

**Universidad de las Ciencias Informáticas**

**Facultad 7**



**Título: Implementación de un sistema para la  
Gestión de Riesgos Operacionales**

Trabajo de Diploma para optar por el Título  
de Ingeniero en Ciencias Informáticas

**Autora:** Yesdaysi González Muñoz

**Tutora:** Ing. Danayi Daniela Hernández Laguna

Ciudad de La Habana, Junio 2010

“Año 52 de la Revolución”

# Declaración de Autoría

Declaro que soy la única autora del presente trabajo y reconozco a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los 22 días del mes de junio del año 2010.

---

Yesdaysi González Muñoz

Autora

---

Ing. Danayi Daniela Hernández Laguna

Tutora

# Resumen

En el presente trabajo se realiza un estudio de los procesos de negocio que se llevan a cabo en las áreas de la Universidad de las Ciencias Informáticas (UCI), en el ámbito de la gestión de riesgos, con el objetivo de lograr un aumento en la calidad de este proceso, debido a que el mismo se realiza sin un método preciso. Se propone como solución a este problema y como objetivo del presente trabajo implementar un sistema informático para la administración y gestión de los riesgos en las áreas de la UCI. Durante su desarrollo, se utilizaron diferentes herramientas y tecnologías, que ayudaron a minimizar el trabajo y lograr un sistema con mayor calidad y eficiencia.

La gestión de riesgos en la universidad debe ocupar un lugar importante, ya que constituye una herramienta indispensable para la toma de decisiones que pudieran conllevar al cumplimiento de los objetivos y metas trazadas por la misma, por los que se espera con este sistema, lograr que en la universidad se le brinde una mayor importancia a este tema, ya que existe una escasa cultura del mismo y no se conoce más allá de lo sugerido por la Resolución 297-MFP. A esta propuesta se arriba después de estudiar los procesos de la gestión de riesgos según lo establecido en el marco conceptual COSO ERM (Enterprise Risk Management), uno de los más conocidos y aplicados a nivel mundial.

**Palabras Claves:** Gestión de riesgos, Resolución 297-MFP, COSO.

# Índice

<b>Introducción .....</b>	<b>1</b>
<b>Capítulo 1 Fundamentación Teórica .....</b>	<b>5</b>
1.1. Riesgos empresariales. Definición .....	5
1.2. Clasificación de los riesgos.....	8
1.3. Riesgos operacionales.....	9
1.4. Gestión del Riesgo. ....	11
1.4.1. La gestión de Riesgos a nivel internacional. ....	12
1.4.2. La Gestión de Riesgos en Cuba.....	20
1.5. Propuesta de un marco conceptual para la gestión de riesgos en la UCI.....	22
1.6. Método para la identificación, evaluación y tratamiento de los riesgos.....	22
1.7. Herramientas y tecnologías. ....	26
1.7.1. Aplicaciones Web .....	26
1.7.2. Lenguaje de programación .....	26
1.7.3. Servidor de aplicaciones web.....	28
1.7.4. Ambiente de Desarrollo Integrado (IDE) .....	28
1.7.5. Marco de trabajo o Framework.....	29
1.7.6. Lenguaje de modelado .....	30
1.7.7. Herramienta de modelado .....	30
1.7.8. Metodología de desarrollo .....	31
1.7.9. Gestor de base de datos .....	31
Conclusiones parciales.....	32
<b>Capítulo 2 Características del sistema .....</b>	<b>33</b>
2.1. Modelo de Dominio .....	33
2.2. Procesos a automatizar.....	35
2.2.1. Requisitos Funcionales.....	38
2.2.2. Requisitos no Funcionales.....	40
2.3. Modelo de Casos de Uso.....	41

2.3.1.	Definición de los actores del sistema.....	42
2.3.2.	Diagrama de Casos de Uso del Sistema.....	42
2.3.3.	Listado de los Casos de Uso del Sistema.....	43
2.3.4.	Casos de uso expandidos.....	45
	Conclusiones parciales.....	50
<b>Capítulo 3</b>	<b>Diseño del sistema.....</b>	<b>51</b>
3.1.	Modelo de Análisis.....	51
3.1.1.	Diagramas de clases del análisis.....	51
3.2.	Modelo de Diseño.....	53
3.2.1.	Diagramas de clases del Diseño.....	53
3.3.	Patrón Arquitectónico. Modelo – Vista – Controlador.....	55
3.4.	Diseño de la Base de Datos.....	57
3.4.1.	Modelo de datos.....	57
3.5.	Tratamiento de errores.....	58
3.6.	Seguridad.....	59
	Conclusiones parciales.....	59
<b>Capítulo 4</b>	<b>Implementación y prueba.....</b>	<b>60</b>
4.1.	Modelo de implementación.....	60
4.1.1.	Diagrama de despliegue.....	60
4.1.2.	Diagramas de componentes.....	62
4.2.	Modelo de prueba.....	63
4.2.1.	Descripción de los casos de prueba de integración.....	64
	Conclusiones parciales.....	66
<b>Conclusiones</b>	<b>.....</b>	<b>67</b>
<b>Recomendaciones</b>	<b>.....</b>	<b>68</b>
<b>Referencias Bibliográficas</b>	<b>.....</b>	<b>69</b>
<b>Bibliografía</b>	<b>.....</b>	<b>71</b>
<b>Anexos</b>	<b>.....</b>	<b>73</b>
Anexo 1	Descripción de las tablas del modelo de datos.....	73

# Introducción

El control interno ha sido preocupación de las entidades económicas, en mayor o menor grado y con diferentes enfoques y terminologías, lo que ha permitido que al pasar del tiempo se hayan planteado diferentes concepciones acerca del mismo.

Desde la década de los 90, a nivel internacional se incrementó el interés por el control interno, lo que también contribuyó a estimular la introducción de la administración de riesgos a los procesos de gestión empresarial. En el año 1992 se publicó en los Estados Unidos el denominado informe COSO I (Committee of Sponsoring Organizations of the Treadway Commission) sobre el control interno, su objetivo era definir un nuevo marco conceptual del control interno, capaz de integrar las diversas definiciones y conceptos que venían siendo utilizados sobre el tema, logrando así que, al nivel de las organizaciones públicas o privadas, de la auditoría interna o externa, o de los niveles académicos o legislativos, se contara con un marco conceptual común, una visión integrada capaz de satisfacer las demandas generalizadas de todos los sectores involucrados. [1]

La Economía Cubana ha transitado por diferentes momentos en materia de control interno, lo cual le ha servido para comprobar que sus normativas de control interno y sus principios no estaban diseñados para proporcionar un grado de seguridad razonable en cuanto a la consecuencia de objetivos dentro de las categorías de Eficacia, Eficiencia, factibilidad de la información financiera y el cumplimiento de las leyes y normas aplicadas.

Debido a esto en los años 2001 y 2002, el Comité de Normas Cubanas de Contabilidad conformó un equipo de trabajo para el estudio y propuesta de un marco conceptual y nuevos enfoques de los sistemas de Control Interno en el país. Como resultado se promulga la Resolución 297-2003 del Ministerio de Finanzas y Precios (MFP) poniendo en vigor las definiciones del Control Interno y el contenido de sus componentes y sus normas.

Pero esta resolución presenta un problema, que es basada en COSO I (1992), en el que la Gestión de Riesgos todavía no se había comenzado a tratar como complemento del Control Interno, solo contenía una evaluación de los mismos. Esta resolución establece que el control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las entidades, pero no provee los componentes necesarios para una correcta gestión de los mismos. No es hasta el año 2004 que se publica COSO II ERM (Enterprise Risk Management), el cual detalla los componentes esenciales de la

gestión de riesgos en las empresas y el contexto en que tales componentes son eficazmente implementados.

En la Universidad de las Ciencias Informáticas (UCI) el riesgo forma parte de todas las decisiones tomadas por la dirección, con independencia de que los resultados sean positivos o negativos. Por tanto, es evidente que gran parte de los proyectos e iniciativas del equipo directivo conllevan un elemento de riesgo. Si bien es cierto que algunos pueden traer consigo consecuencias indeseables, lo es también que los sucesos negativos pudieran evitarse con la implementación de una adecuada gestión de riesgos y en el caso de que ello no fuera posible, ayudaría a minimizar los efectos adversos en caso de que ocurran.

Pero en la UCI, la gestión de riesgos es un tema complejo, ya que este no se realiza una forma completa e integral, debido a que solo se conoce lo establecido en esta resolución y además no existe una cultura del control interno, con sus componentes y normas asociadas.

De un análisis realizado a las diferentes áreas de la UCI, se han recogido una serie de elementos que demuestran lo antes expuesto. Cada una de estas áreas tiene realizado un inventario de los riesgos a la cual está expuesta, además de tener una guía de acciones o guías de control que va a realizar para minimizar estos eventos en caso de que ocurran. Pero estos documentos generalmente son archivados y no se toman en cuenta realmente para llevar a cabo la mitigación de los riesgos, proceso que además de no estar correcto, no es realizado completo, ya que a través de las guías de control es que se les da respuesta a los riesgos identificados. Por todos estos elementos se puede decir que en la UCI no se realiza la Gestión de Riesgos con todos los elementos que la componen, lo cual contribuye a que se deriven una serie de problemas que podrían ser resueltos con una correcta implementación de los mismos.

Además, una de las técnicas actualmente utilizadas en la evaluación de los riesgos, es que el análisis de sus variables (frecuencia y probabilidad) presupone la existencia de información estadística suficiente para aplicar la teoría de las probabilidades. Sin una cantidad determinada de datos sobre ocurrencias pasadas del riesgo y la cuantificación de sus daños, cuando sea pertinente resultará casi imposible evaluar estas variables.

Por todo lo antes expuesto se puede plantear que la evaluación de riesgos en la UCI se realiza sin un método preciso, sólo se identifican los mismos y se propone un plan de acciones para minimizarlos, esto se realiza mediante calificaciones de una o pocas personas, dando lugar a resultados errados. Estos

riesgos sólo se especifican de forma cualitativa y nunca se llega a realizar el análisis cuantitativo de los mismos, que es lo que permite darle un valor al riesgo, y a partir de su valor y el nivel que tenga el riesgo (Bajos, Medios, Altos, Extremos), seleccionar las medidas que se estimen más efectivas para elaborar los planes de prevención de acuerdo con su impacto (o sea, si los riesgos son extremos se le debe dar tratamiento inmediato, si están en las manos del área, sino deben ser trasferidos al nivel superior). Si el riesgo no tiene un valor matemático, es muy difícil determinar cual es la prioridad que se le debe dar, y a partir de ahí tomar las medidas para elaborar los planes de prevención.

Por lo antes planteado, se propone como **problema científico** ¿Cómo viabilizar la automatización del proceso de Gestión de Riesgos?, teniendo como **objeto de estudio** el proceso de Control Interno en la UCI, y el **Campo de Acción** estará encaminado a la Gestión de Riesgos en las diferentes áreas de la UCI. Para dar solución al problema científico planteado se define como **objetivo general** implementar un sistema informático para la administración y gestión de los riesgos.

Para dar cumplimiento al objetivo general se proponen las siguientes **tareas de la investigación**:

- ❖ Evaluar las soluciones actuales en software existentes para el tratamiento de los riesgos en las entidades.
- ❖ Realizar el modelo de dominio para comprender la estructura y dinámica con la que contará el sistema.
- ❖ Identificar los requisitos de software para la implementación de las funcionalidades del sistema.
- ❖ Proponer una arquitectura robusta para adaptar la herramienta al entorno de implementación en que esta se desarrollará.
- ❖ Realizar un diseño que permita la entrada apropiada y un punto de partida para la actividad de implementación.
- ❖ Implementar un sistema para la gestión de riesgos operacionales.

Como resultado de este trabajo de diploma, se espera obtener una solución de software, que permita gestionar los riesgos de las diferentes áreas de la UCI. Además de evaluar la manera en que se lleva a cabo el control interno en cada una de ellas, mediante el monitoreo continuo que se realice.

El presente trabajo está estructurado en cuatro capítulos que se describen a continuación:



En el Capítulo 1 **Fundamentación teórica:** Se hará un estudio de la Gestión de Riesgos tanto en el ámbito internacional como nacional, incluyendo nuestra universidad; así como el estado del arte de las soluciones actuales en software existentes para dar tratamiento a los riesgos, que pueda servir como base para la solución del problema actual al que se enfrenta la universidad. Además, también se analizarán las principales técnicas, tecnologías y herramientas utilizadas para el desarrollo del sistema.

En el Capítulo 2 **Características del sistema:** Se describirán las características básicas y fundamentales del sistema informático a desarrollar, así como una descripción general de cómo debe funcionar el mismo. En este, se realizará un breve análisis de los procesos del negocio que se realizan en las áreas a través del modelo de dominio, especificándose los requerimientos funcionales que plantea el cliente, así como las restricciones que se imponen a través de los requisitos no funcionales del sistema. Se definirán además los actores y casos de uso del sistema a desarrollar.

En el Capítulo 3 **Análisis y diseño del sistema:** Abarcará el desarrollo de la fase de análisis y diseño del sistema, teniendo en cuenta los requisitos funcionales y no funcionales expuestos anteriormente, para dar cumplimiento a los objetivos del sistema. Se formula una arquitectura que permita adaptar el sistema al entorno de implementación que se desarrollará y a la arquitectura a utilizar teniendo en cuenta el framework a utilizar. Además, se realizarán los diagramas de clases del análisis y diseño, así como los diagramas de interacción en correspondencia con los casos de uso antes definidos.

En el Capítulo 4 **Implementación:** Se describirá como fue implementado el sistema. Se realizará el modelo de implementación, con sus respectivos diagramas de componentes, el diagrama de despliegue del sistema y se le realizarán pruebas de integración al sistema.

# Capítulo 1

## Fundamentación Teórica

### Introducción

En este capítulo se realiza una revisión de las diferentes bibliografías relacionadas con el tema de la gestión de riesgos operacionales de Control Interno, a través de la fundamentación teórica y los principios generales de la gestión de los riesgos, tanto en el ámbito internacional como nacional, incluyendo la universidad, así como el estado del arte de las soluciones actuales en software existentes para dar tratamiento a los riesgos, que pueda servir como base para la solución del problema actual al que se enfrenta la universidad. El análisis bibliográfico realizado permite registrar y conocer los diferentes criterios existentes sobre el tema tratado. Además, se analizan las principales técnicas, tecnologías y herramientas utilizadas para el desarrollo de este sistema.

#### 1.1. Riesgos empresariales. Definición

Desde los orígenes de la humanidad ha estado presente el riesgo, en diferentes aspectos de su quehacer cotidiano como la salud, las cosechas, el préstamo de dinero, el ser asaltado por bandidos o el paso de un agente meteorológico.

En la actualidad los riesgos generalmente están proyectados en el ámbito económico, debido a la experiencia derivada de las crisis empresariales y financieras que se han registrado en los últimos 20 años. Estas crisis ha convirtiendo los riesgos empresariales en una propuesta disciplinada y alineada a la estrategia, objetivos, procesos, personas, tecnología, y conocimiento, con el propósito de evaluar y administrar las incertidumbres que la empresa enfrenta a medida que crea valor.

En muchos de los idiomas modernos el significado de la palabra riesgo tiene las mismas raíces – la española “**riesgo**”, la francesa “**risque**”, la italiana “**rischio**”, la alemana “**risiko**” vienen del latín **risicare**. En la antigüedad llamaban risicare a la capacidad de navegar alrededor de un arrecife o roca. [2]

También la palabra está asociada al concepto de “atreverse”, es decir, a elegir una vía de acción que puede llevar al éxito o al fracaso. Según Mauricio León Lefcovich (2005), existe riesgo cuando se tienen

dos o más posibilidades entre las cuales optar, sin poder conocer de antemano los resultados a que conducirá cada una de ellas. [3]

El Diccionario de la Real Academia de la Lengua Española define el riesgo como *la contingencia o proximidad de un daño* y en una segunda acepción, como *cada una de las contingencias que pueden ser objeto de un contrato de seguro*.

El riesgo es un evento incierto, indeseable, imprevisto e involuntario que, en caso de producirse, puede tener consecuencias negativas para quien lo sufre y puede generar al mismo tiempo unas necesidades cuantificables económicamente, haciendo peligrar en determinadas ocasiones la estabilidad económico-financiera de la empresa. [4]

Los riesgos surgen de la incertidumbre que rodea a las decisiones y a los resultados de las organizaciones. También es posible que los resultados de una organización no hayan alcanzado las expectativas, por lo que la incertidumbre en la toma de decisiones que han derivado en este resultado también puede considerarse un elemento de riesgo. [5]

Otra de las definiciones existentes para el riesgo es la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos, por lo cual el riesgo se mide en términos de impacto y probabilidad. [6]

Todas estas definiciones tienen algo en común, solo consideran al riesgo en su aspecto negativo, como algo que solo origina pérdidas, y no en su potencial de oportunidades para mejorar el desempeño empresarial. A diferencia de la concepción habitual, que interpreta el riesgo en términos de peligro o impactos negativos, el estándar de Administración de Riesgos de Australia y Nueva Zelanda(AS/NZS 4360), desde su versión de 1999, [7] define al riesgo como la exposición a las consecuencias de la incertidumbre, la consecuencia de que suceda algo que tenga un impacto sobre los objetivos.[8] Esta última definición resulta más al reconocer que el riesgo, más que un posible resultado no deseado es la posibilidad de desviación de este resultado de lo esperado, planeado o deseado, tanto en sentido favorable como negativo.

Esta doble concepción del riesgo, tanto como fuente de beneficios como de pérdidas futuras, no es del todo nueva: es ampliamente conocida la rentabilidad-riesgo inherente a las decisiones financieras. Por tanto, se reconoce la posibilidad de la obtención de beneficios si se corren determinados riesgos, tal vez buscando considerar ambas caras del riesgo y al mismo tiempo evitar confusiones con la percepción de

pérdida que este término provoca, COSO introduce la palabra “evento” para designar un hecho, que puede ocurrir en el futuro con determinadas consecuencias. De esta forma, señala que los eventos pueden tener impacto negativo, positivo o ambos: los eventos con impacto negativo representan riesgos que pueden impedir la creación de valor o erosionar el valor ya existente. Los eventos con impacto positivo pueden compensar los impactos negativos o representar oportunidades. Las oportunidades son la posibilidad de que un evento ocurra e influya positivamente en el logro de los objetivos, apoya la creación o protección del valor. [9]

Reconociendo entonces que el riesgo no implica necesariamente un resultado negativo, sino un resultado con posibilidades de ocurrencia en el futuro, se pueden vincular a su definición los conceptos de probabilidad e incertidumbre. Probabilidad es la proporción de veces que ocurre un evento particular en un tiempo determinado, asumiendo que las condiciones fundamentales permanecen constantes. La probabilidad se asocia al concepto de aleatoriedad, azar, aunque se desconoce que sucederá en un futuro, se posee información sobre las veces que el evento (riesgo) ocurre en un tiempo y bajo determinadas condiciones. Por el contrario, la incertidumbre es la posibilidad de conocer o predecir el resultado de una situación en el futuro.

La medida del riesgo es el nivel de riesgo. Este en un componente de dos factores: la frecuencia y la consecuencia, también llamada intensidad, repercusión, impacto o severidad del riesgo.

La frecuencia representa el número de ocurrencias de tiempo definido. Es común encontrar el término de probabilidad en lugar de frecuencia. Dado que no siempre se conoce, o no existe, una ley de probabilidad para determinados eventos y dado que no debe medirse la incertidumbre de la misma forma que la probabilidad, no es correcto utilizar indistintamente ambos términos. Si es conocido, o es posible conocer, el número de veces que el evento se manifiesta o tiene lugar en un período de tiempo y espacio determinado y además, las condiciones bajo las que ocurre dicho evento se mantienen sin cambios, puede hablarse de probabilidad del riesgo. Sin embargo, existen riesgos en la empresa de los que no se tiene la información suficiente que permita asignarles una probabilidad de ocurrencia. En estos casos no es correcto hablar de probabilidad, sino de frecuencia del riesgo.

La consecuencia o intensidad no es más que el resultado de un evento, es decir, la magnitud de los efectos de la ocurrencia de un riesgo. La antes mencionada norma australiana (AS/NZS 4360: 1999) define que puede haber más de una consecuencia de un mismo evento, que estas pueden estar en el

rango de positivas a negativas, ser expresadas cualitativa o cuantitativamente y que son determinadas en relación con el logro de los objetivos.

Establecer una medida de ambas características (frecuencia y consecuencias), constituye el objetivo esencial del análisis de riesgos, una de las etapas del proceso de gestión de riesgos.

### 1.2. Clasificación de los riesgos

Los riesgos empresariales tienen diferentes clasificaciones que se han otorgado a partir de su identificación, permitiendo una mejor organización a la gestión de los riesgos. Sin embargo, la clasificación de los riesgos es una tarea de gran complejidad debido a los múltiples factores que pueden causarlos.

Según Yadira Rodríguez Carranza (2008), las clasificaciones que se tratarán en el presente trabajo son las más ajustadas al entorno empresarial cubano. La mayoría de estos fenómenos, que se pueden presentar en las entidades cubanas, son provocados por conductas poco responsables de los trabajadores o por hechos vinculados al objeto social de la entidad. [10]

**El riesgo especulativo:** es aquel cuyo efecto puede producir una pérdida o una ganancia, como por ejemplo las apuestas o los juegos de azar, las inversiones.

**El riesgo puro:** es el que se da en la empresa y existe la posibilidad de perder o no perder, pero jamás ganar. El riesgo puro en la empresa se clasifica a su vez en: *riesgo inherente* y *riesgo incorporado*.

**El riesgo inherente:** es propio de cada empresa en dependencia de la actividad que realice, estos son fenómenos producidos por factores objetivos que vienen de la misma naturaleza de la actividad empresarial. Estos riesgos se deben eliminar o controlar de inmediato, pues la existencia de la entidad depende de la actividad que realiza y como estos están en directa relación con la actividad de la empresa, si esta no los asume no puede existir.

**El riesgo incorporado:** es aquel que no es propio de la actividad de la empresa en cuestión, sino que es producto de conductas poco responsables de un trabajador, el que asume otros riesgos con objeto de conseguir algo que cree que es bueno para él y/o para la empresa, como por ejemplo ganar tiempo, terminar antes el trabajo para destacar, demostrar a sus compañeros que es mejor. Es decir, son riesgos de segundo nivel, que aparecen como resultado de errores o fallas humanas. Este tipo de riesgo se debe eliminar de inmediato.

