Universidad de Costa Rica
Sistema de Estudios de Posgrado

Desarrollo e Implementación de una Metodología para la Administración de Riesgos en el Desarrollo y Adquisición de Sistemas de Información

Trabajo Final de Graduación aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magíster en Administración y Dirección de Empresas con énfasis en Auditoria en Tecnologías de Información

Johnny Villalobos Murillo
Carné 813153

Ciudad Universitaria "Rodrigo Facio", Costa Rica

Año 2007

DEDICATORIA

A Quien me ha dado la vida,
A quienes siempre han estado a mi lado.

Johnny Villalobos

AGRADECIMIENTOS

A mis profesores por sus enseñanzas
A los funcionarios de RECOPE
comprometidos con el proyecto.

Johnny Villalobos

HOJA DE APROBACIÓN

Este Trabajo Final de Graduación fue aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magister con énfasis en Auditoría en Tecnologías de Información.

_____	_____
Dr. Aníbal Barquero Chacón	MAI. Sergio Espinoza Guido
Director Programa de Maestría	Profesor Coordinador
_____	_____
MSc. Xiomar Delgado Rojas	Máster. Óscar Orozco Rodríguez
Profesor Guía	Supervisor Laboral

_____
Lic. Johnny Villalobos Murillo
Estudiante

Indice de Diagramas **vii**

Indice de Gráficos **vii**

Indice de Tablas **vii**

Indice de Figuras **vii**

CONTENIDO

Desarrollo e Implementación de una Metodología para la Administración de Riesgos en el Desarrollo y Adquisición de Sistemas de Información

RESUMEN

Nombre: Villalobos Murillo Johnny

Título del Trabajo Final de Graduación: Desarrollo e Implementación de una Metodología para la Administración de Riesgos en el Desarrollo y Adquisición de Sistemas de Información

Programa de Posgrado en Administración y Dirección de Empresas. –San José, C.R.:

J. Villalobos Murillo., 2007.

El objetivo general del trabajo es: Desarrollar e implementar una metodología para la administración de riesgos en el desarrollo y adquisición de sistemas de información, apoyada en un manual de administración de riesgos y una herramienta computarizada que facilite la identificación, análisis, evaluación, tratamiento, revisión y comunicación de los riesgos en cada una de las etapas del ciclo de vida de desarrollo de sistemas de información o los procedimientos de adquisición de sistemas de información.

La organización investigada se dedica a: abastecer las necesidades del mercado nacional de hidrocarburos, en una forma económica, segura y con cuidado del ambiente.

Para ello el proyecto desarrolla una investigación de tipo cuantitativa, ya que se realiza el estudio cuantitativo del impacto de los riesgos en el los diferentes procesos del *desarrollo y adquisición de sistemas de información* y se propone una metodología que permita ayudar a mitigar el efecto de su materialización.

Dentro de sus principales conclusiones se encuentra que:

- La metodología desarrollada requiere para su aplicación que el proceso de desarrollo y adqusición de sistemas de información esté bien documentado en todas sus etapas e identificados los controles que se utilizan en estas.

Con base en todo lo anterior, se recomienda que:

- El Área de Tecnología Informática adopte una cultura de calidad en el proceso de desarrollo y adquisición de sistemas de información.
- Que la Asesoría en Tenología Informática de RECOPE continúe los esfuerzos iniciados con el presente proyecto, a fin de lograr definir el resto de los procesos que conforman esa área y adaptar la presente metodología de valoración de riesgos a ellos.

Palabras clave: Administración, riesgos, controles, valoración,

Director de la investigación: Máster. Sergio Espinoza Guido

Unidad Académica: Escuela de Ciencias Económicas,
Programa de Posgrado en Administración y Dirección de Empresas
Sistema de Estudios de Posgrado

Introducción

Todo proyecto está expuesto a riesgos. En el área de Tecnologías de Información, en lo que respecta al desarrollo y adquisición de sistemas de información, los riesgos están presentes y, por tanto, es necesario realizar acciones que permitan mitigar el efecto de su materialización. A pesar de que algunos son inevitables, identificarlos a tiempo y tomar acciones de prevención, que permitan una administración adecuada, aumenta las posibilidades de éxito de cualquier proyecto.

De no existir la administración del riesgo, se cae en la "administración riesgosa" que implica la toma de decisiones imprudentes o precipitadas, o tomar decisiones sin fundamento en una atención cuidadosa de los hechos y de los riesgos involucrados.

Es necesario que los funcionarios de una institución y, sobre todo, aquellos que están relacionados con labores de auditoría, que deben regirse según las normas y las políticas establecidas, también se sientan obligados a actuar, de forma consistente, con la ética y los valores.

Tomar una decisión involucra el administrar riesgos, aunque estas decisiones sean en las operaciones diarias o sobre las políticas importantes, los proyectos, en los que se vean afectados los recursos de la institución.

Este proyecto nace por la necesidad de tener una metodología para administrar los riesgos en las instituciones públicas que se ajuste a los lineamientos establecidos por la Contraloría General de la República, en el área de Tecnologías de Información, y más específicamente, en el desarrollo y la adquisición de sistemas de información.

La institución en la cual se va a implementar es la Refinadora Costarricense de Petróleo (RECOPE), institución líder en el desarrollo económico y social de Costa Rica, (véase organigrama en la p. 23). Por ser una guía genérica, la metodología puede ser adoptada por

otras instituciones públicas, con la posibilidad de convertirse en un estándar en el ámbito nacional.

Para el logro de esta metodología se contó con el apoyo de la Auditoría Interna de la Institución, la que coordinó reuniones y talleres con el personal de ese departamento, del Área de Asesoría en Tecnología Informática y demás personal afín a este proyecto.

Es importante dar una visión global del contenido de este documento, el cual está conformado por cinco capítulos y los anexos correspondientes.

En el primer capítulo, se introduce al lector sobre el propósito del proyecto, sus aportes y limitaciones, los objetivos propuestos, así como su proyección social e intereses profesionales.

Seguidamente, en el capítulo dos, se destaca la pertinencia y actualidad del tema que se aborda con su desarrollo, ya que en el cumplimiento del Artículo 18 de la *Ley General de Control Interno Nº 8292*, esta metodología llega a complementar el trabajo de la Auditoría Interna.

El tercer capítulo trata de dar una especificación de cada una de las fases para la elaboración de la metodología que se propone. Con base en los resultados que se especifican en este capítulo, se produce el diseño y la implementación de la metodología, contemplando las pruebas necesarias en los distintos departamentos involucrados, ajustes, evaluación y, por último, su puesta en marcha, que está documentado en el Capítulo IV.

Finalmente, en el último capítulo, una vez establecida e implementada la metodología, se hacen las recomendaciones sobre los procedimientos para su buen funcionamiento y las recomendaciones que se deben realizar dentro de la Institución para lograr los resultados esperados.

Capítulo I. Ubicación del tema en el contexto

1.1 Título

Desarrollo e implementación de una metodología para la administración de riesgos en el desarrollo y adquisición de sistemas de información.

1.2 Objetivo general

Desarrollar e implementar una metodología para la administración de riesgos en el desarrollo y la adquisición de sistemas de información, apoyada en un manual de administración de riesgos y una herramienta computarizada que facilite la identificación, el análisis, la evaluación, el tratamiento, la revisión y la comunicación de los riesgos, en cada una de las etapas del ciclo de vida de desarrollo de sistemas de información o en los procedimientos de adquisición de sistemas de información.

1.3 Objetivos específicos

1. Crear un *Inventario de riesgos* en el desarrollo y la adquisición de sistemas de información, mediante una base de datos documental en la que se almacenen los riesgos identificados en los procesos que conforman las etapas del ciclo de vida del desarrollo de sistemas

2. Desarrollar un procedimiento para el *análisis de los riesgos* identificados, para facilitar la determinación de su posibilidad de ocurrencia, su nivel de riesgo en los procesos que conforman las etapas del ciclo de vida del desarrollo de sistemas, y ayudar en la determinación de vulnerabilidades, de amenazas y de impacto o de grado de perjuicio.

3. Implementar un procedimiento que permita *la evaluación de los riesgos* y establecer un conjunto de parámetros de aceptabilidad. Este procedimiento ayuda en la priorización de los riesgos, según los criterios que la organización establezca.

4. Establecer un procedimiento de *tratamiento de riesgos* a partir de su priorización, y según los criterios de prevención institucionales, para colaborar en el establecimiento de actividades de control interno

5. Desarrollar un procedimiento de *revisión de riesgos* con el propósito de dar seguimiento, en forma continua, a los niveles y factores de riesgo, así como a las medidas aplicadas en la administración de riesgos

6. Definir un procedimiento para generar *la documentación* y facilitar la comunicación, mediante la utilización de una base de datos de riesgos, la cual llevará los registros necesarios sobre la información de probabilidad, ocurrencia, amenazas y consecuencia en las etapas del ciclo de vida de desarrollo de sistemas o en su adquisición, así como el nivel de riesgo asociado y medidas seleccionadas para su administración.

7. Elaborar un análisis de los resultados, de las conclusiones y de las recomendaciones generales del proyecto.

1.4 Entorno organizacional

- **Historia**

De acuerdo con lo localizado en Sitio oficial de RECOPE (s. f.), en 1931, se dicta la Ley del Monopolio de la importación y expendio de gasolina. El responsable de realizar estas tareas fue el Banco de Seguros. En 1933, se autoriza a los expendios privados a vender gasolina a compradores particulares. En 1940 se deroga la Ley del Monopolio y el Estado otorga concesiones a cinco grandes compañías: a la West Indian Oil Company (llamada,

posteriormente, ESSO Standar Oil), a la Texas Company Ltda. (denominada, luego, TEXACO Caribbean Inc), a la Union Oil Company of California (luego, llamada GULF Costa Rica Company), a la Compañía Petrolera de COSTA RICA (llamada, luego, Chevron S.A.) y a CEI de Costa Rica S.A.

En 1961, un grupo privado funda la Refinadora Costarricense de Petróleo Sociedad Anónima (RECOPE S.A.), e inician gestiones para obtener los permisos del Ministerio de Industrias, con el fin de construir una refinería al amparo de la Ley 2426 de Protección y Desarrollo Industrial. En noviembre de 1962, logran dicha autorización bajo el contrato industrial 53-62.

En 1963, se inicia la construcción de la refinería en Moín, Limón, puerto en el Atlántico de Costa Rica y se concluye en 1967. En ese mismo año, se inicia la construcción de la primera línea de oleoducto y se finaliza la primera terminal de distribución en El Alto de Ochomogo, Cartago. Hasta ese momento, el transporte de producto hacia la Meseta Central se hacía por medio del ferrocarril.

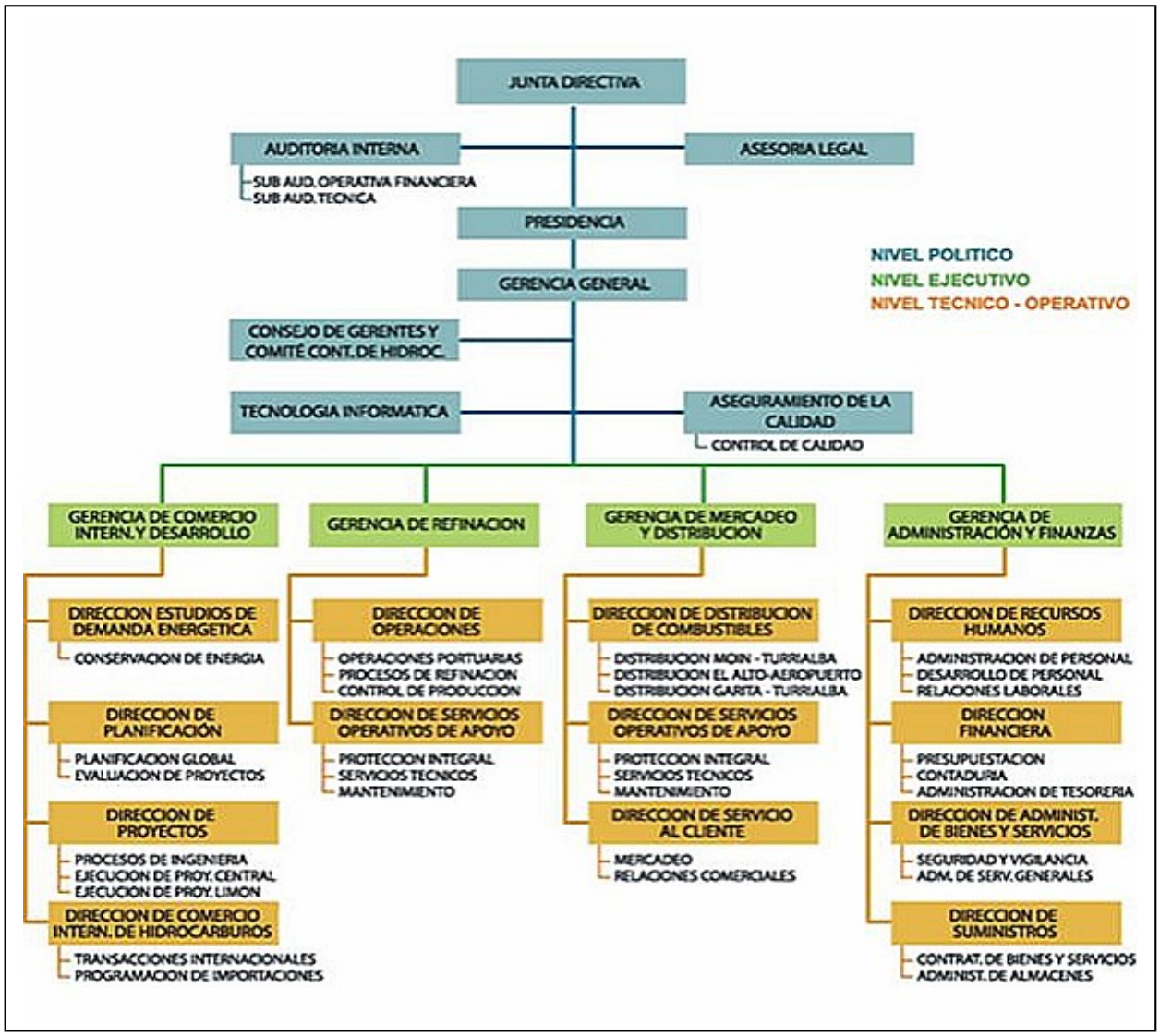
A finales de la década del 60, una comisión especial de la Asamblea Legislativa inicia una investigación sobre el funcionamiento de las distribuidoras privadas y, a finales de 1971, dicta un informe final en el que se evidencian serios incumplimientos de los contratos otorgados por el gobierno.

En 1972, el Ministerio de Economía inicia gestiones para comprar las acciones de la Refinería que, en aquel momento, pertenecían, mayoritariamente, a Allied Chemical.

En 1975, por Decreto Ejecutivo, se decide la nacionalización de la distribución de combustibles. Además, por ley, se le prohíbe a RECOPE operar expendios de combustible al detalle, por lo que las estaciones de servicio pasan a manos privadas.

