
- Cobertura
- Eficiencia
- Calidad
- Satisfacción

Ejemplo:

PERSPECTIVA:	INDICADOR:	OBJETIVO:
Cliente: Servicio de Alta Calidad.	$\%TAC = \frac{NTAC}{NTT} * 100\%$.	Número total de trabajos que afectaron al cliente, a partir de las solicitudes realizadas.

Fig. 27 Definición de indicadores

Para el caso especial de entidades del orden gubernamental, se recomienda trabajar con los siguientes indicadores que se encuentran alineados con el sistema de medida de planeación nacional para evaluar el desempeño de las entidades:

- ✓ ESTRATEGICOS
- ✓ PROYECTOS
- ✓ GESTION
- ✓ SERVICIO

Luego de ser definidos los indicadores claves de desempeño, se deben establecer las estrategias que nos permitirán alcanzar los objetivos propuestos o replantear los existentes. Para se puede utilizar el diagrama causa/efecto el cual es un vehículo para ordenar, de forma muy concentrada, todas las causas que supuestamente pueden contribuir a un determinado efecto y establecer las hipótesis estratégicas (a través de la secuencia sí /entonces).

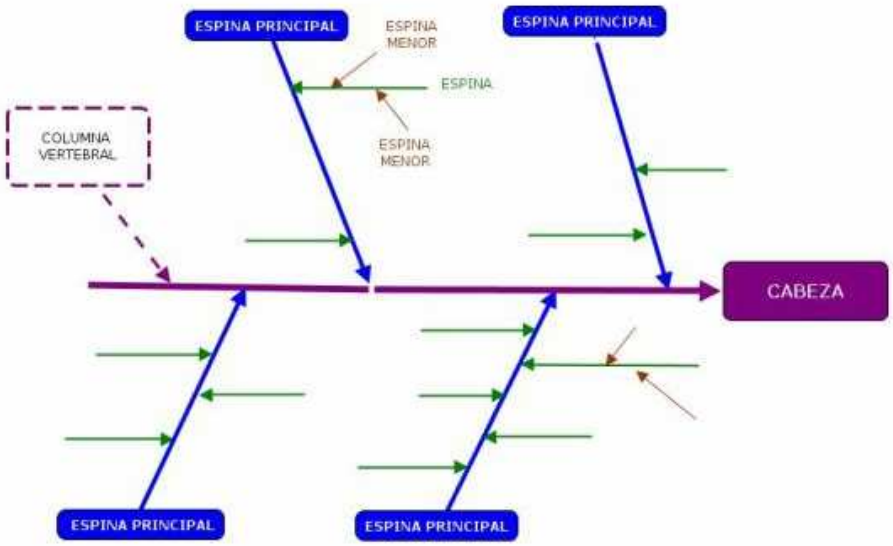


Fig. 28 Diagrama causa – efecto

Los pasos que se deben seguir para la construcción de este diagrama son:

1. Establezca claramente el problema (efecto) que va a ser analizado.

2. Diseñe una flecha horizontal apuntando a la derecha y escriba el problema al interior de un rectángulo localizado en la punta de la flecha.

3. Haga una "Lluvia de ideas" para identificar el mayor número posible de causas que pueda estar contribuyendo para generar el problema, preguntando "¿Por qué está sucediendo?".

4. Agrupe las causas en categorías.

5. Para comprender mejor el problema, busque las subcausas o haga otros diagramas de causa y efecto para cada una de las causas encontradas.

6. Escriba cada categoría dentro de los rectángulos paralelos a la flecha principal. Los rectángulos quedarán entonces, unidos por líneas inclinadas que convergen hacia la flecha principal.

7. Se pueden añadir las causas y subcausas de cada categoría a lo largo de su línea inclinada, si es necesario.

7.5.1.2 Evaluación de la satisfacción de los servicios prestados

La evaluación de la satisfacción de los servicios prestados se realiza con el objetivo de evaluar el nivel de satisfacción del cliente de forma que faciliten la planificación de estrategias de la compañía y su enfoque hacia el cliente. Un ejemplo del formato de evaluación es el siguiente:

Lista de los Servicios prestados en la Entidad Pública	**Valoración**				
	1	**2**	**3**	**4**	**5**

Forma F06

7.5.1.3 Informes gerenciales

Deberán proporcionarse reportes gerenciales/informes de gestión para ser revisados por los directivos en cuanto al avance de la entidad hacia las metas identificadas. Con base en la revisión, los directivos deberán iniciar y controlar las acciones pertinentes.