Otra clasificación es la basada en el criterio de las principales funciones de una empresa, como por ejemplo:

**El riesgo económico:** tiene que ver con la probabilidad de perder la ventaja competitiva, de declinación de la situación financiera, de disminuir el valor de su capital.

**Los riesgos de mercado:** son riesgos relacionados con la inestabilidad de la coyuntura económica, con las pérdidas potenciales por cambios de los precios de los artículos de venta que produce la empresa, con inconvenientes de liquidez.

**El riesgo legal:** se presenta con la probabilidad de producirse pérdidas porque las actividades de la empresa no están conformes con la legislación y la normativa vigente o porque la contraparte no tiene la autoridad legal para realizar una transacción, o porque en un negocio internacional aparece una incoherencia normativa de los países involucrados.

**El riesgo reputacional:** es la posibilidad de pérdidas, a que se ve expuesta la empresa por mala imagen, publicidad negativa, que ocasionan pérdidas a los clientes, disminución de ingresos y procesos judiciales.

**El riesgo de crédito:** se produce normalmente cuando las contrapartes no cumplen sus obligaciones contractuales.

**El riesgo organizacional:** es la probabilidad de pérdidas por errores e ineficiencia de la organización interna de la empresa (fallas del control interno, de las normativas del trabajo).

**De carácter tecnológico:** son los riesgos relacionados con la probabilidad de daños ambientales, averías, incendios, fallas de los equipos tecnológicos.

El riesgo también se puede clasificar como operacional, según el Acuerdo de Capitales de Basilea II, realizado en el año 2006.

**El riesgo operacional:** “El riesgo de pérdida resultante por fallas en los procesos internos, humanos y de los sistemas o por eventos externos.”

### 1.3. Riesgos operacionales

A partir de los años 90 la tendencia existente de los riesgos se enfoca más a la administración de los mismos por parte de la dirección de las empresas, a nivel de actividades, departamentos, por lo que se adopta una visión más amplia del riesgo, incluyendo la parte operativa. Se ha generalizado además la tendencia a la elaboración de los estándares y normas nacionales para la administración de los mismos y

el desarrollo de sistemas informáticos de asesoría para su manejo en los diferentes ámbitos de la actividad económica.

Por tratarse de eventos que se encuentran generados en parte de la operación del negocio de la organización, son responsabilidad de la alta dirección de la misma. Según los lineamientos del Comité de Basilea I, realizado en Suiza, en el 1995, se le debe asignar a la alta dirección la responsabilidad directa de toda pérdida o disminución en el patrimonio de la empresa, por tanto, estos son los máximos responsables de identificar los riesgos operacionales a los cuales su institución está expuesta y asegurar la correcta y adecuada implementación de una gestión eficiente de los mismos.

O sea, la principal meta no es eliminar los riesgos operacionales, sino, ser proactivo en la identificación y gestión de los mismos, para obtener beneficios tangibles.

Los riesgos operacionales, incluyen aquellos riesgos que generan una posibilidad de desviación de los resultados esperados como consecuencia de cambios en los procesos, el comportamiento humano, sistemas internos o por eventos externos.

Utilizando las clasificaciones anteriores, los riesgos de operación pueden ser:

- Tanto propios de la actividad empresarial como provenientes del entorno.
- Económicos.
- Tanto puros como especulativos.
- Estáticos y dinámicos.

Los riesgos operacionales se constituyen de siete grandes categorías de eventos, las cuales se consideran las principales causas de las pérdidas operacionales de las entidades: [11]

- Fraude interno: son los actos que de forma intencionada buscan apropiarse indebidamente de activos de propiedad de la entidad y que implican al menos a un empleado de la misma.
- Fraude externo: son sucesos cometidos por personas ajenas a la entidad, que intentan apropiarse indebidamente de activos que son propiedad de la misma.
- Prácticas de empleo, salud y seguridad en el trabajo: obedecen a actos que son inconsistentes con las leyes o acuerdos de seguridad y salud en el trabajo.
- Prácticas con clientes, productos, y de negocio: son fallas no intencionales o negligentes que impiden satisfacer una obligación profesional con los clientes.

- Daños en activos físicos: hacen referencia a pérdidas o daños en activos físicos de la entidad, originados por desastres naturales u otros sucesos.
- Interrupción del negocio y fallas en los sistemas: obedecen a todas las interrupciones que se producen en el negocio, por motivos tecnológicos y fallas en los sistemas.
- Ejecución, entrega y gestión de los procesos: hacen referencia a las fallas en el procesamiento de las transacciones o en la gestión de los procesos.

### 1.4. Gestión del Riesgo

Según Martínez (1998) existen varias definiciones de gestión de riesgos y todas coinciden en que se trata de un método lógico y sistemático para identificar, evaluar y manejar los riesgos asociados a cualquier actividad, función o proceso, de forma tal que permita a la entidad que lo realiza, aprovechar las oportunidades de expansión minimizando las pérdidas. [12]

Pérez M. y Navarro L. (1999) definen la gestión de riesgos como el proceso para la conservación de los activos fijos y del poder de generación de beneficios de una empresa, mediante la minimización del efecto financiero de las pérdidas accidentales. Asimismo, su principal objetivo es la planificación efectiva de los recursos necesarios para recuperar el equilibrio financiero y la efectividad operativa después de una pérdida fortuita y de esta forma, obtener a corto plazo una estabilidad del costo de los riesgos y a largo plazo la minimización de los riesgos.[13]

Pero sin dudas la definición más acabada desde el punto de vista del alcance de la gestión de riesgos, es la dada por COSO (2004), que en su informe señala: *“La gestión de los riesgos empresariales es un proceso, efectuado por la dirección de la entidad, directores y demás personal, aplicado a la estrategia y al establecimiento de objetivos y que se desarrolla a través de toda la organización, destinado a identificar los eventos potenciales que pueden afectar la entidad y manejar los riesgos dentro de su apetito de riesgo para proveer una seguridad razonable en el logro de los objetivos de dicha entidad”*. [14]

La gestión de riesgos se desarrolla como un proceso, con sus entradas, transformación y salidas. Las entradas al proceso son los eventos (riesgos), la transformación ocurre cuando se analizan los riesgos y se valoran todas las posibles formas de tratamiento que requieren en función de su frecuencia e impacto, y las salidas son los riesgos controlados.



### 1.4.1. La gestión de Riesgos a nivel internacional

Tradicionalmente la gestión de riesgos ha sido considerada como un proceso de tres etapas: identificación, evaluación o análisis y control o tratamiento de riesgos. Aunque estas pudieran llamarse “el núcleo” del proceso de gestión de riesgos, en la práctica, su ejecución sin un nexo con la misión, la estrategia, los objetivos y en general, con la gestión empresarial, le resta eficacia en sus resultados.

Este antiguo paradigma de la gestión de riesgos comenzó a cambiar a mediados de la pasada década, cuando sale a la luz la primera versión del estándar Australiano Neozelandés sobre administración de riesgos. Este propone un proceso más detallado, que incluye además de la identificación, análisis, evaluación y tratamiento de los riesgos, otras tareas que contribuyen a la incorporación de la administración de riesgos a la dirección estratégica de la organización. Estas tareas son: establecer el contexto, comunicar y consultar, y monitorear y revisar.

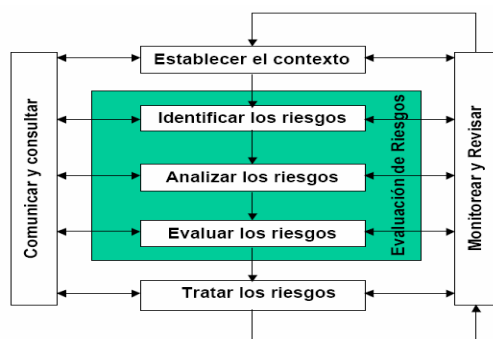


Figura 1. Vista general del proceso de administración de riesgos.

Fuente: Estándar Australiano/Neo Zelandés de Administración de Riesgos.

Establecer el contexto partiendo de las etapas del proceso de gestión de riesgos, no es más que la caracterización del entorno (contexto externo), las condiciones internas de la organización (contexto interno) y el contexto de la administración de riesgos. Establecer el contexto consiste en definir los parámetros básicos dentro de los cuales se deben administrar los riesgos y establecer el alcance para el resto del proceso de gestión de riesgos.

La comunicación y consulta con los interesados son elementos permanentes de todo el proceso de gestión de riesgos. Se justifica esta etapa por la necesidad de un trabajo en equipo que propicie la identificación eficaz de los riesgos, la consideración de diferentes puntos de vista en su evaluación y una administración apropiada de cambios durante el tratamiento de los mismos.

El estándar propone la etapa de monitoreo y revisión de todos los pasos del proceso como condición para la mejora continua. Ya que los cambios que caracterizan el entorno empresarial pueden provocar alteraciones tanto de la frecuencia como del impacto de determinados riesgos, además de que pueden surgir nuevos riesgos, es necesario repetir el ciclo de gestión de riesgos regularmente. Este monitoreo es una fuente de aprendizaje para la organización.

Otra organización, PriceWaterhouse Coopers (PWC), desarrolló un estudio sobre la gestión de los riesgos de operación, cuyos principales elementos se exponen seguidamente.

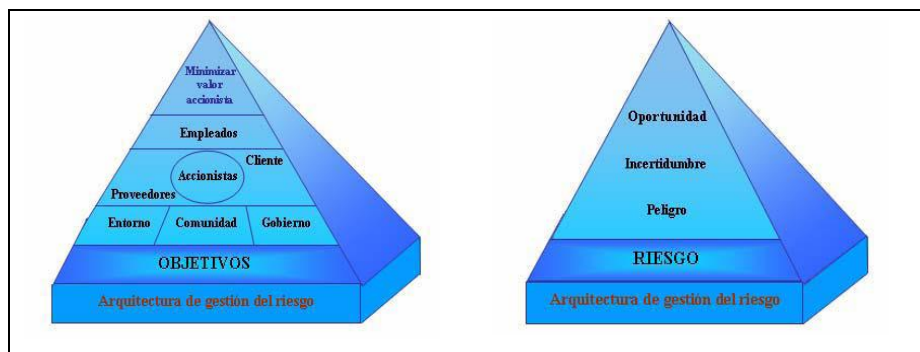
En primer lugar, consideran que la gestión de los riesgos operativos en el máximo nivel tiene dos componentes fundamentales:

- Integridad operativa.
- Materialización o prestación de servicios.

Se entiende por integridad operativa la idoneidad de los controles operativos y el gobierno empresarial. Tiene que ver, por tanto, con la gestión de los riesgos operativos derivados de la falta de supervisión directiva, de errores, fraude, controles internos deficientes e incumplimiento de resoluciones de organismos rectores. [15]

La materialización de las operaciones se relaciona con la capacidad de la empresa para llevar a cabo los procesos empresariales de forma constante. Incluye la gestión de la capacidad, de los proveedores, del servicio, del abastecimiento, de los recursos humanos, del riesgo del proyecto y de las crisis.

En segundo lugar, PWC propone una estructura de administración de los riesgos operativos representado gráficamente por una pirámide de cuatro lados sobre una base. Cada lado representa un aspecto esencial de la misma, en cuya base se instaura una arquitectura de gestión de riesgos que cubre toda la empresa, tal y como se muestra en la figura 2.



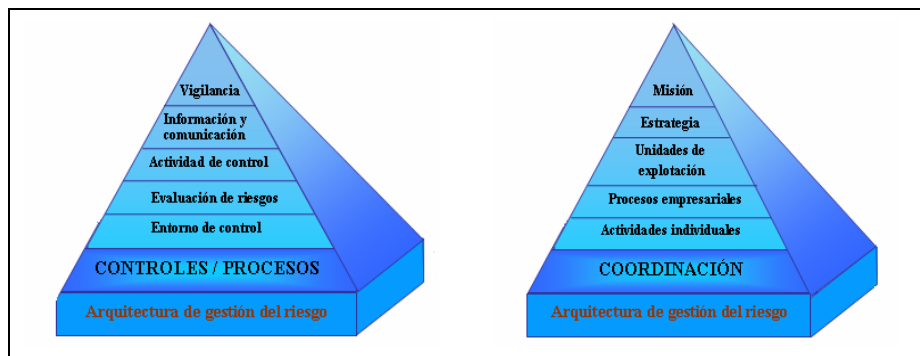


Figura 2. Estructura de la gestión del riesgo operativo.

Fuente: Frost y otros (2002). Manual de gestión de riesgos operativos.

PWC reconoce la necesidad de partir de los objetivos de la entidad en el proceso de la administración de riesgos, pero sitúa en su más alto nivel, la maximización del valor para el accionista. Plantea que los objetivos suelen estar conectados con la necesidad de satisfacer a los grupos de interesados más importantes, que pueden repercutir en el rendimiento de la organización, o que se pueden ver afectados por dicho rendimiento. Los interesados incluyen empleados, propietarios, directivos, asociados empresariales mediante contratos de cooperación, proveedores, clientes, acreedores, comunidad, gobierno. Sin embargo, estos interesados no siempre son visibles para la empresa y pueden estar en contradicción. Los objetivos de la propia organización podrían ser una mejor guía para este proceso.

El segundo lado de la pirámide señala los riesgos. Estos son concebidos desde tres perspectivas diferenciadas: el riesgo como peligro, como oportunidad y como incertidumbre. Gestionar el riesgo como peligro consiste en instalar técnicas de gestión que produzcan las probabilidades de que se produzca el evento negativo, sin incurrir en costos excesivos que paralicen la organización. Gestionar el riesgo como oportunidad significa gestionar el potencial de mejoría del riesgo, tomar decisiones para aprovechar las oportunidades del entorno, aumentar las probabilidades de éxito y reducir probabilidades de fracaso. La gestión del riesgo como incertidumbre, trata de asegurar que el rendimiento real de una organización quede dentro de una banda definida. La gestión del riesgo en esta función trata de reducir la variabilidad entre los resultados previstos y los resultados reales.

El tercer lado de la pirámide (controles y procesos) señala sus componentes: entorno de control, evaluación de riesgos, actividad de control, información y comunicación, vigilancia o supervisión.

La coordinación es el cuarto lado de la pirámide. Está consiste en lograr la debida conexión entre los objetivos de la organización, la estrategia y los procesos con las acciones individuales de los empleados.

La arquitectura de administración de riesgos facilita los recursos y la infraestructura necesaria para asegurar la aplicación consistente de los componentes de la pirámide e incluye: un idioma común, liderazgo, recursos, tecnología, medición, información y organizaciones.

Sin dudas PWC identifica todos los elementos necesarios a tomar en consideración por la administración de los riesgos, pero no están claros en la pirámide la forma en que se relacionan sus diferentes elementos, ni la secuencia lógica de su procedimiento.

La propuesta de COSO parte de la relación entre los objetivos de la entidad, los componentes del proceso de administración de riesgos y los niveles de la entidad, la cual es representada mediante un cubo.



*Figura 3. Relación entre los objetos, niveles organizacionales y componentes de la administración de riesgos empresariales.*

*Fuente: COSO: Enterprise Risk Management.*

Los objetivos de la entidad, representados en columnas, son clasificados en cuatro categorías:

- Estratégicos: Objetivos de alto nivel, alineados con la estrategia y la misión.
- Operacionales: Uso eficaz y eficiente de los recursos.
- De información: Confiabilidad de la información.
- De cumplimiento: Cumplimiento de las regulaciones y leyes aplicables.

Reconoce ocho componentes de la administración de riesgos empresariales:

- ❖ Ambiente interno: Abarca la cultura de la organización, que influye en la conciencia de sus empleados sobre el riesgo y forma la base de los otros componentes de la gestión de los riesgos

corporativos, incluye la filosofía de administración de riesgos de una entidad, su riesgo aceptado, la supervisión ejercida por el consejo de administración, la integridad, valores éticos y competencia de su personal y la forma en que la dirección asigna la autoridad y responsabilidad, y organiza y desarrolla a sus empleados.

- ❖ Establecimiento de objetivos: Los objetivos se fijan a escala estratégica, estableciendo con ellos una base para los objetivos operativos, de información y de cumplimiento. Una condición previa para la identificación eficaz de eventos, la evaluación de sus riesgos y la respuesta a ellos es fijar los objetivos, que tienen que estar alineados con el riesgo aceptado por la entidad, que orienta a su vez los niveles de tolerancia al riesgo de la misma.
- ❖ Identificación de los eventos: la dirección identifica los eventos potenciales que, de ocurrir, afectaran a la entidad y determina si representan oportunidades o si pueden afectar negativamente a la capacidad de la empresa para implantar la estrategia y lograr los objetivos con éxito. Los eventos con impacto negativo representan los riesgos, que exigen la evaluación y respuesta de la dirección. Los eventos con impacto positivo representan oportunidades, que la dirección reconduce la estrategia y el proceso de fijación de objetivos. Cuando identifica los eventos, la dirección contempla una serie de eventos internos y externos que pueden dar lugar a riesgos y oportunidades, en el contexto del ámbito global de la organización.
- ❖ Evaluación de los riesgos: Permite a una entidad considerar la amplitud con que los eventos potenciales impactan en la consecución de los objetivos. Los riesgos se evalúan desde una doble perspectiva – probabilidad e impacto – con una combinación de métodos cualitativos y cuantitativos.
- ❖ Respuestas a los riesgos: Una vez evaluados los riesgos relevantes, la dirección determina cómo responder a ellos. Las respuestas pueden ser: evitar, reducir, compartir y aceptar el riesgo. Al considerar su respuesta, la dirección evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios, y selecciona aquella que sitúe al riesgo residual dentro de las tolerancias al riesgo establecidas.
- ❖ Actividades de control: Son las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las respuestas de la dirección a los riesgos. Estas tienen lugar a través de la organización, a todos los niveles y en todas las funciones. Incluyen aprobaciones, autorizaciones, verificaciones,

conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones.

- ❖ **Información y Comunicación:** la formación pertinente se identifica, capta y comunica de una forma y en un marco de tiempo que permite a las personas llevar a cabo sus responsabilidades. Los sistemas de información usan datos generados internamente y otras fuentes externas. Sus salidas informativas facilitan la administración de riesgos y la toma de decisiones informadas relativas a los objetos. Debe existir una comunicación eficaz fluyendo en todas direcciones dentro de la organización, a todos los niveles, así como una comunicación eficaz con terceros: clientes, proveedores, reguladores, propietarios.
- ❖ **Supervisión:** se revisa la presencia y funcionamiento de los componentes de la administración de riesgos a lo largo del tiempo mediante actividades permanentes de supervisión, evaluaciones independientes o una combinación de ambas técnicas. Las deficiencias que se detectan se comunican de forma ascendente, trasladando los temas más importantes a la alta dirección y al consejo de administración.

Una de las caras del cubo representa los niveles de la organización. Significa que en cada nivel empresarial, que tiene sus propios objetivos definidos, se ejecutan todos los componentes de la administración de riesgos.

Adoptar una u otra propuesta metodológica de gestión de riesgo, debe hacerse valorando las condiciones de la empresa y el entorno en que se desenvuelve su actividad económica, incluyendo el nivel de desarrollo económico y social.

Ninguno de estos modelos de gestión de riesgos profundiza en el tema de los métodos para la evaluación de los riesgos, por no ser ese su objetivo. Como modelos se proponen exponer principios, conceptos y un lenguaje común para todos los implicados en la gestión de riesgos en la sociedad. La selección de los métodos y técnicas está en manos de los encargados de evaluar los riesgos en la empresa.

### **1.4.1.1. Software para la Gestión y Administración de Riesgos**

Los sistemas informáticos en la actualidad son la columna vertebral de cada empresa en el mundo, contribuyendo a contener una fuente de poder invisible, el poder de la información. Hoy en día se cuenta, con una serie de sistemas para la gestión y administración de riesgos, los cuales, son una importante

herramienta para la Auditoría y Control Interno. Su principal objetivo es contribuir con las soluciones integrales propias de cada organización, para que disminuyan los riesgos que puedan afectar en el logro de los objetivos y metas de estas, optimizando cada uno de los procesos de la gestión de riesgos.

### **ERM Suite – Enterprise Risk Management**

Este sistema permite a las empresas identificar, analizar, evaluar, monitorizar y administrar los riesgos corporativos de manera integrada. Posee una biblioteca reutilizable de riesgos, controles y evaluaciones, eventos de pérdida y no conformidades, acciones y planes de tratamiento. Ofrece además una solución perfecta para gestionar riesgos en todos los contextos organizacionales o empresariales.

Esta suite permite la producción de reportes que proporcionan a los gestores una información exacta y rápida en relación con los riesgos, facilitando la toma de decisiones estratégicas y aumentando la confiabilidad en el proceso de gestión de riesgos.

Cuenta con un gran número de elementos para realizar este proceso como:

- ❖ **Definición del contexto:** Define el contexto (actividad, proceso, función, proyecto o activo) en términos de responsabilidades y equipo de trabajo tal como metas y objetivos.
- ❖ **Gestión de procesos:** Provee una plataforma integrada para la descripción y modelado de procesos colaborativos que pueden ser utilizados en el análisis de riesgos.
- ❖ **Identificación de riesgos:** Facilita la identificación de los riesgos, haciendo uso de la aplicación de checklist y de un repositorio unificado de riesgos.
- ❖ **Análisis de riesgos:** Herramienta que permite la aplicación de métodos cuantitativos y cualitativos, o la combinación de ellos. Visualización gráfica de los riesgos significativos.
- ❖ **Controles:** Establece e implementa políticas y procedimientos garantizando la efectividad de las respuestas a los riesgos.
- ❖ **Plan de tratamiento:** Suite completamente integrada para seleccionar, implementar y monitorizar planes de respuesta a los riesgos sin exigir herramientas adicionales o personalizaciones.
- ❖ **Monitoreo:** Actividades de acompañamiento, automáticas o manuales, utilizando listas sintéticas, matrices de riesgo, indicadores de acompañamiento y otras.

