

Instituto Costarricense sobre Drogas

Proceso Continuo e Integrado para la Gestión del Riesgo

Metodología

Proceso Continuo e Integrado para la Gestión del Riesgo

ICD/UI-EI-002:2007

Descripción del documento

Institución: Instituto Costarricense sobre Drogas
Documento: Proceso Continuo e Integrado para la Gestión del Riesgo
Unidad: Unidad de Informática
Elaborado por: Ing. Felipe Ramírez Herrera
Fecha: Enero, 2007
Versión: 1.5

Contenido

1	Presentación	5
2	Alcances del estándar	5
3	Principios básicos	5
3.1	Adaptabilidad	6
3.2	Agilidad	6
3.3	Potenciar la comunicación.....	6
3.4	Aprender de todas las experiencias	7
3.5	Responsabilidad compartida.....	7
4	Proceso de gestión de riesgos	8
4.1	Definición de riesgo	8
4.2	Descripción del proceso	10
4.2.1	Establecer el contexto.....	10
4.2.2	Identificación de las fuentes de riesgo y taxonomías.....	12
4.2.3	Identificación de riesgos	16
4.2.4	Análisis de riesgos	20
4.2.5	Tratamiento de los riesgos.....	29
4.2.6	Monitoreo y revisión	35
4.2.7	Comunicación y consulta	36
4.3	Documentación.....	37
4.3.1	Razones para la documentación.....	37
5	Referencias bibliográficas	40
6	Esquema de la gestión de riesgos	42

1 Presentación

El presente documento contiene el estándar de gestión de riesgos y vulnerabilidades del Instituto Costarricense sobre Drogas.

Este documento presenta la información básica sobre la administración de riesgos que describe los principios, conceptos, recomendaciones y la definición de un proceso formal dividido en seis etapas para administrar los riesgos de forma exitosa para los proyectos y procesos ejecutados por la unidad de tecnología de la información.

2 Alcances del estándar

Este estándar provee un marco conceptual y orientador para el establecimiento e implementación del proceso continuo e integrado de la gestión del riesgo involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.

3 Principios básicos

El estándar de gestión de riesgos propuesto en este documento se basa en la noción de que los riesgos deben tratarse de forma proactiva, que la administración de riesgos forma parte de un proceso formal y sistemático que debe considerarse como una iniciativa positiva.

3.1 Adaptabilidad

La adaptabilidad es una respuesta de comportamiento que permite reaccionar ante hechos que se producen en el entorno y retroalimentar el sistema creando nuevas bases de comportamiento.

3.2 Agilidad

Las actividades relacionadas con la gestión de riesgos no deben limitarse a una única fase del ciclo de vida de un proyecto o una revisión aislada en la etapa inicial de un proceso.

La agilidad exige que el equipo de trabajo valore ininterrumpidamente y administre proactivamente los riesgos durante todas las etapas de un proceso o durante el ciclo de vida de un proyecto porque los continuos cambios en todas las facetas del proyecto significan que los riesgos también están cambiando.

Un enfoque proactivo permite que el equipo acepte el cambio y lo convierta en una oportunidad, evitando así que se vuelva en su contra.

3.3 Potenciar la comunicación

Este principio señala que los riesgos deben ser discutidos de forma abierta, tanto dentro del equipo como con los interesados externos.

Todos los integrantes del equipo de trabajo deben participar en la identificación y análisis de los riesgos. La Dirección General y las jefaturas deben evitar que los riesgos se perciban como algo negativo y animar al personal a que siga este comportamiento.

El personal no debe tener reservas para comunicar sus opiniones con libertad para, de esta forma, evaluar con más precisión el estado del proyecto o proceso y tomar decisiones consensuadas entre los miembros del equipo y los patrocinadores.

3.4 Aprender de todas las experiencias

El aprendizaje puede ayudar a mejorar los resultados. El conocimiento obtenido durante la ejecución de un proceso o proyecto puede reducir la incertidumbre de la toma de decisiones en otros procesos o proyectos cuando la información es poco fiable.

Por este motivo, en el proceso de administración de riesgos incorpora actividades relacionadas con la comunicación y documentación. El análisis directo de los resultados de resultados anteriores fomenta el aprendizaje dentro del equipo mediante el intercambio de opiniones entre los miembros del equipo.

3.5 Responsabilidad compartida

No hay ninguna persona que sea “propietaria” de la gestión de riesgos, la participación activa en el proceso es responsabilidad de todo el personal.

Los funcionarios de una unidad tienen asignadas tareas específicas para analizar los riesgos en el marco de planeamiento general del proyecto o el esquema de responsabilidad definido para los procesos operativos y estratégicos, y cada uno de ellos se responsabiliza de llevarlas a cabo. Las actividades pueden afectar a todas las áreas del proyecto durante todas las fases de los ciclos del proyecto y del proceso de administración de riesgos. Estas actividades van desde la identificación de riesgos en áreas de experiencia o responsabilidad personal hasta el análisis de riesgos, la valoración de riesgos y la ejecución de tareas de control de riesgos durante la ejecución de las actividades de la unidad.

La jefatura de cada unidad se responsabiliza de la organización del equipo de trabajo en las actividades de gestión de riesgos y que dichas actividades se incorporan en todos los procesos.

4 Proceso de gestión de riesgos

De acuerdo con el *Project Management Body of Knowledge (PMBOK® 2004)*, la gestión del riesgo es “el proceso sistemático de identificar, analizar y responder a un riesgo de un proyecto, proceso o programa”.

La gestión del riesgo incluye maximizar la probabilidad y consecuencias de eventos positivos y minimizar la probabilidad y consecuencias de eventos adversos a los objetivos de proyectos, procesos o programas.

4.1 Definición de riesgo

Un riesgo constituye es:

“un evento (o condición) con cierta incertidumbre y si éste ocurre tiene un efecto positivo o negativo en los objetivos del proyecto. Un riesgo tiene una causa y, en caso de ocurrencia, también implica una consecuencia” (PMBOK 2004).

Un riesgo implica simultáneamente amenazas a los objetivos de un proyecto/proyecto y a la vez oportunidades para mejorar dichos objetivos. Los riesgos tienen su origen en la incertidumbre que está presente en todos los proyectos y en general en la ejecución y gestión de los procesos operativos.

Los riesgos conocidos son aquellos que han sido identificados y analizados, es posible establecer un plan específico para atenderlos. Obviamente, los riesgos desconocidos no pueden ser administrados, no obstante, las jefaturas y encargados de procesos pueden encaminar este tipo de riesgos mediante un plan de contingencia basado en experiencias previas con circunstancias similares.