7.5.2 Evaluar lo adecuado del Control Interno

Mediante esta evaluación se hace posible asegurar el logro de los objetivos de control interno establecidos para los procesos de TI a través del compromiso de la dirección de sistemas de monitorear los controles internos, evaluar su efectividad y emitir reportes sobre ellos en forma regular, tomando en consideración aspectos como:

- Monitoreo permanente de control interno
- Comparación con mejores prácticas
- Reportes de errores y excepciones
- Auto evaluaciones
- Reportes gerenciales

Para la aplicación de fase de la etapa de Monitoreo la entidad pública se apoyará en las labores de Auditoria de sistemas que deberá realizar la Oficina o área de Control Interno de la entidad y de no existir esta área, entonces se apoyará en las evaluaciones de control interno que realizan las entidades del orden nacional que tienen como función regular las operaciones y funciones de los entes distritales y departamentales. (Ver Anexo 6)

8. CASO PRÁCTICO APLICADO A LA ENTIDAD PÚBLICA GOBERNACIÓN DE BOLÍVAR12

Estructura de la Planeación Estratégica de Tecnología Informática

8.1 Establecer el Direccionamiento Estratégico de TI

8.1.1 Valores

VALORES	DESCRIPCIÓN
Honestidad	Principios rectores en el actuar diario que deben ponerse en practica por todos los miembros de la organización
Servicio	Satisfacción a las necesidades de los usuarios, en cuanto a las herramientas tecnológicas.
Calidad	Satisfacer totalmente las necesidades eficientemente.
Creatividad	Desarrollo de estrategias para el mejoramiento del servicio y atención a las necesidades de la organización.
Responsabilidad	Manejo eficiente de los productos y servicios que ofrecemos.

8.1.2 Misión

En concordancia con la visión, el gobierno departamental asume el compromiso de ser los promotores del desarrollo departamental de una forma equilibrada involucrando a la totalidad de los actores (publico, privado, solidario, comunitario), conociendo sus intereses, sus motivaciones y compromisos, para que funcionando en un sistema institucional, logremos ubicar al Departamento de Bolívar en el lugar que históricamente le correspondió en el ámbito nacional

8.1.3 Visión

La visión del Gobierno Departamental sobre Bolívar es: En el año 2007, Bolívar es un territorio que avanza en la transformación hacia un modelo de desarrollo humano, productivo, competitivo y sostenible, en el cual sus habitantes actúan honestamente, garantizando un constante desarrollo y la sostenibilidad de los procesos iniciados.

8.2 Diagnóstico Estratégico de TI

8.2.1 Análisis y diagnóstico de la Estructura Organizacional

8.2.1.1 Estructura

En la actualidad la Gobernación de Bolívar se encuentra conformada por 16 dependencias; dichas dependencias cada una tiene una persona encargada de su dirección así como también las tareas que le corresponden a cada una en el ámbito laboral en el que se desenvuelve la entidad.

Haciendo revisión detallada de esta organización y de las áreas que la conforman por niveles jerárquicos nos encontramos con que *no existe en la entidad un departamento o área de sistemas encargado de las tareas y/o actividades correspondientes que este tipo de departamento demanda*, siendo este tipo de actividades delegadas a otro tipo de departamentos, específicamente los departamentos de Proyectos Especiales y la Secretaría de Logística y Recursos Físicos, las cuales dentro de sus funciones tienen a cargo actividades como, el manejo del programa de modernización tecnológica, bases de datos y sistemas de información, compra de equipos y mantenimiento físico, cuyo desarrollo es de vital importancia pero no suficiente para el correcto funcionamiento de los sistemas de la Gobernación de Bolívar.

Al ser encomendadas o delegadas actividades correspondientes al departamento de sistemas a dos (2) áreas ajenas a este y completamente diferentes, se corre el riesgo de *falta de sinergia en el desarrollo de las actividades, ocasionada por la falta de información eficaz y eficiente entre las dos (2) áreas*, en lo que se refiere a las actividades desarrolladas en lo que a la parte de sistemas se refiere.

Actividades de carácter organizativo del área de sistemas son encomendadas a la Secretaría de Logística y Recursos Físicos, dentro de este tipo de actividades se encuentra la contratación de pólizas de seguros para los equipos así como también aquellas que tienen que ver con la parte legal de adquisición de equipos de computo, software licenciado, entre otras.

8.2.1.2 Personal

El personal encargado de las TI en la Gobernación de Bolívar, hace parte de las dos (2) áreas mencionadas anteriormente (Secretaría de Logística y Recursos Físicos y La Unidad de Proyectos Especiales), dicho personal se encuentra vinculado a la entidad de maneras diferentes por parte de cada una de las áreas en mención, ya que el

personal encargado de los mantenimientos correctivos y preventivos a los equipos y recursos de TI bajo el mando de la Secretaría de Logística y Recursos Físicos se encuentran vinculados a la entidad a través de ordenes de prestación se servicios, mientras que las tareas correspondientes a la Unidad de Proyectos Especiales, las cuales tienen que ver con la modernización tecnológica, entre otras, son contratadas a terceros por la Gobernación de Bolívar a través de esta área.

En lo que concierne a la capacitación del personal encargado de llevar a cabo las actividades correspondientes a las TI, se puede decir que actualmente el personal con que se cuenta es el idóneo para las actividades de TI que se llevan a cabo en la Gobernación de Bolívar, sin ser este suficiente pensando en innovaciones futuras y en el avance tecnológico progresivo de las TI.

8.2.1.3 Funciones

Las funciones generales en lo que concierne a las TI, de las áreas encargadas se resumen a las funciones de la Secretaría de Logística y Recursos Físicos debido a que no existe en la entidad documento alguno en el que se haga constar las funciones de las Unidad de Proyectos Especiales con respecto a las TI, sin obviar que dichas funciones si se llevan a cabo en la practica diaria de la entidad, las funciones por área son:

Unidad de Proyectos Especiales:

- Manejo del programa de modernización tecnológica
- Gestión de Bases de datos y sistemas de información
- Compra de equipos bajo comprobación de la necesidad.