Diagrama 1

Organigrama de RECOPE



Fuente: http://www.recope.go.cr/acerca/estructura_organizativa/organigrama.htm

1. 5 Impacto

El proyecto se desarrolló con un costo económico muy bajo para la Refinadora Costarricense de Petróleo (RECOPE), ya que deben considerarse las horas de trabajo en que los funcionarios participaron en reuniones, talleres y otras actividades a lo largo del desarrollo y la implementación del proyecto. Por su carácter de guía genérica, la

metodología seguida podría ser adoptada por otras instituciones públicas, con la posibilidad de convertirse en un estándar en el ámbito nacional.

1.5.1 Beneficios de la práctica

- Aumentar el conocimiento sobre la administración de riesgos en el CVDS de sistemas de información.
- Investigar y profundizar en la normativa existente sobre el control interno para proteger y conservar el patrimonio público, y garantizar la eficiencia y la eficacia de las operaciones en el desarrollo y adquisición de SI.
- Contribuir a las buenas prácticas gerenciales, que posibiliten una mejora continua en el proceso de toma de decisiones; aplicando los conocimientos obtenidos en el programa de Maestría, por medio de una metodología para la administración de riesgos en el área del desarrollo y adquisición de los sistemas de información, acorde con la normativa del país.

1.5.2 Beneficios para la institución patrocinadora en el área del desarrollo y adquisición de sistemas de información y administración de riesgos

- Contribuir en la administración eficiente y eficaz del patrimonio público,
- Apoyar el desarrollo o adquisición de sistemas de información en forma controlada.
- Ayudar a la Auditoría Interna en la valoración de riesgos institucionales.
- Sistematizar la evaluación del cumplimiento, suficiencia y validez del control interno en los sistemas de información

1.5.3 Beneficios para el programa de Maestría

Dentro de los beneficios está el mejoramiento de la imagen de la UCR, como parte de su *responsabilidad social*, donde es llamada a colaborar con el desarrollo del país. Una de las mejores formas de lograr esta contribución es que sus estudiantes desarrollen proyectos en este campo. Los proyectos que se llevan a cabo en la Maestría en Auditoría de Tecnologías

de Información ayudan a las instituciones públicas o empresas privadas a hacer un uso adecuado de las tecnologías de información, y colaboran en la consecución de sus objetivos estratégicos, lo que repercute, en forma directa, en un mejor uso de las tecnologías de información en Costa Rica.

1.6 Operacionalidad de las variables

Administración de riesgos

Consiste en un proceso de identificación, evaluación, selección y ejecución de medidas para la administración de riesgos (SEVRI, 2005). Se diseñan instrumentos, entre los que se encuentran formularios y registros que faciliten las diferentes partes del proceso de administración de riesgos.

Amenaza

Suceso que puede desencadenar en un incidente en la Institución y producir daños materiales o pérdidas inmateriales en sus activos, (MAGERIT, 1997). En este caso, estas pérdidas se pueden presentar en los sistemas de información desarrollados o adquiridos por la Institución

Análisis de riesgos

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta la Institución (MAGERIT, 1997). Un uso metódico de la información para determinar qué tan frecuentemente pueden suceder eventos especificados y la magnitud de sus consecuencias. En el análisis de riesgos se determina su nivel a partir de la probabilidad y las consecuencias de aquellos eventos que sean detectables, en el proceso de identificación de riesgos. La metodología suministra herramientas de valoración de riesgos, con base en estimaciones y calificaciones que proporcionan los funcionarios evaluadores asignados.

Ciclo de vida de desarrollo de sistemas de información

El ciclo de vida para el desarrollo de sistemas es un conjunto de etapas que los usuarios, analistas, diseñadores de sistemas y otros funcionarios involucrados realizan para desarrollar e implantar un sistema de información computarizado (CGR, 1995).

Comunicación de riesgos

La comunicación de riesgos es una actividad de carácter permanente que consiste en la preparación y la distribución de información oportuna sobre riesgos a todos los interesados. Los informes, y las consultas se generan mediante opciones de la aplicación computacional que apoya a la metodología.

Criterios

Se refiere a un valor que se establece y se define en un proceso de evaluación para juzgar el mérito de un objeto o un componente.

Criterios institucionales de prevención

Criterios institucionales de prevención de riesgos son, entonces, los valores definidos por la Institución para juzgar el riesgo al que se enfrenta un proceso de desarrollo o un proceso de adquisición de sistema de información.

Evaluación de riesgos

Es el proceso para establecer las prioridades de administración de riesgos, mediante el cotejo del nivel de riesgo, respecto a los patrones establecidos u otro criterio que determine la administración.

Factores de riesgo

Un factor de riesgo es toda circunstancia o situación que aumenta las probabilidades para que una amenaza se materialice. Se refiere a todos aquellos elementos: objetos (materia prima), instrumentos (máquinas, equipos, herramientas), ambientes, instalaciones locativas, gestión administrativa, acciones humanas, que “encierran una capacidad potencial” para

producir lesiones o pérdidas materiales. La probabilidad de no ocurrencia y, por ende, de evitar las posibles consecuencias, depende de la eliminación o control del elemento agresivo.

Herramienta computarizada

Una herramienta computarizada es un programa de cómputo, que provee una ventaja técnica para realizar la tarea de administración de riesgos.

Metodolodía para la identificación de riesgos

Es el proceso para determinar qué puede suceder, por qué y cómo, mediante la identificación de eventos de índole interno y externo que puedan afectar, de forma significativa, los objetivos fijados por la administración. La aplicación computacional de la metodología suministra formularios de identificación de riesgos, los cuales se almacenan en una base de datos de riesgos, lo que permite establecer un inventario de riesgos que puede utilizarse en evaluaciones posteriores.

Inventario de riesgos

Es un repositorio de información documental (base de datos) sobre los riesgos presentes en los procesos de desarrollo o la adquisición de sistemas de información. En el inventario de riesgos se realiza una documentación del proceso de valoración de ellos, que consiste en el registro de toda la información asociada a los riesgos.

Impacto

Son las consecuencias que, sobre un activo o sistema de información, tiene la materialización de la amenaza (MAGERIT, 1997), que conllevan los sistemas de información desarrollados o adquiridos, sobre los objetivos de la Institución.

Niveles de riesgo

Es el grado de exposición al riesgo que se determina a partir del análisis de la probabilidad de ocurrencia del evento, y de la magnitud de su consecuencia potencial sobre el cumplimiento de los objetivos fijados. Permite establecer la importancia relativa del riesgo (SEVRI, 2005).

Revisión de riesgos

La revisión de riesgos consiste en un seguimiento de éstos, y a las medidas que toma la administración respecto a ellos, para determinar la eficacia y la eficiencia para enfrentarlos. (SEVRI, 2005).

Riesgo

Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos y cause daños o perjuicios a la Organización (MAGERIT, 1997). En la metodología que se desarrolla e implementa, el riesgo se asocia a los procesos de diseño o de adquisición de sistemas de información.

Riesgo asociado

El riesgo asociado, en el contexto nacional, se refiere a la estimación de exposición a que una amenaza se materialice sobre uno o más procesos de las etapas de desarrollo de sistemas o sobre un proceso de adquisición de ellos.

Tratamiento de riesgos

Selección o implementación de opciones apropiadas para tratar el riesgo, con el fin de que se puedan manejar, de antemano, sus posibles efectos o consecuencias.

Vulnerabilidad

Es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo, considerando, en este caso, los procesos del desarrollo del sistema de información, o de adquisición del sistema de información.

Capítulo II. Diagnóstico de la situación actual del tema

1.1 Sistema

Se entiende por sistema al conjunto de componentes que interactúan entre sí, para lograr un objetivo común.

Según Laudon (1996) "Un *sistema de información* puede definirse técnicamente como un conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una institución".

En las tecnologías de información, un sistema de información es el medio por el cual los datos van de una persona o departamento hacia otros, y puede ser cualquier cosa: desde una simple comunicación interna entre los elementos de la organización, hasta complejos sistemas de cómputo.

Para el desarrollo de un sistema de información existen diferentes metodologías, las cuales se componen de una serie de etapas que deben ser controladas para garantizar su buen desempeño.

Según Pressman (2001), existen tres estrategias para el desarrollo de sistemas: el método clásico del ciclo de vida de desarrollo de sistemas, el método de desarrollo por análisis estructurado y el método de construcción de prototipos de sistemas.

El ciclo de vida de un sistema de información es un enfoque que sostiene que los sistemas son desarrollados, de mejor manera, mediante el uso de un ciclo determinado de las actividades del analista y del usuario. En el caso de Costa Rica, estas etapas están bien identificadas en las especificaciones que, para sistemas de información, establece la Contraloría General de la República, a saber:

- Estudio preliminar
- Estudio de factibilidad
- Análisis y determinación de requerimientos

- Diseño conceptual del sistema
- Diseño físico del sistema
- Desarrollo de la programación
- Desarrollo de la documentación
- Pruebas del sistema
- Implantación
- Evolución post implantación

Este órgano declara en la *Ley No. Nº. 8292* del 31 de julio del 2002 (Costa Rica**,** 4 de setiembre de 2002)**,** que debe haber control en la administración pública cuando se desarrollan sistemas de información, y, literalmente, en el artículo 16, que se refiere a sistemas de información dice:

> "Deberá contarse con sistemas de información que permitan a la administración activa tener una gestión documental institucional, entendiendo ésta como el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar de modo adecuado la información producida o recibida en la organización, con el fin de prevenir cualquier desvío en los objetivos trazados.
>
> a) Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requerido para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.
>
> b) Armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y el manejo eficientes de los recursos públicos.

c) Establecer las políticas, los procedimientos y los recursos para disponer de un archivo institucional, de conformidad con lo señalado en el ordenamiento jurídico y técnico.” (p. 9-10).

1.2 Administración pública

Administración proviene del latin "ad-ministrare", que significa servir, o de "ad manus traher" que se refiere a la idea de manejar o gestionar.

Se entiende por administración pública, la organización integrada por un personal profesional, apoyada de medios económicos y materiales públicos, que pone en práctica las decisiones tomadas por el gobierno. Está constituida por todo lo que la hace efectiva: funcionarios y edificios públicos, entre otros. Por su función, es el vínculo entre la ciudadanía y el poder político (Laudon, 1986).

1.3 Concepto de riesgo

Para efectos de este trabajo, se define el concepto riesgo como toda posibilidad de que un evento pueda perjudicar el desarrollo normal de las funciones de la entidad, y afectar el logro de sus objetivos.

Se puede afirmar que no hay actividad de la vida, ya sea estudio, negocios o cualquier asunto, que no incluya la palabra riesgo. Por esta razón, el hombre desde sus inicios buscó formas de protegerse contra las eventualidades y desarrolló mecanismos para evitar, llevar a un nivel razonable o detectar riesgos, por medio de acciones preventivas.
Según el Estándar australiano (AS/NZS 4360, 1999), el riesgo es la posibilidad de que suceda algo que tenga impacto sobre los objetivos.

El estudio del tema no es nuevo. El adquirir software o desarrollarlo requiere establecer políticas dirigidas a la administración de riesgos, que le permita a la entidad pública

conocer y controlar, aquellos eventos que pueden afectar el cumplimiento de sus objetivos. En el área de tecnologías de información, el desarrollo o la adquisición de sistemas de información es un punto reconocido como de alto riesgo, para lo cual se hace necesario usar herramientas, aplicar y respetar normas que le permitan a las entidades ser cada vez más eficientes y estar acorde con las nuevas tendencias en administración.

Uno de los principales orígenes de los problemas dentro del entorno informático, es la inadecuada administración de riesgos; y una institución como RECOPE, no está exenta de este problema. La metodología propuesta permite contar con una técnica para utilizar en la administración de riesgos, con procedimientos que se apoyan en estándares, además de una herramienta computarizada, necesaria para proveer opciones apropiadas en la implementación de controles en el tratamiento y mejor manejo de los riesgos. Se toman en cuenta aspectos como:

- La evaluación de los riesgos propios de los procesos informáticos.
- La evaluación de los peligros o causas de los riesgos.
- Los controles utilizados para minimizar las amenazas de riesgos.
- La evaluación de los elementos del análisis de riesgos.
- La necesidad de contar con una herramienta automatizada a la medida y conforme con el marco legal del país.

1.4 Administración del riesgo

Es preciso incluir el concepto administración del riesgo en las instituciones, ya que todas las organizaciones, independientemente de su naturaleza, su tamaño, y su razón de ser, son susceptibles a diferentes riesgos o eventos que pueden poner en peligro el logro de sus objetivos (COSO y ERM). Desde el punto de vista del control, el modelo COSO (Committee of Sponsoring Organizations), explica que la eficiencia del control es la reducción de los riesgos, es decir, el objetivo principal del control es la eliminación o disminución de éstos, con el fin de que el proceso y sus controles garanticen, de manera

razonable, que los riesgos están administrados o se están reduciendo y, por tanto, que los objetivos de la organización van a ser alcanzados.

Se debe valorar continuamente lo que puede fallar y recordar que:

- Al identificar estos factores de riesgo, se definen las causas (internas o externas) y los efectos de las situaciones de riesgo.
- Al estudiar estos riesgos es posible determinar la probabilidad de ocurrencia y, con base en este análisis, valorar los riesgos para medir la exposición de la entidad a los impactos del riesgo.
- Con la información de todos estos elementos se obtiene la definición de criterios, que permiten la formulación del estándar de control que se consolida en la política de administración de riesgos.

Debido a la cantidad, la diversidad y las características de las entidades en sus funciones, a la estructura, la relación con la ciudadanía y el perfil del compromiso social, entre otros, es necesario ubicar las áreas, los procesos, los procedimientos, las dependencias y los controles dentro de los cuales puede caerse en riesgos que ponen en peligro la buena gestión y los resultados. También, se debe tener en cuenta que los riesgos están determinados por factores de carácter externo, llamados del entorno, así como factores de carácter interno.

Con este trabajo, se desea desarrollar e implementar una metodología para la administración de riesgos en el desarrollo y la adquisición de sistemas de información, aspecto fundamental para tener una visión sistémica de la gestión, de manera que no se vea esta herramienta como algo aislado del accionar administrativo. El diseño se establece a partir de la identificación de los factores internos o externos a la entidad, que pueden generar los riesgos que afecten el cumplimiento de sus objetivos.

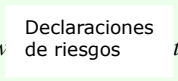
1.5 Los sistemas de información y la administración de riesgos

Se han identificado dos enfoques distintos para la administración de riesgos. Uno es reactivo y el otro es proactivo. En la administración reactiva de riesgos, el equipo del proyecto reacciona a los efectos de los riesgos (los problemas reales) conforme ocurren; mientras que en la administración proactiva de riesgos, el equipo del proyecto cuenta con un proceso visible para administrarlos. Implica que este proceso se puede medir y repetir.