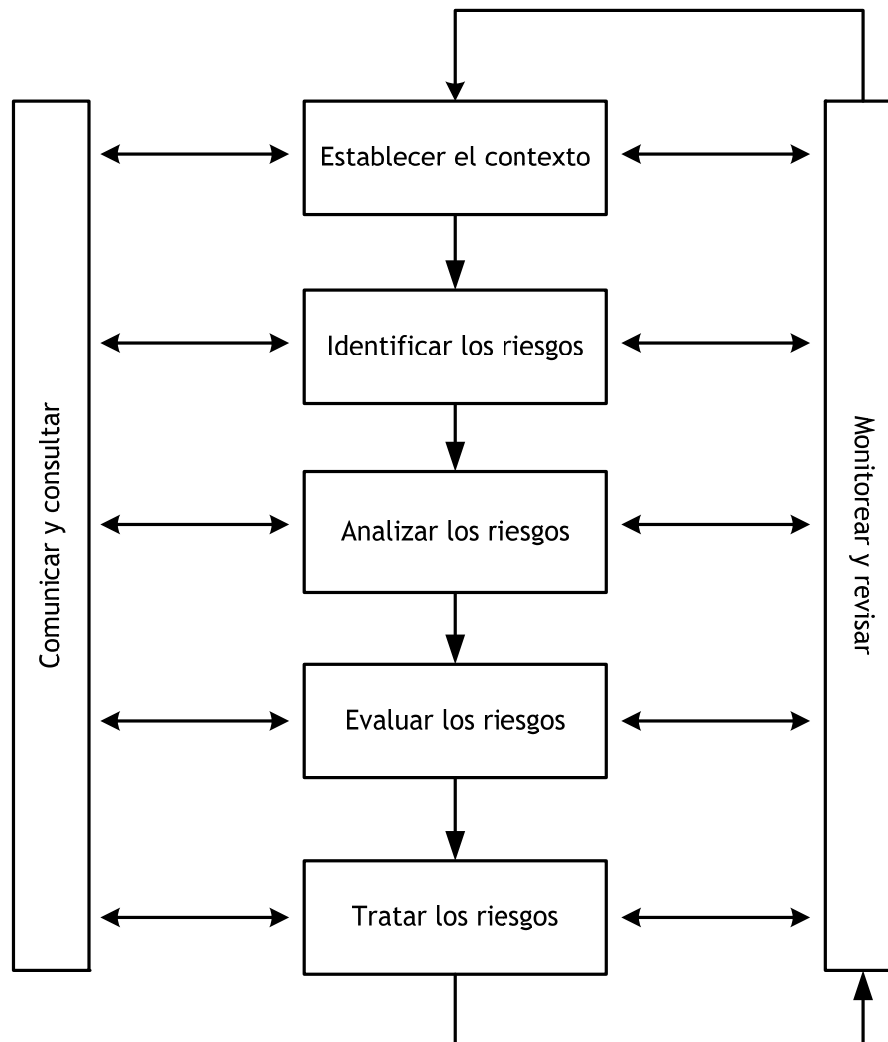
A nivel organizacional, los riesgos son vistos como amenazas al éxito de los proyectos. Los riesgos que son considerados como amenazas pueden ser aceptados si estos están en balance con un beneficio que se obtiene al tomar dichos riesgos (ej. reducción de tiempos y costos). Por su parte, los riesgos que se perciben como oportunidades se persiguen para el beneficio de los objetivos operacionales de la unidad.

Para el éxito, la organización debe estar comprometida a aplicar la administración de riesgos a lo largo de todos sus procesos y proyectos. Una medida del compromiso organizacional es su dedicación a reunir datos detallados sobre los riesgos y su caracterización.

La gestión de riesgos es una parte integral del proceso de administración. La gestión de riesgos es un proceso multifacético, llevado a cabo a menudo por un equipo multidisciplinario. Es un proceso iterativo de mejora continua.

4.2 Descripción del proceso

Gráficamente el proceso de la gestión del riesgo está configurado de la siguiente manera:



4.2.1 Establecer el contexto

Deben identificarse y documentarse las metas, objetivos, estrategias, alcance y parámetros de la actividad, o parte de la organización a la cual se está aplicando el proceso de gestión de riesgos. El proceso debería ser llevado a cabo con plena consideración de la necesidad de balancear costos, beneficios y oportunidades.

También deberían especificarse los recursos requeridos y los registros que se van a llevar.

Establecer el alcance y los límites de una aplicación del proceso de administración de riesgos involucra:

- a) Definir el proyecto o proceso y establecer sus metas y objetivos.
- b) Identificar las etapas o fases del proyecto o el proceso administrado y sus respectivos hitos.
- c) Definir las actividades que constituyen cada una de las etapas/fases considerando:
 - Roles y responsabilidades de las distintas partes de la organización que participan en la administración de riesgos.
 - Los artefactos de las actividades.
 - Las relaciones entre el proyecto y otros proyectos o partes de la organización.
 - Elementos o atributos de incertidumbre susceptibles a riesgos.
 - Documentación de las tareas/procedimientos de cada una de las actividades.
- d) Estimar las principales variables de control del proceso o proyecto.
- e) Elaborar un inventario de las fuentes genéricas de riesgo y las áreas de impacto aplicables al proceso o proyecto.

4.2.2 Identificación de las fuentes de riesgo y taxonomías

4.2.2.1 Fuentes genéricas de riesgo

La identificación de fuentes de riesgo y áreas de impacto provee una estructura para identificación y análisis de riesgos. A raíz de la gran cantidad potencial de fuentes e impactos, desarrollar una lista genérica focaliza las actividades de identificación de riesgos y contribuye a una administración más efectiva.

Las fuentes de riesgo y áreas de impacto genéricas son seleccionadas de acuerdo a su relevancia para la actividad bajo estudio.

Los componentes de cada categoría genérica pueden formar la base para un estudio completo de riesgos.

Cada fuente genérica tiene numerosos componentes, cualquiera de los cuales pueden dar lugar a un riesgo. Algunos componentes estarán bajo control de la organización que realiza el estudio, mientras que otros estarán fuera de su control. Cuando se identifican los riesgos se necesita considerar a ambos tipos. Las fuentes genéricas de riesgo incluyen:

- a) **Relaciones comerciales y legales:** entre la organización y otras organizaciones (por ejemplo proveedores, subcontratistas y arrendatarios).
- b) **Circunstancias económicas:** De la organización, país, internacionales, como asimismo factores que contribuyen a esas circunstancias (por ejemplo tipos de cambio).
- c) **Comportamiento humano:** Tanto de los involucrados en la organización como de los que no lo están.
- d) **Eventos naturales.**
- e) **Circunstancias políticas:** Incluyendo cambios legislativos y factores que pudieran influenciar a otras fuentes de riesgo.
- f) **Aspectos tecnológicos y técnicos:** Tanto internos como externos a la organización.
- g) **Actividades y controles gerenciales.**

h) **Actividades individuales.**

El análisis de riesgo se puede concentrar en impactos en un área solamente o en varias áreas posibles de impacto.