Secretaria de Logística y Recursos Físicos:

- Suministrar los bienes y servicios que requieren las dependencias de la Administración Central del Departamento para el desarrollo de sus funciones y velar por su uso racional.
- Proveer a las diferentes dependencias de los programas y aplicaciones tendientes a la sistematización y automatización de sus procesos y procedimientos con el fin de que sean eficientes y eficaces en el cumplimiento de sus funciones.
- Coordinar y asesorar a las dependencias de la Administración Central del Departamento en su diseño y adecuación organizacional, que le permitan el cumplimiento y el desarrollo de los procesos, procedimientos y funciones.

8.2.1.4 Contexto

La Gobernacion de Bolivar considera que las areas encargadas de las actividades correspondientes a las TI y que hacen las veces de departamento de sistemas brindan seguridad, apoyo y soporte a todos los funcionarios de las diferentes áreas de la organización, en la solución de los problemas generados en el manejo cotidiano de herramientas informáticas.

Frente a los centros de información de otras entidades publicas, nos encontramos en desventaja, por la falta de apoyo por parte de los directivos en el desarrollo e implementación de nuevas tecnologías para el mejoramiento de los procesos.
La poca utilización por parte de la administración de las herramientas informáticas existentes como apoyo a la toma de decisiones en pro al mejoramiento administrativo.

8.2.2 Análisis y Diagnostico de TI

8.2.2.1 Descripción de Aplicaciones Existentes

1. *Atlas Pro*
Área Responsable: ***Unidad de Presupuesto***
Área Usuaria: ***Unidad de Presupuesto***

Descripción:
Software utilizado para las funciones de presupuesto, contabilidad, tesorería y apoyo logístico, funciona en sistemas Windows, y desarrollado en lenguaje FoxPro, adquirido con licencias de funcionamiento.

Diagnóstico: Actualización
De acuerdo con la dinámica institucional se valorará la inclusión de nuevas funcionalidades.

2. *SaigtWeb*
Área Responsable: ***InfoPublicas***
Área Usuaria: ***Unidad de Rentas***

Descripción:
Es un aplicativo para la sistematización del recaudo del impuesto a los vehículos, impuesto al consumo y otras rentas departamentales,

diseñado en ambiente Web enable, bajo sistema operativo LINUX y un motor de base de datos en ORACLE, dicho software se adquirió junto con sus manuales de funcionamiento y su respectiva licencia por medio de la firma InfoPublicas a Global Corporation S.A. firma desarrolladora y productora del aplicativo.

Diagnóstico: Mantenimiento
Sistema Estable. Ampliación y actualización del Sistema que responda a los requerimientos de las actividades llevadas a cabo, así como de los usuarios.

8.2.2.2 Descripción del Entorno Informático

Existen en la Gobernación de Bolívar 101 equipos de escritorio con sus respectivos periféricos y 2 equipos portátiles, todos propiedad de la entidad, adquiridos ya sea por recursos propios o por donaciones de otras entidades.
También se encuentran funcionando en la Gobernación de Bolívar equipos de otras entidades, como es el caso de la firma InfoPublicas.

La gran mayoría de los equipos en la entidad son equipos cuyo tiempo de funcionamiento a superado su vida útil, y solo una pequeña parte de los equipos se encuentra en buen estado y en perfecto funcionamiento. Solo por reseñar uno de los casos, aún en la Gobernación de Bolívar se encuentran funcionando equipos con procesadores de la familia x86, los cuales hicieron su aparición en el mercado a mediados de los 80's y que, teniendo en cuenta el avance de la tecnología informática, este tipo de procesadores se vuelve obsoleto al momento de querer trabajar con aplicaciones actuales o aplicaciones que requieren de un nivel mayor de procesamiento, como es el caso de la mayoría de las dependencias de la Gobernación de Bolívar, las cuales trabajan con grandes volúmenes de información haciendo de esta forma que el trabajar con este tipo de equipos se convierta en una tarea tediosa y poco productiva para la organización.

No solo la capacidad de procesamiento aqueja a los equipos de computo de la Gobernación de Bolívar, también la falta de capacidad de estos de almacenar la cantidad de información necesaria para poder llevar a cabo el trabajo en una forma normal. Es aquí donde encontramos equipos con capacidades de almacenamiento casi nulas con respecto a la información que se maneja en la entidad, equipos con capacidades de almacenamiento extremadamente menores a las que se necesitan en la actualidad y por ende obsoletas.

Siendo los equipos de cómputo una herramienta necesaria en el desarrollo de las actividades llevadas a cabo diariamente por los empleados de la Gobernación de Bolívar, es de vital importancia que estos se encuentren en el mejor estado posible y que presten además el servicio que de ellos se necesita.

Red de Datos y Comunicaciones

En lo que concierne a las red de datos y comunicaciones el hecho mas notable en lo que a la red de datos y comunicaciones de la Gobernación de Bolívar se refiere, es que a pesar de la necesidad que se tiene en la entidad de la red, no se cuenta en la entidad con una persona encargada de la administración de la misma y mucho menos con personas encargadas de tener a la red en continua operación.