Entre los enfoques mencionados existe una transición, que es la prevención del riesgo, la cual se produce en las etapas de planeación de un proyecto. Es recomendable que el equipo de trabajo aplique acciones para evitar que ocurran los riesgos. En la administración de riesgos, aunque la prevención es una forma de evitar sus síntomas, no es un remedio para eliminar la causa.

En la administración proactiva de riesgos, el equipo de trabajo estima, en forma continua, los riesgos y los utiliza para tomar decisiones en todas las etapas del proyecto.

Gráfico Nº 1. *El proceso de administración proactiva de riesgos.*



Fuente: Fuente: *http://www* *tam/technet/admon/estrategia/art10/art105.asp* (modificado)

Al analizar la importancia del enfoque de la administración proactiva de riesgos, se vio la necesidad de que RECOPE contara con un manual de administración de riesgos fundamentada en el "Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados" de la CGR y una herramienta computarizada, con el fin de que tuviera los instrumentos necesarios, para la prevención del riesgo en cada una de las etapas del ciclo de vida del desarrollo de sistemas de información o los

procedimientos de adquisición de sistemas de información. Uno de los puntos medulares del este trabajo ha sido lograr integrar las directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), establecidas por la Contraloría General de la República. En el desarrollo de esta metodología se garantiza el cumplimiento de las resoluciones emanadas de esa entidad, la cual especifica: "Ámbito de aplicación. Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional por áreas, sectores, actividades o tarea que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo." (CGR, 2005, p. 11).

Estas disposiciones pretenden que toda institución que aplique el SEVRI tenga información que apoye la toma de decisiones y la ubique en un nivel de riesgo aceptable y se promueva, así, un logro de objetivos institucionales.

El SEVRI establece que debe existir una estructura organizacional que genere conciencia, responsabilidad y una actitud proactiva en los funcionarios, que dé apoyo a su operación, así como que se generen mecanismos de coordinación y comunicación entre el personal y las unidades internas.

El funcionamiento del SEVRI contempla puntos importantes que se establecen en el gráfico Nº1 y que permiten una secuencia de ejecución lógica:

1. El primer paso de la administración proactiva de riesgos, es la *identificación de riesgos* que están presentes, y que pueden llegar a materializarse, en cada una de las etapas del proceso de desarrollo y la adquisición de sistemas de información. Para realizar esta identificación se debe seleccionar un grupo de expertos de tecnologías de información de la Institución, involucrados con estos procesos.

   Esta identificación brinda, al equipo del proyecto, datos sobre las oportunidades, indicios e información que le permiten conocer los principales riesgos antes de que

afecten al proyecto. Se puede hacer un inventario ordenado y sistemático de ellos, enlistar los riesgos y dar, luego, una descripción de cada uno y de sus posibles efectos, en la forma en que aparece seguidamente:

Tabla 1. Formato para la especificación de riesgos

RIESGO	**DESCRIPCIÓN**	**POSIBLES CONSECUENCIAS**
Posible evento de una situación que pueda afectar el desarrollo normal de las funciones de la entidad y le impidan el logro de sus objetivos.	Características generales o las formas en que manifiesta el riesgo identificado.	Posibles efectos ocasionados por el riesgo, de tipo económico, social, administrativo, entre otros

Cada institución define su estructura de riesgos al establecer esta lista detallada con los riesgos encontrados, su descripción y sus posibles consecuencias. A partir de ella, se puede elaborar una tabla con los factores de riesgo que se ponderan, según el criterio de los encargados en la Institución, y crear una lista agrupada por área de atención y categoría, en: alto, mediano o bajo.

2. El segundo paso es realizar un análisis de riesgos. Con los datos de un riesgo, se pueden tomar decisiones importantes para que el proyecto no se vea afectado. En un riesgo, se reconocen dos factores: probabilidad e impacto.

    a. La probabilidad de un riesgo es la posibilidad de que ocurra el evento en la realidad, por tanto, es recomendable asignar un número o probabilidad. Cuando el número es cero, la probabilidad de afectar al proyecto es nula; en caso contrario, lo afecta, más o menos, según sea su valor, el cual no puede exceder de 100%.

    b. El impacto de un riesgo calcula la gravedad de los efectos, o la de una pérdida, si el riesgo llegara a suceder.

        Si se evalúa una lista de riesgos, se debe tener clara la amenaza completa (exposición al riesgo). Puede darse el caso de que un riesgo con una probabilidad alta tenga un impacto bajo y puede ignorarse sin complicaciones; puede presentarse,

también, que un riesgo con un alto impacto tenga una probabilidad baja de causar daño y pueda ignorarse. Lo recomendable es administrar aquellos que tienen una exposición alta, o sea, probabilidad e impacto altos.

3. La planificación de acciones contra riesgos, es el siguiente paso. Ésta implica establecer prioridades en las acciones por llevarse a cabo, desarrollar acciones para afrontar los riesgos particulares, y crear un plan integrado de administración de riesgos.
   Un plan de administración de riesgos (Galway, 2004) resume cómo es implementada en un proyecto en particular. Los elementos que deben incluirse en un plan de administración de riesgos son:

   • Metodología. Establecer la administración de riesgo que se ejecuta en el proyecto.

   • Tareas y responsabilidades. Saber quiénes son las personas responsables de implementar las tareas específicas, y brindar los informes relacionados con la administración de riesgo.

   • Presupuesto y plazos: determinar cuáles son los costos y plazos estimados para ejecutar las tareas relacionadas con los riesgos.

   • Categoría de riesgos. Determinar cuáles son las categorías de los riesgos que se identifican.

   • Probabilidad de riesgo e impacto. Definir cuáles son las probabilidades y los impactos de los riesgos que se evalúan. Cuáles son las técnicas cualitativas o cuantitativas que se utilizan para evaluar los riesgos.

   • Documentación de los riesgos. Determinar los formatos de los informes y los procesos que se utilizan para las actividades de la administración de riesgos.

4. Como se observa en el gráfico Nº1, el seguimiento o evaluación de riesgos es el cuarto paso. Se trata de vigilar el estado de los riesgos y las acciones que se han aplicado para reducirlos. El seguimiento de los riesgos es primordial para la implementación de un plan de acciones eficaz. Como se ve, es establecer las unidades para medir el riesgo y

los eventos de activación necesarios para garantizar que funcionan las acciones planificadas.

5. Como último paso en el proceso de administración proactiva, está el control de riesgos, el cual debe combinarse con los procesos de administración del proyecto, para controlar los planes de acciones, corregir las variaciones de los planes, responder a los eventos de activación y mejorar el proceso de administración de riesgos.

El SEVRI, además de los anteriores, incluye tres pasos más:

6. Revisión de riesgos, la cual debe llevarse a cabo en forma continua y consiste en dar seguimiento, al menos, a cuatro aspectos, según la CGR (12 de julio del 2005):

   a) el nivel de riesgo
   b) los factores de riesgo
   c) el grado de ejecución de las medidas para la administración de riesgos
   d) la eficacia y la eficiencia de las medidas ejecutadas para la administración de riesgos.

La revisión de riesgos debe ejecutarse de forma continua, y la información que se genere en esta actividad debe servir de insumo para:

   a) elaborar los informes del SEVRI
   b) ajustar de forma continua, las medidas para la administración de riesgos
   c) evaluar y ajustar los objetivos y metas institucionales

6. Debe documentarse (CGR, 2005)**,** la información sobre los riesgos y las medidas para la administración de riesgos que se genere en cada actividad de la valoración del riesgo (identificación, análisis, evaluación, administración y revisión).

   Asimismo, deben establecerse registros de riesgos que incluyan, como mínimo, la información sobre su probabilidad, la consecuencia, el nivel de riesgo asociado y las medidas seleccionadas para su administración.

   En relación con las medidas para la administración de riesgos debe documentarse, como mínimo, su descripción, los resultados esperados en tiempo y espacio, los recursos

necesarios y los responsables para llevarlas a cabo.

Debe velarse porque los registros sean accesibles, comprensibles y completos, y que la documentación se realice de forma continua, oportuna y confiable.

Toda esta información debe servir de base para la elaboración de los informes del SEVRI, dirigidos a los sujetos interesados. Ésta puede ser requerida por la Contraloría General de la República o la Auditoría interna, por lo que debe estar actualizada en todo momento.

8. Comunicación de riesgos. Se debe ofrecer información, en relación con los riesgos institucionales, a los sujetos interesados, internos y externos, y a la institución

1.6 Clasificación de amenazas de riesgo en entorno informático

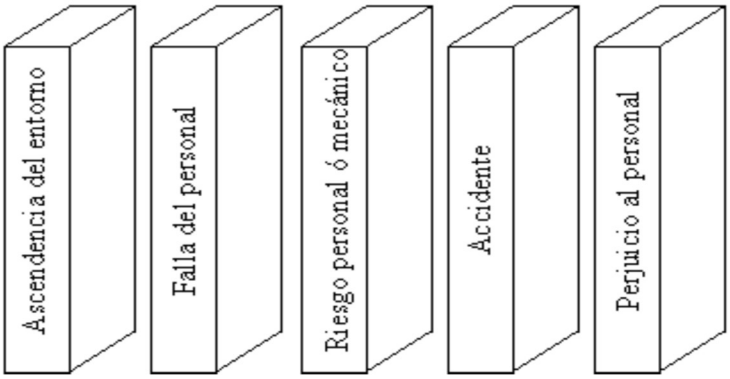
Naturales. Se refiere a los cambios naturales, principalmente, y que pueden afectar, manera importante, el desempeño normal del entorno informático.

Accidentales: Son las más frecuentes que existen como:

- Errores de los usuarios finales. Incorrecta interpretación de datos
- Errores de los operadores. Uso inadecuado del equipo o programas
- Error administrativo. Incorrectas medidas de respaldo o seguridad
- Errores de salida. Dispositivos mal configurados.
- Errores del sistema. Daños en archivos del sistema operativo.
- Errores de comunicación. Fallas de red
- Deliberadas. Accesos no autorizados, modificaciones no autorizadas, sabotaje.

Según la teoría de Heinrich (citado en *Administración y Finanzas*) los accidentes pueden darse como una serie de fichas de dominó colocadas en el borde: cuando una cae, una reacción en cadena es completada.

FIGURA No. 1 Teoría de Dominó de Heinrich



Fuente: http://www.monografias.com/Administracion_y_Finanzas/index.shtml

1.7 Valoración del riesgo

Cuando se hace una evaluación de riesgos se obtiene un resultado. Éste se confronta con los controles identificados en el elemento de control y, además con el objetivo de establecer prioridades para su manejo y políticas establecidas. Se hace necesario tener claros los puntos de control que existen en los diferentes procesos, ya que permiten obtener información para efectos de tomar decisiones.

Para realizar la valoración de los controles existentes es necesario tomar en cuenta que se clasifican en:

- *Preventivos*: aquellos que actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.
- *Detectivos*, pueden ser manuales o computarizados, se diseñan para descubrir un evento, un resultado no previsto o irregularidad, permiten tomar medidas inmediatas. Se utilizan para supervisar la ejecución del proceso y verificar la eficacia de los controles preventivos.
- *Correctivos:* aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

1.8 El procedimiento para la valoración del riesgo

Es necesario describir los controles existentes, estableciendo si son preventivos, detectivos o correctivos y responder las siguientes preguntas:

1. ¿Están documentados los controles?
2. ¿Se están aplicando en la actualidad?
3. ¿Son efectivos para administrar el riesgo?

Como parte del proceso una vez que se responde a todas las preguntas, se procede a realizar la valoración, de la siguiente forma:

- Una vez calificados y evaluados los riesgos, deben ser analizados frente a los controles existentes en cada riesgo.
- Ponderar según la tabla establecida, teniendo en cuenta las respuestas a las preguntas formuladas anteriormente.
- Ubicar en la matriz de calificación, de acuerdo con los resultados obtenidos en la valoración del riesgo.

Se debe tener en cuenta criterios como:

- No existen controles
- Los controles existentes no son efectivos
- Los controles existentes son efectivos, pero no están documentados
- Los controles son efectivos y están documentados.

Así para la valoración del riesgo

- Se mantiene el resultado de la evaluación antes de los controles
- Cambia el resultado a una casilla inferior de la matriz de evaluación antes de los controles (el desplazamiento depende de si el control afecta al impacto o a la probabilidad o ambos)
- Pasa a escala inferior (el desplazamiento depende de si el control afecta el impacto o la probabilidad o ambos)

Capítulo III. Análisis de la situación diagnosticada

Actualmente, la mayoría de las instituciones públicas no cuentan con una herramienta específica para la administración de riesgos en el desarrollo o la adquisición de sistemas de información, razón por la cual la elaboración de esta metodología, servirá para disminuir pérdidas y maximizar oportunidades en esta área.

La metodología provee una guía genérica para la administración de riesgos en el desarrollo y la adquisición de sistemas de información. Permite la identificación, el análisis, la evaluación, el tratamiento, la revisión y la comunicación de los riesgos para cada una de las etapas de desarrollo o de adquisición de sistemas de información.

3.1 Descripción de la metodología propuesta

La metodología ayuda en la identificación de los factores de riesgo para las actividades de las etapas que conforman los procesos. Surge como producto de un proyecto de graduación, realizado en una Institución que requiere aplicar las normas establecidas por la Contraloría General de la República, y que permite:

- Apoyar la administración del Área de Asesoría en Tecnología Informática (ATI).
- en su función de administrar los riesgos de sus procesos.
- Documentar los controles que se aplican a los factores de riesgo.
- Ayudar a la auditoría interna a revisar el cumplimiento de las etapas de los procesos de tecnologías de información.
- Autoevaluar los procesos por parte de la administración del Área de Asesoría en Tecnología Informática.