Las áreas de impacto incluyen a las siguientes:

- a) Base de activos y recursos de la organización, incluyendo al personal.
- b) Ingresos y derechos
- c) Costos de las actividades, tanto directos como indirectos.
- d) Personas.
- e) Comunidad.
- f) Desempeño.
- g) Cronograma y programa de actividades.
- h) El ambiente.
- i) Intangibles tales como la reputación, gestos de buena voluntad, calidad de vida.
- j) Comportamiento organizacional.

4.2.2.2 *Otras clasificaciones de riesgo*

Distintas disciplinas a menudo categorizan las fuentes de riesgo de otra forma, utilizando términos tales como azares o exposiciones de riesgo. Estas clasificaciones pueden ser subconjuntos de las fuentes de riesgo listadas anteriormente.

Los siguientes son algunos ejemplos:

- a) **Enfermedades:** afectando a humanos, animales y plantas.
- b) **Económicos:** fluctuaciones en la moneda, tasas de interés, mercado accionario.
- c) **Ambientales:** ruidos, contaminación, polución.
- d) **Financieros:** riesgos contractuales, malversaciones de fondos, fraudes, multas.
- e) **Humanos:** motines, huelgas, sabotajes, errores.

- f) **Desastres naturales:** condiciones climáticas, terremotos, incendios de bosques, plagas, actividad volcánica.
- g) **Salubridad y seguridad ocupacional:** medidas de seguridad inadecuadas, administración de seguridad pobre.
- h) **Responsabilidad por productos:** errores de diseño, calidad bajo estándar, pruebas inadecuadas.
- i) **Responsabilidad profesional:** consejo equivocado, negligencia, error de diseño.
- j) **Daños a la propiedad:** fuego, inundaciones, terremotos, contaminación, error humano.
- k) **Responsabilidad pública:** acceso, egreso y seguridad pública.
- l) **Seguridad:** desfalcos, vandalismo, robo, apropiación indebida de información, penetración ilegal.
- m) **Tecnológicos:** innovación, obsolescencia, explosiones y dependencia.

4.2.2.3 Clasificación de los riesgos basada en taxonomía

Se pueden utilizar las clasificaciones o categorías de los riesgos, denominadas también taxonomías de riesgos, para varios propósitos. Durante la identificación de riesgos, pueden utilizarse para estimular el pensamiento sobre los riesgos que pueden producirse en las distintas áreas del proyecto. Durante la puesta en común de ideas, las clasificaciones de riesgos también aligeran la complejidad de trabajar con muchas cantidades de riesgos porque los riesgos parecidos pueden incluirse en un mismo grupo.

También pueden emplearse para proporcionar una terminología unificada que el equipo de trabajo puede utilizar para supervisar y notificar el estado de los riesgos a lo largo del proyecto. Por último, las clasificaciones de los riesgos son muy útiles para establecer las bases de conocimiento de riesgo para empresas e industrias porque proporcionan la base para indexar nuevas contribuciones y buscar y recuperar información existente.

La tabla siguiente muestra una clasificación de alto nivel de las fuentes de riesgo de los proyectos.

CATEGORÍA:	TIPO:
Personas	Clientes Usuarios finales Patrocinadores Participantes Personal Organización Conocimientos Políticas Moral
Proceso	Misión y metas Toma de desiciones Características del proyecto Presupuesto, costo y programación Requerimientos Diseño Creación Pruebas
Tecnología	Seguridad Entorno de desarrollo y prueba Herramientas Implementación Soporte técnico Entorno operativo Disponibilidad
Entorno	Legal Normativo Competencia Económico Tecnología Organizacional

Existen muchas taxonomías o clasificaciones para los riesgos de proyectos generales de desarrollo de software. Entre las clasificaciones conocidas y más mencionadas que describen las fuentes de riesgo de proyectos de desarrollo de software se incluyen las realizadas por *SEI Software Risk Taxonomy (CMU/SEI-93-TR-6)*.

4.2.3 Identificación de riesgos

Este paso busca identificar los riesgos a administrar. Según el PMBOK® 2004, “la identificación de los riesgos involucra determinar cuáles riesgos pueden afectar un proyecto [o proceso] y documentar sus características”.

Es crítica una identificación amplia utilizando un proceso sistemático bien estructurado, porque los riesgos potenciales que no se identifican en esta etapa son excluidos de un análisis posterior. La identificación debería incluir todos los riesgos, estén o no bajo control de la organización.

4.2.3.1 Paso 1: Declaraciones de riesgo

Una declaración de riesgo es una expresión de lenguaje natural que describe la relación entre una situación o atributo real de un proceso (o proyecto) y una segunda situación o atributo de proceso (o proyecto) no realizado.

La primera parte de la declaración de riesgo se denomina condición e incluye y describe una situación o atributo del proceso (o proyecto) existente que el equipo de trabajo prevé que puede resultar en una pérdida en el desempeño o en una reducción de beneficios.

La segunda parte de la declaración de riesgo se denomina consecuencia y describe el atributo o situación no deseable del proyecto. Las dos declaraciones están unidas por un “por lo tanto” o “como consecuencia” que implica una relación incierta (en otras palabras, inferior al 100%) pero causal.

El proceso de declaración en dos partes ofrece la ventaja de unir las consecuencias de riesgo con las condiciones de riesgo visibles (y controlables en potencia) dentro del proyecto en la fase preliminar de la identificación de riesgos.

Es necesario tener en cuenta que las declaraciones de riesgo no son declaraciones “determinísticas o condicionales”, sino declaraciones de hechos que exploran las posibles pero no realizadas consecuencias. Durante los pasos de análisis y planeamiento, la posibilidad de utilizar declaraciones “determinísticas” hipotéticas puede servir de ayuda para sopesar las alternativas y elaborar planes mediante árboles de decisiones. Sin embargo, la meta en la identificación de riesgos consiste en identificar la mayor cantidad posible de riesgos y es preferible dejar los análisis “qué pasaría” para la fase de planeamiento.

Cuando se formule una declaración de riesgo, el equipo deberá tener en cuenta tanto la causa del resultado potencial menos deseado así como el propio resultado. La declaración de riesgo debe incluir el estado visible de la situación (condición) dentro del proceso (o proyecto) así como el estado visible de las situaciones que puedan producirse (consecuencia).