En la actualidad la Gobernación de Bolívar cuenta con una infraestructura de red bastante pobre en cuanto a la parte estructural del cableado trazado para esta.

En el trazado actual del cableado encontramos partes en el que el cable no se encuentra protegido del medio hecho que lo hace vulnerable a riesgos causados por factores ambientales, como humedad, temperatura, entre otros, en algunos tramos muy a pesar de la protección del cable se comete el error de haber trazado el cable de red junto con el cable de corriente eléctrica lo que afecta la transmisión normal de los datos, debido al campo eléctrico producido por los cables que transportan electricidad.

La red de la Gobernación de Bolívar cuenta actualmente con 140 puntos de red, distribuidos así, 53 en el primer piso de los cuales solo 29 se encuentran operando normalmente, 39 en el segundo piso de los cuales solo 19 se encuentran en funcionamiento, y 48 en el tercer piso de los cuales solo 22 operan normalmente, es decir, de los 140 puntos de red ubicados en el edificio de la Gobernación de Bolívar solo 70 de estos se encuentran en funcionamiento, siendo la falta de mantenimiento y el mal estado del cableado la causa principal de la in-operabilidad de los puntos.
De igual forma se pudo constatar la falta de utilización de estándares para el trazado del cableado de red en la Gobernación de Bolívar

En cuanto a tecnología utilizada para la interconexión de los puntos de red se han utilizado en la Gobernación dos (2) tipos de tecnologías como lo son tecnología wire o cableada y en algunos tramos tecnología inalámbrica o wireless, haciendo de esta forma mas difícil establecer pautas o normas para mantener la seguridad de dicha red, debido a que los niveles de seguridad en estos dos (2) tipos de tecnología se maneja de manera diferente, en esta parte

también hay que hacer referencia a que en los planos entregados al equipo auditor no se especifica el tipo de tecnología de red que se esta utilizando en ciertas dependencias de la entidad, es decir que en los planos(no se entregaron planos sino copias de gráficos preeliminares) no se muestra con claridad en que tramos de la red se usa cual tecnología, ya se cableada o inalámbrica.

En lo que concierne a equipos de red es notable que no existe en la entidad un lugar acondicionado para tal fin, y estos equipo se encuentran ubicados indistintamente en diferentes áreas de la entidad(CIG, 1º piso; Nomina, 2º piso; Secretaría del Talento Humano, 3º piso) y a cargo de personas que no están capacitadas para operarlos en caso de presentarse alguna eventualidad, hay casos en los que los equipos de red están ubicados en el mismo lugar donde funciona un equipo de escritorio lo que incrementa el riesgo de una falla en la conectividad de los equipos interconectados a través del dispositivo de red, llámese switch o concentrador, además que la persona encargada del equipo como en el caso anterior no esta capacitada para operarlo.

En los lugares en los que se encuentran ubicados los equipos de red no se han tomado en cuenta medidas preventivas de seguridad y accidentes, como por ejemplo planes contra incendios.
En la secretaria de agua potable se presenta un caso especial, en cuanto a la red, debido a que los usuarios de los equipos adquirieron un switch de 24 puertos por recomendación de otro funcionario de la Gobernación y mediante este interconectan a la red los equipos que usan, aumentando así el trafico de paquetes de datos a través de un solo punto de red al cual esta conectado el dispositivo de red en mención, hecho que deriva en una falta de eficiencia en la transmisión de los datos en el trafico normal de la red, desde esta parte de la misma.

Existe actualmente una conexión a Internet de la cual no se beneficia toda la organización, ya sea por la falta de un ancho de banda mayor o por la no necesidad del servicio en algunos puntos de la red, en lo que concierne al ancho de banda contratado por la Gobernación de Bolívar se pudo constatar que este es suficiente para los puntos de red que se encuentran actualmente con el servicio pero que si en algún momento se necesitara la inclusión de otros puntos al servicio de Internet este seria insuficiente, hecho que hace notar que el ancho de banda contratado no es suficiente para suplir la necesidad de Internet en todo el edificio dado el caso de una eventualidad de conexiones necesarias.

Haciendo referencia a otro tipo de conexión además de la Internet se supo, que existe una conexión a través de una VPN con la Caja

Agraria, dicha conexión cuenta con las medidas de seguridad necesarias para evitar accesos no deseados.

Existen actualmente en la Gobernación de Bolívar dos (2) dominios de red, uno de estos dominios es manejado por la firma InfoPublicas y el otro por la Gobernación de Bolívar, la existencia de dos dominios si bien de cierta forma simplifica la administración de la red, el punto en contra es la manera de establecer comunicación entre equipos que se encuentran ubicados en dominios diferentes, que si bien es posible, se requiere de recursos adicionales de red tales como el enrutamiento dentro de la misma. (Ver Anexo 7)

8.2.3.3 Diagnóstico del Desarrollo Informático

Actualmente existen programas informáticos para ciertos procesos. El área operativa cuenta con dos 2 programas, uno de ellos adquirido con licencia de fucnionamiento para el manejo de presupuesto y cartera y el otro funciona bajo la licencia de una firma que presta el servicio de outsourcing para el manejo de la funcion de rentas entre otros procesos.