- ❖ Gestión de eventos: Completa automatización del tratamiento de los eventos, no conformidades y acciones correctivas/preventivas, utilizando métodos mundialmente consagrados para solución de problemas y la planificación de acciones.
- ❖ Inteligencia empresarial: Dispone reportes por área de negocio y auxilia a los usuarios en la identificación de áreas con problemas.

### **Audicontrol**

Es un software orientado al usuario final, para apoyar las actividades de diseño e implementación de Sistemas de Gestión de Riesgos Operacionales (SGRO) en los procesos de la cadena de valor, procesos de Tecnología de la Información (TI) y aplicaciones de computador (sistemas de información automatizados). Cuenta con una gestión de riesgos por procesos (permite identificar, medir, controlar y monitorear los riesgos de cada proceso o sistema).

Este sistema permite a las empresas evaluar los riesgos potenciales que podrían presentarse en los nuevos servicios y negocios automatizados. Cuenta con un mapa de riesgo para los sistemas en desarrollo o adquisición y la fundación de los servicios de información.

También cuenta con una base de datos de conocimientos con los resultados de estudios realizados, personalizada con circunstancias particulares de las empresas (bases de trabajo), guías de control y autoevaluación del control, para dependencias usuarias de los nuevos sistemas y el departamento de sistemas, así como manuales de control interno para el departamento de sistemas y las nuevas aplicaciones desarrolladas o adquiridas.

### **Risk Advisor**

Es una herramienta que asiste paso a paso la implementación del Sistema de Administración Integral del Riesgo (SAIR), en todos los procesos, proyectos u otras actividades críticas para el logro de los objetivos y metas estratégicas de una empresa. Permite identificar el nivel real de exposición de riesgos de la organización y generar diversos mapas de riesgos a diferentes niveles.

Combina proactivamente la información sobre las amenazas, vulnerabilidades y medidas correctoras, para determinar con exactitud qué activos corren verdaderamente riesgo. Despeja las dudas sobre cuándo y dónde se debe centrar esfuerzos de seguridad, con lo que se ahorra tiempo y dinero.



Este sistema provee además una metodología y una guía genérica para la implementación del proceso de gestión de riesgos, considerando todas las etapas: Entender el contexto, identificar, analizar, valorar, tratar y monitorear todos los riesgos que puedan afectar los objetivos y metas de la organización.

### 1.4.2. La Gestión de Riesgos en Cuba

En Cuba, en el ámbito legislativo, no existe una legislación específica para la gestión de riesgos en forma integral y abarcadora de toda la organización. En realidad la necesidad de conocimientos sobre sus técnicas particulares surge con la promulgación de la Resolución No. 297-2003 sobre el Control Interno del MFP, la cual identifica la evaluación de los riesgos como el segundo componente del sistema de control interno de una organización.

Esta resolución surge a partir de la necesidad de normar el conjunto de procedimientos y normas, por cada empresa o entidad, teniendo en cuenta las leyes y procedimientos en el país.

Además, establece que el control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las entidades. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza, se evalúa la vulnerabilidad del sistema. [16]

Este sistema de control interno, al igual que la primera versión de COSO (1992), cuenta con 5 componentes básicos:

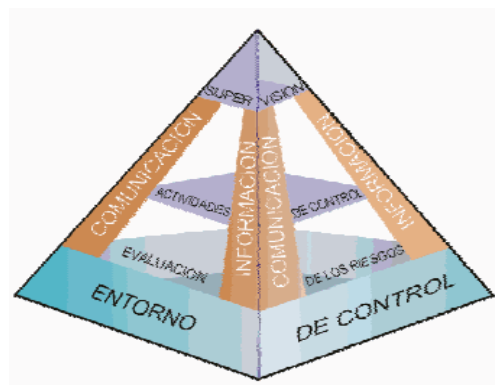


Figura 4. Relación entre los componentes de la resolución 297.

Fuente: Resolución 297-MFP.

Estos cinco componentes, están interrelacionados y no se pueden ver de forma independiente, constituyendo su integración la clave del éxito para su adecuado funcionamiento. Cada uno de estos

componentes tiene una orientación importante, lo que contribuye a un sistema de control interno integrado, que evalúa si la estructura es adecuada al tamaño de la entidad, tipo de actividad y objetivos aprobados, así como, que la línea de responsabilidad y autoridad estén bien definidas, al igual que los canales por lo que fluye la información.

**El Ambiente o Entorno de Control:** constituye la base de todos los demás componentes, es la plataforma para el desarrollo de las acciones y refleja la actitud asumida por la alta dirección en relación con la importancia del control interno y su incidencia sobre las actividades de la entidad y sus resultados, por lo que debe tenerse presente todas las disposiciones, políticas y regulaciones que se consideren necesarias para su implementación y desarrollo exitoso. Además, en esta etapa se definen y establecen aspectos organizativos que requiere la entidad para su funcionamiento, se diseña la preparación del personal y se crea una cultura ética.

**La Evaluación de Riesgos:** es un paso importante para cualquier organización, ya que se enfrentan diariamente a diversos riesgos, tanto de origen externo como interno, que tienen que ser evaluados. La primera condición previa a la evaluación de los riesgos es la identificación de los objetivos a distintos niveles. La evaluación de riesgos consiste en la identificación y el análisis de los riesgos relevantes que puedan afectar el éxito de los objetivos. Debido a diversos factores, los riesgos pueden estar cambiando continuamente, por lo que deben estar orientados al futuro y para ello es necesario disponer de mecanismos para identificar los nuevos riesgos y enfrentar los conflictos asociados al cambio.

**Las Actividades de Control:** son las políticas y procedimientos que contribuyen a que se lleven a cabo todas las tareas orientadas por la dirección. Ayudan a asegurar que se tomen todas las medidas que sean necesarias para controlar los riesgos que afectan el cumplimiento de los objetivos y son aplicables en toda la organización, a todos los niveles y en todas las funciones.

**La Información y Comunicación:** se necesita a todos los niveles de la organización, para identificar, evaluar, y responder a los riesgos. En esta etapa se capta, procesa y transmite información de tal modo que llegue a todos los sectores, por lo que los informes deben transmitirse a través de una comunicación eficaz, con una información clara y con un grado de detalle ajustado al nivel de la toma de decisiones para apoyar la política, misión y objetivos de la entidad.

**La Supervisión y Monitoreo:** es el proceso que evalúa la calidad del control interno y determina si este opera en la forma esperada y si es necesario hacer modificaciones en el mismo. Esta etapa debe ser

monitoreada con instrumentos de supervisión eficaces (observaciones, revisiones sorpresivas) realizadas de forma permanente por los directivos y auditores internos, con el objetivo de poder asegurar que el control interno funciona de forma adecuada y determinar el grado de efectividad de la actividad de control. En este proceso es de vital importancia que se accione con medidas concretas sobre los resultados obtenidos en la supervisión y se interactúe de forma inmediata en la solución de los problemas detectados.

Sin dudas el desarrollo de la evaluación de riesgos en el marco de la citada resolución ha prestado deficiencias, entre cuyas causas está la escasa cultura de gestión de riesgos presente en un gran número de entidades cubanas y que incluye el desconocimiento de técnicas de evaluación, más allá de lo sugerido por esta resolución.

### **1.5. Propuesta de un marco conceptual para la gestión de riesgos en la UCI**

Por todo lo antes expuesto, la Resolución 297-2003 del MFP no provee todos los elementos necesarios para una correcta implementación de la gestión de riesgos, por lo que se propone que la metodología a usar por la universidad esté basada en el marco conceptual y estándar, COSO II, que brinda todos los elementos necesarios para la gestión de los riesgos empresariales, dentro de los cuales se encuentran los riesgos operacionales. Además, es el marco conceptual más usado en el mundo en cuanto a la gestión de riesgos, por la gran especificidad de su contenido, que ha servido de guía a un gran número de empresas en el mundo. De esta manera, no solo se podrán gestionar los riesgos operacionales en la universidad, sino que también se podrán gestionar cualquier tipo de riesgos empresariales que se presenten, mejorando la calidad del control interno.

### **1.6. Método para la identificación, evaluación y tratamiento de los riesgos**

La identificación, evaluación y tratamiento de los riesgos constituyen el núcleo de la administración de riesgos. Su ejecución requiere de técnicas específicas que han sido desarrolladas a lo largo del tiempo y aplicadas en áreas aisladas o por entidades, para alcanzar los objetivos planteados, sin sufrir mayores consecuencias cuando se presenten eventos que generen riesgo y poder plantear oportunamente las acciones correctivas y preventivas que puedan mitigar su impacto o a prevenir su ocurrencia.

## **Identificación de los riesgos**

Según Edmundo Pelegrin (2004), el proceso de identificar los riesgos debe incluir un ambiente en el que las personas sientan la libertad de expresar puntos de vista especulativos o controversiales. Cuando los riesgos se perciben como algo negativo, los integrantes de un equipo se sienten renuentes a informar sobre ellos. En algunos proyectos, el mencionar los riesgos nuevos se toma como una queja. En ciertas situaciones, una persona que habla de los riesgos recibe el calificativo de conflictiva y las reacciones se encuentran en la persona, antes que en los riesgos. Bajo estas circunstancias, los miembros de un equipo tienen reservas para comunicar sus opiniones con libertad. Seleccionan y suavizan la información de riesgos que deciden compartir, para que no resulte demasiado negativa en relación con las expectativas de los demás integrantes. [17]

El proceso de identificación de los riesgos debe ser permanente e interactivo, integrado al proceso de planeación, teniendo en cuenta los factores que pueden incidir en la aparición de los riesgos, ya sean externos o internos, en los cuales se debe verificar si hay señales de cambio en sus estructuras o en los procesos y tendencias que podrían exponer la empresa a riesgos. En este proceso se debe determinar qué, dónde, cuándo, cómo, por qué o por quién, pueden ser originados los hechos que influyen en la obtención de los resultados. [18]

El resultado final de este proceso es un inventario lo más completo posible de los riesgos a que está expuesta la organización por áreas, procesos, productos, proyectos. Este inventario se debe hacer continuamente, al igual que la identificación de nuevos riesgos, que pueden ir surgiendo o cambiando, al cambiar las condiciones tecnológicas, los requerimientos de seguridad, entre otros factores, por lo que este debe ser un proceso dinámico. La actualización permanente de este inventario se convierte en una condición necesaria para el logro de un proceso eficaz de gestión de riesgos.

## **Evaluación de los riesgos**

Una de las finalidades que se persigue con la identificación de los riesgos es la evaluación de los mismos. Esta incluye la magnitud de las consecuencias de los eventos potenciales y sus frecuencias, para establecer el nivel de riesgo y el establecimiento de un orden de prioridad para el tratamiento de los mismos. La evaluación de riesgos es utilizada para asistir en la decisión de tolerar o tratar un riesgo.

Si no existen datos estadísticos sobre ocurrencias pasadas del riesgo no se conoce la dimensión del daño que pueda causar, no puede utilizarse la teoría de las probabilidades. Gil Lafuente (1993) explica que para

poder aplicar la teoría de las probabilidades son necesarias dos condiciones: una sucesión de fenómenos que se hayan repetido en determinadas condiciones y además, poder aplicar los resultados obtenidos sobre otro fenómeno sometido a las mismas condiciones. [19] Resulta pues, más adecuado, el término de “frecuencia” para señalar la periodicidad de manifestación de un riesgo.

La metodología de evaluación de los riesgos de una entidad consiste en una combinación de las técnicas cualitativas y cuantitativas. Se aplican técnicas cualitativas cuando los riesgos no se prestan a la cuantificación o cuando no están disponibles datos suficientes y creíbles para una evaluación cuantitativa o la obtención y análisis de ellos no resulte eficiente por su coste. Las técnicas cuantitativas típicamente aportan más precisión y se usan en actividades más complejas y sofisticadas, para complementar las técnicas cualitativas. [20]

Tanto el análisis cualitativo como el cuantitativo se calculan mediante la fórmula:

$$R = P \times I$$

$R$  es el valor del riesgo.

$P$  es la probabilidad o frecuencia de ocurrencia del riesgo.

$I$  es la consecuencia o impacto que puede ocasionar a la organización la materialización del riesgo.

Cuando se realiza un análisis cualitativo, se utilizan formas descriptivas para representar la magnitud de impactos potenciales y la posibilidad de ocurrencia. La propia entidad diseña una escala ajustada a las circunstancias, de acuerdo a su necesidad particular o a la del riesgo evaluado.

El análisis cuantitativo contempla valores numéricos. La calidad de este proceso depende de lo exactas y completas que estén estas cifras utilizadas, la forma en la cual son expresadas la probabilidad y el impacto y la forma en la que pueden ser combinadas para proveer el nivel del riesgo que puede variar de acuerdo con el tipo del riesgo.

Las técnicas cuantitativas de evaluación de riesgos pueden utilizarse cuando existe suficiente información para estimar la probabilidad o consecuencia del riesgo, empleando mediciones de intervalo o de razón. Los métodos cuantitativos incluyen técnicas probabilísticas y no probabilísticas. Una consideración importante en la evaluación cuantitativa es la disponibilidad de la información precisa, ya sea de fuentes internas o externas y uno de los retos que plantea el uso de estas técnicas es el de obtener suficientes datos válidos. [21]

Las técnicas probabilísticas miden la probabilidad y la consecuencia de un determinado número de resultados, basándose en premisas del comportamiento de los eventos en forma de distribución estadística. Los modelos de valor en riesgo son los más conocidos dentro de las técnicas probabilísticas. [22]

Las técnicas no probabilísticas se emplean para cuantificar la consecuencia de un posible evento sobre hipótesis de distribuciones estadísticas, pero sin asignar una probabilidad de ocurrencia al acontecimiento. De este modo, estas técnicas requieren, por parte de la dirección, la determinación por separado de esta probabilidad. [23]

Las evaluaciones de riesgo se representan de forma tal que faciliten su utilización. En especial, en la evaluación cualitativa, donde los riesgos no se resumen en una cifra o intervalo numérico, se perfeccionan los mapas de riesgos.

Un mapa de riesgo o una matriz de riesgo, es una representación gráfica de la probabilidad y consecuencia de uno o más riesgos. Los riesgos se representan de manera que los más significativos (mayor probabilidad de ocurrencia) resalten, diferenciándolos de los menos significativos (menor probabilidad de ocurrencia). Cada nivel de riesgo puede diferenciarse por color. [24]

Los riesgos se organizan en orden de prioridad, en función de su nivel. El tratamiento que requiere cada uno de ellos depende de su nivel de prioridad y la naturaleza del riesgo. Los riesgos de alta prioridad exigen medidas más costosas y urgentes, que los riesgos de escasa probabilidad y leve consecuencia.

### **Tratamiento de los riesgos**

Una vez que se tienen identificados los riesgos y evalúan las opciones para tratar este riesgo, se procede a preparar e implementar los planes para dar tratamiento a estos riesgos de acuerdo con la prioridad que tengan.

Después de identificar y evaluar cada riesgo, es decisión de la empresa o entidad tratarlos o no. Si un riesgo no es tratado esto significa que es asumido o retenido. Cuando se trate de riesgos de bajo impacto financiero la empresa puede optar por asumirlos, ya que podría resultar más costosa la aplicación de alguna medida que la pérdida que pudiera ocasionar el riesgo en caso de que se produjera.

Las opciones de tratamiento de los riesgos se evalúan sobre la base de su eficacia para reducir las pérdidas potenciales y/o alcanzar un beneficio adicional. La opción más apropiada será la que alcance un balance favorable entre el costo de su implementación y los beneficios derivados de la misma.

Un análisis particular merecen los riesgos de muy poca frecuencia pero con impactos severos. Su tratamiento quizás amerite acciones más estrictas.

## 1.7. Herramientas y tecnologías

### 1.7.1. Aplicaciones Web

Las aplicaciones web son soluciones informáticas que los usuarios utilizan accediendo al servidor a través de Internet o una intranet. Estas son desarrolladas no sobre una plataforma o sistema operativo, sino que se montan sobre un servidor en una intranet o Internet al cual se accede a través de un navegador de web, y contienen bases de datos e información dinámica. Estas aplicaciones permiten usar al máximo las ventajas de Internet, ya sean intranet o extranet, de este modo la información que se captura en el sistema desde los diferentes clientes, es procesada automáticamente en tiempo real.

### 1.7.2. Lenguaje de programación

PHP es un lenguaje script de programación, interpretado en el lado del servidor, bajo el acrónimo de **Hypertext Preprocessor**, el cual se utiliza para el desarrollo de páginas web dinámicas. Generalmente se ejecuta en un servidor web, tomando el código PHP como entrada y creando páginas web como salidas. La mayor parte de su sintaxis ha sido tomada de lenguajes de programación como C, Java y Perl. Puede ser desplegado en la mayoría de los servidores web y en casi todos los sistemas operativos. Actualmente es muy popular y extendido en la web, debido a que es una tecnología de código abierto y sus fragmentos de código se intercalan fácilmente en páginas HTML.

PHP posee importantes características, como por ejemplo:

- ❖ **Velocidad:** No solo brinda velocidad en la ejecución, sino que además no crea demoras en la máquina. Por esta razón no debe requerir demasiados recursos del sistema.
- ❖ **Estabilidad:** PHP utiliza su propio sistema de administración de recursos y dispone de un sofisticado método de manejo de variables, conformando un sistema robusto y estable.
- ❖ **Seguridad:** el sistema debe poseer protecciones contra ataques. PHP provee diferentes niveles de seguridad, estos pueden ser configurados desde el archivo **.ini**

- ❖ **Simplicidad:** Usuarios con experiencia en C y C++ podrán utilizar PHP muy rápidamente y con facilidad. Aprenderlo también es muy simple.
- ❖ **Sintaxis cómoda:** PHP cuenta con una sintaxis similar a la de C, C++ o Perl. Lo más destacado ocurre a nivel semántico: el tipado es muy poco estricto. Es decir, cuando creamos una variable no hay que indicar de que tipo es, pudiendo guardar en ella cualquier tipo. Es muy flexible y cómodo para desarrollar, aunque los errores que se cometen pueden ser mucho más graves y difíciles de corregir, al reducirse mucho las posibilidades del intérprete para detectar incompatibilidades entre las variables.
- ❖ **Multiplataforma:** PHP funciona en diversos sistemas operativos, Servidores HTTP y Bases de Datos.
- ❖ **Ejecución en Servidor:** Las páginas que se ejecutan en el servidor pueden realizar accesos a bases de datos, conexiones en red y otras tareas para crear la página final que verá el usuario. Dado que la página resultante contiene únicamente código HTML, es compatible con todos los navegadores.
- ❖ **Compatibilidad con bases de datos:** Una de las características más fuertes del PHP es su amplio soporte para una gran cantidad de bases de datos. Tiene acceso a un gran número de gestores de bases de datos: Adabas D, dBase, Empress, Ingress, InterBase, FrontBase, DB2, Infomix, mSQL, MySQL, ODBC, Oracle, PostgreSQL, Sybase y otras.
- ❖ **Extensa librería de funciones:** Cuenta con una extensa librería de funciones, que facilitan enormemente el trabajo de los desarrolladores.
- ❖ **Expansión:** PHP está alcanzando unos niveles de uso tan elevados que hacen que el conocimiento sea algo indispensable para los profesionales del desarrollo en Internet. Se estima que es usado por cientos de miles de programadores y muchos millones de sitios informan de que lo tienen instalado, sumando más del 20% de los dominios en Internet.

Por todo lo expuesto anteriormente, se toma PHP como el adecuado para implementar la propuesta de sistema del presente trabajo, ya que es un lenguaje estable y además incluye una gran variedad de características, que lo hacen muy popular, entre los lenguajes script.



## 1.7.3. Servidor de aplicaciones web

El servidor web que se ha decidido proponer es el Apache, debido a su configurabilidad, robustez y estabilidad, que hacen que cada vez más servidores lo utilicen a escala mundial, lo que se debe en gran parte a que es Freeware bajo licencia GPL, y a las múltiples posibilidades que brinda.

El hecho de ser multiplataforma, es también una característica importante para su enorme proliferación. Hay versiones para los sistemas operativos más usados (Windows, Linux, Unix, Solaris, Mac, entre otros).

Otra de las características más atractivas que posee este servidor, es que continuamente está añadiendo nuevas características y mejoras, lo cual garantiza un crecimiento futuro. Además, es relativamente fácil de configurar, puesto que solamente existe un fichero de configuración.

Este servidor está estructurado por módulos. La configuración de cada módulo se hace mediante la configuración de las directivas que están contenidas dentro del módulo. Los módulos de Apache se pueden clasificar en 3 categorías: [25]

- ❖ **Módulos Base:** Módulo con las funciones básicas del Apache.
- ❖ **Módulos Multiproceso:** Maneja las peticiones realizadas al servidor. Se han diseñado varios módulos multiproceso para cada uno de los sistemas operativos sobre los que se ejecuta el Apache, optimizando el rendimiento y rapidez del código.
- ❖ **Módulos Adicionales:** Cualquier otro módulo que le señala una funcionalidad al servidor.
- ❖ Todas las funciones básicas de los módulos y sus configuraciones se pueden encontrar en el fichero de configuración *httpd.conf*.

## 1.7.4. Ambiente de Desarrollo Integrado (IDE)

El NetBeans IDE es un ambiente libre de desarrollo integrado para desarrolladores de software. El mismo ofrece todas las herramientas necesarias para crear escritorios profesionales, Enterprise, Web y aplicaciones móviles en diferentes lenguajes, entre ellos PHP. Este IDE es de fácil instalación y uso, se ejecuta en Windows, Linux, Mac y Solaris, además está disponible en múltiples idiomas.

También cuenta con otras características como:

- ❖ Simple configuración de nuevos proyectos, tanto para trabajo local o remoto, además de la posibilidad de personalizar el entorno de trabajo.

- ❖ Cuenta con un autocompletado de código inteligente y capaz, que se nutre del código fuente para proporcionar acceso directo a sus distintos elementos y mejor aún, permite navegar entre elementos, haciendo clic en ellos, por lo que no se limita al autocompletado, sino que ofrece ayuda sobre los distintos indicadores.
- ❖ No solo acepta Plugins, sino que el mismo entorno integra un gestor de Plugins, haciendo sencilla su instalación y desinstalación.
- ❖ Cuenta con un depurador de código no solo PHP, sino también existe la posibilidad de depurar código JavaScript.