Como parte de un análisis de riesgos exhaustivo, los miembros del equipo deberían buscar coincidencias y agrupaciones naturales de las condiciones de las declaraciones de riesgo del proyecto y retroceder por la cadena causal de condición en busca de una causa raíz subyacente común.

También puede resultar práctico seguir la cadena causal hacia adelante desde el binomio “condición – consecuencia” de la declaración de riesgo para examinar los efectos en la organización y el entorno fuera del proyecto para obtener una mejor perspectiva de las pérdidas totales u oportunidades perdidas asociadas con una condición determinada del proyecto.

Durante la identificación del riesgo es habitual que el equipo identifique varias consecuencias para la misma condición. Algunas veces, las consecuencias de riesgo identificadas en un área del proceso o proyecto pueden convertirse en una condición de riesgo en otra área.

Los equipos deben registrar estas situaciones para poder tomar las decisiones adecuadas durante el análisis y el planeamiento de riesgos teniendo en cuenta las dependencias e interacciones causales entre los riesgos.

Dependiendo de las relaciones entre los riesgos, el cierre de un riesgo puede cerrar un grupo entero de riesgos dependientes y cambiar el perfil de todo el proceso o proyecto. La documentación de estas relaciones en la fase preliminar de identificación de riesgos puede proporcionar información muy útil para crear un planeamiento de riesgos flexible, completo y que utilice de forma eficaz los recursos disponibles del proyecto resolviendo la causa original. Las ventajas de capturar este tipo de información en la fase de identificación deben compararse rápidamente con los análisis y las prioridades subsiguientes y, a continuación, volver a examinar las dependencias y la causa raíz durante la fase de planeamiento para los riesgos más importantes.

4.2.3.2 Paso 2: Identificar las consecuencias de los riesgos

La intención es generar una lista amplia de eventos que podrían afectar a cada elemento de la estructura referida en la Cláusula 4.1.6. Estos son luego considerados en mayor detalle para identificar lo que puede suceder.

4.2.3.3 Paso 3: Identificar los síntomas/disparadores de los riesgos

Habiendo identificado una lista de eventos, es necesario considerar causas y escenarios posibles.

Hay muchas formas en que se puede iniciar un evento. Es importante que no se omitan las causas significativas.

4.2.3.4 Herramientas y técnicas sugeridas

Los enfoques utilizados para identificar riesgos incluyen:

- **Lluvias de ideas (*brainstorming*):** Es una de las técnicas más utilizadas en la identificación de riesgos. La meta es obtener una lista amplia de riesgos que pueden presentarse durante la ejecución de un proceso o proyecto y puede utilizarse posteriormente como insumo en el análisis cualitativo y cuantitativo.
- **Técnica Delphi (juicio de expertos):** Es una forma de lograr un consenso de expertos en un tema (en este caso un riesgo), cada uno de los expertos participa de forma anónima al brindar su juicio.
- **Entrevistas:** Los riesgos pueden identificarse a través de los administradores de proyectos (jefes de unidades funcionales) o bien directamente con los individuos encargados de ejecutar directamente las actividades del proceso o proyecto.
- **Listas de verificación:** Se pueden desarrollar con base en información o conocimiento histórico que ha sido acumulado de experiencias similares (en proyectos o procesos) y otras fuentes de información.
- **Análisis de escenarios e hipótesis:** Se plantean hipótesis y escenarios y de cada uno de ellos se determina su validez, los riesgos surgen de la incompletitud, inconsistencia o inexactitud de las hipótesis o de los escenarios.
- **Técnicas basadas en diagramas:** Pueden incluir diagramas de causa y efecto (*Ishikawa/fishbone*), diagramas de flujo y de sistemas (muestran interacciones), diagramas de influencia (una representación gráfica de un problema que muestra las influencias

causales, ordenamiento temporal de eventos y otras relaciones), así como los diagramas de ingeniería de software.

- **Documentación existente.**

El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión y los tipos de riesgos.

Los productos de esta etapa serán:

- **Riesgos:** Un riesgo constituye un evento (o condición) con cierta incertidumbre y si éste ocurre tiene un efecto positivo o negativo en los objetivos del proyecto o proceso.
- **Disparadores:** Se les llama a menudo “síntomas del riesgo” o “señales de alarma” y son indicadores de que un riesgo está apunto de ocurrir.

4.2.4 Análisis de riesgos

Los objetivos de análisis son separar los riesgos menores y aceptables de los riesgos mayores, y proveer datos para asistir en la evaluación y tratamiento de los riesgos. El análisis de riesgos involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias. Pueden identificarse los factores que afectan a las consecuencias y probabilidades. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes.

Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

4.2.4.1 *Determinar los controles existentes*

Identificar la administración, sistemas técnicos y procedimientos existentes para controlar los riesgos y evaluar sus fortalezas y debilidades. Pueden ser apropiadas las herramientas mencionadas en el apartado anterior, como asimismo los enfoques tales como inspecciones y técnicas de auto-evaluación de controles ('CSA').

4.2.4.2 *Consecuencias y probabilidades*

La magnitud de las consecuencias de un evento, si el mismo ocurriera, y la probabilidad del evento y sus consecuencias asociadas, se evalúan en el contexto de los controles existentes. Las consecuencias y probabilidades se combinan para producir un nivel de riesgo. Se pueden determinar las consecuencias y probabilidades utilizando análisis y cálculos estadísticos.

Alternativamente cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podrá ocurrir un evento o resultado particular.

Para evitar prejuicios subjetivos cuando se analizan consecuencias y probabilidades, deberían utilizarse las mejores técnicas y fuentes de información disponibles.

Se pueden incluir las siguientes fuentes de información:

- a) Registros anteriores.
- b) Experiencia relevante.
- c) Prácticas y experiencia de otras instituciones en procesos o actividades similares.
- d) Literatura relevante.
- e) Experimentos y prototipos.
- f) Modelos económicos, de ingeniería u otros.
- g) Opiniones y juicios de especialistas y expertos.

Las técnicas incluyen:

- a) Entrevistas estructuradas con expertos en el área de interés.
- b) Utilización de grupos multidisciplinarios de expertos.
- c) Evaluaciones individuales utilizando cuestionarios.
- d) Uso de modelos de computador u otros.
- e) Uso de árboles de fallas y árboles de eventos.

Siempre que sea posible, debería incluirse el nivel de confianza asignado a las estimaciones de los niveles de riesgo.