A pesar de que es política nacional la modernización de las entidades públicas por medio de la utilización de tecnologías de información, la resistencia o falta de interes por parte de la administración para apoyar esta directriz, es la causa del estancamiento tecnológico en que se encuentra actualmente la entidad.

La Gobernacion de Bolivar requiere la construccion de un sistema de información integrado, que contribuya a la modernización de la entidad, bajo la perspectiva de una optimización permanente de los procesos que apoyan las condiciones de acceso de toda la población a los servicios que esta entidad presta.

Actualmente en la Gobernación de Bolívar no se llevan a cabo procesos de desarrollo de software, solo se hace mantenimiento y actualizaciones a las bases de datos con las que se trabaja.

8.2.3 Construcción de la Matriz DOFA

FACTORES CRITICOS DE ÉXITO	
No.	**FACTOR CRITICO DE ÉXITO**
1	Manejo de información, por parte de los usuarios encargados de la alimentación del sistema.
2	Gerencia de la información por parte de los administradores de bases de datos.
3	Recursos humanos calificados
4	Bienes y suministros

FACTORES CRITICOS DE ÉXITO
FACTOR CRITICO DE EXITO : Manejo de información
ASPECTOS IMPORTANTES
Entregar oportunamente
Tener consistencia
Velar por la integridad
Mantener actualizada
Brindar confiabilidad
Satisfacer requerimientos

ANALISIS INTERNO	
FACTOR CRITICO DE EXITO : Manejo de Información	
FORTALEZAS	**DEBILIDADES**
Existe la información en archivos organizados	A pesar de la existencia de una red de datos esta es insuficiente y obsoleta.
Hay compromiso directivo para sistematizar la información	No hay Central de Información
Existe recurso humano capacitado	Inexistencia de aplicaciones integradoras de información
Existen Equipos de Computo	De vida útil agotada y no actualizados

ANALISIS EXTERNO	
FACTOR CRITICO DE EXITO : Manejo de la Información	
OPORTUNIDADES	**AMENAZAS**
Cambios en la legislación	Falta de continuidad en la dirección e Inestabilidad Laboral
Presupuesto	Reglamentación de las leyes
Modernización del estado	Falta de Compromiso Personal de los Funcionarios
Tecnología	

Proyectos para municipios	

	FORTALEZAS (F) • Existe la información en archivos organizados • La dirección es consciente de la necesidad de sistematizar la información. • Existe recurso humano capacitado • Existen Equipos de Computo	**DEBILIDADES (D)** • A pesar de la existencia de una red de datos esta es insuficiente y obsoleta. • No hay Central de Información. • Inexistencia. de aplicaciones integradoras de información. • De vida útil agotada y no actualizados
OPORTUNIDADES (O) • Presupuesto • Modernización del estado • Tecnología	**ESTRATEGIAS FO** • Gerenciar proyectos de implementación del Sistema de información de la Gobernación. • Desarrollar y actualizar periódicamente estándares para la normalización de la información en los términos de definición, codificación, estructura y valor	**ESTRATEGIAS DO** • Implementación de una red de datos funcional y acorde a las necesidades. • Realizar el montaje de la Central de información. • Desarrollo de aplicación para integrar la información.
AMENAZAS (A) • Inestabilidad Laboral • Falta de continuidad en la dirección • Falta de Compromiso	**ESTRATEGIAS FA** • Talleres de capacitación, concientización, sensibilización y motivación personal • Crear comité asesor de informática con funciones de planeación del desarrollo de sistemas de información.	**ESTRATEGIAS DA** • Brindar a los funcionarios todas las herramientas tecnológicas necesarias para la ejecución de las actividades asignadas. • Elaborar Manuales de procedimientos prácticos para los usuarios