La metodología utiliza un manual, en el cual se describen las técnicas por usar en la administración de los riesgos. Se debe entender como técnica al conjunto de procedimientos que se apoyan en estándares y utilizan notaciones específicas en términos

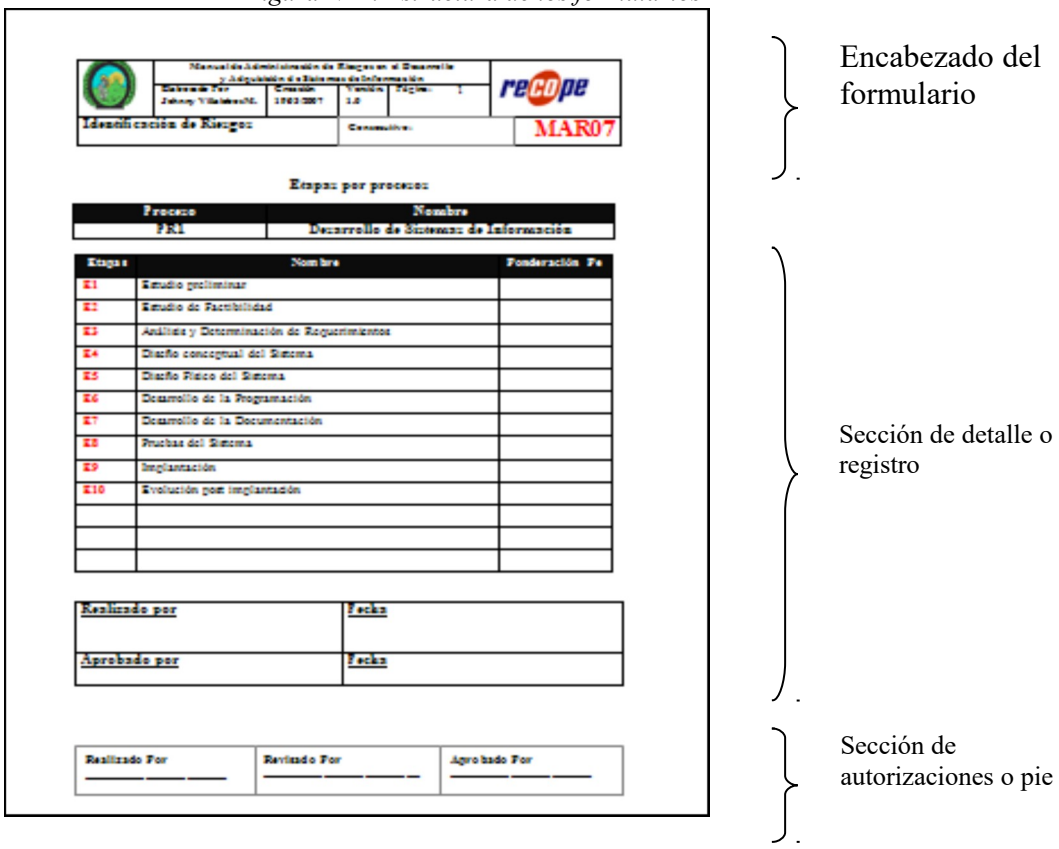
de sintaxis, de semántica y de criterios de calidad, en cuanto al estilo de sus formularios y su administración.

Los formularios sirven para registrar información de los procedimientos que se utilizan en cada etapa del proceso de administración de los riesgos. Los formularios que se proponen tienen una estructura y un propósito que se detallarán en la siguiente sección. (ver Anexo I, Formularios propuestos).

3.2 Estructura de los formularios que se utilizan

Se ha establecido un estándar para los formularios que se utilizan en esta metodología. Éstos tienen tres secciones: encabezado del formulario, detalle o registro y pie de página o autorizaciones. A continuación, se muestra uno de ellos como ejemplo de la estructura utilizada.

Figura Nº 2. Estructura de los formularios



Fuente: Propia

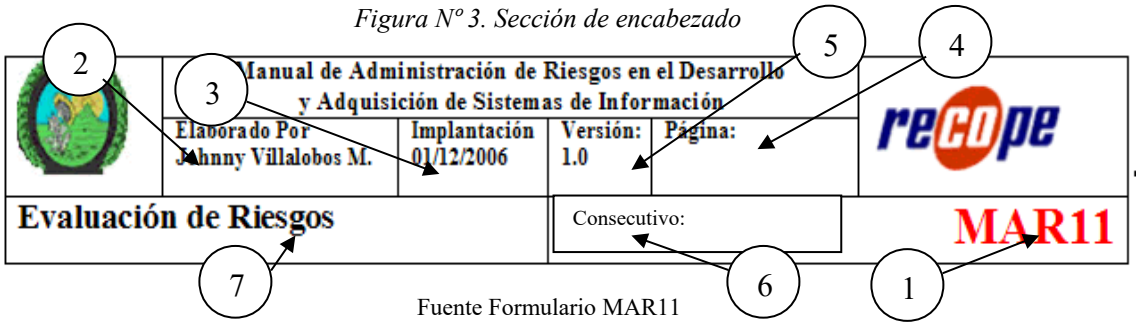
Seguidamente, se da una descripción de su contenido.

3.2.1 Contenido del encabezado del formulario

Esta sección está conformada por:

1. Identificador del proceso
2. Responsable de su elaboración
3. Fecha de implantación
4. Número de página
5. Número de versión
6. Número consecutivo
7. Nombre o descripción

Figura Nº 3. Sección de encabezado



Fuente Formulario MAR11

Descripción

1. Identificador del proceso
   Para la identificación del proceso, se cuenta con el nombre del proceso y un código identificador.

2. Responsable de su elaboración
   Es el nombre del funcionario que diseña el formulario.

3. Fecha de creación
   Es la fecha en la cual el formulario se pone en operación. Esta fecha se debe cambiar en el caso de que el formulario sea modificado.

4. Número de página
   El número de página del formulario. Algunos formularios requieren más de una página.

5. Número de versión

Para los formularios que sufran cambios en su estructura física o en su contenido, se debe actualizar el número de versión, así como su fecha de implantación.

6. Número de consecutivo
   El número de consecutivo, se le adiciona a cada formulario, lo que permite llevar un control de las copias entregadas.

3.2.2 Contenido del detalle del formulario

El detalle del formulario es el área en la cual se diseñan las tablas, campos de información, campos de datos y elementos adicionales que representan el proceso de administración de riesgos al cual corresponde el formulario. En él radica lo fuerte del control, ya que es en esta sección donde se llevan a cabo los diferentes registros. Como cada formulario está plenamente identificado, la referencia a la información contenida en ellos es, perfectamente, ubicable para su seguimiento.

Toda la información que se recolecta en ellos es un insumo para efectos de cumplir los objetivos organizacionales y respaldo para los procesos que se realizan en tecnologías de información, además es información necesaria para la aplicación informática.

3.2.3 Contenido de autorizaciones o pie del formulario

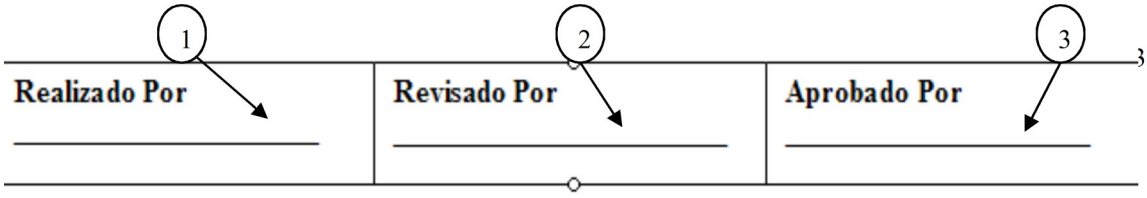
En esta sección se establece la responsabilidad en el seguimiento del formulario. Consta de tres partes, en las que deben plasmarse las firmas de los funcionarios responsables, según sea el caso:

1. Firma del funcionario que completa el formulario

2. Firma del funcionario responsable de revisar el contenido del formulario y la pertinencia de éste.

3. Firma del funcionario que aprueba el formulario desde su diseño hasta su implementación.

Figura N° 4.Imagen parcial de un formulario, sección pie del formulario



Fuente Formulario MAR11

3.3 Administración de formularios

Cada formulario cuenta con un registro físico o un registro digital, así como información sobre la versión, el responsable del formulario y el último consecutivo. Para la administración de versiones y entrega de formulario, se debe designar a un funcionario del departamento.

Para la administración de los formularios, la metodología incluye un formulario específico, cuyo identificador de procesos es MAR01 (Control de formularios). Con este formulario se controlan las versiones, la cantidad de copias entregadas y los números consecutivos de cada uno de ellos.

3.3.1 Proceso de administración de formularios

3.3.1.1 Entrega de formularios

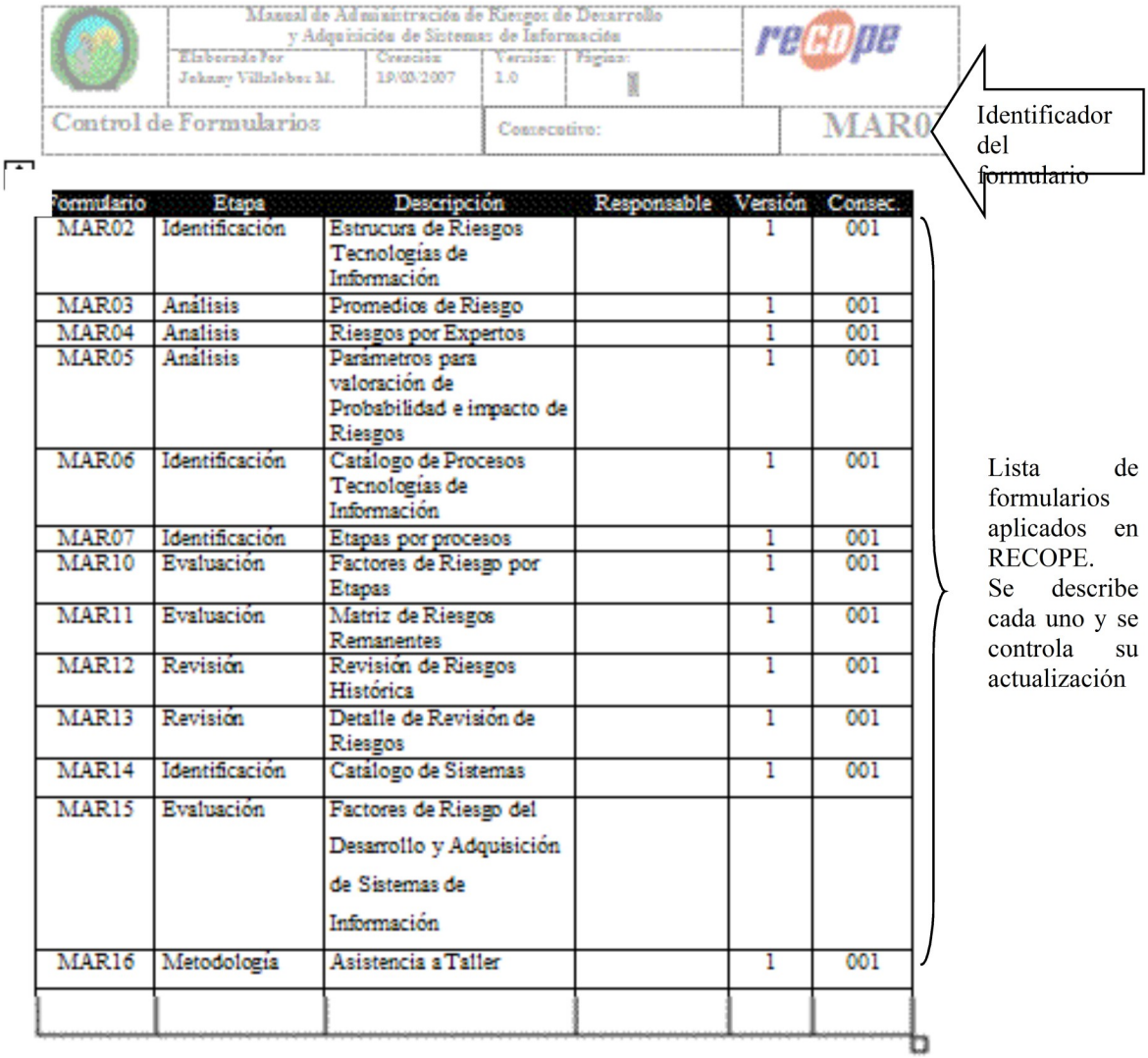
Cada formulario puede ser fotocopiado para ser entregado al funcionario asignado. Cada copia entregada debe llevar el consecutivo respectivo, y se debe actualizar la información del consecutivo en el formulario MAR01.

En este formulario, se especifica el nombre de cada formulario que ha sido elaborado y autorizado; se puede identificar la etapa del proceso a la que está dirigido con su

correspondiente descripción. Incluye el nombre del responsable, la versión y el consecutivo.

En una institución como RECOPE, se ha dado seguimiento a los requerimientos para la administración de riesgos en el desarrollo y la adquisición de sistemas de información y se ha confeccionado una serie de formularios que respaldan la metodología que se propone. El formulario MAR01 contiene, en su detalle, los distintos formularios confeccionados y en el caso de que surja la necesidad de crear algunos otros, deben agregarse a este índice de instrumentos que apoyan la labor de control o administración del riesgo.

A continuación, se muestra el formulario MAR01, en el que se resalta su contenido:



Manual de Administración de Riesgos de Desarrollo y Adquisición de Sistemas de Información

recope

Elaborado Por: Johnny Villalobos M. | Creación: 19/09/2007 | Versión: 1.0 | Página:

Control de Formularios | Consecutivo: | MAR0

Identificador del formulario

Formulario	Etapa	Descripción	Responsable	Versión	Consec.
MAR02	Identificación	Estrucura de Riesgos Tecnologías de Información		1	001
MAR03	Análisis	Promedios de Riesgo		1	001
MAR04	Análisis	Riesgos por Expertos		1	001
MAR05	Análisis	Parámetros para valoración de Probabilidad e impacto de Riesgos		1	001
MAR06	Identificación	Catálogo de Procesos Tecnologías de Información		1	001
MAR07	Identificación	Etapas por procesos		1	001
MAR10	Evaluación	Factores de Riesgo por Etapas		1	001
MAR11	Evaluación	Matriz de Riesgos Remanentes		1	001
MAR12	Revisión	Revisión de Riesgos Histórica		1	001
MAR13	Revisión	Detalle de Revisión de Riesgos		1	001
MAR14	Identificación	Catálogo de Sistemas		1	001
MAR15	Evaluación	Factores de Riesgo del Desarrollo y Adquisición de Sistemas de Información			
MAR16	Metodología	Asistencia a Taller		1	001

Lista de formularios aplicados en RECOPE. Se describe cada uno y se controla su actualización

Realizado Por _____ | Revisado Por _____ | Aprobado Por _____

Fuente propia

3.3.1.2 Modificaciones a plantillas de formularios

Cada formulario puede ser modificado, previo análisis, revisión y aprobación. Una vez aprobada una modificación, se deben recuperar las copias del formulario que se estén utilizando y que no tengan información registrada. Posterior a la recuperación, se modifica la plantilla del formulario, indicando el nuevo número de versión y el nuevo consecutivo.

La metodología de administración de riesgos implica una serie de procesos. Estos deben seguir una secuencia lógica de pasos, y en cada paso se utiliza un formulario de control o registro.