Por todas estas características se ha decidido proponer este potente IDE para el desarrollo del sistema.

### 1.7.5. Marco de trabajo o Framework

**Codeigniter** es un conjunto de herramientas para programadores que utilizan PHP, con licencia Open Source. Su objetivo es permitirles a los programadores, desarrollar proyectos mucho más rápido, utilizando un rico juego de librerías para tareas comúnmente necesarias, así como una interfaz simple y estructura lógica para acceder a esas librerías.

Entre las principales características podemos encontrar: [26]

- ❖ Realmente rápido: es difícil encontrar un entorno de trabajo con un desempeño como el suyo.
- ❖ Verdaderamente liviano: el núcleo del sistema sólo requiere unas pocas y pequeñas librerías. Las librerías adicionales son cargadas dinámicamente a pedido
- ❖ Usa MVC (Modelo-Vista-Controlador): lo que permite una buena separación entre la lógica y presentación.
- ❖ Extensible: el sistema puede ser fácilmente extensible a través del uso de plugins y librerías asistentes, o a través de extensión de clases o ganchos del sistema.
- ❖ Genera URLs limpias: estas URLs son limpias y amigables a los motores de búsqueda.
- ❖ Paquetes: vienen con un conjunto de librerías que le permiten realizar las tareas de desarrollo web más comúnmente necesarios como por ejemplo acceder a una base de datos.

Debido a que las características antes mencionadas simplifican el trabajo y minimizan la duración del proyecto, se ha decidido proponer este potente framework, para el desarrollo del sistema.

## 1.7.6. Lenguaje de modelado

Lenguaje Unificado de Modelado o UML por sus siglas en inglés (Unified Modeling Language), es el lenguaje de modelado más conocido y utilizado en la actualidad. Este es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema. También ofrece un estándar para describir modelos del sistema, incluyendo aspectos como procesos del negocio, funciones del sistema y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y componentes reutilizables.

Se puede aplicar en el desarrollo de software integrando gran variedad de formas para dar soporte a una metodología de desarrollo, que puede ser Proceso Unificado de Rational (RUP), pero no especifica en sí mismo que metodología o proceso usar. Por todo lo antes expuesto se decide utilizar este lenguaje para el modelado del sistema.

## 1.7.7. Herramienta de modelado

Se selecciona el Visual Paradigm debido a que es una herramienta para UML profesional, que soporta el ciclo de vida completo del desarrollo de software. Esta herramienta ayuda a una más rápida construcción de aplicaciones de calidad, mejores y a un menor coste. Permite dibujar todo tipo de diagramas de clases, realizar ingeniería inversa, generar código a través de diagramas, así como generar documentación. También brinda abundantes tutoriales de UML, demostraciones interactivas de UML y proyectos de UML. [27]

Algunas características de esta herramienta CASE son:

- ❖ Soporta UML versión 2.1.
- ❖ Soporta ingeniería inversa para varios lenguajes.
- ❖ Genera código a través de diagramas o modelos.
- ❖ Transforma diagramas Entidad-Relación en tablas de bases de datos.
- ❖ Ingeniería inversa de bases de datos, desde sistemas gestores de bases de datos a diagramas Entidad-Relación.

## 1.7.8. Metodología de desarrollo

RUP, es una metodología, la más utilizada actualmente, ya que es adaptable a cualquier tipo de proyecto, intenta reducir la complejidad del software por medio de una estructura y la preparación de las tareas pendientes en función de los objetivos de la fase y la actividad actual.

El ciclo de vida de RUP se caracteriza por:

- ❖ **Dirigido por casos de uso:** Los casos de uso reflejan lo que los usuarios futuros necesitan y desean, lo cual se capta cuando se modela el negocio y se representa a través de los requerimientos. A partir de aquí los casos de uso guían el proceso de desarrollo, ya que los modelos que se obtienen como resultado de los diferentes flujos de trabajo, representan la realización de los casos de uso.
- ❖ **Centrado en la arquitectura:** La arquitectura muestra la visión común del sistema completo en la que el equipo de proyecto y los usuarios deben estar de acuerdo, por lo que describe los elementos del modelo que son más importantes para su construcción, los cimientos del sistema que son necesarios como base para comprenderlo, desarrollarlo y producirlo económicamente. RUP se desarrolla mediante iteraciones, comenzando por los CU relevantes desde el punto de vista de la arquitectura.
- ❖ **Iterativo e Incremental:** RUP propone que cada fase se desarrolle en iteraciones. Una iteración involucra actividades de todos los flujos de trabajo, aunque desarrolla fundamentalmente algunos más que otros. Por ejemplo, una iteración de elaboración centra su atención en el análisis y diseño, aunque refina los requerimientos y obtiene un producto con un determinado nivel, pero que irá creciendo incrementalmente en cada iteración.

Se selecciona RUP como metodología de desarrollo, ya que brinda una infraestructura flexible de desarrollo de software que proporciona prácticas recomendadas, probadas y una arquitectura confiable, además proporciona un entorno de procesos de desarrollo confiable, basado en estándares, además de ser configurado según la necesidad de la organización y del proyecto.

## 1.7.9. Gestor de base de datos

**PostgreSQL** es un gestor de Base de Datos relacional orientado a objetos, con prestaciones y funcionalidades equivalentes a muchos gestores de bases de datos comerciales. Es libre, publicado bajo

licencia BSD y dirigido por una comunidad de desarrolladores y organizaciones que trabajan en su desarrollo.

Posee numerosas ventajas como por ejemplo:

- ❖ Instalación ilimitada: nadie puede demandarlo por violar acuerdos de licencia, puesto que no hay costo asociado a la licencia de software.
- ❖ Estabilidad y confiabilidad: este es un gestor bastante estable y confiable.
- ❖ Extensible: el código fuente está disponible para todos y sin costo.
- ❖ Multiplataforma: está disponible en casi todos los sistemas operativos existentes.
- ❖ Diseñado para ambientes de alto volumen: se puede almacenar grandes volúmenes de datos.
- ❖ Alta concurrencia: permite que mientras un proceso escribe en una tabla, otros accedan a la misma tabla sin necesidad de bloqueos.

Los bloques de código que se ejecutan en el servidor pueden ser escritos en varios lenguajes, con la potencia que cada uno de ellos brinda, desde las operaciones básicas de la programación, tales como bifurcaciones y bucles, hasta las complejidades de la programación orientada a objetos o la programación funcional.

Por todo este grupo de características, que hacen el trabajo más fácil a los programadores, se propone como gestor de base de datos a PostgreSQL.

### **Conclusiones parciales**

En el capítulo se brindaron definiciones relacionadas con los riesgos y la gestión de riesgos en el entorno empresarial. Llegando a la conclusión de que la calidad de este proceso, se ha convertido hoy en día, en uno de los principales objetivos estratégicos de las organizaciones, debido a la contribución de este proceso al buen funcionamiento de la misma. Además, se realizó un análisis completo de las tecnologías que serán utilizadas a lo largo del desarrollo del sistema propuesto. Una vez conocidas las herramientas óptimas, y los conceptos a utilizar, se puede empezar a desarrollar la propuesta de sistema.

---

# Capítulo 2

## Características del sistema

### Introducción

En este capítulo se presenta la propuesta de sistema que dará solución al problema propuesto, así como una descripción general de cómo debe funcionar el mismo. Se hace un análisis de los procesos del negocio, mediante un modelo de dominio y una descripción de lo que el sistema debe hacer, para la cual se identifican las funcionalidades requeridas y las restricciones que se imponen a través de los requisitos funcionales y no funcionales. Además, se definen los actores y casos de uso del sistema, con las correspondientes especificaciones de los casos de uso.

#### 2.1. Modelo de Dominio

En la metodología de desarrollo a utilizar, en su primera fase de desarrollo se define la realización del modelo de negocio, con el objetivo de describir los procesos, existentes u observados, para comprenderlos y detectar las mejoras potenciales en los mismos. Cuando estos procesos no se pueden identificar claramente, RUP propone realizar un modelo de dominio, el cual constituye un subconjunto del modelo de negocio.

El modelo de dominio ayuda a comprender los conceptos que utilizan, captura los tipos de objetos más importantes en el contexto del usuario y del sistema. Los objetos del dominio representan los conceptos que existen o eventos que ocurren en el entorno en que trabaja el sistema. Este modelo se describe específicamente mediante diagramas de clases, utilizando el lenguaje de modelado UML.

Teniendo en cuenta que los procesos del negocio no se pueden definir claramente, se describe el negocio a través del modelo de dominio, el cual contiene una representación de las clases conceptuales del mundo real, no de sistemas informáticos.

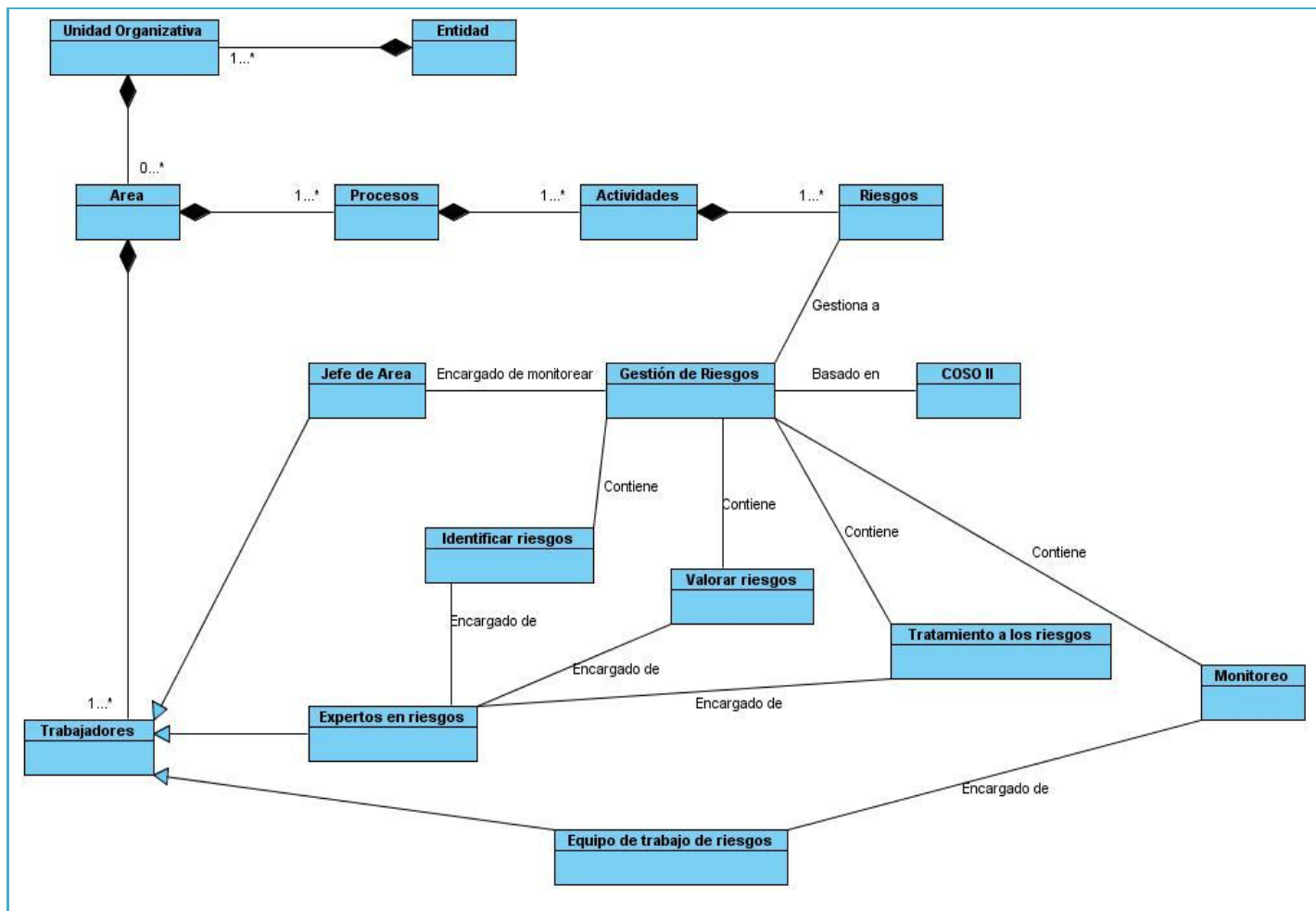


Figura 5. Modelo de dominio.

A continuación se describen los conceptos utilizados en el modelo de dominio, para lograr un mejor entendimiento del contexto que se está describiendo:

**Entidad:** representa el máximo nivel, o sea, la máxima dirección de la universidad, que contiene varias unidades organizativas.

**Unidad Organizativa:** representa el nivel superior de las áreas, que pueden ser Vicerrectorías, áreas independientes o direcciones independientes que se subordinan al rector.

**Áreas:** representa el campo de acción en el que se va a aplicar la gestión de los riesgos.

**Procesos:** representan un conjunto completo de actividades necesarias para dar cumplimiento a los objetivos.

**Actividades:** conjunto de acciones necesarias para realizar un proceso.

**Riesgo:** es la contingencia de que suceda algo que tendrá un impacto en los objetivos. Se mide en términos de una combinación de la probabilidad de ocurrencia de un evento y la consecuencia.

**Gestión de Riesgos:** es la combinación de las políticas, procedimientos, medidas y prácticas adoptadas para el tratamiento de los riesgos.

**COSO II:** es el marco conceptual para la gestión de riesgos, en el cual estará basada la metodología a utilizar por el sistema.

**Identificar riesgo:** comprende la identificación de los riesgos relevantes a que se enfrenta el área, que pueden incidir en el logro de los objetivos principales de la misma.

**Valorar riesgo:** los riesgos se evalúan desde una doble perspectiva – probabilidad e impacto -, permite considerar la amplitud de los mismos.

**Tratamiento a los riesgos:** se seleccionan las medidas que se estimen más efectivas para elaborar los planes de prevención de los riesgos.

**Monitoreo:** representa la revisión de la presencia y funcionamiento de los componentes de la administración de riesgos a lo largo del tiempo mediante actividades permanentes de supervisión, que permiten calcular la exposición que presenta el área a los riesgos detectados, así como la calidad de su Control Interno.

**Trabajador:** es una entidad virtual, que representa la generalización de los roles que puede cumplir algún actor en una situación determinada.

**Expertos en riesgos:** grupo de personas que proporcionan su opinión sobre la evaluación que se le debe dar a cada riesgo.

**Equipo de trabajo de riesgos:** grupo de personas constituidas por el jefe de área y los directivos de la misma, que son los encargados de que la gestión de riesgos se realice de la forma más eficaz posible y de monitorear la misma.

### 2.2. Procesos a automatizar

Teniendo en cuenta los datos arrojados de investigaciones desarrolladas sobre los diversos sistemas existentes en el mundo sobre Gestión de Riesgos, además de los datos recogidos del problema existente



y según lo que se necesita, se determinaron las principales características y funcionalidades con las que contará el sistema.

El sistema será capaz de realizar todo el proceso de gestión de riesgos a través de una metodología que se propone en este acápite, poniendo en práctica los conceptos de probabilidad y consecuencia, así como el grado de exposición a los diferentes riesgos que presenta el área, evaluando de esta manera el control interno en cada una de ellas. También permitirá a partir de las guías de control, realizar revisiones a las mismas.

El sistema cuenta con varios procesos a automatizar, cada uno con actividades específicas. En una primera parte se procede a la Evaluación de los Riesgos, que cuenta con tres actividades: identificación de los riesgos, valoración del riesgo y tratamiento. En la identificación del riesgo, se identifican todos los riesgos que, de ocurrir, afectarán al área y se determina si representan oportunidades o si pueden afectar negativamente, el logro de los objetivos del área.

Después de tener los riesgos identificados se realiza una valoración del mismo, lo que permite a la entidad considerar la magnitud con que los riesgos potenciales impactan en la consecución de los objetivos. Los riesgos se evalúan desde una doble perspectiva – probabilidad y consecuencia – con una combinación de métodos cualitativos y cuantitativos.

Esta evaluación se realiza mediante la fórmula matemática:

$$R = P \times C$$

Para los valores de probabilidad y consecuencia hay una escala en la que se le da valores a cada nivel que pueda tomar:

Probabilidad		Consecuencia	
Nivel	Valor	Nivel	Valor
Muy Baja	1	Baja	5
Baja	2	Leve	10
Media	3	Moderada	15
Alta	4	Alta	20
Muy Alta	5	Muy Alta	25

*Tabla 1. Escala para la probabilidad y la consecuencia.*

Con el valor numérico obtenido se hace una representación gráfica del riesgo, a través de una matriz de riesgos, dividida por colores que representan el nivel de gravedad del riesgo (Bajo, Medio, Alto, Extremo), de manera que los riesgos más significativos resalten, diferenciándolos de los menos significativos.

		Consecuencia				
		Baja	Leve	Moderada	Alta	Grave
Probabilidad	Muy Alta	Yellow	Yellow	Orange	Red	Red
	Alta	Yellow	Yellow	Yellow	Orange	Red
	Media	Light Green	Light Green	Yellow	Orange	Orange
	Baja	Light Green	Light Green	Yellow	Yellow	Yellow
	Muy Baja	Light Green	Light Green	Light Green	Yellow	Yellow

Figura 6. Matriz de Riesgos.

Al obtener un valor matemático que permita considerar la amplitud del evento, se pueden escoger las medidas que se estimen más efectivas para elaborar los planes de prevención, de acuerdo con el impacto de cada riesgo.

El otro proceso con el que contará el sistema es el de Supervisión y Monitoreo mediante el cual, la misma área puede evaluar su nivel de exposición al riesgo, a través de las guías de control.

En este proceso el área toma las guías de control elaborada para cada riesgo y paso a paso se va revisando el nivel de cumplimiento, las actividades que se cumplieron se denotarán con un Sí, las que no se cumplieron se denotarán con un No.

Teniendo la cantidad de actividades cumplidas y no cumplidas, se puede calcular el nivel de exposición al riesgo a partir de la siguiente fórmula:

$$ER = (ACN \times 100) / TAC$$

*ER es el nivel de exposición al riesgo.*

*ACN es la cantidad de acciones de control evaluadas de negativas.*

*TAC es el total de actividades de control.*

El resultado de este valor es un número en la escala del 1 – 100, el cual expresa el nivel de exposición al riesgo que tienen los diferentes riesgos. Cuando se tienen todos los valores de la exposición de todos los riesgos, estos números se promedian y el resultado final estará representado en un gráfico en el cual el color representa la medida en la que se está llevando a cabo el control interno en las áreas.

Exposición al riesgo	
Exposición	Evaluación del Control Interno
0 – 25 (Verde)	Satisfactorio
26 – 50 (Amarillo)	Aceptable
51 – 75 (Naranja)	Deficiente
76 – 100 (Rojo)	Malo

*Tabla 2. Escala de la evaluación del control interno.*

De acuerdo con esta evaluación, el área valora como se lleva a cabo su propio control interno y de ahí las medidas que debe tomar en caso que su control interno se evalúe de deficiente o malo.

Este proceso debe ser repetido con frecuencia, debido a que se le debe dar seguimiento a los planes de medidas para el tratamiento a los riesgos, lo cual permite ir evaluando sistemáticamente la efectividad de las medidas implementadas, incorporar nuevos riesgos o reevaluar los identificados según los nuevos contextos.

### 2.2.1. Requisitos Funcionales

#### RF 1. Autenticar usuario.

#### RF 2. Gestionar usuario.

RF 2.1 Crear usuario.

RF 2.2 Modificar usuario.

RF 2.3 Eliminar usuario.

#### RF 3. Gestionar roles.

RF 3.1 Crear rol.

RF 3.2 Modificar rol.

RF 3.3 Eliminar rol.

### **RF 4. Gestionar funcionalidades.**

RF 4.1 Crear funcionalidades.

RF 4.2 Modificar funcionalidades.

RF 4.3 Eliminar funcionalidades.

### **RF 5. Administrar roles por usuarios.**

RF 5.1 Asignar roles por usuario.

RF 5.2 Eliminar roles de usuarios.

### **RF 6. Administrar funcionalidades por rol.**

RF 6.1 Asignar funcionalidades por rol.

RF 6.2 Eliminar funcionalidades de un rol determinado.

### **RF 7. Administrar información del Área.**

RF 7.1 Introducir datos del área.

RF 7.2 Introducir datos de los procesos y actividades del área.

RF 7.3 Consultar información del área.

### **FR 8. Administrar evaluación de los riesgos.**

RF 8.1 Realizar identificación del riesgo.

RF 8.2 Realizar valoración del riesgo.

RF 8.3 Identificar tratamiento de los riesgos identificados.

RF 8.4 Consultar evaluación de riesgos.

### **RF 9. Administrar monitoreo.**

RF 9.1 Iniciar monitoreo.

RF 9.2 Calcular el grado de exposición al riesgo.

RF 9.3 Evaluar el control interno del área.

RF 9.4 Consultar información de monitoreo.

### **RF 10. Generar reportes.**

RF 10.1 Generar reportes de identificación de riesgos.

RF 10.2 Generar reportes de evaluación de riesgos.

RF 10.3 Generar reportes de monitoreo de riesgos.

RF 10.4 Generar reportes generales.

### **2.2.2.Requisitos no Funcionales**

#### Software

##### *Servidor*

- ✓ Se utilizará un servidor con sistema operativo Ubuntu 7.10 o superior.
- ✓ Como servidor web se utilizará el Apache versión 2.0.50 o superior.
- ✓ Se utilizará PostgreSQL versión 8.2.4 o superior como gestor de bases de datos.

##### *Cliente*

- ✓ Se requiere versiones de Windows 2000 o superior, así como Linux y sus correspondientes distribuciones.
- ✓ En las computadoras de los clientes sólo se requiere de un navegador para Internet (Internet Explorer versión 4.5 o superior, Mozilla Firefox versión 2.0 o superior).

#### Hardware

##### *Estaciones de Trabajo*

- ✓ Se requiere tarjeta de red.
- ✓ Se requiere tengan al menos 256 MB de memoria RAM.
- ✓ Se requiere una capacidad de disco duro de 1 GB como mínimo.
- ✓ Se requiere una velocidad del procesador de 800 MHz como mínimo.