8.3 Identificación de Necesidades y Descripción de los Sistemas de Información

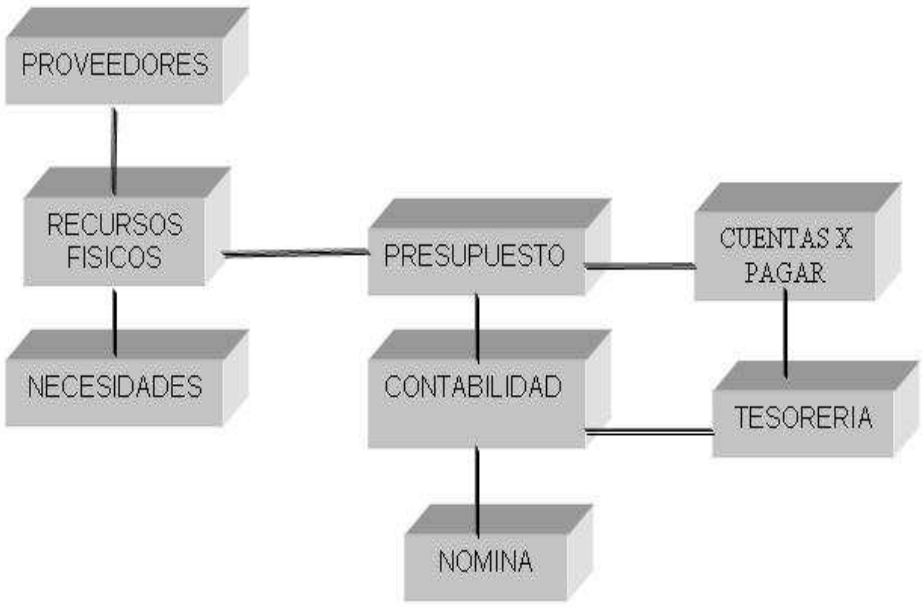
8.3.1 Necesidades de Informática

Las necesidades de informática en la Gobernación de Bolívar se resumen en la existencia de nuevas tecnologías y al correcto uso de estas en los procesos llevados a cabo en la institución los cuales reciben apoyo de las TI. Dicha necesidad se hace evidente mas que todo en la parte de comunicaciones y redes de datos de la institución, la cual es de cierta forma obsoleta debido al uso actual que se le esta dando y también a la calidad de servicio que presta.

Se hace necesario en la Gobernación de Bolívar la actualización de una gran mayoría de los equipos de escritorio utilizados en las actividades diarias de la entidad, hecho corroborado en una reciente auditoria se sistemas contratada por la misma entidad.
Se hace necesaria la implementación de una nueva y funcional red de datos acorde a las necesidades que demandan los usuarios como agentes activos en los procesos llevados a cobo en la entidad.

8.3.2 Modelo Conceptual de Datos

8.3.2.1 Entidades y Agrupación de Entidades



8.3.3 Especificaciones de los Sistemas de Información

Atlas Pro

El estado en que se encuentra el software es el siguiente, En lo que concierne a la trascripción de datos se pudo constatar la no existencia de manuales de trascripción para las operaciones que se manejan mediante este medio de entrada de información, los documentos procesados en la trascripción no se marcan con ningún tipo de sello que los identifique como ya procesados por el sistema lo que podría generar duplicidad y redundancia de información en las bases de datos que maneja el software, también se hizo evidente la falta de un manual de procedimientos para administradores del sistema en caso de este ser requerido para alguna eventualidad.

En lo que concierne al control que se lleva a el software, es claro que se tiene un alto control de funcionamiento empezando por la recepción de documentos para su posterior procesamiento por parte del sistema ya que solo se reciben documentos en un formato establecido, y dejando evidencia escrita de las inconsistencias encontradas en los documentos, así como también existen funciones asignadas por escrito a cada funcionario, el punto en contra en este aspectos de control seria la evidente falta de una completa y segura segregación de funciones ya que los procesos de codificación, grabación y verificación son realizados por una misma persona.

En cuanto al aspecto de seguridad de archivos se tiene una correcta aplicación de la política de backups, para la cual existe una persona encargada de estos, así como también existen medios magnéticos rotulados para su correcta identificación, en lo que ciertamente hay fallas es en el tratamiento que se da a la información por parte de software ya que se constato que esta no es almacenada bajo ningún tipo de técnica criptográfica que no permita el fácil acceso a el contenido por parte de terceras personas.

En lo que compete a informes generados por el sistema por errores de captura, se constato que este genera un listado con la suficiente información sobre los posibles errores para poderlos detectar, en lo que realmente existe un riesgo es en la individualización de los errores ya que no se generan logs por errores producidos, el software cuenta con un completo sistema de validación de datos lo que lo hace bastante confiable al momento de la captura de datos.

En cuanto a informes generados por el sistema para su distribución, se hizo evidente la falta de una hoja remisoria del informe que permita el seguimiento claro y transparente del conducto o ruta que se les da a estos.

No se mantiene un registro de informes y documentos producidos por el sistema para su distribución lo que dificulta la tarea de la producción de informes de distribución.

Se prohíbe dentro de la entidad la distribución de informes a usuarios no autorizados, cumpliéndose a cabalidad esta prohibición, esta tarea facilita o restringe en cierta forma el flujo de información a otras áreas de la entidad e incluso fuera de esta.

SaigtWeb

El estado actual del software es de balance positivo. Se encontró un sistema de información bastante completo y robusto en cuanto a aspectos de seguridad y planeación de funcionamiento, con manuales de trascripción y de funcionamiento. Se tiene además respaldo físico de los documentos que contienen la información ingresada al sistema, además se cuenta con servidores configurados en forma de espejo brindando seguridad a la información archivada y el proceso de respaldo de la información es llevado a cabo diariamente.

Existe además una perfecta segregación de funciones en cuanto al proceso de trascripción de datos lo que evita el riesgo de operaciones de trascripción dudosas, y los errores ocurridos durante este proceso son llevados al equipo de control para su revisión.

Las funciones de codificación, grabación y verificación son realizadas por personas diferentes lo que pone en evidencia lo dicho anteriormente sobre la segregación de funciones.

En cuanto a la seguridad de los archivos de sistema se encontró un ambiente confiable, para este sistema de información existe un manual de procedimiento en el que se describe el contenido y el manejo que se le debe dar a los archivos. El proceso de backup que se menciono anteriormente entra a jugar un papel muy importante es esta parte de la seguridad, como se dijo anteriormente, el sistema de respaldo de información es llevado a cabo diariamente y por una persona encargada exclusivamente de esta tarea.

Además los datos procesados por el sistema son almacenados mediante la utilización se técnicas criptográficas lo que eleva el nivel de seguridad en cuanto a la transacción de información, llegándose también al punto de restringir el acceso a ciertos archivos mediante códigos de seguridad.