4.2.4.3 Tipos de análisis

El análisis de riesgos puede ser llevado con distintos grados de refinamiento dependiendo de la información de riesgos y datos disponibles. Dependiendo de las circunstancias, el análisis puede ser cualitativo, semi-cuantitativo o cuantitativo o una combinación de estos.

El orden de complejidad y costos de estos análisis en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo. En la práctica, a menudo se utiliza primero el análisis cualitativo para obtener una indicación general del nivel de riesgo. Luego puede ser necesario llevar a cabo un análisis cuantitativo más específico. El detalle de los tipos de análisis es el siguiente:

4.2.4.3.1 Análisis cualitativo

El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran. Estas escalas se pueden modificar o ajustar para adaptarlas a las circunstancias, y se pueden utilizar distintas descripciones para riesgos diferentes.

4.2.4.3.2 Medidas cualitativas de consecuencia o impacto:

El impacto del riesgo calcula la gravedad de los efectos adversos, la magnitud de una pérdida o el costo potencial de la oportunidad si el riesgo llega a producirse dentro del proyecto. Debe tratarse de una medida directa de la consecuencia del riesgo tal y como se define en la declaración de riesgo. Puede calcularse en términos financieros o con una escala de medición subjetiva. La ventaja de expresar todos los impactos del riesgo en términos financieros es que los patrocinadores del proyecto se familiarizarán antes con la información. El impacto financiero puede traducirse en costos a largo plazo de operaciones y soporte técnico, la pérdida de cuota de mercado, costos a corto plazo por trabajos adicionales o los costos de las oportunidades.

En el resto de situaciones, el uso de una escala de valores subjetiva de 1 a 5 o de 1 a 10 es más adecuada para calcular el impacto. Si todos los riesgos de una lista maestra de riesgos utilizan las mismas unidades de medida, las técnicas de asignación de prioridades simples funcionarán.

NIVEL:	DESCRIPTOR:	EJEMPLO DE DESCRIPCIÓN DETALLADA:
1	Insignificante	Sin perjuicios, baja pérdida financiera.
2	Menor	Tratamiento de primeros auxilios, liberado localmente se contuvo inmediatamente, perdida financiera media.
3	Moderado	Requiere tratamiento médico, liberado localmente pero contenido con asistencia externa, pérdida financierera alta.
4	Mayor	Perjuicios extensivos, pérdida de capacidad de producción, liberación externa, sin efectos nocivos, pérdida financiera mayor.
5	Catastrófico	Muerte, liberación tóxica externa con efectos nocivos, enorme pérdida financiera.

Nota: Las medidas utilizadas deberían reflejar las necesidades y naturaleza de la organización y actividad bajo estudio.

4.2.4.3.3 Medidas cualitativas de probabilidad:

La probabilidad¹ de riesgo es una medida que calcula la probabilidad de que la situación descrita en el apartado de consecuencias de los riesgos de la declaración de riesgos llegue a producirse de verdad. Las probabilidades son claramente difíciles de calcular y aplicar, a pesar de contar con la ayuda de las bases de datos de riesgo de empresas e industrias, cuyos datos muestran los cálculos basados en infinidad de proyectos.

Sin embargo, la mayoría de equipos de proyecto pueden expresar con palabras sus experiencias, interpretar los informes y proporcionar una amplia gama de expresiones de lenguaje natural para indicar rangos de probabilidad numéricos. Por ejemplo, las simples expresiones “bajo, medio, alto” pueden expresar valores de probabilidad claros (17%, 50%, 84%), aunque también pueden emplearse términos más complejos como, por ejemplo, “muy poco probable,” “improbable,” “probable,” “casi con total seguridad”, que expresan incertidumbre frente a probabilidades.

NIVEL:	DESCRIPTOR:	DESCRIPCIÓN:
A	Casi certeza	Se espera que ocurra en la mayoría de las circunstancias.
B	Probable	Probablemente ocurrirá en la mayoría de las circunstancias.
C	Posible	Podría ocurrir en algún momento.
D	Improbable	Pudo ocurrir en algún momento.
E	Raro	Puede ocurrir en circunstancias excepcionales.

4.2.4.3.4 Exposición al riesgo

La exposición al riesgo calcula la amenaza general que supone el riesgo combinando la información que expresa la probabilidad de una pérdida real con información que indica la

¹ Para clasificar los riesgos es recomendable la asignación de un valor numérico a la probabilidad (Análisis Cuantitativo). La probabilidad de un riesgo debe ser mayor que cero o el riesgo no representa una amenaza para el proyecto. Asimismo, la probabilidad debe ser menor que 100% o el riesgo es una certeza, en otras palabras, es un problema identificado.

magnitud de la pérdida potencial en un único valor numérico. El equipo puede usar la magnitud de la exposición al riesgo para clasificar los riesgos. En el caso más simple de análisis de riesgo cuantitativo, la exposición al riesgo se calcula multiplicando la probabilidad de riesgo por el impacto.

Cuando las puntuaciones se utilizan para cuantificar la probabilidad y el impacto, es muy práctico crear una matriz que tenga en cuenta las posibles combinaciones de las puntuaciones y las asigne a las categorías de riesgo bajo, medio o alto. Para utilizar la puntuación de probabilidad tripartita, en la que 1 es bajo y 3 alto, los resultados pueden expresarse en una tabla, donde cada casilla es un valor posible para la exposición al riesgo. En esta disposición es muy fácil clasificar los riesgos en la categoría de bajo, medio y alto dependiendo de su posición en las bandas diagonales de la puntuación ascendente.

4.2.4.4 Matriz de análisis de riesgo cualitativo y determinación del nivel de riesgo

PROBABILIDAD:	CONSECUENCIAS:				
	Insignificantes 1	Menores 2	Moderadas 3	Mayores 4	Catastróficas 6
A (Casi certeza)	Alto	Alto	Extremo	Extremo	Extremo
B (Probable)	Medio	Alto	Alto	Extremo	Extremo
C (Posible)	Bajo	Medio	Alto	Extremo	Extremo
D (Improbable)	Bajo	Bajo	Medio	Alto	Extremo
E (Raro)	Bajo	Bajo	Medio	Alto	Alto

NIVEL:	CATEGORÍA:	DESCRIPCIÓN:
Bajo	Aceptable tal cual	No requiere mitigación.
Medio	Aceptable con controles	Se debe verificar que existan controles para este riesgo y estén operativos.
Alto	Indeseable	Debe ser mitigado con controles de ingeniería o administrativos dentro de un período mínimo de 12 meses.
Extremo	Inaceptable	Debe ser mitigado con controles de ingeniería o administrativos dentro de un período mínimo de 6 meses.