3.4 Proceso de administración de riesgos

Para llevar a cabo la administración de riesgos en una forma efectiva, es necesario tener un orden en la realización del proceso, para lo cual se han establecido pasos, que deben llevarse a cabo, tal y como se muestra en la siguiente lista:

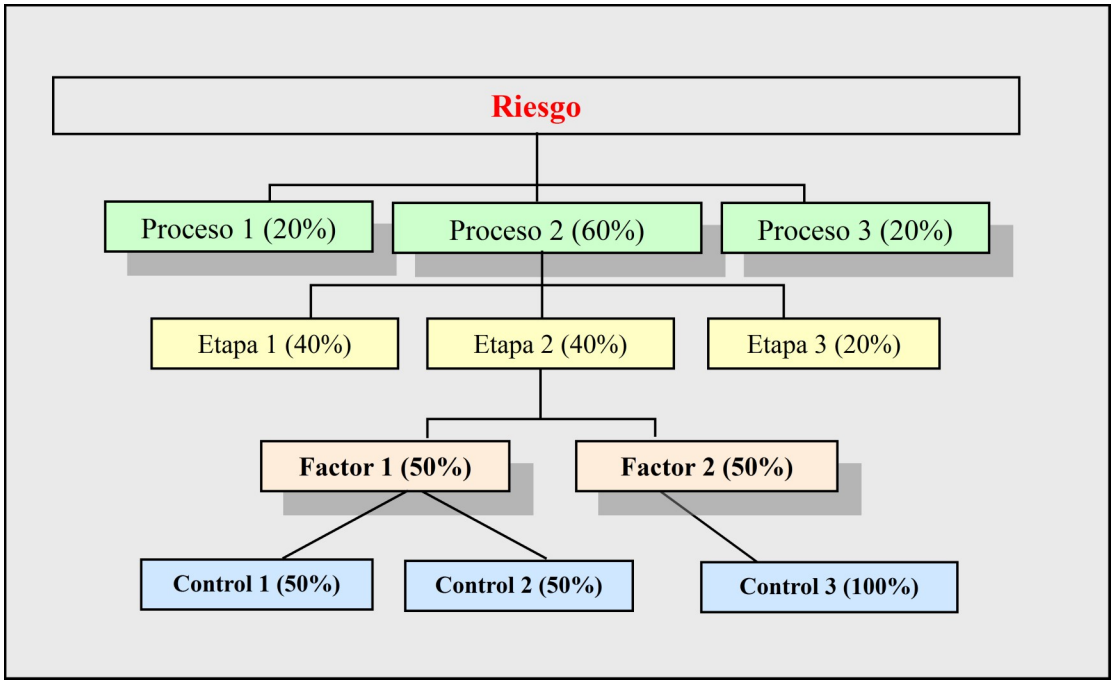
1. Identificar los riesgos que se pueden materializar en procesos de tecnologías de información.
2. Determinar la probabilidad e impacto de estos riesgos.
3. Priorizar cada uno de estos riesgos.
4. Determinar el riesgo en ausencia de controles, y el riesgo que la administración está dispuesta a aceptar.
5. Identificar los procesos de tecnologías de información.
6. Realizar la ponderación respectiva de estos procesos, respecto al riesgo o riesgos identificados en el punto 3.

7. Determinar, para cada proceso identificado, las etapas que se realizan en la Institución.
8. Ponderar cada etapa, respecto al proceso identificado.
9. Identificar los factores de riesgos relacionados con las etapas identificadas.
10. Realizar una ponderación, para cada factor de riesgo, respecto a la etapa.
11. Identificar, para cada factor de riesgo, los controles actuales.
12. Ponderar cada control con el factor de riesgo.
13. Determinar el riesgo remanente, o riesgo en presencia de controles.
14. Construir una matriz de riesgos remanente.
15. Realizar una evaluación del cumplimiento de controles.
16. Documentar y divulgar los resultados de la evaluación.

Una vez que se realiza el paso 14, y teniendo la matriz de riesgos remanente, se pueden llevar a cabo las revisiones al cumplimiento de los controles.

Gráficamente, el proceso de control de un riesgo puede visualizarse como sigue.

Figura Nº 6. Proceso de control



Fuente propia

Seguidamente, se hace una descripción detallada de cada uno de los pasos enlistados, con el fin de documentarlos y comprender cómo la metodología propuesta es aplicada, así como el procedimiento correspondiente.

3.4.1 Identificación de riesgos

Se procede a identificar aquellos riesgos que están presentes y que pueden llegar a materializarse. Con este fin se puede utilizar la estructura de riesgos institucional, o, en su defecto la estructura de riesgos seleccionada por los funcionarios de tecnologías de información como los riesgos más significativos que pueden afectar la consecución de los objetivos de tecnologías de información, y, por consiguiente, los objetivos estratégicos de la Institución.

- Procedimiento para la identificación de riesgos

1. Seleccionar un grupo de expertos de tecnologías de información de la Institución, relacionados con los procesos de desarrollo y de adquisición de sistemas de información.
2. Entregar a cada uno de ellos una copia de la lista de la estructura de riesgos que la

Figura Nº 7. Imagen parcial formulario MAR02

Fuente: Propia

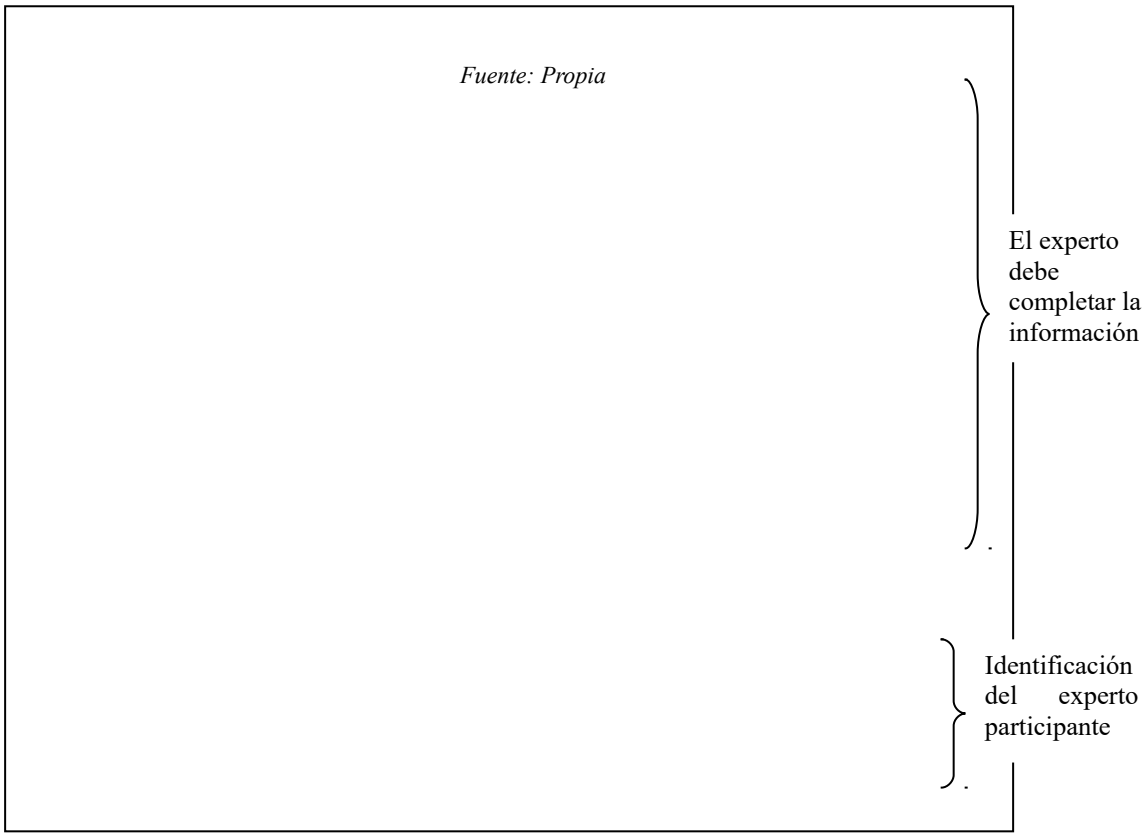
ɔrga al
AR02,
nente.

Detalle del formulario

3. Entregar a cada uno de los expertos una copia del formulario MAR04, con el propósito de que hagan una valoración del riesgo respecto a los procesos de desarrollo y de adquisición de sistemas de información.

   Este formulario consta de dos partes. En la primera se establece el análisis del experto, que consiste en anotar un valor al impacto (Imp) y a la probabilidad de ocurrencia del riesgo (Prob). En la segunda parte, se debe anotar el nombre del experto, la firma y la fecha en que realizó el análisis, como se observa en la siguiente figura:

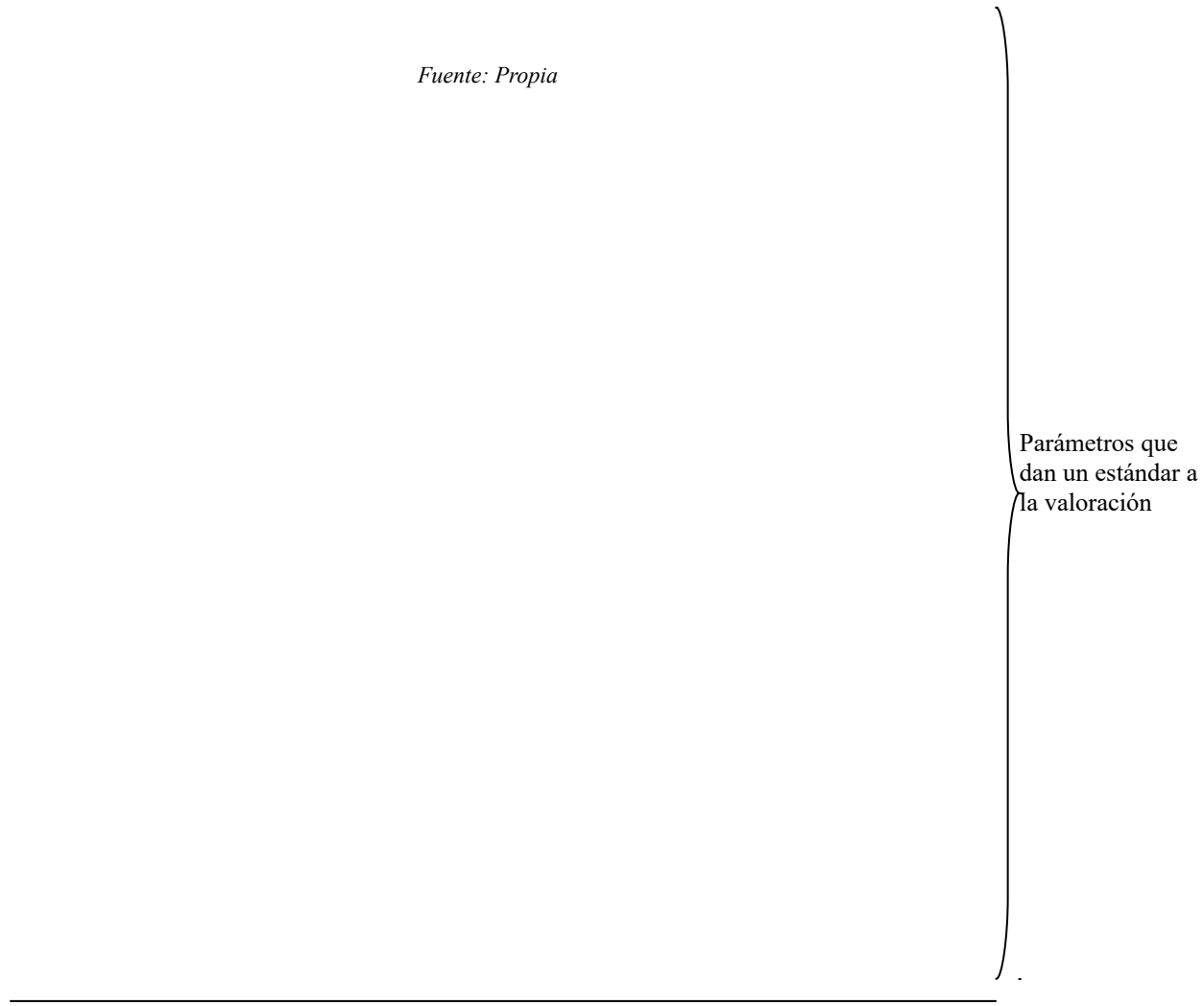
Figura Nº 8. Imagen parcial formulario MAR04



Fuente: Propia

4. Entregar a cada experto una copia del formulario MAR05, el cual contiene los criterios de probabilidad y su impacto. La valoración del experto se hará utilizando los criterios de probabilidad de ocurrencia del riesgo y el impacto de ese riesgo. En este formulario, se especifica el nivel de probabilidad y su descripción, así como el nivel y la descripción del impacto, con el fin de que cada experto use un estándar para poder completarlo. A continuación, se muestra el detalle del formulario.

Figura Nº 9. Imagen parcial formulario MAR05



Fuente: Propia

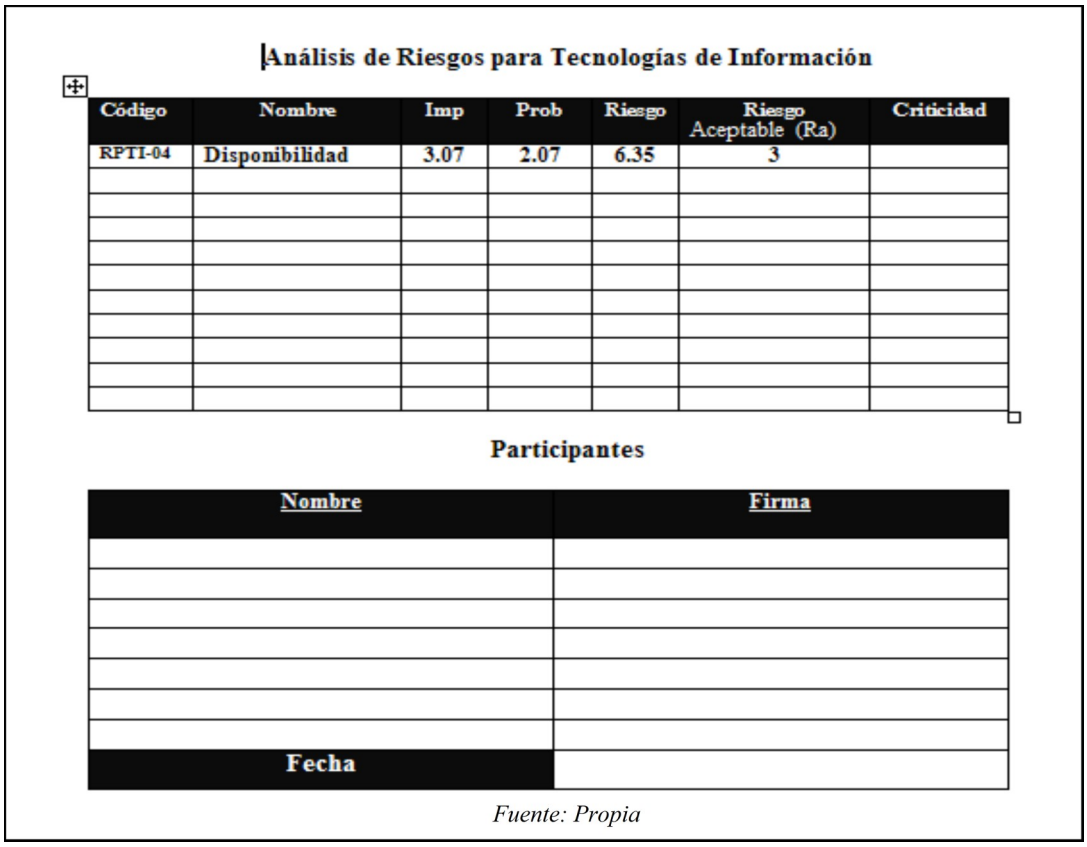
5. Entregar al facilitador del proceso de identificación de riesgos, los formularios MAR04, para que proceda a calcular los promedios de probabilidad de impacto de los riesgos seleccionados por los expertos.