##### *Servidores*

- ✓ Se requiere tarjeta de red.
- ✓ Se requiere que tengan al menos 512MB de memoria RAM.
- ✓ Se requiere una capacidad de disco duro de 40GB como mínimo.
- ✓ Se requiere una velocidad del procesador de 2.0 GHz como mínimo.

### Restricciones en el diseño y la implementación

- ✓ El análisis y diseño del sistema estará basado en la metodología de desarrollo RUP con el uso del lenguaje de modelado UML.
- ✓ Se usará Visual Paradigm como herramienta CASE para el modelado de los artefactos que se generan con cada flujo de trabajo.
- ✓ El sistema se desarrollará con tecnología PHP versión 5.2.5 o superior.
- ✓ Se utilizará como IDE de desarrollo el NetBeans.
- ✓ La base de datos se implementará en PostgreSQL versión 8.2.4 o superior.

### Apariencia o interfaz externa

- ✓ La interfaz debe ser lo más sencilla posible, para que las personas que no posean muchos conocimientos en el área de la informática no necesiten tanto tiempo de preparación para aprender a trabajar con el sistema. También debe ser agradable, de fácil uso, y que favorezca al buen estado de ánimo del usuario.

### Usabilidad

- ✓ Debe ser de fácil y de rápido manejo para todos los usuarios.
- ✓ Cualquier persona que tenga conocimientos básicos en computación o que haya interactuado anteriormente con la web, podrá usar este sistema.

## 2.3. Modelo de Casos de Uso

El Modelo de Casos de Uso del Sistema permite que los desarrolladores de software y los clientes lleguen a un acuerdo sobre los requisitos, es decir, sobre las condiciones y posibilidades que debe cumplir el sistema. Además, proporciona la entrada fundamental para el análisis, diseño y pruebas.

### 2.3.1. Definición de los actores del sistema





Actores	Justificación
	Entidad virtual que representa todos los usuarios del sistema.
	Encargado de la gestión de los usuarios, roles y funcionalidades del sistema, además de administrar roles por usuarios y funcionalidades por rol.
	Usuarios del sistema que solo pueden visualizar la información existente en el mismo, de acuerdo con el nivel de acceso que posean.
	Usuario del sistema encargado de entrar todos los datos de su área al sistema, evaluar los riesgos, calcular la exposición al riesgo, así como generar los reportes necesarios. Es el único usuario que puede gestionar toda la información del área.

Tabla 3. Definición de los actores del sistema

### 2.3.2. Diagrama de Casos de Uso del Sistema

Un diagrama de casos de uso del sistema (DCUS) representa gráficamente a los procesos y su interacción con los actores. Además, facilita el entendimiento de los procesos a realizar por el sistema para el desarrollador.

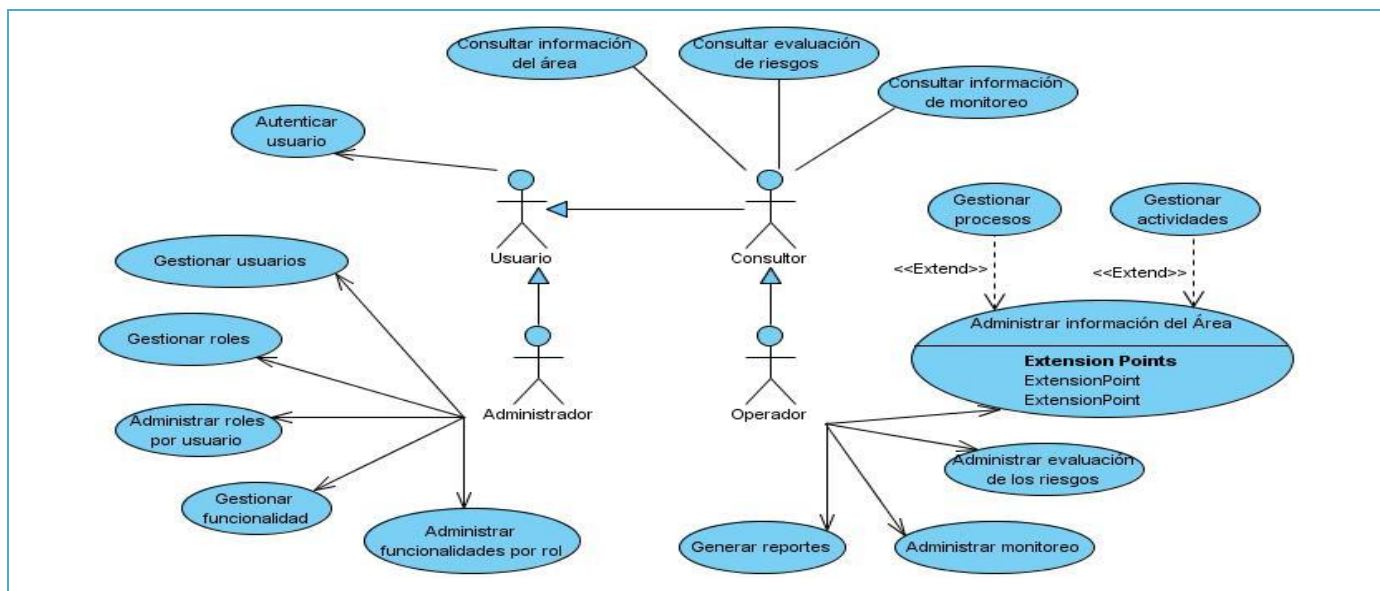


Figura 7. Diagrama de casos de uso del sistema.

### 2.3.3. Listado de los Casos de Uso del Sistema

La forma en que los actores usan el sistema se representa con un caso de uso. De manera más precisa, un caso de uso especifica una secuencia de acciones que el sistema puede llevar a cabo interactuando con sus actores.

CU-1	Autenticar usuario
<b>Actor</b>	Usuarios del sistema.
<b>Descripción</b>	Todos los usuarios del sistema deben estar autenticados para poder acceder a la información del mismo, según su nivel de acceso.
<b>Referencia</b>	RF 1.

*Tabla 4. Descripción del caso de uso Autenticar usuario.*

CU-2	Gestionar usuarios del sistema.
<b>Actor</b>	Administrador.
<b>Descripción</b>	El administrador del sistema puede gestionar la información referente a todos los usuarios existentes en el sistema, o sea, puede crear un nuevo usuario, modificar los datos de algún usuario que ya existe o eliminarlos.
<b>Referencia</b>	RF 2, RF 2.1, RF 2.2, RF 2.3.

*Tabla 5. Descripción del caso de uso Gestionar usuarios del sistema*

CU-3	Gestionar roles.
<b>Actor</b>	Administrador.
<b>Descripción</b>	El administrador del sistema puede gestionar la información referente a los roles que van a existir en el sistema.
<b>Referencia</b>	RF 3, RF 3.1, RF 3.2, RF 3.3.

*Tabla 6. Descripción del caso de uso Gestionar roles.*

CU-4	Administrar roles por usuarios.
<b>Actor</b>	Administrador
<b>Descripción</b>	El administrador del sistema puede asignar los roles a los diferentes usuarios que el sistema posee o eliminar roles a los usuarios.
<b>Referencia</b>	RF 5, RF 5.1, RF 5.2.

*Tabla 7. Descripción del caso de uso Administrar roles por usuarios.*

CU-5	Gestionar funcionalidades.
<b>Actor</b>	Administrador.
<b>Descripción</b>	El administrador del sistema puede gestionar la información referente a las funcionalidades que van a existir en el sistema.



<b>Referencia</b>	RF 4, RF 4.1, RF 4.2, RF 4.3.
-------------------	-------------------------------

*Tabla 8. Descripción del caso de uso Gestionar funcionalidades.*

CU-6	Administrar funcionalidades por rol.
<b>Actor</b>	Administrador
<b>Descripción</b>	El administrador del sistema puede asignar las funcionalidades a los diferentes roles o eliminar funcionalidades de los roles.
<b>Referencia</b>	RF 6, RF 6.1, RF 6.2.

*Tabla 9. Descripción del caso de uso Administrar funcionalidades por rol.*

CU-7	Administrar información del Área.
<b>Actor</b>	Operador
<b>Descripción</b>	El usuario del sistema entra los datos referentes al área a la que pertenece.
<b>Referencia</b>	RF 7, RF 7.1, RF 7.4.

*Tabla 10. Descripción del caso de uso Administrar información del Área.*

CU-8	Gestionar procesos.
<b>Actor</b>	Operador
<b>Descripción</b>	El usuario del sistema entra los datos referentes a los procesos del área a la que pertenece.
<b>Referencia</b>	RF 7.2.

*Tabla 11. Descripción del caso de uso Gestionar procesos.*

CU-9	Gestionar actividades.
<b>Actor</b>	Operador
<b>Descripción</b>	El usuario del sistema entra los datos referentes al área a la que pertenece.
<b>Referencia</b>	RF 7.3.

*Tabla 12. Descripción del caso de uso Gestionar actividades.*

CU-10	Administrar evaluación de los riesgos
<b>Actor</b>	Operador
<b>Descripción</b>	El usuario del sistema entra los datos referentes a la evaluación de los riesgos.
<b>Referencia</b>	RF 8, RF 8.1 RF 8.2 RF 8.3

*Tabla 13. Descripción del caso de uso Administrar evaluación de los riesgos*

CU-11	Administrar monitoreo
-------	-----------------------

<b>Actor</b>	Operador
<b>Descripción</b>	El usuario introduce todos los datos referentes al monitoreo.
<b>Referencia</b>	RF 9, RF 9.1, RF 9.2.

*Tabla 14. Descripción del caso de uso Administrar monitoreo.*

CU-12	Consultar información del área.
<b>Actor</b>	Consultor.
<b>Descripción</b>	Los usuarios pueden consultar la información de acuerdo con el nivel de acceso que tengan.
<b>Referencia</b>	RF 7.3

*Tabla 15. Descripción del caso de uso Consultar información del área.*

CU-13	Consultar evaluación de riesgos.
<b>Actor</b>	Consultor
<b>Descripción</b>	Los usuarios pueden consultar la información referente a la evaluación de los riesgos, de acuerdo con el nivel de acceso que tengan al sistema.
<b>Referencia</b>	RF 8.4.

*Tabla 16. Descripción del caso de uso Consultar evaluación de riesgos.*

CU-14	Consultar información de monitoreo.
<b>Actor</b>	Consultor
<b>Descripción</b>	Los usuarios pueden consultar la información referente al monitoreo, de acuerdo con el nivel de acceso que tengan al sistema.
<b>Referencia</b>	RF 9.3.

*Tabla 17. Descripción del caso de uso Consultar información de monitoreo.*

CU-15	Generar reportes
<b>Actor</b>	Operador
<b>Descripción</b>	Usuario del sistema que debe gestionar todos los reportes que sean necesarios en el área.
<b>Referencia</b>	RF 10, RF 10.1, RF 10.2, RF 10.3, RF 10.4.

*Tabla 18. Descripción del caso de uso Generar reportes.*

### 2.3.4. Casos de uso expandidos

<b>Caso de uso</b>	
CU-16	Administrar información del Área.
<b>Actores:</b> Operador	
<b>Resumen:</b>	El usuario del sistema entra los datos referentes al área a la que pertenece.

<b>Referencias</b>	RF 7, RF 7.1, RF 7.4.	
<b>Curso Normal de los Eventos</b>		
<i>Sección “Crear datos del área”</i>		
<b>Acción del actor</b>	<b>Respuesta del sistema</b>	
1. El caso de uso inicia cuando el actor introduce por primera vez los datos pertenecientes al área.	2. El sistema verifica que los campos tengan más de diez caracteres. 3. El sistema almacena los datos introducidos. 4. Se muestra un mensaje informándole al operador que ya se ha creado la información y finaliza el caso de uso.	
<b>Flujos alternos</b>		
	2. Si los campos no tienen más de diez caracteres a la hora de poner la descripción, el sistema marca los campos de rojo.	
<i>Sección “Modificar datos del área”</i>		
<b>Acción del actor</b>	<b>Acción del actor</b>	
1. El caso de uso inicia cuando el actor edita o modifica los datos pertenecientes al área.	2. El sistema almacena los cambios efectuados. 3. Se muestra un mensaje informándole al operador que ya se han modificado los datos y finaliza el caso de uso.	

Tabla 19. Descripción del caso de uso Administrar información del Área.

<b>Caso de uso</b>	
CU-17	Administrar evaluación de los riesgos.
<b>Actores:</b> Operador	
<b>Resumen</b>	El usuario del sistema entra los datos referentes a la evaluación de los riesgos.
<b>Referencias</b>	RF 8, RF 8.1 RF 8.2 RF 8.3
<b>Curso Normal de los Eventos</b>	
<b>Sección “Gestionar identificación del riesgo”</b>	
<b>Crear riesgo</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
1. El caso de uso comienza cuando el operador selecciona la actividad para la cual va a identificar los riesgos.	2. El sistema muestra la interfaz para que el operador

<p>3. El operador introduce los datos de los riesgos.</p>	<p>introduzca los datos de los riesgos.</p> <p>4. El sistema almacena los datos.</p> <p>5. Se muestra un mensaje informándole al operador que el riesgo ha sido creado satisfactoriamente y finaliza el caso de uso.</p>
<b>Modificar riesgo</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
<p>1. El caso de uso comienza cuando el operador selecciona el riesgo que va a modificar.</p> <p>3. El operador introduce los datos del riesgo.</p>	<p>2. El sistema muestra la interfaz para que el operador introduzca los datos del riesgo a modificar.</p> <p>4. El sistema almacena los cambios.</p> <p>5. Se muestra un mensaje informándole al operador que el riesgo ha sido modificado satisfactoriamente y finaliza el caso de uso.</p>
<b>Eliminar riesgo</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
<p>1. El caso de uso comienza cuando el operador selecciona el riesgo que va a eliminar.</p> <p>4. El usuario escoge la opción aceptar.</p> <p>5. El operador elimina el riesgo.</p>	<p>2. El sistema muestra la pantalla para que el operador elimine el riesgo.</p> <p>3. El sistema muestra un mensaje preguntándole al operador si está seguro de que desea borrar el riesgo.</p> <p>6. El sistema borra los datos.</p> <p>7. Se muestra un mensaje para informar al operador de que la acción de control ha sido eliminada satisfactoriamente y finaliza el caso de uso.</p>
<b>Curso alternativo</b>	
<p>1. El usuario escoge la opción cancelar y finaliza el caso de uso.</p>	
Sección “ <b>Administrar valoración del riesgo</b> ” <b>Seleccionar valores.</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>

<ol style="list-style-type: none"> <li>1. El caso de uso inicia cuando el actor selecciona los valores de la probabilidad y consecuencia para el riesgo identificado en la sección anterior.</li> <li>5. El actor visualiza el color obtenido para definir el nivel del riesgo y finaliza el caso de uso.</li> </ol>	<ol style="list-style-type: none"> <li>2. El sistema realiza el cálculo de la fórmula planteada para los valores de probabilidad y consecuencia.</li> <li>3. Se muestra el resultado potencial del riesgo.</li> <li>4. El sistema muestra el resultado antes obtenido a través de una matriz de riesgos.</li> </ol>
<b>Modificar valores.</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
<ol style="list-style-type: none"> <li>1. El caso de uso inicia cuando el actor selecciona los nuevos valores de la probabilidad y consecuencia para el riesgo seleccionado.</li> </ol>	<ol style="list-style-type: none"> <li>2. El sistema realiza el cálculo de la fórmula planteada para los nuevos valores de probabilidad y consecuencia.</li> <li>3. Se muestra el resultado potencial del riesgo.</li> <li>4. El sistema muestra el resultado antes obtenido a través de una matriz de riesgos.</li> </ol>
<b>Sección “Gestionar tratamiento del riesgo”</b>	
<b>Crear acción de control</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
<ol style="list-style-type: none"> <li>1. El caso de uso comienza cuando el operador introduce las acciones de control para los riesgos identificados, así como el responsable de cada acción.</li> </ol>	<ol style="list-style-type: none"> <li>2. El sistema almacena las guías de control.</li> <li>3. Se muestra un mensaje para informar al operador de que la acción de control ha sido creada satisfactoriamente y finaliza el caso de uso.</li> </ol>
<b>Modificar acción de control</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
<ol style="list-style-type: none"> <li>1. El caso de uso comienza cuando el operador selecciona la acción de control que va a modificar.</li> </ol>	<ol style="list-style-type: none"> <li>2. El sistema muestra la pantalla para que el operador realice los cambios.</li> </ol>

3. El operador introduce los datos de la acción de control a modificar.	4. El sistema almacena los cambios. 5. Se muestra un mensaje para informar al operador de que la acción de control ha sido modificada satisfactoriamente y finaliza el caso de uso.
<b>Eliminar acción de control</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
1. El caso de uso comienza cuando el operador selecciona la acción de control que va a eliminar.  4. El usuario escoge la opción aceptar. 5. El operador elimina la acción de control.	2. El sistema muestra la pantalla para que el operador elimine la acción de control. 3. El sistema muestra un mensaje preguntándole al operador si está seguro de que desea borrar la acción de control.  6. El sistema almacena los cambios. 7. Se muestra un mensaje para informar al operador de que la acción de control ha sido eliminada satisfactoriamente y finaliza el caso de uso.
<b>Curso alternativo</b>	
4. El usuario escoge la opción cancelar y finaliza el caso de uso.	

Tabla 20. Descripción del caso de uso Administrar evaluación de los riesgos.

<b>Caso de uso</b>	
CU-18	Administrar monitoreo.
<b>Actores:</b> Operador	
<b>Resumen:</b>	El usuario introduce todos los datos referentes al monitoreo.
<b>Referencias</b>	RF 9, RF 9.1, RF 9.2.
<b>Sección “Iniciar monitoreo”</b>	
<b>Acción del actor</b>	<b>Respuesta del sistema</b>
1. El caso de uso inicia cuando el actor presiona la opción iniciar monitoreo.	2. El sistema muestra la pantalla de iniciar monitoreo con un mensaje en rojo: “Una vez que usted inicie este monitoreo, se realizará un cierre de la gestión de riesgos, por tanto, no podrá realizar acciones en esa parte del sistema, sólo

<p>3. El actor procede a llenar la descripción del monitoreo y pulsa el botón iniciar.</p> <p>5. El usuario presiona el botón aceptar y comienza el monitoreo.</p>	<p>tendrá acceso al monitoreo, hasta tanto culmine con el mismo” y para llenar la descripción del monitoreo.</p> <p>4. El sistema muestra un mensaje que dice “¿Está seguro de que desea continuar?”</p>
<p>Sección “Exposición al riesgo”</p>	
<p><b>Acción del actor</b></p>	<p><b>Respuesta del sistema</b></p>
<p>1. El caso de uso inicia cuando el actor escoge la guía de control ya realizada, que va a utilizar.</p> <p>3. El actor procede a seleccionar las respuestas a cada acción de la guía.</p>	<p>2. El sistema muestra la guía seleccionada.</p> <p>4. El sistema de acuerdo con las actividades marcadas, calcula el nivel de exposición al riesgo mediante la fórmula establecida.</p> <p>5. Muestra el resultado final en un gráfico y finaliza el caso de uso.</p>
<p>Sección “Evaluación del Control Interno”</p>	
<p><b>Acción del actor</b></p>	<p><b>Respuesta del sistema</b></p>
<p>1. El caso de uso inicia cuando el operador da clic la opción evaluar control interno.</p>	<p>2. El sistema mediante una fórmula establecida calcula la evaluación del control interno.</p> <p>3. Se muestra el valor de la evaluación mediante un gráfico y finaliza el caso de uso.</p>

Tabla 21. Descripción del caso de uso Administrar monitoreo.

### Conclusiones parciales

Para poder pasar a diseñar el sistema fue necesario hacer una detallada descripción de cada uno de los procesos que se llevan a cabo la gestión de riesgos, logrando una mejor comprensión del mismo, así como un levantamiento de cada uno de los requisitos funcionales y no funcionales para la futura aplicación.

# Capítulo 3

## Diseño del sistema

### Introducción

En este capítulo se propone un diseño para el sistema, que permita una entrada apropiada y un punto de partida para la futura implementación del sistema, teniendo en cuenta los requisitos funcionales y no funcionales antes propuestos. Se formula una arquitectura que permita adaptar el sistema al entorno de implementación que se desarrollará y los patrones de diseño a utilizar, así como las vistas arquitectónicas del sistema. Además, se realizarán los diagramas de clases y los diagramas de interacción en correspondencia con los casos de uso antes definidos.

#### 3.1. Modelo de Análisis

En el modelo del análisis, se observa una especificación más exacta de los requisitos, ya que este se encarga de estructurarlos de modo que sea más fácil su separación, comprensión, modificación y en general su mantenimiento, creando así una primera aproximación al modelo de diseño.

##### 3.1.1. Diagramas de clases del análisis

Una clase del análisis representa una abstracción de una o varias clases y/o subsistemas de diseño. Se centra en el tratamiento de requisitos funcionales y pospone los no funcionales para el diseño, según RUP siempre se ajusta a alguno de los estereotipos siguientes: interfaz, control o entidad.

- ✓ **Clase interfaz:** Modelan la interacción entre el sistema y sus actores.
- ✓ **Clase control:** Coordinan la realización de uno o unos pocos casos de uso, coordinando las actividades de los objetos que implementan la funcionalidad del caso de uso, por lo que definen el flujo de control y las transacciones dentro de un caso de uso, delegando el trabajo a otros objetos.
- ✓ **Clase entidad:** Modelan información que posee larga vida y que es a menudo persistente, además de los fenómenos, conceptos y sucesos que ocurren en la vida real.

Los diagramas de clases son diagramas de estructura estática que muestran las clases del sistema y sus interrelaciones. Estos diagramas son los más utilizados en el modelado de sistemas orientados a objetos



por constituir el pilar básico del modelado con UML para mostrar lo que el sistema puede hacer (análisis), y cómo puede ser construido (diseño). A continuación se muestran algunos diagramas de clases del análisis.