El análisis cualitativo se utiliza:

- Como una actividad inicial de tamiz, para identificar los riesgos que requieren un análisis más detallado.
- Cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo.
- Cuando los datos numéricos son inadecuados para un análisis cuantitativo.

4.2.4.4.1 Análisis semi-cuantitativo

En el análisis semi-cuantitativo, a las escalas cualitativas, tales como las descritas arriba, se les asignan valores. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades. Los números pueden ser combinados en cualquier rango de fórmula dado que el sistema utilizado para priorizar confronta el sistema seleccionado para asignar números y combinarlos. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis

cuantitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo.

Se debe tener cuidado con el uso del análisis semi-cuantitativo porque los números seleccionados podrían no reflejar apropiadamente las relatividades, lo que podría conducir a resultados inconsistentes. El análisis semi-cuantitativo puede no diferenciar apropiadamente entre distintos riesgos, particularmente cuando las consecuencias o las probabilidades son extremas.

A veces es apropiado considerar la probabilidad compuesta de dos elementos, a los que se refiere generalmente como frecuencia de la exposición y probabilidad.

Frecuencia de la exposición es la extensión a la cual una fuente de riesgo existe, y probabilidad² es la medida de la frecuencia de que, cuando existe esa fuente de riesgo, le seguirán las consecuencias. Deberá ejercerse precaución en las situaciones en que las relaciones entre los dos elementos no es completamente independiente, cuando hay una fuerte relación entre frecuencia de la exposición y la probabilidad.

Este enfoque se puede aplicar en el análisis semi-cuantitativo y cuantitativo.

4.2.4.4.2 *Análisis cuantitativo*

El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semicuantitativos) utilizando datos de distintas fuentes. La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados.

Las consecuencias pueden ser estimadas modelando los resultados de un evento o conjunto de eventos, o extrapolando a partir de estudios experimentales o datos del pasado. Las consecuencias pueden ser expresadas en términos de criterios monetarios, técnicos o humanos, o

² Matemáticamente hablando, la probabilidad p de aparición de un suceso S de un total de n casos posibles igualmente factibles es la razón entre el número de ocurrencias h de dicho suceso y el número total de casos posibles n . $p = P\{S\} = h / n$.

cualquier otro criterio referido en la Cláusula 4.1.5. En algunos casos se requiere más de un valor numérico para especificar las consecuencias para distintos momentos, lugares, grupos o situaciones.

La probabilidad es expresada generalmente como una probabilidad, una frecuencia, o una combinación de exposición y probabilidad.

La forma en que se expresan las probabilidades y las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo variarán de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de riesgo.

4.2.4.4.3 *Análisis de sensibilidad*

Dado que algunas de las estimaciones realizadas en el análisis cuantitativo son imprecisas, deberá llevarse a cabo un análisis de sensibilidad para comprobar el efecto de los cambios en los supuestos y en los datos.

4.2.4.5 *Evaluación de riesgos*

La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

El análisis de riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación de riesgos deberían considerarse sobre la misma base. En consecuencia, la evaluación cualitativa involucra la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y la evaluación cuantitativa involucra la comparación de un nivel numérico de riesgo contra criterios que pueden ser expresados como un número específico, tal como, un valor de fatalidad, frecuencia o monetario.

El producto de una evaluación de riesgo es una lista de riesgos con prioridades para una acción posterior.

Deberían considerarse los objetivos de la organización y el grado de oportunidad que podrían resultar de tomar el riesgo.

Las decisiones deben tener en cuenta el amplio contexto del riesgo e incluir consideración de la tolerabilidad de los riesgos sostenidos por las partes fuera de la organización que se benefician de ellos.

Si los riesgos resultantes caen dentro de las categorías de riesgos bajos o aceptables, pueden ser aceptados con un tratamiento futuro mínimo. Los riesgos bajos y aceptados deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen aceptables.

Si los riesgos no caen dentro de la categoría de riesgos bajos o aceptables, deberían ser tratados utilizando una o más de las opciones de tratamiento que se describen a continuación.

4.2.5 Tratamiento de los riesgos

El tratamiento de los riesgos involucra identificar el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

4.2.5.1 Identificar opciones para tratamiento de los riesgos

Las opciones para el tratamiento de los riesgos no son necesariamente mutuamente exclusivas y apropiadas en todas las circunstancias, incluyen lo siguiente:

4.2.5.1.1 Evitar el riesgo decidiendo no proceder con la actividad que probablemente generaría el riesgo (cuando esto es practicable).

Evitar riesgos puede ocurrir inadecuadamente por una actitud de aversión al riesgo, que es una tendencia en mucha gente (a menudo influenciada por el sistema interno de una organización).

Evitar inadecuadamente algunos riesgos puede aumentar la significación de otros.

La aversión a riesgos tiene como resultado:

- Decisiones de evitar o ignorar riesgos independientemente de la información disponible y de los costos incurridos en el tratamiento de esos riesgos.
- Fallas en tratar los riesgos.
- Dejar las opciones críticas y/o decisiones en otras partes.
- Diferir las decisiones que la organización no puede evitar.
- Seleccionar una opción porque representa un riesgo potencial más bajo independientemente de los beneficios.

4.2.5.1.2 Reducir o controlar la probabilidad de la ocurrencia

Se pueden mencionar las siguientes acciones:

- a) Programas de auditoria y cumplimiento.
- b) Condiciones contractuales.
- c) Revisiones formales de requerimientos, especificaciones, diseño, ingeniería y operaciones.
- d) Inspecciones y controles de procesos.
- e) Administración de inversiones y cartera.
- f) Administración de proyectos.
- g) Mantenimiento preventivo.
- h) Aseguramiento de calidad, administración y estándares.
- i) Investigación y desarrollo, desarrollo tecnológico.

- j) Capacitación estructurada y otros programas.
- k) Supervisión.
- l) Comprobaciones.
- m) Acuerdos organizacionales.
- n) Controles técnicos.

4.2.5.1.3 Reducir o controlar las consecuencias

Estos pueden incluir los siguientes procedimientos:

- Planeamiento de contingencia.
- Arreglos contractuales.
- Condiciones contractuales.
- Características de diseño.
- Planes de recupero de desastres.
- Barreras de ingeniería y estructurales.
- Planeamiento de control de fraudes.
- Minimizar la exposición a fuentes de riesgo.
- Planeamiento de cartera.
- Política y controles de precios.
- Separación o reubicación de una actividad y recursos.
- Relaciones públicas.
- Pagos ex gratia³.

³ Se da este nombre al pago que efectúa una institución sin tener responsabilidad legal alguna de indemnizar una pérdida. Normalmente, se persigue con el pago ex gratia evitar los gastos excesivos que se producirán al tener que demostrar judicialmente, o de modo análogo la improcedencia de dicho pago, cuyo importe no compensaría la cuantía de aquellos gastos.