6. El facilitador debe utilizar el formulario MAR03 para registrar los promedios de probabilidad e impacto por cada riesgo, así como el valor del riesgo que se calcula por la formula Vr= P*I, donde Vr es el valor del riesgo, P es el promedio de probabilidades, I es el promedio de impacto de ese riesgo. Este riesgo recibe el nombre de riesgo en ausencia de controles.

7. Declarar, en el formulario MAR03, el consenso de los participantes, el riesgo aceptable o los riesgos que la administración está dispuesta a aceptar.

El contenido del formulario MAR03 se observa a continuación.

Figura Nº 10. Imagen parcial formulario MAR03



Análisis de Riesgos para Tecnologías de Información

Código	Nombre	Imp	Prob	Riesgo	Riesgo Aceptable (Ra)	Criticidad
RPTI-04	Disponibilidad	3.07	2.07	6.35	3	

Participantes

Nombre	Firma
Fecha	

Fuente: Propia

8. El facilitador debe ordenar los riesgos en orden de criticidad descendente, según la siguiente tabla:

Tabla Nº 2. Criticidad de riesgos

Riesgo	Criticidad
1 - 5	Bajo
5 - 10	Medio
10 - 15	Alto

Fuente: RECOPE

El desarrollo de sistemas de información está caracterizado por una serie de procesos o etapas, conocidas como Ciclo de Vida de Desarrollo de Sistemas, en adelante CVDS.

El CVDS, al contar con varias etapas, proporciona a la metodología la posibilidad de aplicarse al nivel de una etapa. Por ejemplo, una etapa fundamental del CVDS es el mantenimiento de sistemas, en el cual se pueden realizar cambios a sistemas o incorporación de nuevos elementos al sistema.

3.4.2 Análisis de riesgos

El objetivo principal del análisis de riesgos en esta metodología es identificar la posibilidad de ocurrencia y su impacto en las etapas que conforman el CVDS o el proceso de adquisición de sistemas de información.

La metodología utiliza un análisis cuantitativo de riesgos, el cual se basa en la estimación de la magnitud de las consecuencias potenciales, de la probabilidad de que ellas ocurran y del nivel de riesgo asociado. Se determinan, además, los factores de riesgos que están presentes en cada una de las etapas y los controles asociados a cada factor de riesgo.

- Procedimiento para el Análisis de Riesgos

1. Para realizar el análisis, se debe seleccionar un grupo de expertos de tecnologías de información de la Institución, relacionados con los procesos de desarrollo y de adquisición de sistemas de información.

2. Con el criterio de los expertos, se establecen los nombres apropiados para los procesos de desarrollo y de adquisición de sistemas de información

3. Una vez establecidos los nombres, se registran en el formulario MAR06 y se indica, en él, el identificador o código de proceso (PR#), el nombre del proceso y la ponderación del proceso, respecto al riesgo.

Figura N°11. Imagen parcial formulario MAR06

Catálogo de Procesos Tecnologías de Información

Código	Proceso	Riesgo	Ponderación Pr
PR1	Desarrollo de Sistemas de Información		
PR2	Adquisición de Sistema de Infomación		
PR3	Mantenimiento Adaptativo		
PR4	Conversión		
PR5	Migración		
PR6	Interfaz		
PR7	Mantenimiento Correctivo		

Realizado por	**Fecha**
Aprobado por	**Fecha**

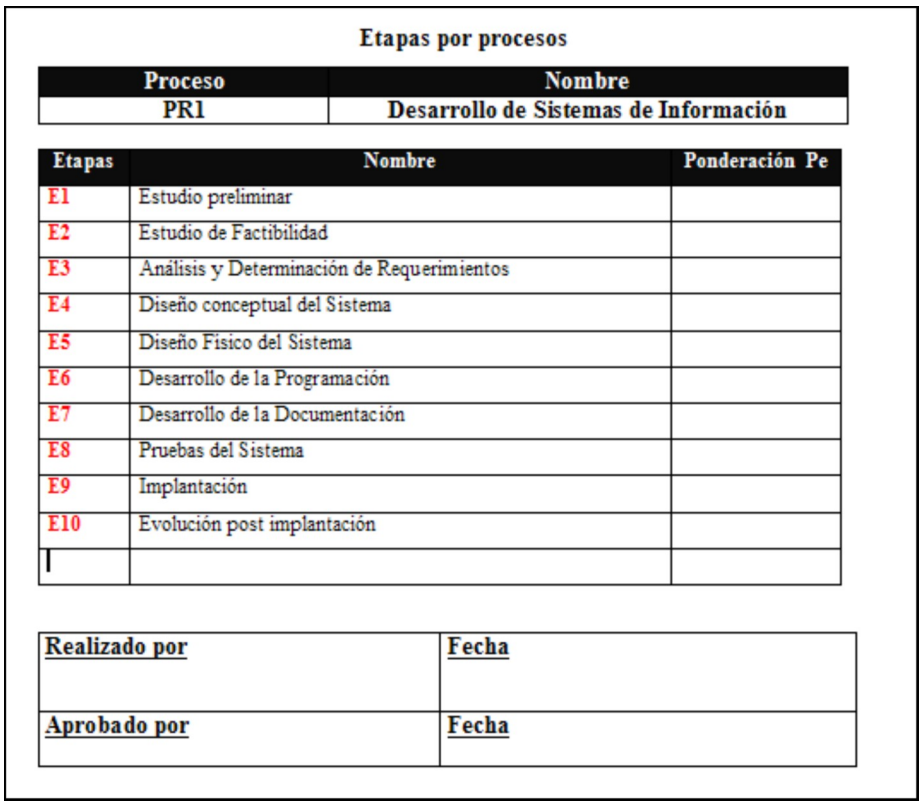
Fuente: Propia

4. Para cada uno de los procesos identificados en el formulario MAR06, deben detallarse las etapas que los constituyen y el promedio de la ponderación de cada una de estas etapas.

5. A cada uno de los expertos se le entrega una copia del formulario MAR07 para que proceda a estimar para cada etapa, la ponderación del impacto de ésta en el proceso.

   Seguidamente se observa el formato del formulario MAR07.

Figura Nº 12. Imagen parcial formulario MAR07



Etapas por procesos

Proceso	Nombre
PR1	Desarrollo de Sistemas de Información

Etapas	Nombre	Ponderación Pe
E1	Estudio preliminar	
E2	Estudio de Factibilidad	
E3	Análisis y Determinación de Requerimientos	
E4	Diseño conceptual del Sistema	
E5	Diseño Fisico del Sistema	
E6	Desarrollo de la Programación	
E7	Desarrollo de la Documentación	
E8	Pruebas del Sistema	
E9	Implantación	
E10	Evolución post implantación	

Realizado por	Fecha
Aprobado por	Fecha

Fuente: Propia

Como ejemplo de etapas del proceso de desarrollo de sistemas de información, se citan las etapas del CVDS presentes en el manual sobre normas de control interno relativas a sistema de información computadoriza, de la Contraloría General de la República de Costa Rica:

Tabla Nº 3. Etapas del Ciclo de Vida de Desarrollo de Sistemas

Etapas
Estudio preliminar
Estudio de factibilidad
Análisis y determinación de requerimientos
Diseño conceptual del sistema
Diseño físico del sistema
Desarrollo de la programación
Desarrollo de la documentación
Pruebas del sistema
Implantación
Evolución post implantación

Fuente: Manual sobre Normas técnicas de control interno relativas a los sistemas de información computadorizados

3.4.3 Evaluación de riesgos

A partir del análisis de riesgos, se deben identificar los factores de riesgo en cada una de las etapas y los controles existentes.

Cada control es, a su vez, evaluado para determinar su idoneidad, la cual está en función de aspectos como los siguientes:

- *Documentación*. Se refiere a que el control esté, adecuadamente, descrito en documentos apropiados, tales como manuales, procedimientos, instructivos.
- *Registro*. Se refiere a que exista evidencia, escrita que el control se ha realizado.
- *Efectividad*. Se refiere a que el control está implementado, y que, realmente, su aplicación disminuye la influencia del factor de riesgo.
- *Costo / Beneficio*. Se refiere a que cada control implementado produzca más beneficio que costo.

- **Procedimiento de evaluación del riesgo**

1. El grupo de trabajo formado por expertos debe identificar factores de riesgo por etapas del proceso de desarrollo o de adquisición de sistemas de información, es decir, circunstancias o situaciones que aumenten la probabilidad de que la amenaza se materialice en cada etapa.

   Como ejemplo de factores de riesgo para la etapa *Estudio preliminar* del Desarrollo de sistemas de información, se tiene:

   - Inadecuada selección de personal
   - Establecimiento de tiempo de duración impreciso
   - Desconocimiento del área de estudio
   - Falta de definición del problema específico
   - Desconocimiento de información sobre procedimientos actuales
   - Volumen de información impreciso
   - Fuentes de datos desconocidas
   - Tiempos entre la entrada de datos y las salidas no determinados

2. Mediante la utilización del formulario MAR10, se registran los factores de riesgo, así como los controles actuales que se utilizan para reducir el impacto del factor.

Factores de Riesgo por Etapas

Proceso	
PR1	DESARROLLO DE SISTEMAS DE INFORMACION
Etapa	
E1	ESTUDIO PRELIMINAR

Factor Riesgo	Pf	Control	Responsable	Documento	D	R	E	BC	Id

VF porcentaje de impacto del factor sobre el riesgo

Características del Control

D	Procedimientos del control documentados	25%
R	Se mantiene evidencia de la ejecución del control	25%
E	El control está integrado a procesos	25%
BC	La aplicación del control tiene más beneficio que costo	25%
Id	Porcentaje de Idoneidad del control	100%

Realizado por	**Fecha**
Aprobado por	**Fecha**

Fuente: Propia

3. Cada factor debe ponderarse respecto a la etapa, indicando con esto qué porcentaje de la etapa puede afectarse si el factor de riesgo se materializa.

4. Cada factor de riesgo puede tener uno o más controles, en algunos casos puede ser que el factor no tenga controles.

5. Para establecer la idoneidad de un control (porcentaje de reducción del control al factor de riesgo), se hace con las características de control, que se indican en el formulario MAR10, (véase Figura 13).

6. Completados los pasos anteriores, se procede a llenar la matriz de riesgos remanentes. Para este proceso se utiliza el formulario MAR11, que a continuación

MATRIZ DE RIESGOS REMANENTES

Riesgo	R	Ra	Proceso	Pr	Etapa	Pe	Factor	Pf	Control	Id	Rc	RR
R1	10	6	P1	60	E1	50	F1	75	C1	75	1.68	0.57
							F2	25	C2	100	0.75	0
					E2	25	F3	100	C3	100	1.50	0
					E3	25	F4	100	C4	50	0.75	0.75
	10										4.68	1.32

R = Valor del riesgo en ausencia de controles
Ra = Riesgo aceptable por la administración
Pr = Ponderación del proceso para el riesgo
Pe = Ponderación de la etapa en el proceso
Pf = Ponderación del factor en la etapa
Id = Idoneidad del control
Rc = Riesgo en presencia de controles
RR = Riesgo Remanente

Hecho por:_____

Aprobado por:_____

Fuente: Propia

7. Una vez completada la matriz es necesario realizar el registro de información en la aplicación informática para obtener los resultados de la evaluación.

3.4.4 Administración de riesgos

En la administración de riesgos se identifican, evalúan, seleccionan y ejecutan las medidas para los riesgos presentes en los procesos, la administración puede atender los riesgos, anularlos, modificarlos, prevenirlos, transferirlos y retenerlos. La retención de los riesgos consiste en no tomar ninguna de las medidas anteriores, y decidir afrontar las consecuencias del riesgo sobre los objetivos.

- **Procedimiento para la administración de riesgos**

Utilizando la información presente en la matriz de riesgos remanentes de la aplicación informática, se procede a identificar aquellos controles cuya idoneidad es menor al 100%, o ausencia completa de controles para factores de riesgo de una etapa en particular.

La matriz de la aplicación también permite visualizar aquellas etapas que no han sido adecuadamente cubiertas en su totalidad por medio de controles y a las cuales se debe prestar atención.

Para realizar el procedimiento para la administración de riesgos se deben seguir los siguientes pasos:

1. Obtener la lista de controles cuyo valor de idoneidad es menor al 100%
2. Obtener la lista de los riesgos cuyo valor de riesgo remanente en la matriz, es diferente de cero.
3. Con la información obtenida en los pasos 1 y 2 se debe redactar un informe para la administración respecto a los hallazgos obtenidos.
4. Considerando los criterios de aceptación de riesgo, aceptar riesgos residuales superiores al nivel mínimo deseado, que por los criterios definidos deben aceptarse en exposiciones superiores al nivel de confort.

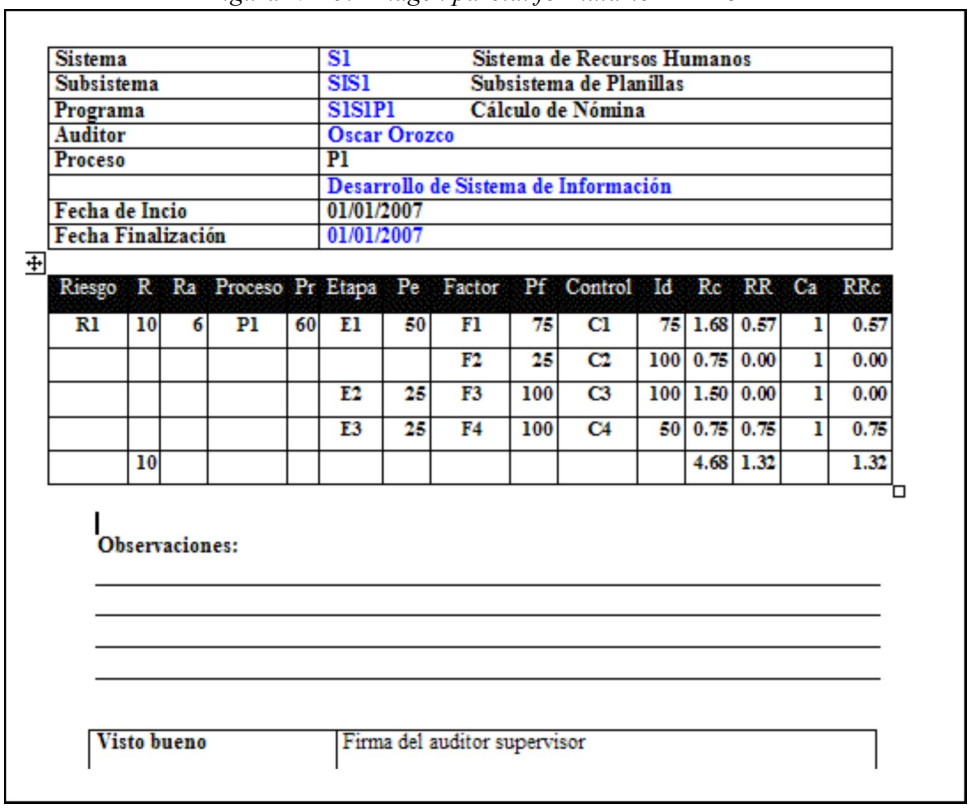
3.4.5 Proceso de revisión de riesgos

La revisión de riesgos es realizada por funcionarios de la auditoría interna de la institución, o puede ser realizada como una autoevaluación del Área de Asesoría en Tecnología Informática. Esta revisión consiste en verificar la efectividad de los controles existentes. La efectividad se evalua mediante criterios de efectividad previamente definidos por la auditoria interna, cuyos valores están en un rango de cero a uno, donde cero es el fallo completo de la efectividad y el valor uno la efectividad completa.