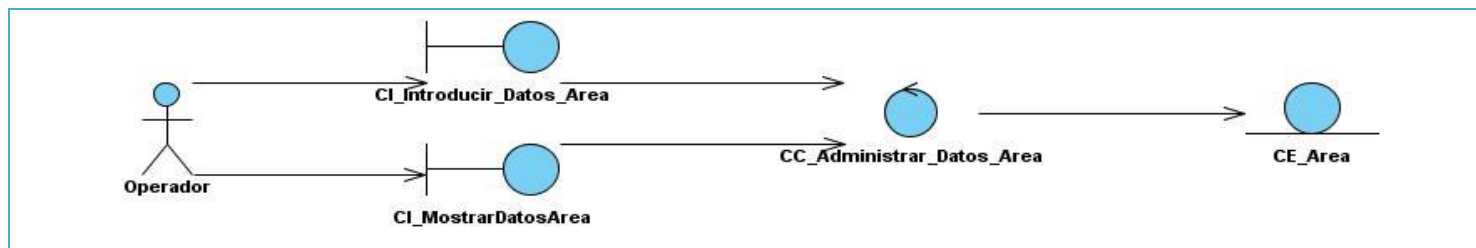


Figura 8. Diagrama de clases del análisis CU Administrar información del área.

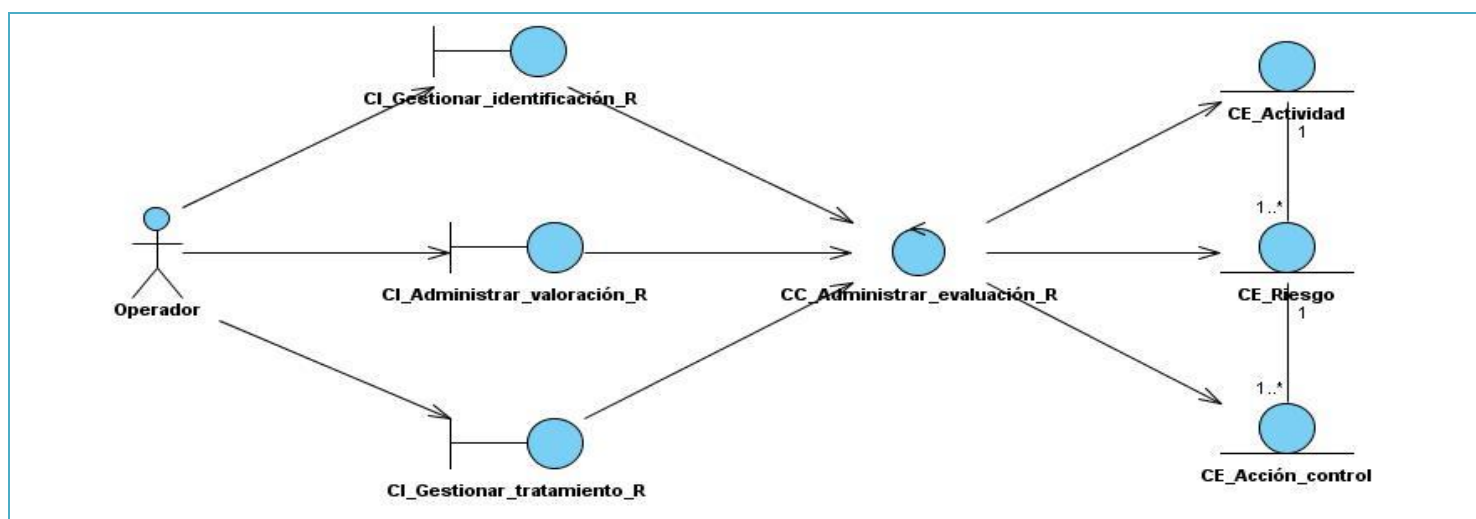


Figura 9. Diagrama de clases del análisis CU Administrar evaluación del riesgo.

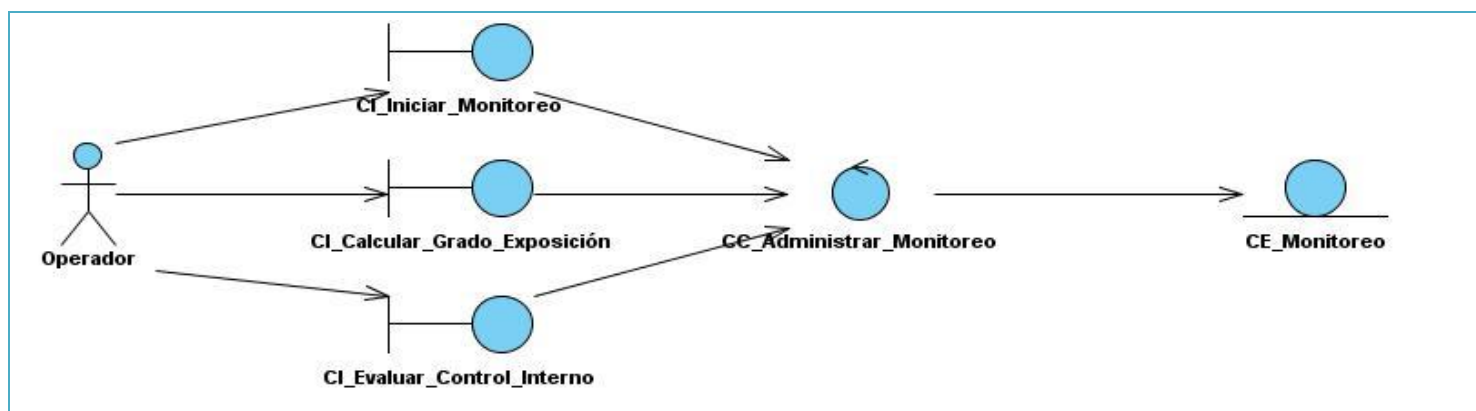


Figura 10. Diagrama de clases del análisis CU Administrar monitoreo.

### 3.2. Modelo de Diseño

El modelo de diseño es un modelo de objetos que describe la realización física de los casos de uso, centrándose tanto en los requisitos funcionales, como los no funcionales, teniendo una correspondencia directa con los elementos físicos del ambiente de implementación. Es usado como una entrada inicial en las actividades de implementación y prueba, ya que constituye una abstracción del modelo de implementación y el código fuente.

#### 3.2.1. Diagramas de clases del Diseño

Los diagramas de clases del diseño al igual que los del análisis, son utilizados para describir la estructura del sistema de manera gráfica, mostrando sus clases, atributos y las relaciones entre ellos. En el caso del sistema propuesto en este trabajo, un sistema web, los diagramas poseen rasgos que se distinguen del resto de las aplicaciones, ya que se hace más insistencia en los detalles de la presentación, centrándose en la representación de las páginas, las relaciones entre ellas y las clases que utiliza el sistema. A continuación se representan los diagramas de clases del diseño usando prototipos web, para cada uno de los casos de uso definidos para el sistema, de forma tal que facilite la comprensión de las relaciones entre los distintos componentes. A continuación se muestran algunos diagramas de clases del diseño.

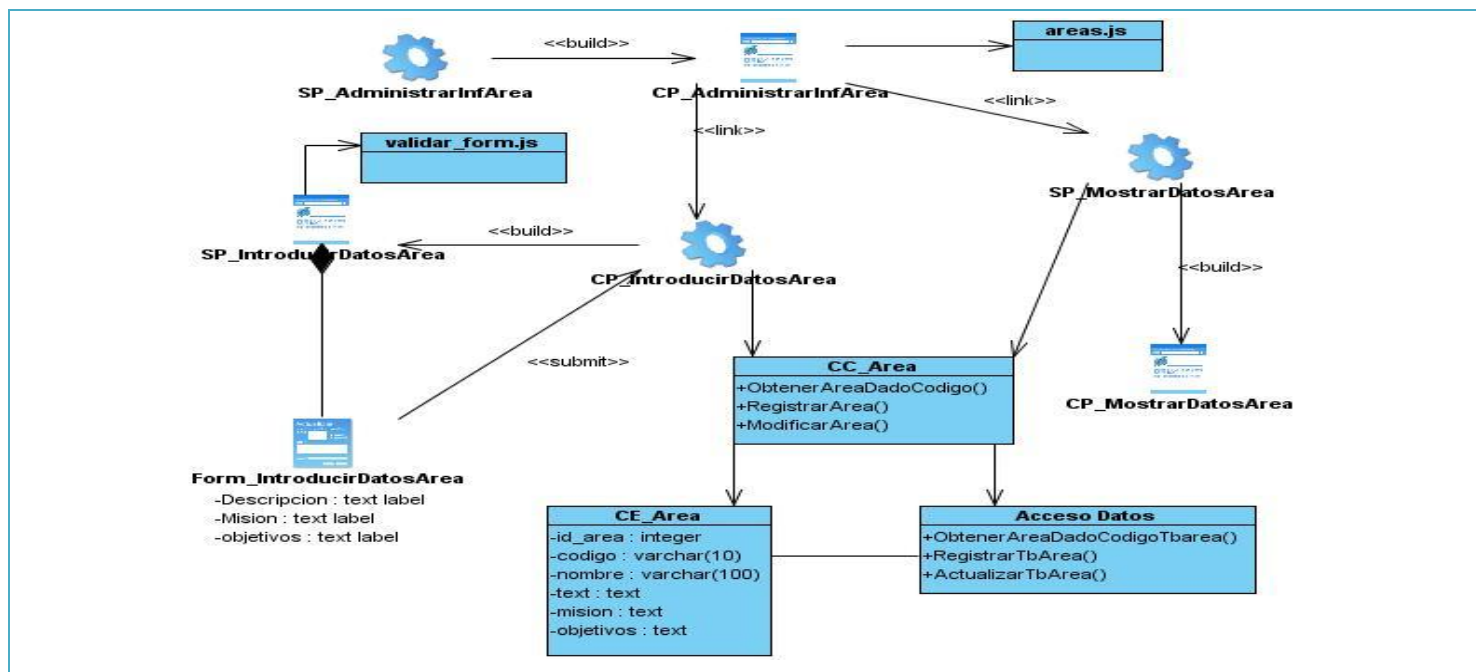


Figura 11. Diagrama de clases del diseño CU Administrar información del área.

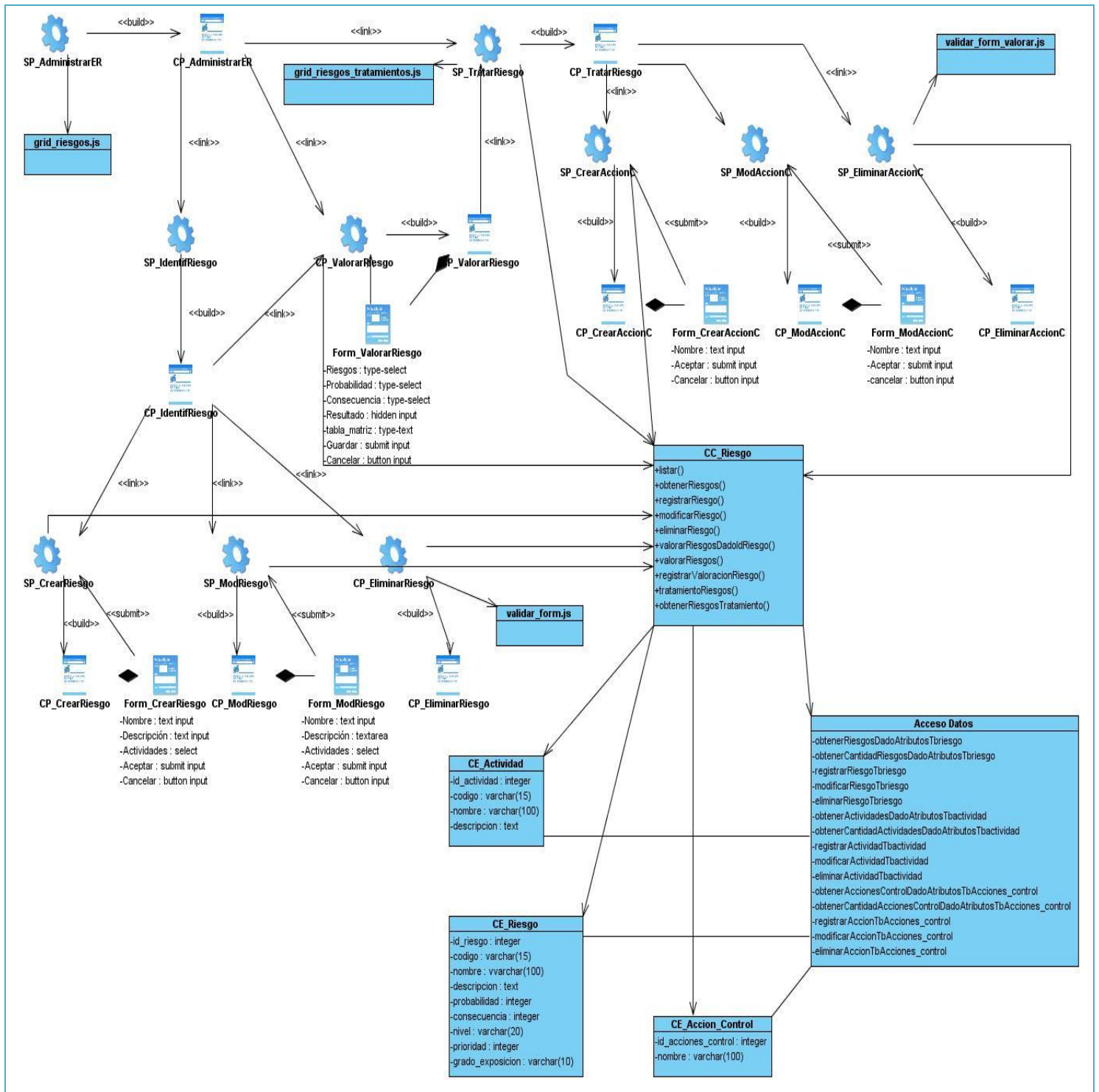


Figura 12. Diagrama de clases del diseño CU Administrar evaluación de riesgos.

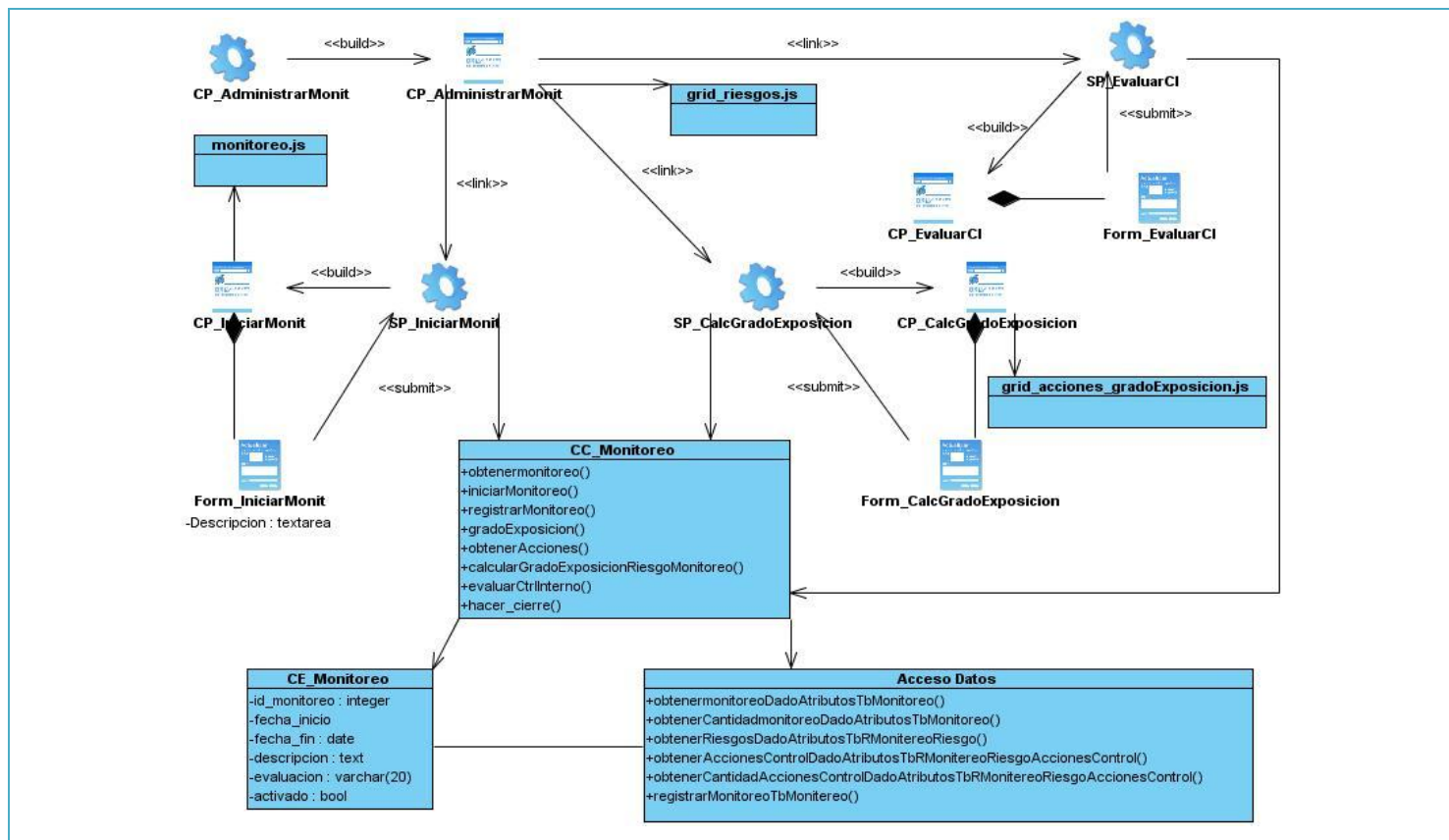


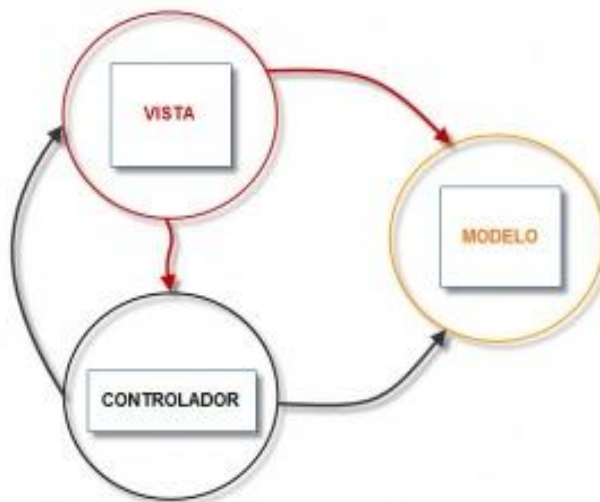
Figura 13. Diagrama de clases del diseño CU Administrar monitoreo.

### 3.3. Patrón Arquitectónico. Modelo – Vista – Controlador

La arquitectura de software es el conjunto de decisiones significativas sobre la organización de un sistema, la selección de los elementos estructurales y sus interfaces de los cuales el sistema está compuesto junto con su comportamiento. [29] Describe los cimientos del sistema que son necesarios como base para comprenderlo, desarrollarlo y producirlo económicamente. La misma se representa en 4 + 1 vistas arquitectónicas. La arquitectura debe estar estrechamente relacionada con los casos de uso, ya que los casos de uso deben encajar en la arquitectura cuando se llevan a cabo y por otro lado, la arquitectura debe permitir el desarrollo de todos los casos de uso requeridos, por tanto, ambos deben evolucionar en paralelo.

Uno de los patrones arquitectónicos más utilizados para desarrollar aplicaciones es el Modelo – Vista – Controlador (MVC), el cual divide una aplicación en tres módulos claramente identificables y con

funcionalidad bien definida: el modelo, las vistas y el controlador. A continuación se muestra una representación de la interacción de los componentes de este patrón.



*Figura 14. Interacción entre los componentes del patrón MVC.*

**Modelo:** es la representación gráfica de la información con la cual el sistema opera, o sea, se limita a lo relativo de la vista y su controlador facilitando las presentaciones visuales complejas. El sistema también puede operar con más datos no relativos a la presentación, haciendo uso integrado de otras lógicas de negocio y de datos afines con el sistema modelado. Es el responsable de acceder a la capa de almacenamiento de los datos.

**Vista:** es la representación del modelo en un formato adecuado para interactuar, usualmente es la interfaz de usuario. Estas son las responsables de recibir los datos del modelo y mostrarlas al usuario.

**Controlador:** es el que responde a los eventos, usualmente acciones del usuario, e invoca peticiones al modelo y probablemente a la vista. Este sirve como intermediario entre el Modelo, la Vista y cualquier otro recurso necesario.

Tanto la vista como el controlador dependen del modelo, el cual no depende de las otras clases. Esta separación permite construir y probar el modelo, independientemente de la representación visual.