En la parte de los informes de errores producidos por el sistema durante el proceso de captura de información, el sistema esta capacitado para generar un listado de errores, pero sin generar un log o informe individual por cada error producido. Cuenta también el sistema con un manual de descripción de los posibles errores arrojados, para así poder sobrellevar de la mejor manera el error que se presente.

Durante el proceso de captura, no se utilizan totales de control para rastrear posibles errores, lo que limita el rastreo de errores solo a los informes generales que produce el sistema.

En cuanto a informes generados por el sistema, ajenos a informes de errores, estos se distribuyen con una hoja remisoria lo que permita el seguimiento claro y transparente del conducto o ruta que se les da a estos, para que así no caigan en manos de personas no autorizadas, hecho que aun así se prohíbe dentro de la entidad, al igual se mantiene un registro de informes y documentos producidos por el sistema para su distribución, lo que hace aun mas fácil esta tarea, el manual de distribución de informes se encuentra incluido en el manual de usuario del sistema

8.4 DEFINICIONES ESTRATÉGICAS

8.4.1 Objetivos estratégicos de TI Y Estrategias de TI

	No.1	No.2	No.3
OBJETIVOS	Motivar al personal para que tenga un mejor desempeno de sus táreas asignadas dentro de sus funciones y que tenga sentido de pertenencia con la Institución	Crear y mantener el sistema de información integral que permita la planificación, ejecución, seguimiento y monitoreo del plan de desarrollo del actual gobierno del dpto de Bolivar.	Crear infraestructura física del Centro de Información e Informática de la Gobernación de Bolivar.
ESTRATEGIAS	- Talleres de capacitación, concientización, sensibilización y motivación personal. - Crear comité asesor de informática con funciones de planeación del desarrollo de sistemas de información.	- Gerenciar proyecto de implementación del Sistema de información de la Gobernación - Desarrollar y actualizar periódicamente estándares para la normalización de la información en los términos de definición, codificación, estructura y valor. - Desarrollo de aplicación para integrar la información	- Implementar y/o adecuar la red de Datos. - Realizar el montaje de la Central de información.

APLICACION DEL GOBIERNO DE TI

Calculo de Desempeño de GTI

	¿Que tan importantes son los siguientes resultados para su GTI, en una escala de 1 a 5?	¿Cuál es la influencia del GTI en su negocio en una escala de 1 a 5	**TOTAL**
Uso Costo-Efectivo de la TI	4	2	8
Uso efectivo de TI para el área financiera	5	5	25
Uso efectivo de TI para el crecimiento	2	2	4
Uso efectivo de TI para adquirir flexibilidad de negocios	3	3	9
Total Importancia:	14	**Total:**	46
Calculo Desempeño del GTI :	**65,71**	**(Total x 100)/(5xTotal importancia)=CGTI**	

Después de la aplicación de la matriz para el calculo del desempeño del Gobierno de TI en la Gobernación de Bolívar se pudo constatar que la entidad presenta un total de 65,71 puntos de nivel de desempeño de GTI un puntaje muy por debajo de los estándares mundiales, ya que se calcula que las entidades con un desempeño de GTI por encima de 74 puntos son las que obtienen un mayor desempeño financiero, aunque este hecho puede ser tomado desde el punto de vista, que la Gobernación de Bolívar como entidad publica no busca el lucro sino el cumplimiento de políticas en cumplimiento de un programa de gobierno.

Identificación del Origen de Necesidades

Dominio/ Arquetipo	**Principios de TI**	**Arquitectura de TI**	**Estrategias de Infraestructura de TI**	**Necesidades de aplicativos para el negocio**	**Inversiones en TI**
Monarquía de Negocios					
Monarquía de TI		**X**	**X**		

Federal	**X**				
Duopolio de TI				**X**	
Feudal					**X**
Anarquía					
Desconocido					

Se observa que los requerimientos para el desarrollo del negocio surgen del alto nivel, quien desempeña el papel estratégico de gobierno de TI. Así mismo se observa que los requerimientos de aplicativos y priorización de inversiones surgen de cada área o unidad de negocio independientemente.

Definicion del lugar donde se toman las decisiones

Dominio/ Arquetipo	**Principios de TI**	**Arquitectura de TI**	**Estrategias de Infraestructura de TI**	**Necesidades de aplicativos para el negocio**	**Inversiones en TI**
Monarquía de Negocios					
Monarquía de TI	**X**	**X**	**X**		**X**
Federal					
Duopolio de TI				**X**	
Feudal					
Anarquía					
Desconocido					

En esta matriz se observa que la toma de decisiones se centraliza mas en el dominio Monarquía de TI, excepto para el dominio Necesidades de Aplicativos para el negocio, en donde la decisión es tomada en el arquetipo denominado por el GTI como Duopolio de TI (Ejecutivos de TI y ejecutivos de negocios).