- Procedimiento para la revisión de riesgos

1. Ejecutar la aplicación informática y seleccionar la opción Revisión de riesgos. Escoger la opción Nueva revisión, que le muestra los controles que debe revisar y calificar. Así mismo con el formulario MAR13 se deja registro en papel de esta revisión. (figura N^{o} 15)

Figura Nº 15. Imagen parcial formulario MAR13



Sistema	S1	Sistema de Recursos Humanos
Subsistema	SIS1	Subsistema de Planillas
Programa	S1SIP1	Cálculo de Nómina
Auditor	Oscar Orozco	
Proceso	P1	
	Desarrollo de Sistema de Información	
Fecha de Incio	01/01/2007	
Fecha Finalización	01/01/2007	

Riesgo	R	Ra	Proceso	Pr	Etapa	Pe	Factor	Pf	Control	Id	Rc	RR	Ca	RRc
R1	10	6	P1	60	E1	50	F1	75	C1	75	1.68	0.57	1	0.57
							F2	25	C2	100	0.75	0.00	1	0.00
					E2	25	F3	100	C3	100	1.50	0.00	1	0.00
					E3	25	F4	100	C4	50	0.75	0.75	1	0.75
	10										4.68	1.32		1.32

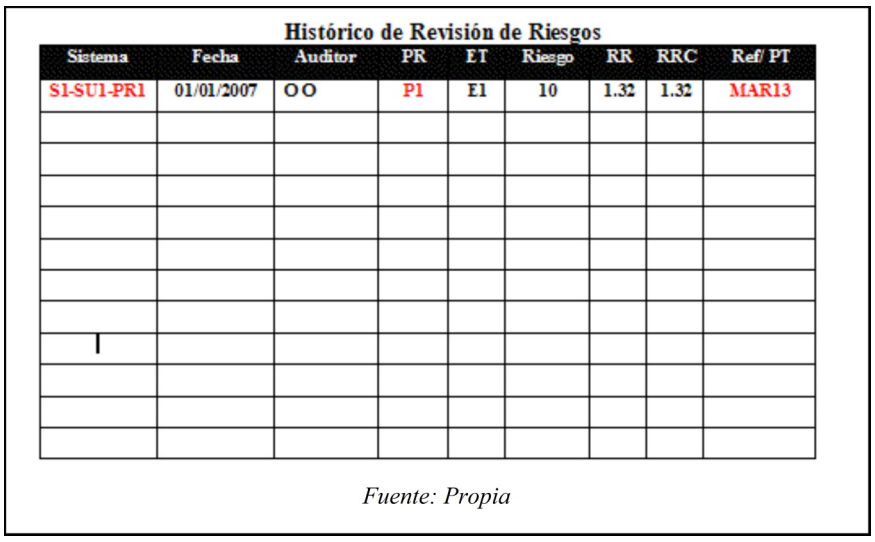
Observaciones:

Visto bueno	Firma del auditor supervisor

Fuente: Propia

2. Posterior a la utilización del formulario MAR13, se debe anotar en el formulario MAR12, el control de evaluaciones hechas, llamado Histórico de revisiones.

Figura Nº 16. Imagen parcial formulario MAR12



Histórico de Revisión de Riesgos

Sistema	Fecha	Auditor	PR	ET	Riesgo	RR	RRC	Ref/ PT
S1-SU1-PR1	01/01/2007	OO	P1	E1	10	1.32	1.32	MAR13

Fuente: Propia

El formulario MAR13 provee la información necesaria para generar informes sobre la administración de riesgos de desarrollo o de adquisición de sistemas de información en la institución.

Capítulo IV. Propuesta para mejorar la situación

Fundamentado teóricamente en el capítulo anterior, este proyecto ha contado con una serie de pasos muy importantes que se han llevado a cabo en conjunto con la institución patrocinadora. Cabe destacar la participación activa del Máster Óscar Orozco Rodríguez, quien fue el designado por la Institución para liderar la coordinación del proyecto.

Los controles de seguridad y su implantación requieren de una gestión de la organización, y la participación informada de todo el personal que trabaja con el sistema de información. Este personal es el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización, en general, del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos; exige una revisión periódica en la que se aprende de la experiencia y se adapta a nuevas tecnologías, porque los sistemas de información están en evolución continua, tanto propia como del entorno.

A partir de esta experiencia, se da un detalle del proceso y su implementación. Una vez que se conoce a la persona encargada de coordinar dentro de la Institución, se establece el cronograma de trabajo y se programan tres talleres, los que se describen a continuación.

4.1 Primer taller

- **Nombre**

  Introducción a la Administración de riesgos en Tecnologías de Información

- **Participantes**

  Funcionarios del Área de Asesoría en Tecnología Informática, Presidencia y Subauditoría técnica.

- **Temas tratados**
  - Marco legal para la administración de riesgos
  - Administración de riesgos
  - Ciclo de vida de desarrollo de sistemas
  - Estructuras de riesgos en tecnologías de información

- **Formularios utilizados**
  - MAR01 Control de formularios
  - MAR02 Estructura de riesgos institucionales TI
  - MAR03 Análisis de riesgos
  - MAR04 Análisis de riesgos por expertos
  - MAR05 Parámetros de valoración de probabilidad e impacto
  - MAR06 Catálogo de procesos de tecnología de información
  - MAR07 Etapas por procesos

- **Resultados obtenidos**
  - Estructuras de riesgos de TI

    Se establecen los riesgos para TI con su código.

Tabla Nº 4. Análisis de riesgos para TI

Código	Nombre	Impacto	Probabilidad	Riesgo
RPTI-01	Relevancia	2.727	1.636	4.461
RPTI-02	Integridad de la información	3.455	2	6.909
RPTI-03	Acceso	2.636	1.818	4.793
RPTI-04	Disponibilidad	3.364	2.182	7.339
RPTI-05	Infraestructura tecnológica	3.818	2.273	8.678

Fuente: Taller 1

  - Selección de riesgos por administrar

Catálogo de procesos de tecnología de información, respecto a los riesgos cuyo valor es mayor o igual a siete (véase *Tabla Nº 2. Criticidad de riesgos)*

Tabla Nº 5. Riesgos a administrar en TI

Código	Nombre	Riesgo
RPTI-05	Infraestructura tecnológica	8.678
RPTI-04	Disponibilidad	7.339
RPTI-02	Integridad de la información	6.909

Fuente: Taller 1

- Definición de las etapas que comprenden el desarrollo y adquisición de sistemas de información.

Tabla Nº 6. Etapas CVDS

Etapa	Nombre
E1	Estudio preliminar
E2	Estudio de factibilidad
E3	Análisis y determinación de requerimientos
E4	Diseño conceptual del sistema
E5	Diseño físico del sistema
E6	Desarrollo de la programación
E7	Desarrollo de la documentación
E8	Pruebas del sistema
E9	Implantación
E10	Evolución post-implantación

Fuente: CVDS

4.2 Segundo taller

- **Nombre**

Ponderación de procesos y etapas del desarrollo y adquisición de sistemas de información respecto a los riesgos seleccionados por la administración

- **Participantes**

Funcionarios del Área de Asesoría en Tecnología Informática y Subauditoría técnica

- **Temas tratados**
  - Declaración del riesgo aceptado por la administración
  - Ponderación de procesos, respecto de los riesgos seleccionados para administrar
  - Ponderación de las etapas que constituyen los procesos de desarrollo y de adquisición de sistemas de información

- **Formularios utilizados**
  - MAR03 Análisis de riesgos

- MAR06 Catálogo de procesos de tecnología de información
- MAR07 Etapas por procesos

- **Resultados obtenidos**
  - Declaración del riesgo aceptado por la administración

Tabla Nº 7. Riesgo aceptado

Código	Nombre	Riesgo	Aceptado
RPTI-05	Infraestructura tecnológica	8.678	4
RPTI-04	Disponibilidad	7.339	3
RPTI-02	Integridad de la información	6.909	3

Fuente: Expertos TI RECOPE

  - Ponderación de los procesos de desarrollo y de adquisición de sistemas de información, en los riesgos seleccionados por la administración

Tabla Nº 8. Ponderación de procesos

Procesos: Desarrollo y adquisición de sistemas de información		
Código	Nombre	Ponderación
RPTI-05	Infraestructura tecnológica	30%
RPTI-04	Disponibilidad	60%
RPTI-02	Integridad de la información	50%

Fuente: Taller 2

  - Ponderación de las etapas que constituyen los procesos de desarrollo y de adquisición de sistemas de información

Tabla Nº 9 Etapas CVDS y su ponderacuón

Etapa	Nombre	Ponderación
E1	Estudio preliminar	6.66
E2	Estudio de factibilidad	6.66
E3	Análisis y determinación de requerimientos	26.66
E4	Diseño conceptual del sistema	8.33
E5	Diseño físico del sistema	6.66
E6	Desarrollo de la programación	11.66
E7	Desarrollo de la documentación	5
E8	Pruebas del sistema	13.33
E9	Implantación	8.33

E10	Evolución post-implantación	6.66

Fuente: Taller 2

4.3 Tercer taller

- **Nombre**

Determinación de factores de riesgo y controles en las etapas de los procesos de desarrollo y de adquisición de sistemas de información

- **Participantes**

Funcionarios del Área de Asesoría en Tecnología Informática y Subauditoría técnica

- **Temas tratados**
  - Determinación y ponderación de factores de riesgos para las etapas de los procesos de desarrollo y de adquisición de sistemas de información
  - Determinación y ponderación de controles existentes
  - Análisis de idoneidad de cada control
  - Evaluación de la efectividad de los controles

- **Formularios utilizados**
  - MAR10 Factores de riesgo por etapa
  - MAR11 Matriz de riesgos remanentes
  - MAR12 Histórico de revisiones de riesgos
  - MAR13 Revisión de riesgos
  - MAR15 Factores de riesgo de desarrollo y de adquisición de sistemas de información

- **Resultados obtenidos**
  - Factores de riesgos por etapas y sus correspondientes controles
  - Matriz de riesgos remanentes

4.4 Resultados generales

El trabajo realizado en los talleres ha permitido poner a prueba los formularios diseñados como parte de la metodología y cuya información es un insumo para la aplicación informática que brinda los siguientes resultados:

- Análisis de riesgo remanente
- Controles sujetos a mejoras
- Situación actual de los riesgos
- Riesgos no cubiertos
- Análisis de efectividad de los controles

Capítulo V. Conclusiones

5. 1 Cumplimiento de objetivos

A partir del trabajo desarrollado en la Refinadora Costarricense de Petróleo, en este capítulo se plasman las conclusiones que se obtienen una vez cumplidos los objetivos propuestos para este proyecto. Es importante resaltar que se ha desarrollado e implementado la metodología, junto con su correspondiente manual, el cual ha sido utilizado en los talleres, así como la aplicación informática para facilitar los procesos de administración de riesgo en el desarrollo y la adquisición de sistemas de información, con los siguientes resultados:

1. Con la información derivada de los talleres realizados, se crea el *inventario de riesgos*, el cual contempla no solamente datos respecto a la estructura de riesgos de tecnologías de información, sino, también, datos sobre los principales procesos que conforman esa área, específicamente de desarrollo y adquisición de sistemas de información. Además, se registra información sobre las etapas que conforman el ciclo de vida de desarrollo de sistemas, los factores de riesgos que afectan estas etapas y los diferentes controles con que se cuenta por parte de la Institución para mitigar los factores de riesgo.

El inventario de riesgos se implementa, también, en una base de datos relacional en la aplicación informática como se muestra en la figura Nº17, en la que se observan los diferentes riesgos que conforman la estructura de riesgos del Área de Asesoría en Tecnologías de Información. En esta figura se muestran los riesgos más significativos seleccionados por los expertos.

Figura Nº 17. Imagen parcial aplicación informática, Estructura de riesgos de TI

Código		Riesgo (Impacto, Probabilidad)
R2	Integridad	6.91
R4	Disponibilidad	7.34
R5	Infraestructura Tecnológica	8.678

Fuente: Propia

2. Se desarrolla e implementa un procedimiento para el análisis de los riesgos identificados y registrados en el ***inventario de riesgos***, el cual se pone en práctica en el taller de análisis de riesgos. Como resultado del análisis de riesgos se obtienen los valores de impacto y probabilidad de los riesgos, además de la ponderación o peso de cada etapa del ciclo de vida de desarrollo de sistemas, tal como se muestra en la figura Nº18. Esta información se registra en la base de datos de la aplicación informática, para ser utilizada, posteriormente, en otros talleres y etapas de la metodología.

Figura Nº 18. Imagen parcial aplicación informática, Peso por etapa

Fuente: Propia

3. Se implementa un procedimiento para la ***evaluación de los riesgos*****,** en él se establecen los diferentes parámetros de evaluación; se utiliza, también, información sobre la cuantía el riesgo que la administración está dispuesta a aceptar. Se establecen los parámetros para la evaluación de los controles y, con la colaboración de los funcionarios de la Institución, se procede a evaluarlos. La información obtenida se anota en los formularios respectivos y, posteriormente, se registra en la base de datos de la aplicación informática. Para este procedimiento, se elabora una lista de factores de riesgos para las etapas del ciclo de vida del desarrollo de sistemas, estos factores se agrupan en factores genéricos para facilitar su comprensión, y se ponderan los factores de riesgo en cada una de las etapas. Un ejemplo de esto se muestra en la siguiente figura Nº 19, en la que se observa que para la etapa E1, se cuenta con cuatro factores de riesgo, cada uno con un peso de un 25% en la etapa.