### 3.4. Diseño de la Base de Datos

#### 3.4.1. Modelo de datos

Un modelo de datos es aquel que describe de una forma abstracta cómo se representan los datos, sea en una empresa, en un sistema de información o en un sistema de gestión de bases de datos. Básicamente consiste en una descripción de algo conocido como contenedor de datos, así como los métodos a almacenar y recuperar información de dichos contenedores. [30]

Para lograr un mayor entendimiento del modelo de datos se pueden consultar la descripción de las tablas en el [Anexo 1 Descripción de las tablas del modelo de datos.](#)

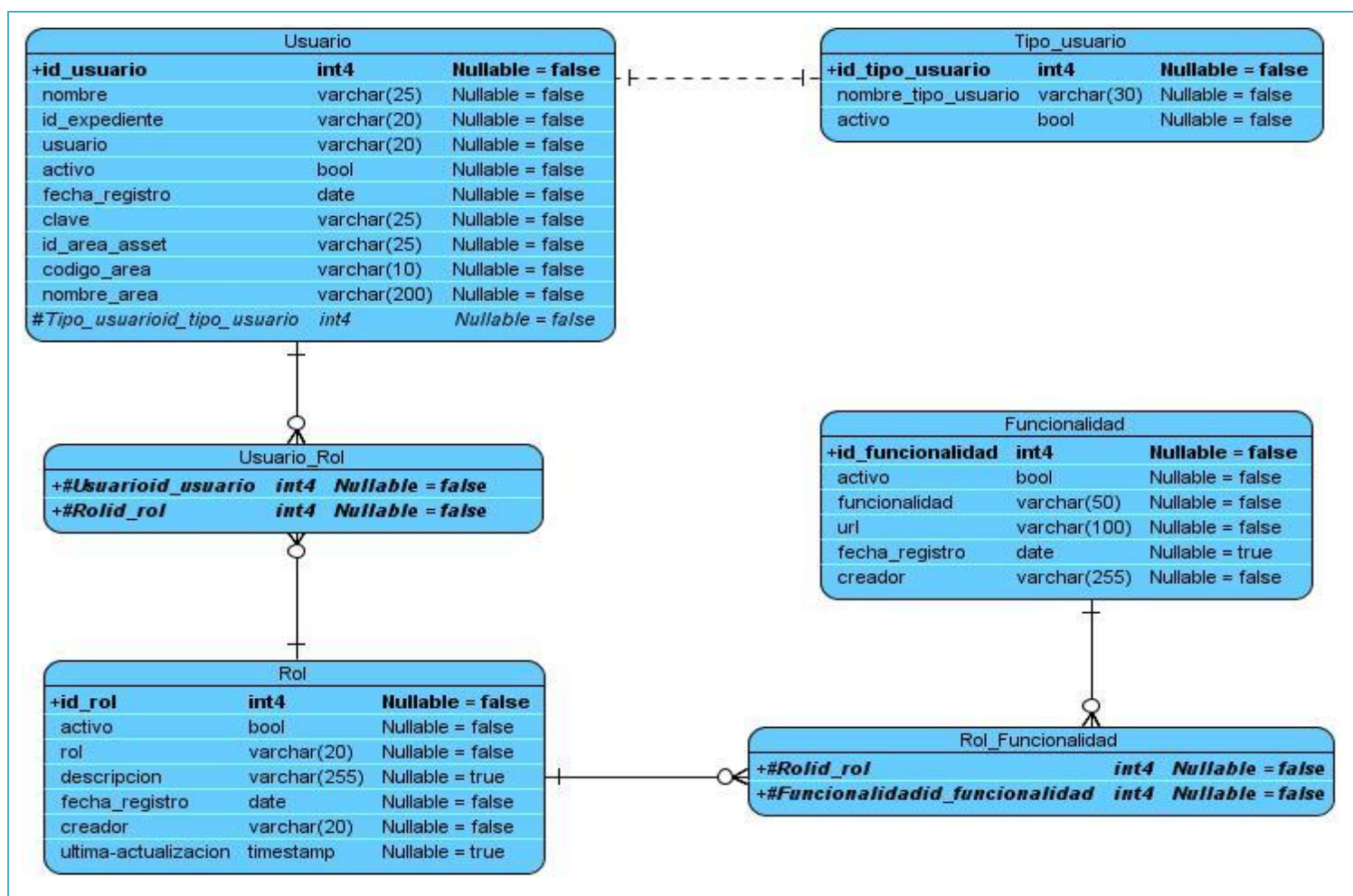


Figura 15. Modelo de datos para el esquema de Seguridad.

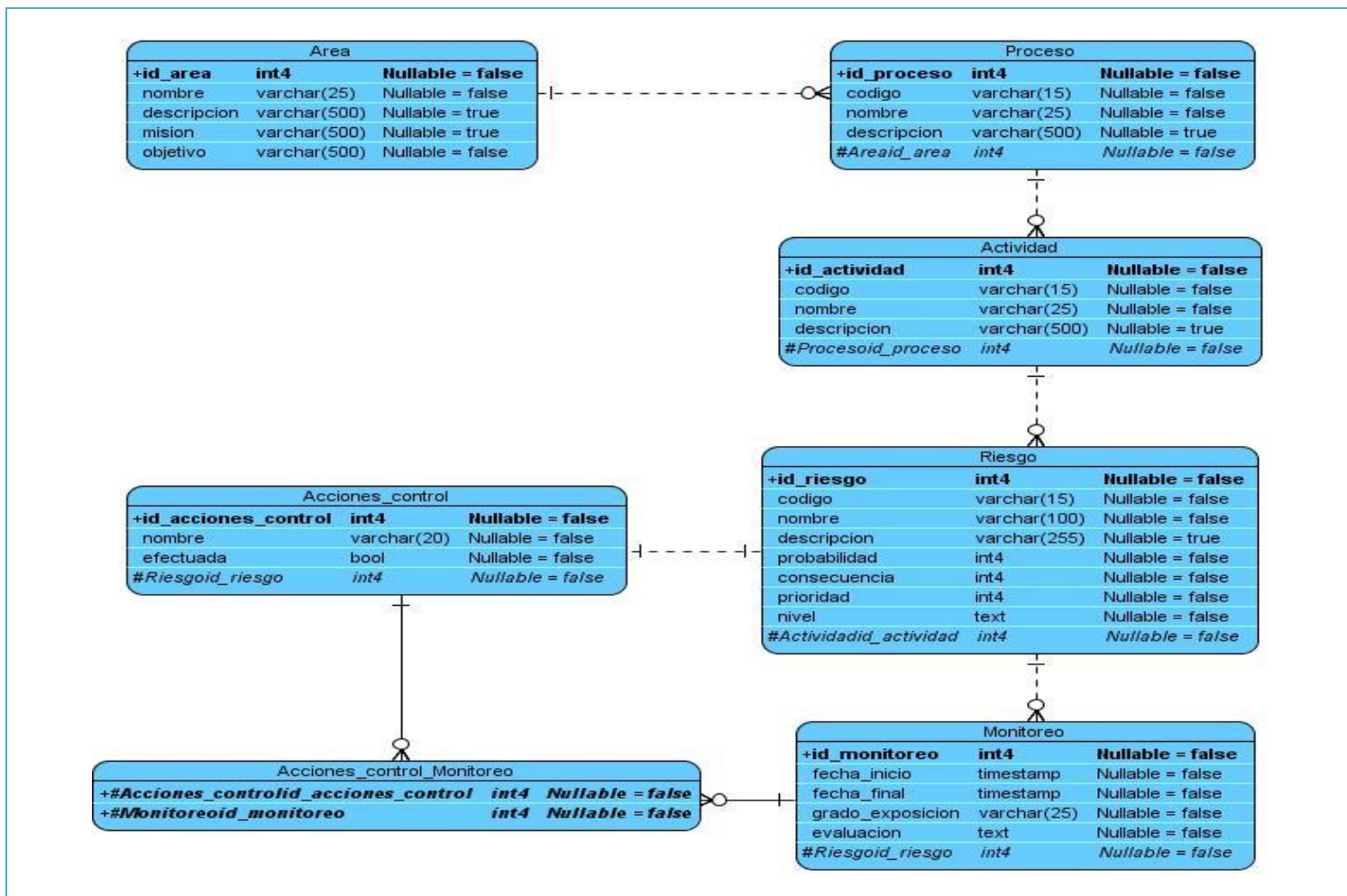


Figura 16. Modelo de datos para el esquema de Gestión de Riesgos.

### 3.5. Tratamiento de errores.

El tratamiento de errores es un paso preciso para el buen funcionamiento del sistema. Los errores más comunes que se pueden representar están relacionados con la interacción con la base de datos, fundamentalmente en los procesos de creación, eliminación y/o modificación de datos. Se establecieron mecanismos para visualizar información, evitando así, en la medida de lo posible la introducción manual de los datos y logrando minimizar los errores que pueda tener el sistema. Se muestran mensajes indicando los errores cometidos en correspondencia con las validaciones realizadas.

Para el tratamiento de errores se utilizaron mensajes de texto en la misma página donde se ejecuta la acción, permitiéndole al usuario corregir sus errores con facilidad y continuar con la actividad efectuada.

### 3.6. Seguridad.

En el mundo de hoy la información constituye un elemento de vital importancia, es necesario que existan mecanismos de seguridad que garanticen la protección de los datos que se manipulan en la aplicación y que los usuarios según su rol solo puedan realizar las acciones que le corresponden y por tanto obtener información únicamente de las tareas para las que tienen autorización.

A partir de esa idea para mantener la integridad, confiabilidad y disponibilidad de la información que se maneja, se tuvo en cuenta para el acceso a la aplicación, una previa autenticación, donde el sistema comprueba que las credenciales coincidan con las almacenadas y le dé los privilegios correspondientes. En caso contrario se redirecciona a una página que dice que no tiene acceso a la funcionalidad y brinda un vínculo a la página principal, para que tenga la posibilidad de autenticarse nuevamente.

Además, cuenta con un control de acceso a cada página, logrando que los usuarios tengan acceso solo a la información que realmente le está permitida. En este sentido, sólo el administrador del sistema es el encargado de asignar permisos a cada usuario.

Una buena práctica a seguir será realizar salvadas sistemáticas de la Base de Datos para evitar pérdidas de información por cualquier motivo que pueda presentarse. Estas salvadas deberán almacenarse en otros sistemas de cómputo independientes al servidor de Bases de Datos o en algún dispositivo de almacenamiento.

### Conclusiones parciales

En este capítulo quedó establecido el estilo arquitectónico utilizado para el desarrollo del sistema; además, las clases del diseño se representaron a través de los diagramas de clases del diseño, la interacción de las mismas a partir de los diagramas de secuencias y el modelo de datos a través de los diagramas entidad relación.



# Capítulo 4

## Implementación y prueba

### Introducción

En este capítulo se presentará el modelo de implementación, donde se describe cómo los elementos del modelo de diseño, se implementan en términos de componentes, como ficheros de código fuente, ejecutables, entre otros. El modelo de implementación describe también cómo se organizan los componentes de acuerdo con los mecanismos de estructuración y en el lenguaje o lenguajes de programación utilizados y cómo dependen los componentes unos de otros. Su propósito fundamental es desarrollar la arquitectura y el sistema como un todo.

Un componente es el empaquetamiento físico de los elementos de un modelo, como son las clases en el modelo de diseño. [30]

#### 4.1. Modelo de implementación.

El modelo de implementación está compuesto por componentes y subsistemas que constituyen la composición física de la implementación. Fundamentalmente, se describe la relación que existe desde los paquetes y clases del modelo de diseño a subsistemas y componentes físicos. Este artefacto describe cómo se implementan los componentes, congregándolos en subsistemas organizados en capas y jerarquías, señala las dependencias entre estos.

##### 4.1.1. Diagrama de despliegue.

El modelo de despliegue es un modelo de objetos que describe la funcionalidad entre los nodos de cómputo. Se utiliza como entrada fundamental en las actividades de diseño e implementación debido a que la distribución del sistema tiene una influencia principal en su diseño.

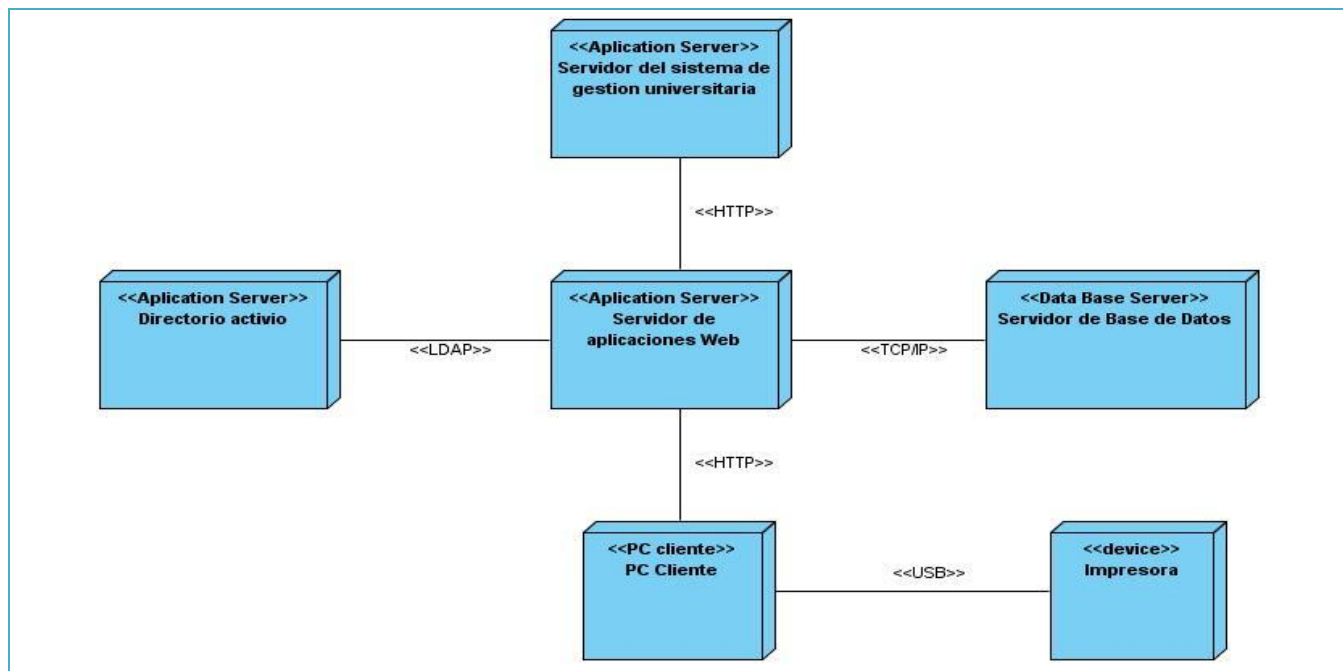


Figura 17. Diagrama de despliegue.

Recurso	Breve descripción de su uso
Nodo Servidor de aplicaciones web.	Contiene los componentes necesarios para montar el Sistema de Gestión de Riesgos. Se utiliza el servidor web apache.
Nodo servidor de base de datos.	Contiene la base de datos donde se encuentran los datos correspondientes al Sistema de Gestión de Riesgos. Se utiliza PostgreSQL.
Nodo PC Cliente.	PC que interactúa con los servidores del Sistema de Gestión de Riesgos. Se encuentran los componentes necesarios para visualizar las interfaces gráficas de dicho sistema.
Nodo Servidor del dominio.	Contiene la base de datos de los usuarios del dominio. El Sistema de Gestión de Riesgos necesita datos que le ofrece esta base de datos a través de un servicio web.
Nodo servidor de sistema de gestión universitaria.	Contiene la aplicación web del sistema de gestión universitaria. El Sistema de Gestión de Riesgos necesita datos que le ofrece esta aplicación a través de un servicio web.
Dispositivo impresora.	Impresora instalada en el nodo cliente para permitir la impresión de la información obtenida del Sistema de Gestión de Riesgos.

Tabla 22. Descripción de los nodos del diagrama de despliegue.

### 4.1.2. Diagramas de componentes.

Los diagramas de componentes se distinguen de los demás diagramas por su contenido. En la mayoría de los casos contienen componentes, interfaces y relaciones entre ellos. Y como los demás, pueden contener paquetes utilizados para agrupar elementos de modelos. En estos diagramas se manifiestan las organizaciones y dependencias lógicas entre componentes. Dado que los diagramas de componentes muestran los elementos de software que constituyen una parte reusable, sus interfaces y sus interrelaciones, en muchos aspectos se puede considerar que un diagrama de componentes es un diagrama de clases a gran escala. [31] A continuación se muestran algunos diagramas de componentes.

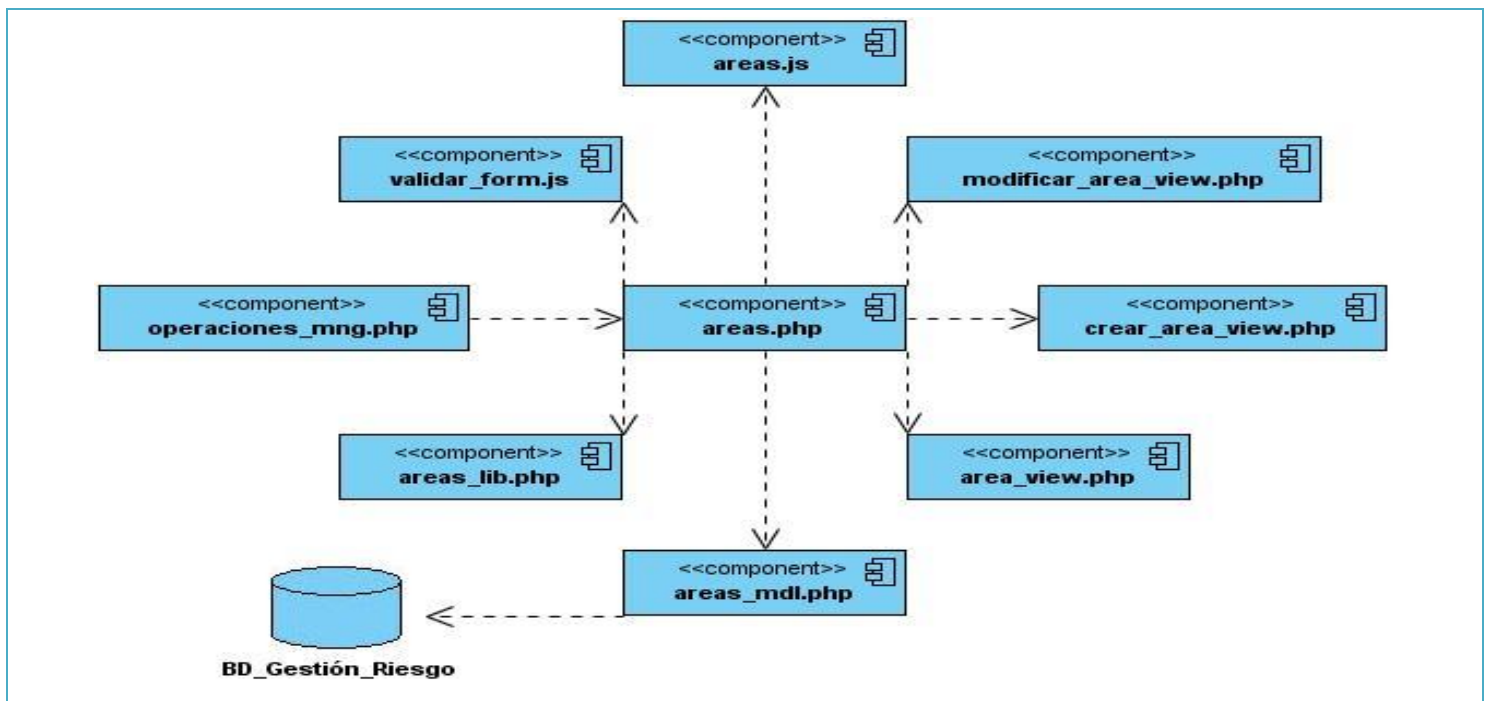


Figura 18. Diagrama de componentes CU Administrar información del área.

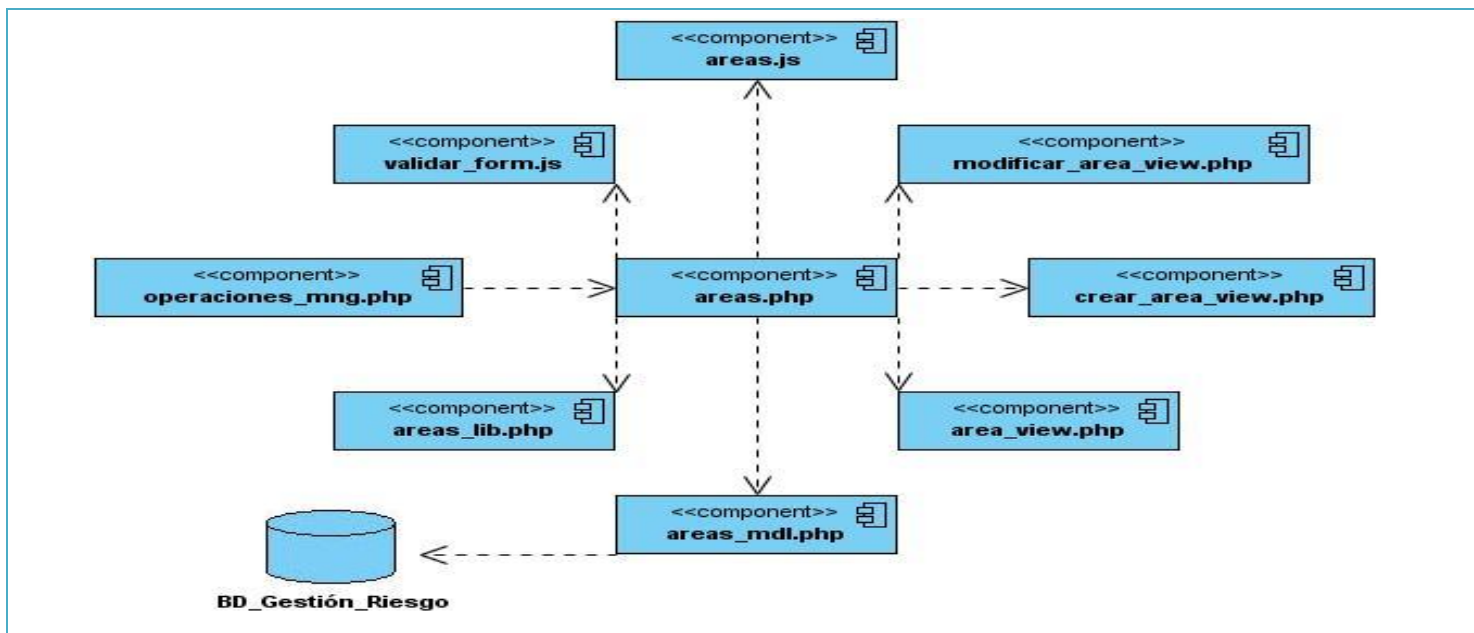


Figura 19. Diagrama de componente del caso de uso Administrar evaluación de riesgo.