4.2.5.1.4 *Transferir los riesgos*

Esto involucra que otra parte soporte o comparta parte del riesgo. Los mecanismos incluyen el uso de contratos, arreglos de seguros y estructuras organizacionales tales como sociedades.

La transferencia de un riesgo a otras partes, o la transferencia física a otros lugares, reducirá el riesgo para la organización original, pero puede no disminuir el nivel general del riesgo para la sociedad.

Cuando los riesgos son total o parcialmente transferidos, la organización que transfiere los riesgos ha adquirido un nuevo riesgo, que la organización a la cual ha transferido el riesgo no pueda administrarlo efectivamente.

4.2.5.1.5 *Retener los riesgos*

Luego de que los riesgos hayan sido reducidos o transferidos, podría haber riesgos residuales que sean retenidos. Deberían ponerse en práctica planes para administrar las consecuencias de esos riesgos si los mismos ocurrieran, incluyendo identificar medios de financiar dichos riesgos. Los riesgos también pueden ser retenidos en forma predeterminada, por ejemplo cuando hay una falla para identificar y/o transferir apropiadamente o de otro modo tratar los riesgos.

A la reducción de las consecuencias y probabilidades se las puede referir como control de riesgos. El control de riesgos involucra determinar el beneficio relativo de nuevos controles a la luz de la efectividad de los controles existentes. Los controles pueden involucrar políticas de efectividad, procedimientos o cambios físicos.

4.2.5.1.6 *Aceptar los riesgos*

Los responsables del proyecto o proceso deciden no lidiar con el riesgo debido a que no quieren afectar el rendimiento o cambiar la planificación actual o se desconoce un plan de manejo implementable para este riesgo.

4.2.5.2 *Evaluar opciones de tratamiento de los riesgos*

Las opciones deberían ser evaluadas sobre la base del alcance de la reducción del riesgo, y el alcance de cualquier beneficio u oportunidad adicional creadas, tomando en cuenta los criterios desarrollados. Pueden considerarse y aplicarse una cantidad de opciones ya sea individualmente o combinadas.

La selección de la opción más apropiada involucra balancear el costo de implementar cada opción contra los beneficios derivados de la misma. En general, el costo de administrar los riesgos necesita ser conmensurada con los beneficios obtenidos.

Cuando se pueden obtener grandes reducciones en el riesgo con un gasto relativamente bajo, tales opciones deberían implementarse. Otras opciones de mejoras pueden ser no económicas y necesita ejercerse el juicio para establecer si son justificables.

Las decisiones deberían tener en cuenta la necesidad de considerar cuidadosamente los riesgos raros pero severos, que podrían justificar medidas de seguridad que no son justificables por fundamentos estrictamente económicos.

En general el impacto adverso de los riesgos debería hacerse tan bajo como sea razonablemente practicable, independientemente de cualquier criterio absoluto.

Si el nivel de riesgo es alto, pero podrían resultar oportunidades considerables si se lo asume, tal como el uso de una nueva tecnología, entonces la aceptación del riesgo necesita estar basada en una evaluación de los costos de tratamiento y los costos de rectificar las consecuencias potenciales versus las oportunidades que podrían depararse de tomar el riesgo.

En muchos casos, es improbable que cualquier opción de tratamiento del riesgo sea una solución completa para un problema particular. A menudo la organización se beneficiará sustancialmente mediante una combinación de opciones tales como reducir la probabilidad de los riesgos, reducir sus consecuencias, y transferir o retener algunos riesgos residuales. Un ejemplo es el uso efectivo de contratos y la financiación de riesgos sustentados por un programa de reducción de riesgos.

Cuando el costo acumulado de implementación de todos los tratamientos de riesgos excede el presupuesto disponible, el plan debería identificar claramente el orden de prioridad bajo el cual deberían implementarse los tratamientos individuales de los riesgos. El ordenamiento de prioridad puede establecerse utilizando distintas técnicas, incluyendo análisis de “ranking” de riesgos y de costo-beneficio. Los tratamientos de riesgos que no puedan ser implementados dentro de los límites del presupuesto disponible deben esperar la disponibilidad de recursos de financiamiento adicionales, o, si por cualquier razón todos o algunos de los tratamientos restantes son considerados importantes, debe plantearse el problema para conseguir el financiamiento adicional.

Las opciones de tratamiento de los riesgos deberían considerar cómo es percibido el riesgo por las partes afectadas y las formas más apropiadas de comunicárselo a dichas partes.

4.2.5.3 Preparar planes de tratamiento

Los planes deberían documentar cómo deben ser implementadas las opciones seleccionadas.

El plan de tratamiento debería identificar las responsabilidades, el programa, los resultados esperados de los tratamientos, el presupuesto, las medidas de desempeño y el proceso de revisión a establecer.

El plan también debería incluir un mecanismo para evaluar la implementación de las opciones contra criterios de desempeño, las responsabilidades individuales y otros objetivos, y para monitorear los mojones críticos de implementación.

4.2.5.4 Implementar planes de tratamiento

Idealmente, la responsabilidad por el tratamiento del riesgo debería ser llevada a cabo por aquellos con mejor posibilidad de controlar el riesgo. Las responsabilidades deberían ser acordadas entre las partes en el momento más temprano posible.

La implementación exitosa del plan de tratamiento del riesgo requiere un sistema efectivo de administración que especifique los métodos seleccionados, asigne responsabilidades y compromisos individuales por las acciones, y los monitoree respecto de criterios especificados.

Si luego del tratamiento hay un riesgo residual, debería tomarse la decisión de si retener este riesgo o repetir el proceso de tratamiento.

4.2.6 Monitoreo y revisión

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento de los riesgos, las estrategias y el sistema de administración que se establece para controlar la implementación. Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos. Pocos riesgos permanecen estáticos.

Es esencial una revisión sobre la marcha para asegurar que el plan de administración se mantiene relevante. Pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo

de administración de riesgos. La revisión es una parte integral del plan de tratamiento de la administración de riesgos.

4.2.7 Comunicación y consulta

La comunicación y consulta son una consideración importante en cada paso del proceso de administración de riesgos. Es importante desarrollar un plan de comunicación para los interesados internos y externos en la etapa más temprana del proceso. Este plan debería encarar aspectos relativos al riesgo en si mismo y al proceso para administrarlo.

La comunicación y consulta involucra un diálogo en ambas direcciones entre los interesados, con el esfuerzo focalizado en la consulta más que un flujo de información en un sólo sentido del tomador de decisión hacia los interesados.