Teniendo en cuenta lo anterior el análisis respectivo que se hace sobre la toma de decisiones, en la Gobernación de Bolívar se puede decir que el tipo de GTI que se presenta es centralizado, esto tiene beneficios respecto a ciertos aspectos como por ejemplo:

Elemento estratégico.	**Beneficios**

Mecanismos clave de GTI	- Manejo a través de toda la organización. - Arquitectura de procesos. - Presupuesto aprobado. - Hacer seguimiento del valor aportado al negocio por TI.
Infraestructura de TI	Capas de Servicios compartidos administrados centralizadamente

Identificación de Escenarios y Recursos Informáticos y Tecnología Informática de la Gobernación de Bolívar

Plantilla de Recopilación de Datos						
Identifique los activos que su grupo debe desarrollar, administrar, dar soporte o mantener						
Nombre del Activo	Clasificación del Activo(Repercusión alta, media o baja en la empresa)					
PC's de escritorio	Alta					
Complete la información siguiente por cada activo						
Nivel de defensa	Temores o riesgos que se intentan evitar (amenazas)	Como puede suceder (vulnerabilidades)	Nivel de Exposición (A, M, B)	**Descripciones de los controles actuales**	Probabilidad (A, M, B)	**Preocupaciones de Control, nuevos controles posibles**
Físico	Fraude y Robo, desastre y sabotaje	Falta de inventario, Daño eléctrico	A	----------	M	Aplicación del proceso COBIT DS12
Aplicación						
Host						
Red						
Datos	Acceso llegal	Acceso a horas no laborales	M	Vigilantes externos	M	Aplicación del proceso COBIT DS 5

Plantilla de Recopilación de Datos	
Identifique los activos que su grupo debe desarrollar, administrar, dar soporte o mantener	
Nombre del Activo	Clasificación del Activo(Repercusión alta, media o baja en la empresa)
Software Atlas Pro	Alta
Complete la información siguiente por cada activo	

Nivel de defensa	Temores o riesgos que se intentan evitar (amenazas)	Como puede suceder (vulnerabilidades)	Nivel de Exposición (A, M, B)	**Descripciones de los controles actuales**	Probabilidad (A, M, B)	**Preocupaciones de Control, nuevos controles posibles**
Físico						
Aplicación	Errores y Omisiones	Duplicidad de información	B	Personal capacitado	B	Aplicación del proceso COBIT DS 11 y M2
Host						
Red						
Datos	Acceso Ilegal y Perdida de Información	Acceso no deseado por parte de terceros	A	----------	M	Aplicación del proceso COBIT DS 5

Plantilla de Recopilación de Datos						
Identifique los activos que su grupo debe desarrollar, administrar, dar soporte o mantener						
Nombre del Activo	Clasificación del Activo(Repercusión alta, media o baja en la empresa)					
Software SaigtWeb	Alta					
Complete la información siguiente por cada activo						
Nivel de defensa	Temores o riesgos que se intentan evitar (amenazas)	Como puede suceder (vulnerabilidades)	Nivel de Exposición (A, M, B)	**Descripciones de los controles actuales**	Probabilidad (A, M, B)	**Preocupaciones de Control, nuevos controles posibles**
Físico						
Aplicación	Errores y Omisiones	Duplicidad de información y rastreo de errores	B	----------	B	Aplicación del proceso COBIT DS 11 y M2
Host						
Red						
Datos						

9. REFERENCIAS BIBLIOGRAFICAS

[1] *La Contribución del Balanced Scorecard al Proceso de Gobierno de Tecnología de Información (TI) Universidad del CEMA*

[2] *CobiT (Control Objetives for Information and related Technology) es una herramienta para el gobierno, el control y la Auditoria de información y tecnologías relacionadas. Este modelo fue desarrollado por la Fundación de Auditoria y Control de Sistemas de Información como una norma generalmente aplicable y aceptada de buenas prácticas para la seguridad y el control de la tecnología de información.*

[3] *ADMINISTRACION DE RIESGOS. Estándar Australiano/Neozelandés AS/NZS 4360:1999*

[4] *The IT Balanced ScoreCard – A Roadmap to effective Governance of a Shared Services IT Organization. Saul Ronald Information Systems Control Journal, Chicago, volumen 2, Marzo-abril 2000.*

[5] *Confederación Alemana de Cooperativas, DGRV, Gobernabilidad de Tecnologías de Información; Agosto de 2005*

[6] *Security Risk Management Guide, Microsoft,*
http://www.microsoft.com/spain/technet/recursos/articulos/srsgch04.mspx

[7] *Modelo de riesgo para las operaciones. Diciembre 2000 versión 1.0. Microsoft Operations Framework http//:www.microsoft.com/mof.*

[8] *COBIT. Objetivos de Control, Abril de 1998 2ª Edición, Pág. 13.*

[9] *ITGOVERNONEPAGE05-MIT. Weill Peter & Ross W. Jeanne. Noviembre 2004.*

[10] *Esta metodología usa la puntuación del riesgo para clasificarlos en una lista ordenada en forma descendente, en donde el orden determina la secuencia de amenazas a las que se está expuesto. De esta forma el ítem de más alto puntaje se percibe como el criterio de mayor riesgo y el último como el de menor riesgo.*

[11] *Para efectos de la clasificación de los controles en la matriz, una "celda" es la intersección entre un componente y una amenaza a la que está expuesto.*

[12] *Consultoria para evaluar la plataforma tecnológica de la Gobernación de Bolívar por Arthur Andersen. Septiembre de 2000.*