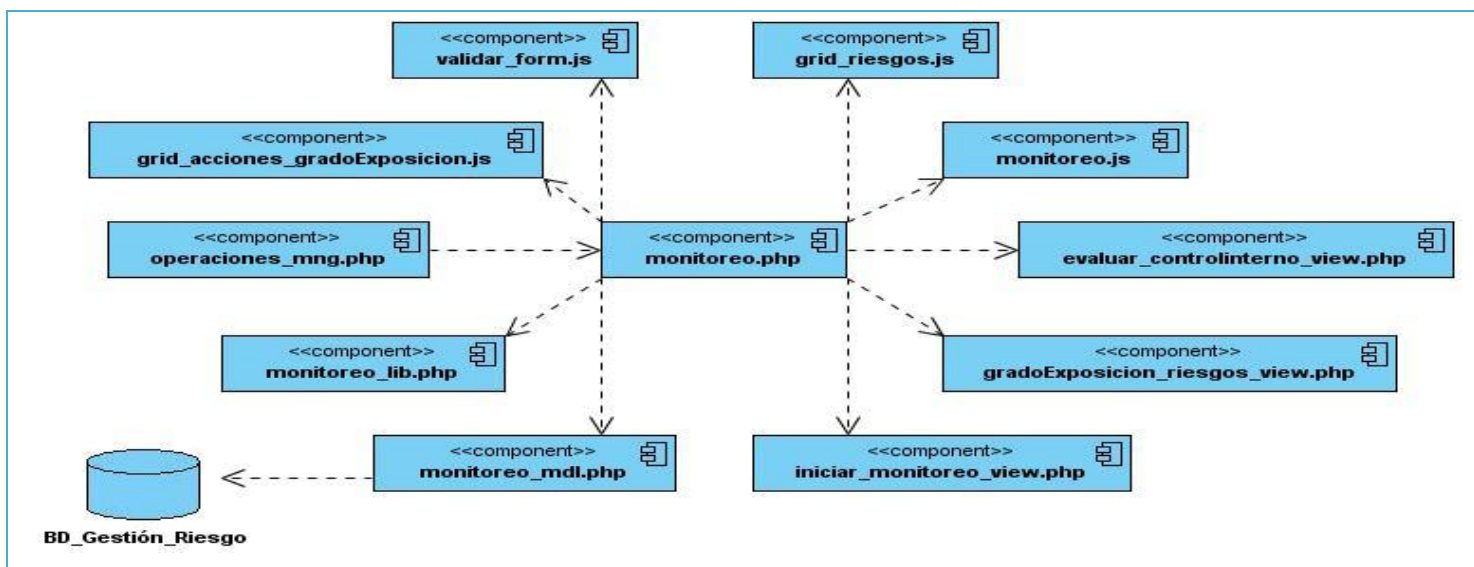


Figura 20. Diagrama de componentes CU Administrar monitoreo.

## 4.2. Modelo de prueba.

A continuación se describen los casos de prueba desarrollados por cada caso de uso definido, especificándose los resultados y las condiciones que debe dar el sistema.

**4.2.1. Descripción de los casos de prueba de integración.**

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El administrador del sistema intenta autenticarse pero escribe mal su usuario o contraseña.	El sistema muestra un mensaje que dice error en clave (si el usuario introdujo mal la clave) o usted no es un usuario del sistema (si el usuario introdujo mal el usuario) y seguidamente muestra otro mensaje: usted no tiene acceso a la funcionalidad solicitada y muestra un vínculo a la página de autenticación.	La operación se repite hasta que el usuario corrige los datos.

*Tabla 23. Prueba de integración para el caso de uso: Autenticar usuario.*

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El administrador del sistema va a crear los datos de un usuario y no introduce todos los datos obligatorios.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios.	La operación se repite hasta que el usuario corrige los datos.
El administrador del sistema va a modificar los datos de un usuario y no llena todos los campos obligatorios.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios para poder modificar los datos del usuario y muestra en rojo los datos obligatorios.	La operación se repite hasta que el usuario corrige los datos.

*Tabla 24. Prueba de integración para el caso de uso: Gestionar usuario.*

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El administrador del sistema va a crear un rol y no introduce los datos obligatorios.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios y muestra en rojo los datos obligatorios.	La operación se repite hasta que el usuario corrige los datos.
El administrador del sistema va a modificar un rol y no introduce todos los datos obligatorios.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios y muestra en rojo los datos obligatorios.	La operación se repite hasta que el usuario corrige los datos.

*Tabla 25. Prueba de integración para el caso de uso: Gestionar roles.*

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El administrador del sistema va a crear una funcionalidad y no introduce todos los datos obligatorios.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios y muestra en rojo los datos obligatorios que no se han llenado.	La operación se repite hasta que el usuario corrige los datos.
El administrador del sistema va a modificar una funcionalidad y deja campos obligatorios sin llenar.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios y muestra en rojo los datos obligatorios que no se han llenado.	La operación se repite hasta que el usuario corrige los datos.

*Tabla 26. Prueba de integración para el caso de uso: Gestionar funcionalidades.*

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El operador no introduce todos los datos obligatorios de la información del área.	El sistema marca en rojo los campos obligatorios que no están correctos (los campos que no estén llenos o tengan menos de 10 caracteres)	La operación se repite hasta que el Operador corrige el error.

*Tabla 27. Prueba de integración para el caso de uso: Administrar información del área.*

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El operador no introduce todos los datos obligatorios de la información de los procesos.	El sistema marca en rojo el campo obligatorio de la descripción del proceso (debe tener más de 10 caracteres).	La operación se repite hasta que el Operador corrige el error.

*Tabla 28. Prueba de integración para el caso de uso: Gestionar procesos.*

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El operador no entra todos los datos obligatorios de la información de las actividades.	El sistema marca en rojo el campo obligatorio de la descripción de la actividad (debe tener más de 10 caracteres).	La operación se repite hasta que el Operador corrige el error.

*Tabla 29. Prueba de integración para el caso de uso: Gestionar actividades.*

<b>Entrada</b>	<b>Resultados</b>	<b>Condiciones</b>
El operador va a crear un riesgo y no introduce todos los datos obligatorios.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios y muestra en rojo los datos	La operación se repite hasta que el Operador corrige el error.

	obligatorios que no se han llenado.	
El operador va a modificar los datos de un riesgo y deja campos obligatorios vacíos.	El sistema muestra un mensaje que dice que tiene que llenar todos los campos obligatorios y muestra en rojo los datos obligatorios que no se han llenado.	La operación se repite hasta que el Operador corrige el error.

*Tabla 30. Prueba de integración para el caso de uso: Administrar evaluación de riesgos.*

### Conclusiones parciales

En este capítulo se presentaron el diagrama de despliegue del sistema para la implantación y la utilización de la aplicación y los diagramas de componentes para la representación en componentes físicos; además fueron descritos algunos casos de prueba de integración realizado al sistema.

# Conclusiones

Una vez culminada la investigación se arribó a las siguientes conclusiones:

- ❖ La necesidad de incorporar la gestión de riesgos a los procesos de la UCI, está dada tanto por la obligación de garantizar la gestión de las amenazas y reducir a niveles aceptables los impactos adversos.
- ❖ En la literatura consultada se encontró diversidad de conceptos en materia de riesgos en los que se brinda especial atención a los elementos comunes referentes a las etapas y los enfoques para la gestión de riesgos, como son: la identificación, análisis y tratamiento de los riesgos.
- ❖ La Resolución 297/03 del Ministerio de Finanzas y Precios no ofrece una metodología que facilite la identificación, evaluación y tratamiento de los riesgos.
- ❖ Se obtuvo una solución informática para la gestión de riesgos operacionales, que permite la identificación, evaluación, tratamiento y monitoreo continuo de los riesgos de las áreas de la UCI.
- ❖ La utilización del sistema implementado permite obtener un aumento en la calidad del proceso de gestión de riesgos, ya que proporciona una mayor organización en la información. Además, facilita el trabajo a todos los usuarios involucrados con esta tarea, disminuye el margen de errores posibles y agiliza este proceso
- ❖ La solución propuesta contribuye a la informatización de la UCI.



## Recomendaciones

Se recomienda:

- ❖ Implementar los cuatro casos de uso restantes: Consultar información del área, Consultar evaluación de riesgos, Consultar monitoreo y Generar reportes.
- ❖ Diseñar e implementar un repositorio de riesgos, procesos, actividades y acciones de control, con el objetivo de facilitar el trabajo para las personas encargadas de este proceso en las áreas, dando la posibilidad de partir de procesos, actividades, riesgos y acciones de control almacenadas, que pueden ser utilizados en diferentes evaluaciones de riesgos, de una forma fácil y efectiva.
- ❖ Que el sistema no solo sea aplicado en las áreas de la UCI, sino que se extienda a las facultades regionales.

## Referencias Bibliográficas

1. Ladino, Enrique. Control interno Informe Coso. Disponible en:  
<http://www.monografias.com/trabajos12/comcoso/comcoso.shtml>
2. León Lefcovich, Mauricio. Marco teórico conceptual sobre gestión de riesgos.
3. Koprinarov, Bratoy; El riesgo empresarial y su gestión analítica, 2005.
4. Martínez Carrera, R (1998): "Situación actual y perspectivas de la Administración de Riesgos en Cuba", Intervención en el 1er Seminario Nacional sobre Administración de Riesgos, La Habana, Cuba.
5. Campoverde Vélez, Félix. Administración de los Riesgos Empresariales. Disponible en:  
<http://www.monografias.com/trabajos52/riesgos-empresariales/riesgos-empresariales.shtml>
6. Durán A., M. V. y Abreu H., M. (2007): Metodología para el proceso Identificación de Riesgos. Consultoría BISE S. A. V Encuentro Internacional de Contabilidad, Auditoría y Finanzas. La Habana.
7. Estándar Australiano/Neo Zelandés(AS/NZS: 4360(1999)): Administración de Riesgos.
8. Ídem a 7.
9. Traducido de COSO (2004): Enterprise Risk Management – Integrated Framework. Executive Summary.
10. Rodríguez Carrazana, Yadira. Modelo de identificación de los riesgos de control interno para la actividad empresarial.
11. Arbeláez, Juan Camilo. Riesgo Operacional: reto actual de las entidades financieras. Revista de Ingeniería de la Universidad de Medellín, julio-diciembre, vol. 5, número 009, p.97-110.
12. Martínez Carrera, R. (1998): Situación actual y perspectivas de la Administración de Riesgos en Cuba. Primer Seminario Nacional sobre Administración de Riesgos, Cuba.
13. Pérez M. y Navarro L. (1999): La gerencia de riesgos en la alta dirección de la empresa.
14. COSO (2004): Enterprise Risk Management – Integrated Framework.

15. Manual de Gestión de Riesgos Operativos. Deusto España, p.14.
16. MFP. Resolución No 297-2003, Anexo 1, p.9.
17. Pelegrin Pérez, Edmundo Lázaro. La administración de los Riesgos, su impacto en la empresa cubana. Cuba, UPR, 2006.
18. Oñate Fragozo, Henry. Manual de Control interno.
19. Gil Lafuente, A.M. (1993) El análisis financiero en la incertidumbre. Ariel Economía, España, p.63.
20. COSO (2004): Gestión de Riesgos Corporativos. Técnicas de Aplicación, p.47.
21. Ídem a 20. p.52.
22. Ídem a 20. p.53.
23. Ídem a 20. p.54.
24. Gálvez Santizo, Brenda María. Evaluación del ambiente de control interno de una empresa que fabrica productos plásticos aplicando el informe del comité de las organizaciones patrocinadoras de la comisión Treadway (COSO).
25. Cuenca, Carlos Luis. Descripción de la arquitectura en módulos del Apache. Explicación y enumeración de las funcionalidades asociadas a cada módulo.
26. Pablo Martínez, Ruiz Díaz, Sebastián Waisbrot. Manual de Codeigniter en español.
27. Lenguaje Unificado de Modelado. Disponible en: <http://www.buenastareas.com/ensayos/Lenguaje-Unificado-De-Modelado/145516.html>
28. Larman, C. "UML y Patrones", Segunda edición, Pearson Prentice Hall, España, 2003, ISBN: 84-205-3438-2.
29. Barros, Joan. *Modelo de datos*. Disponible en: <http://joanbarros.wordpress.com/2007/09/>
30. The Unified Modeling Language for Object-Oriented Development. s.l. :Rational Software Corp, 1997.
31. Jacobson, Ivar, Booch, Grady y Rumbaugh, James. El Proceso Unificado de Desarrollo de Software. Volumen I. La Habana: Félix Varela, 2004.

## Bibliografía

- ❖ ALVARADO CORTES, CESAR. “UN NUEVO ENFOQUE PARA LA INTERVENCION EFECTIVA DEL RIESGO”. EL RIESGO OPERACIONAL SU ANALISIS Y EVALUACION. Bogotá 27 de junio de 2007.
- ❖ AS/NZS 4360. E. Administración de riesgos. Australia.1999.
- ❖ Beldar Muñoz, Víctor. *Prevención de los riesgos, Implementación de un sistema de control de los riesgos de operación en la empresa*. Colombia, 2005. Disponible en: [www.gestiopolis.com](http://www.gestiopolis.com).
- ❖ Campoverde Vélez, Félix. Administración de los Riesgos Empresariales. Disponible en: <http://www.monografias.com/trabajos52/riesgos-empresariales/riesgos-empresariales.shtml>
- ❖ Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO II - El Enfoque Integrado para la Administración Corporativa de Riesgos Enterprise Risk Management - Integrated Framework. Septiembre 2004.
- ❖ COSO II: Enterprise Risk Management. Bogotá D.C., Colombia. Disponible en: [www.nasaudit.com](http://www.nasaudit.com)
- ❖ COSO (2004): Gestión de Riesgos Corporativos. Técnicas de Aplicación.
- ❖ Danze, Carlos. RIESGO OPERACIONAL. Disponible en: [www.dpya-sa.com.ar](http://www.dpya-sa.com.ar)
- ❖ Dorta Velásquez, José Andrés. *La evaluación de los riesgos como componente básico del sistema de Control Interno*. España, 2004.
- ❖ Durán A., M. V. y Abreu H., M. (2007): Metodología para el proceso Identificación de Riesgos. Consultoría BISE S. A. V Encuentro Internacional de Contabilidad, Auditoría y Finanzas. La Habana.
- ❖ Enterprise Risk Management – Integrated Framework. Executive Summary.
- ❖ Estándar Australiano/Neo Zelandés(AS/NZS: 4360(1999)): Administración de Riesgos.
- ❖ Fernández Menta, Adriana. Nuevo marco COSO de gestión de riesgos.
- ❖ Jacobson, Ivar, Booch, Grady y Rumbaugh, James. El Proceso Unificado de Desarrollo de Software. Volumen I. La Habana: Félix Varela, 2004.

- ❖ *Koprinarov, Bratoy*. El riesgo empresarial y su gestión. Publicado, 12 de mayo de 2005. Disponible en: <http://www.analitica.com/va/economia/opinion/5753437.asp>
- ❖ Larman, C. "UML y Patrones", Segunda edición, Pearson Prentice Hall, España, 2003, ISBN: 84-205-3438-2.
- ❖ Laski, Julian. La necesidad de gestionar el riesgo operacional. Buenos Aires, Argentina. Disponible en: <http://www.pkfargentina.com.ar/doc/prensa/la-necesidad.pdf>
- ❖ LOS NUEVOS CONCEPTOS DE CONTROL INTERNO (INFORME COSO).
- ❖ Manual de Gestión de Riesgos Operativos. Deusto España.
- ❖ Ministerio de Finanzas y Precios. Resolución 297/03.
- ❖ Pelegrin Pérez, Edmundo Lázaro. La Administración de los Riesgos, su impacto en la empresa cubana. Cuba, UPR, 2006. (REVISAR).
- ❖ Pérez M. y Navarro L. (1999): La gerencia de riesgos en la alta dirección de la empresa.
- ❖ Pérez Solórzano, Pedro Manuel. *Los cinco componentes del Control Interno*. 26 de enero de 2007. Disponible en: [http://www.degerencia.com/articulo/los\\_cinco\\_componentes\\_del\\_control\\_interno](http://www.degerencia.com/articulo/los_cinco_componentes_del_control_interno)
- ❖ Rodríguez Carrazana, Guerra Garcés, Reyes Santos. *MODELO DE IDENTIFICACIÓN DE LOS RIESGOS DE CONTROL INTERNO PARA LA ACTIVIDAD EMPRESARIAL*. Disponible en: <http://www.eumed.net/ce/2009a/cgs.htm>
- ❖ Rodríguez, Corbetta. La administración del riesgo operacional Responsabilidad social corporativa. Hot Topics. Año 3. Edición Especial. 2007.
- ❖ Rodríguez, R., "Situación actual y perspectivas de la Administración de Riesgos en Cuba" en el 1er Seminario Nacional sobre Administración de Riesgos, Mayo 1998.
- ❖ Romero Fernández, Ariel. LA GESTIÓN DE RIESGOS COMO INSTRUMENTO PREVENTIVO. Mayo 2003.
- ❖ Santos Prieto, Iván. ADMINISTRACIÓN DE LOS RIESGOS DE CONTROL INTERNO: PRINCIPALES FUNCIONES Y TÉCNICAS. Universidad Central de Las Villas, Cuba.
- ❖ The Unified Modeling Language for Object-Oriented Development. s.l.:Rational Software Corp, 1997.

## Anexos

### Anexo 1 Descripción de las tablas del modelo de datos.

<b>Descripción:</b> datos de los usuarios del sistema.		
<b>Atributo</b>	<b>Tipo</b>	<b>Descripción</b>
<u>id_usuario</u>	integer	Identificador del usuario.
nombre	varchar	Nombre del usuario del dominio.
id_expediente	varchar	Número de solapín.
usuario	varchar	Usuario del dominio.
activo	binary	Campo que dice si el usuario está activo o no.
fecha_registro	date	Fecha en la que se registró el usuario.
clave	varchar	Contraseña del usuario.
id_area_asset	varchar	Código de asset.
Código_area	varchar	Código del área a la que pertenece el usuario.
nombre_area	varchar	Nombre del área a la que pertenece el usuario.

*Tabla 31. Descripción de la tabla Usuario.*

<b>Descripción:</b> tipo de usuario que se autentica, que puede ser local o del dominio.		
<b>Atributo</b>	<b>Tipo</b>	<b>Descripción</b>
<u>id_tipo_usuario</u>	integer	Id del tipo de usuario que se autentica.
nombre_tipo_usuario	varchar	Id del tipo de usuario.
activo	binary	Campo que dice si el usuario está activo o no.

*Tabla 32. Descripción de la tabla Tipo\_usuario.*

<b>Descripción:</b> relación entre los usuarios y roles.		
<b>Atributo</b>	<b>Tipo</b>	<b>Descripción</b>
<u>Id_usuario</u>	integer	Identificador del usuario.
<u>Id_rol</u>	integer	Identificador del rol.

*Tabla 33. Descripción de la tabla Usuario\_Rol.*

<b>Descripción:</b> datos de los roles del sistema.		
<b>Atributo</b>	<b>Tipo</b>	<b>Descripción</b>
<u>id_rol</u>	integer	Id del rol del usuario que se autentica.
activo	binary	Campo que dice si el usuario está activo o no.
rol	varchar	Rol de los usuarios.
descripción	varchar	Descripción del rol.
fecha_registro	date	Fecha en la que se registró el rol.
creador	varchar	Persona que creo el rol.

ultima_actualizacion	timestamp	Ultima actualización del rol.
----------------------	-----------	-------------------------------

Tabla 34. Descripción de la tabla Rol.

<b>Nombre:</b> Rol_Funcionalidad.		
<b>Descripción:</b> relación entre los roles y las funcionalidades a las que tienen acceso.		
Atributo	Tipo	Descripción
id_funcionalidad	integer	Id de la funcionalidad.
id_rol	integer	Id del rol.

Tabla 35. Descripción de la tabla Rol\_Funcionalidad.

<b>Descripción:</b> datos de las funcionalidades del sistema.		
Atributo	Tipo	Descripción
id_funcionalidad	integer	Id de la funcionalidad.
activo	binary	Campo que dice si el usuario está activo o no.
funcionalidad	varchar	Nombre de la funcionalidad.
url	varchar	Dirección de la URL de la funcionalidad.
fecha_registro	date	Fecha en la que se registró el rol.
creador	varchar	Persona que creó el rol.

Tabla 36. Descripción de la tabla Funcionalidad.

<b>Descripción:</b> información del área de la que se va a gestionar los riesgos.		
Atributo	Tipo	Descripción
id_area	integer	Id del área.
nombre	varchar	Nombre del área.
descripción	varchar	Descripción del área.
misión	varchar	Misión del área.
objetivos	varchar	Objetivos del área.

Tabla 37. Descripción de la tabla Área.

<b>Descripción:</b> información de los procesos que se manejan en el área.		
Atributo	Tipo	Descripción
id_proceso	integer	Id del proceso.
nombre	varchar	Nombre del proceso.
descripción	varchar	Descripción del proceso.

Tabla 38. Descripción de la tabla Proceso.

<b>Descripción:</b> información de las actividades por procesos que se manejan en el área.		
Atributo	Tipo	Descripción
id_actividad	integer	Id de la actividad.
código	varchar	Código de la actividad.

nombre	varchar	Nombre de la actividad.
descripción	varchar	Descripción de la actividad.

Tabla 39. Descripción de la tabla Actividad.

**Descripción:** datos de los riesgos.

Atributo	Tipo	Descripción
<u>id_riesgo</u>	integer	Identificador del riesgo.
código	varchar	Código del riesgo.
nombre	varchar	Nombre del riesgo.
descripción	varchar	Descripción del riesgo.
probabilidad	integer	Evaluación de la probabilidad de que se materialice el riesgo.
consecuencia	integer	Evaluación de la consecuencia de que se materialice el riesgo.
prioridad	integer	Nivel de prioridad de los riesgos para efectuar las acciones de control.
grado_exposición	varchar	Grado de exposición que posee una actividad a un riesgo determinado.

Tabla 40. Descripción de la tabla Riesgo.

**Descripción:** datos de los monitoreos que se planifiquen.

Atributo	Tipo	Descripción
<u>id_monitoreo</u>	integer	Id del monitoreo.
fecha	timestamp	Fecha de inicio del monitoreo.
evaluación	varchar	Evaluación del monitoreo.

Tabla 41. Descripción de la tabla Monitoreo.

**Descripción:** datos de las acciones de control.

Atributo	Tipo	Descripción
<u>id_acciones_control</u>	integer	Id de las acciones de control.
nombre	varchar	Nombre de la acción de control.
efectuada	binary	Campo que dice si la acción está efectuada o no.

Tabla 42. Descripción de la tabla Acciones\_control.

**Descripción:** relación entre el riesgo y el monitoreo.

Atributo	Tipo	Descripción
<u>id_acciones_control</u>	integer	Id de las acciones de control.
<u>id_monitoreo</u>	integer	Id del monitoreo.

Tabla 43. Descripción de la tabla Acciones\_control\_Monitoreo.