Es importante la comunicación efectiva interna y externa para asegurar que aquellos responsables por implementar la administración de riesgos, y aquellos con intereses creados comprenden la base sobre la cual se toman las decisiones y por qué se requieren ciertas acciones en particular.

Las percepciones de los riesgos pueden variar debido a diferencias en los supuestos, conceptos, las necesidades, aspectos y preocupaciones de los interesados, según se relacionen con el riesgo o los aspectos bajo discusión. Los interesados probablemente harán juicios de aceptabilidad de los riesgos basados en su percepción de los mismos.

Dado que los interesados pueden tener un impacto significativo en las decisiones tomadas, es importante que sus percepciones de los riesgos, así como, sus percepciones de los beneficios, sean identificadas y documentadas y las razones subyacentes para las mismas comprendidas y tenidas en cuenta.

4.3 Documentación

Debería documentarse cada etapa del proceso de administración de riesgos. La documentación debería incluir los supuestos, los métodos, las fuentes de datos y los resultados.

4.3.1 Razones para la documentación

Las razones para la documentación son las siguientes:

- a) Demostrar que el proceso es conducido apropiadamente.
- b) Proveer evidencia de un enfoque sistemático de identificación y análisis de riesgos.
- c) Proveer un registro de los riesgos y desarrollar la base de datos de conocimientos de la organización.
- d) Proveer a los tomadores de decisión relevantes de un plan de administración de riesgos para aprobación y subsiguiente implementación.
- e) Proveer un mecanismo y herramienta de responsabilidad.
- f) Facilitar el continuo monitoreo y revisión.
- g) Proveer una pista de auditoría.
- h) Compartir y comunicar información.

Las decisiones concernientes al alcance de la documentación pueden involucrar costos y beneficios y deberían tomar en consideración los factores mencionados arriba.

Para administrar correctamente el riesgo, se requiere una documentación apropiada. Esto puede necesitar ser suficiente para satisfacer a una auditoría independiente. Las decisiones concernientes al alcance de la documentación pueden involucrar costos y beneficios y debería tomar en cuenta los factores riesgo mencionados en los apartados anteriores. La declaración de la política de administración de riesgos debería definir la documentación necesaria.

En cada etapa del proceso, la documentación debería incluir:

- a) Objetivos.
- b) Fuentes de información.
- c) Supuestos.
- d) Decisiones.

4.3.1.1 Declaración de cumplimiento y diligencia debida

En algunas circunstancias puede requerirse una declaración de cumplimiento y diligencia debida, de forma tal que los gerentes tomen conocimiento formal de su responsabilidad por el cumplimiento de las políticas y procedimientos de administración de riesgos.

4.3.1.2 Registro de riesgos

Por cada riesgo identificado el registro de riesgo comprende:

- a) Declaración.
- b) Ubicación en el contexto organizacional.
- c) Síntomas/Disparadores
- d) Consecuencias
- e) Probabilidad e Impacto.
- f) Nivel de exposición.
- g) Opciones de tratamiento y respuesta / controles existentes.

4.3.1.3 Programa de tratamiento de riesgos y plan de acción

Un tratamiento de riesgos y plan de acción documenta los controles gerenciales a adoptar y lista la siguiente información:

- a) Responsables de la implementación del plan.
- b) Recursos requeridos.

- c) Asignación de presupuesto.
- d) Calendario de implementación.
- e) Detalles del mecanismo y frecuencia de la revisión de cumplimiento del plan de tratamiento.

4.3.1.4 *Monitorear y auditar documentos*

Los registros de monitoreo y auditoria deberían documentar:

- a) Detalles del mecanismo y frecuencia de la revisión de riesgos y del proceso de administración de riesgos como un todo.
- b) Los resultados de las auditorias y de otros procedimientos de monitoreo.
- c) Detalles de cómo son seguidas e implementadas las recomendaciones de las revisiones.

5 Referencias bibliográficas

- [HIGUE96] Ronald P. Higuera y Yacov Y. Haimes, “Software Risk Management”, SEI Technical Report CMU/SEI-96-TR-012 ESC-96-012 (Pittsburgh, PA: Software Engineering Institute—Universidad Carnegie Mellon, 1996.
- [CARR93] Marvin J. Carr y otros, “Taxonomy-Based Risk Identification”, SEI Technical Report CMU/SEI-93-TR-6 ESC-TR-93-183 (Pittsburgh, PA: Software Engineering Institute—Universidad Carnegie Mellon, 1993.
- [SEA05] Robert C. Seacord y Allen D. Householder, “A Structured Approach to Classifying Security Vulnerabilities”, SEI Technical Note CMU/SEI-2005-TN-003 (Pittsburgh, PA: Software Engineering Institute—Universidad Carnegie Mellon, 2005.
- [SOM02] Ian Sommerville. Ingeniería de Software. Sexta Edición. Editorial Addison Wesley. México. 2002.
- [STON02] Gary Stoneburner y otros. “Risk Management Guide for Information Technology Systems”. Recommendations of the National Institute of Standards and Technology SP 800–30. National Institute of Standards and Technology. 2002
- [PMBOK00] Project Management Institute Inc. (www.pmi.org). “A guide to project management body of knowledge (PMBOK® Guide)”. Edición 2000. Pennsylvania, EUA. 2000.
- [PMBOK04] Project Management Institute Inc. (www.pmi.org). “A guide to project management body of knowledge (PMBOK® Guide)”. Edición 2004. Pennsylvania, EUA. 2004.
- [DOD00] Departamento de Defensa. “Standard Practice for System Safety”. MIL-STD-882D. Febrero 2000.

- [DOD03] Departamento de Defensa. "Risk Management Guide for DoD Acquisition". MIL-STD-882D. Quinta Edición (Versión 2.0). Junio 2003.
- [ROBIN02] Allison Robin y otros. "Disciplina de administración de riesgos Versión 1.1". Microsoft Solutions Framework. Microsoft Corporation. 2002.
- [SAA99] Standards Association of Australia. Risk management. AS/NZS 4360:1999. Strathfield, NSW : Standards Association of Australia, 1999.
- [GALL05] Gallagher, Brian P. y otros. "Taxonomy of Operational Risks" (CMU/SEI-2005-TN-36). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2005.
- [MURP96] Murphy, Richard L. y otros. "Continuous Risk Management Guidebook". PA: Carnegie Mellon University, 1996.
- [WILL99] Williams, Ray C. y otros. "Software Risk Evaluation (SRE) Method Description (Version 2.0)" (CMU/SEI-99-TR-029, ADA001008). PA: Software Engineering Institute, Carnegie Mellon University, 1999.

6 Esquema de la gestión de riesgos