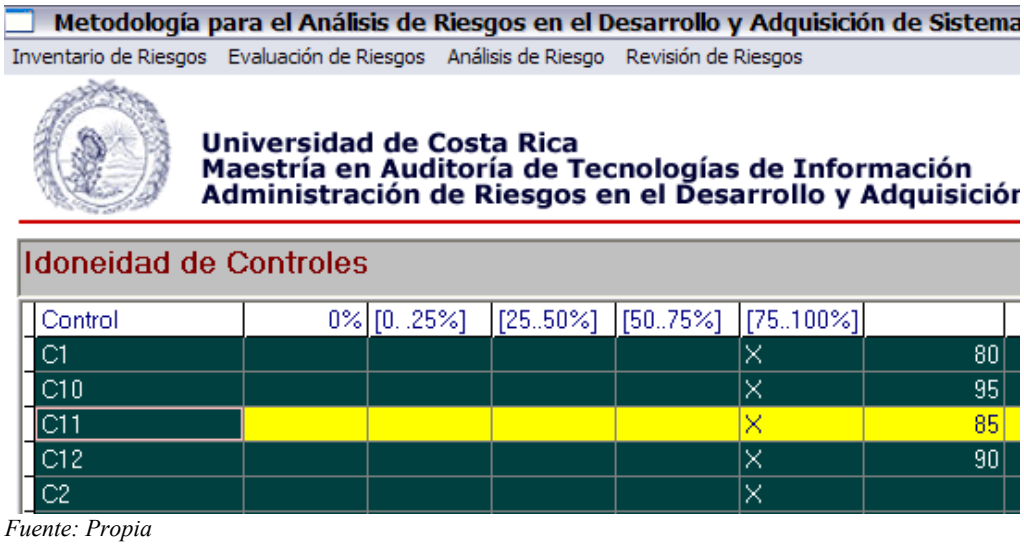
Figura Nº 19. Imagen parcial aplicación informática, Factores de riesgos por etapas

Etapa	Factor	Pf	
E1	F1	25	
E1	F2	25	
E1	F3	25	
E1	F4	25	
E10	F1	50	
E10	F4	50	

Fuente: Propia

4. Se desarrolla e implementa un procedimiento de ***tratamientos de riesgos***, con base en la información obtenida sobre riesgos que no están cubiertos por los controles y sobre controles que no son idóneos. La aplicación informática provee esta información, mediante consultas específicas, como se muestra en la siguiente figura Nº 20, en la cual está marcado el control 11, el que posee una idoneidad del 85%.

Figura Nº 20. Imagen parcial aplicación informática, Idoneidad de los controles



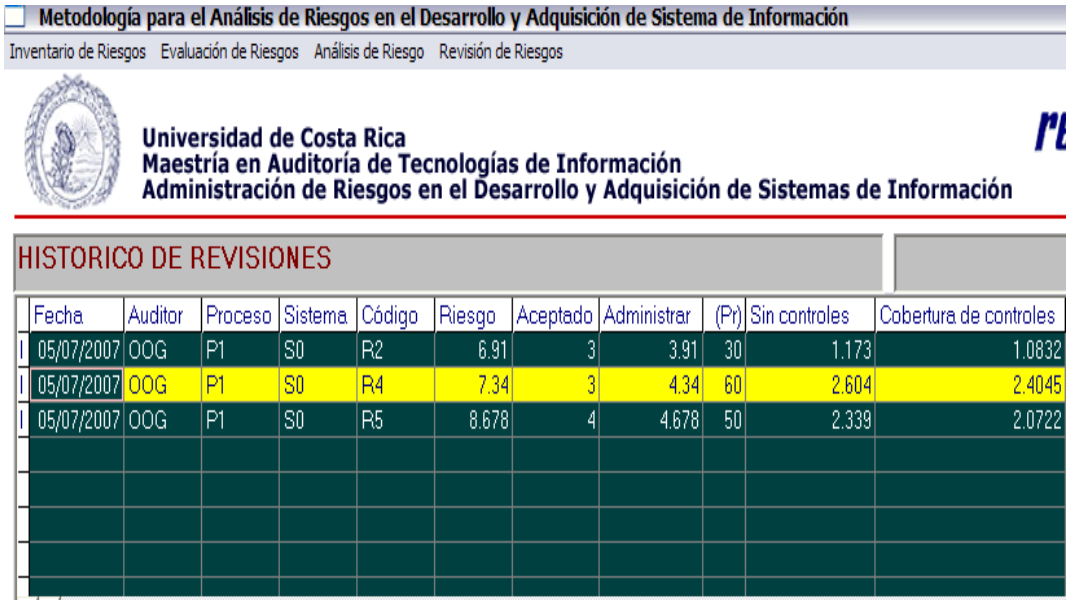
Control	0%	[0..25%]	[25..50%]	[50..75%]	[75..100%]	
C1					X	80
C10					X	95
C11					X	85
C12					X	90
C2					X	

Fuente: Propia

La información anterior ayuda al funcionario responsable de la administración de riesgos a preparar un informe sobre controles que están sujetos a mejoras, dirigido a la administración, con el propósito de que se tomen las acciones respectivas.

5. Para el procedimiento de ***revisión de riesgos***, se implementa una opción en la aplicación informática, la cual permite, en forma automática, la creación de una plantilla de revisión. Ésta indica los controles que se deben revisar para todas las etapas del ciclo de vida de desarrollo de sistemas de información. Se lleva un archivo histórico de todas las revisiones que se han hecho, en el que se muestran los resultados obtenidos y los problemas presentados. La información puede ser accesada en cualquier momento y sirve como apoyo para futuras revisiones. Una muestra de esta información se puede observar en la figura Nº 21, la cual contiene el resumen de una revisión

Figura Nº 21. Imagen parcial aplicación informática, Histórico de revisiones



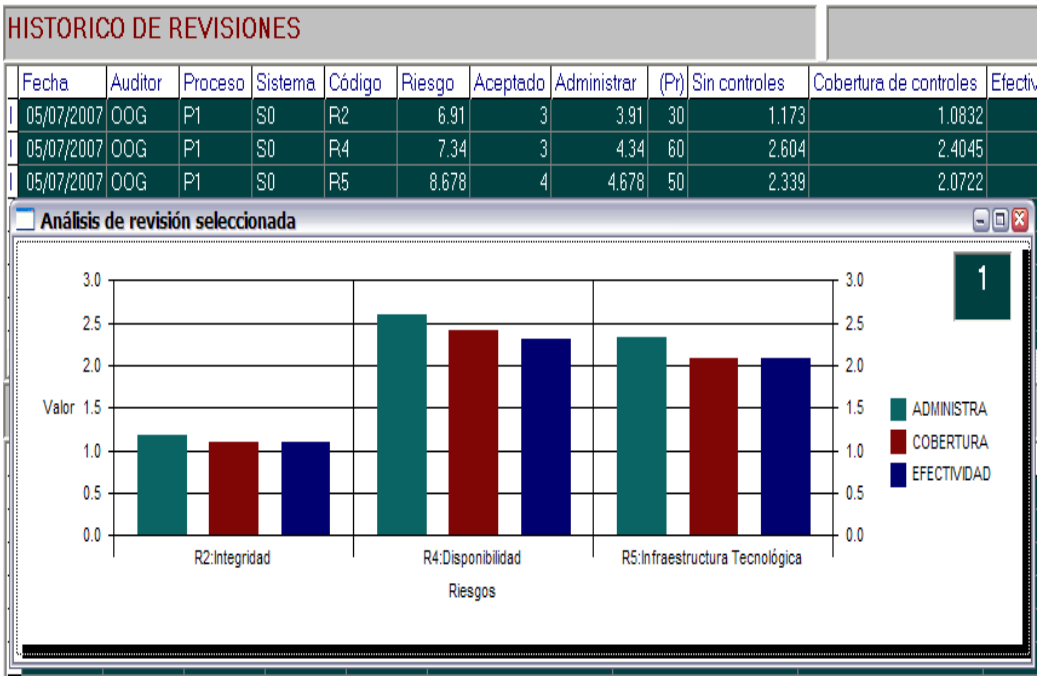
Fecha	Auditor	Proceso	Sistema	Código	Riesgo	Aceptado	Administrar	(Pr)	Sin controles	Cobertura de controles
05/07/2007	OOG	P1	S0	R2	6.91	3	3.91	30	1.173	1.0832
05/07/2007	OOG	P1	S0	R4	7.34	3	4.34	60	2.604	2.4045
05/07/2007	OOG	P1	S0	R5	8.678	4	4.678	50	2.339	2.0722

Fuente: Propia

De este resumen se obtiene información respecto a la fecha, al auditor a cargo, al proceso y al sistema evaluado, al riesgo que se revisa, al riesgo presente y al riesgo que la administración acepta, a la ponderación del proceso en el riesgo, al riesgo sin aplicar controles y a la cobertura de los controles, en caso de que ninguno falle. Puede obtenerse información más detallada de cualquiera de las revisiones.

6. ***La documentación*** relacionada con el proceso de administración de riesgos, se registra en formularios y en la base de datos de la aplicación informática, lo que permite obtener información histórica de revisiones y facilita la elaboración de informes hacia la administración, hacer análisis más elaborados en forma rápida y de fácil comprensión. Una muestra de esto se observa en la figura Nº 22, en la que se grafica, por medio de la aplicación informática, el resultado de la revisión.

Figura Nº



Fuente: Propia

En esta figura se observan, en forma gráfica, los resultados de la revisión. En este caso, en particular, se trata de una revisión efectuada el día 7 de mayo de 2007, por el auditor OOG, para el proceso P1 Desarrollo y adquisición de sistemas de información. En la revisión se obtienen resultados sobre el riesgo en ausencia de controles y la cobertura de ellos. Por ejemplo, en el caso del riesgo R4, el cual, en ausencia de controles es 2.604. Si se aplican los controles actuales, se obtiene como resultado un valor de 2.404; esto debido a que algunos controles no son completamente idóneos e, inclusive, no existen controles para algunos factores y etapas del proceso.

5.2 Análisis de los resultados

1. La creación de un inventario de riesgos, la capacitación suministrada a los funcionarios en los talleres y las actividades realizadas, fomentan una disposición al cumplimiento de la normativa de control interno, relativa a los sistemas de información y al establecimiento del sistema específico de valoración de riesgos, por parte del Área de Asesoría en Tecnología Informática de RECOPE.

2. Como cumplimiento a la normativa sobre control interno, relativa a los sistemas de información, la Institución ha adoptado como metodología de desarrollo el ciclo de vida de desarrollo de sistemas y sus correspondientes etapas, las cuales son insumos esenciales en la metodología de administración de riesgos

3. En la identificación y el análisis de riesgo no se detectan riesgos altos; sin embargo, se identifican tres riesgos de criticidad media, los cuales se trabajan a lo largo de talleres y reuniones. De igual forma, se estableció la ponderación del proceso de desarrollo y de adquisición de sistemas de información, con respecto a cada uno de estos riesgos, sus respectivas etapas y los factores de riesgo en cada una de ellas.

4. La administración entrega la lista de controles actuales para cada factor, los cuales son calificados según los criterios de idoneidad. Como resultado de esta calificación, se observan controles que no son del todo idóneos y están sujetos a mejoras; de igual forma, se observan algunos factores que no tienen control e, inclusive, una etapa que no cuenta con controles.

5. Se logró integrar en una misma herramienta de evaluación, la valoración de la efectividad del control y la valoración del riesgo, componentes que se han venido evaluando en forma separada por la mayoría de instituciones del sector público.

6. Surgieron expectativas tanto del área de auditoría interna como de la Administración, con respecto a la posibilidad de implantar la presente metodología a

otros procesos de Tecnología Informática y otras áreas de la empresa como la evaluación de procesos de la Gerencia de Comercio Internacional y Desarrollo.

5. 3 Recomendaciones

Con base en la experiencia de la implementación de esta metodología, en la Refinadora Costarricense de Petróleo S.A. se puede recomendar:

1. Revisar el Manual para el proceso de desarrollo de sistemas de información que se utiliza actualmente en la Institución, con el propósito de incorporar elementos respecto a riesgos y controles, en cada una de las etapas del ciclo de vida de desarrollo de sistemas de información.

2. Cada control por utilizar en las etapas del ciclo de vida del desarrollo de sistemas, debe contar con su correspondiente registro. La forma y el contenido del registro debe hacerse utilizando criterios de calidad, para lo cual es conveniente contar con el apoyo del área de Aseguramiento de Calidad de la Institución. De igual forma, debe establecerse el procedimiento de administración de estos registros, para garantizar su uso correcto.

3. Una vez revisados y aceptados los controles y sus correspondientes registros, se deben incorporar a la base de datos de la aplicación informática para actualizar la información.

4. Es necesario que se establezca un cronograma de revisiones anuales, con base en la metodología y la aplicación informática. En estas revisiones, se verifica la idoneidad y la efectividad de los controles, con el propósito de informar a la administración sobre su cumplimiento, para que se tomen las medidas respectivas.

5. Las áreas de tecnologías de información, en esta u otra Institución, poseen varios procesos; no obstante, el alcance de la metodología implementada es exclusiva para los procesos de desarrollo y de adquisición de sistemas de información, ésta puede aplicarse a otros procesos.

6. Para aplicar la presente metodología a otros procesos, es necesario hacer una revisión detallada de ellos, tal y como se hizo con los procesos de desarrollo y de adquisición de sistemas de información. Se deben establecer las etapas que conforman el proceso, los factores de riesgo de cada etapa y los controles respectivos.

7. Adoptar por parte del Área de Tecnología Informática una cultura de calidad en el proceso de desarrollo y adquisición de sistemas de información, partiendo de la base que toda actividad deberá están debidamente documentada.

8. Que la Asesoría en Tecnología Informática de RECOPE continúe los esfuerzos iniciados con el presente proyecto, a fin de lograr definir el resto de los procesos que conforman esa área y adaptar la presente metodología de valoración de riesgos a ellos.

Referencias bibliográficas

Delgado R., X. (1997). *Auditoría en Informática.* San José: Costa Rica: EUNED.

Derrien, Y. (1993). *Técnicas de la Auditoría informática.* México: AlfaOmega.

Echenique García, J. (2001). *Auditoría en Informática***.**.(2ª ed.).
México: Editorial McGraw Hill.

Fairley, R. (1994). *Ingeniería de software*. México, Editorial McGraw-Hill.

Fitzgerald, J. (1992). *Controles internos para sistemas de Computación.*
México: Editorial Limusa.

Galway, L. (February, 2004) Quantitative Risk Analysis for Project Management: A critical review. *RAND Corporation working paper*.

González, C. (1996). *Sistemas de base de datos.*
Cartago: Editorial Tecnológica de Costa Rica..

Korth, H. (1993). *Fundamentos de bases de datos*. (2ª ed.).
México: Editorial McGraw-Hill.

Laudon, K. (1996). *Administración de los sistemas de información*. (3 ª ed.),
México: Prentice Hall Hispanoamericana.

Muñoz Razo, C. (2002). *Auditoría en sistemas computacionales.*
México: Pearson Educación.

Pressman, R. (2001). *Ingeniería de software. Un enfoque práctico***.**
(4th ed.) México: Editorial McGrawHill.

Senn, J. A. (1992). *Análisis y diseño de sistemas de información.*
(2ª ed.). México:Editorial McGrawHill.

Anexo I. Formularios usados en la metodología