PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSTGRADO

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE RIESGO OPERACIONAL PARA ENTIDADES FINANCIERAS - SIRO

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN INFORMÁTICA MENCIÓN EN INGENIERÍA DEL SOFTWARE

AUTOR: CARLOS AVALOS RUIZ

ASESOR: MAYNARD KONG WONG

JURADOS: JOSE ANTONIO POW SANG PORTILLO
MARIANO ADAN GONZALES ULLOA

Lima, Noviembre de 2012

Resumen

El presente proyecto nace como resultado de la necesidad que tienen las Instituciones financieras de realizar la gestión de los riesgos debido a la incertidumbre que pasan a partir de eventos pequeños, predecibles y frecuentes, por lo que en el mes de junio del 2004 En el nuevo Acuerdo de Capitales de BASILEA – II se define lo Siguiente: “el riesgo de pérdida directa debido a la inadecuación o a fallos en los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación”,

El presente estudio es una introducción en los modelos cuantitativos del riesgo operacional para la creación de una herramienta Software. Esta investigación estará limitada a la gestión de los riesgos operativos en el ámbito la administración cuantitativa y el desarrollo de la herramienta software para lograrlo, proponiendo la construcción e implantación de un software para la gestión del riesgo operacional, aplicando una adaptación del proceso de construcción de software Rational Unified Process, que incluye el flujo de trabajo de procesos y el flujo de trabajo de soporte para el desarrollo del software teniendo en cuenta que para el proceso de implantación y puesta en marcha del software se realizara de acuerdo a los lineamientos de la entidad financiera pues cada una tiene estándares propios.

Este proyecto pretende apoyar e impulsar el cumplimiento normativo dispuesto por la Superintendencia de Banca Seguros y AFP’s en cuanto a la Gestión del Riesgo Operacional. La herramienta, permitirá a las entidades financieras cumplir de manera más rápida y eficiente los requisitos para alcanzar el método del estándar alternativo, lo cual le permitirá reducir el requerimiento patrimonial a causa del Riesgo Operacional. La misma que constituye en un motor de cambio para ayudarle a integrar la gestión del Riesgo Operacional en las diferentes áreas de su institución.

El proyecto permitirá la construcción e implantación de un software Sistema de Riesgo Operacional para Entidades Financieras que impulsará el establecimiento de una cultura adecuada y propicia para la gestión del riesgo operacional, al mismo tiempo reducir el esfuerzo para lograr una adecuada gestión del riesgo operacional.

Introducción

Las instituciones financiera que, cuentan con la autorización de la Superintendencia de Banca y Seguros y que gozan de autonomía económica, financiera y administrativa brinda los servicios de Ahorros; que es la captación de los fondos del público a través de las diferentes modalidades y de Crédito, que es la colocación de los fondos captados.

En la actualidad con la inclusión del RIESGO OPERACIONAL en el Nuevo Acuerdo de Capitales de BASILEA (*Fontnouvelle)* refleja uno de los cambios más significativos en la gestión financiera, donde su importancia está desplazando el tradicional interés por los riesgos de crédito y mercado, centrando los esfuerzos actuales del sector financiero.

Su carácter cualitativo dificulta el desarrollo de herramientas de identificación, medición y control, y las exigencias reguladoras definen los nuevos retos planteados para el sistema financiero. La gestión del riesgo aplica para las entidades financieras, bancarias y micro financieras del sistema peruano y que son supervisados por la Superintendencia de Banca y Seguros (SBS).

El riesgo operativo es otro componente gestión de riesgo según BASILEA II que son las mejores se reunieron los 10 países más ricos del mundo y pensaron por que perdían tanto y ahí se definió los riesgos: Personas, procesos, tecnología información y aspectos externos en esto se basa el riesgo operacional que es la base de Basilea II.

La necesidad es la de llegar a los modelos cuantitativos así que el presente estudio es una introducción en los modelos cuantitativos basados en una herramienta Software que permita llegar a los modelos cuantitativos. La gestión de los riesgos operativos plantea la adopción de estándares para una adecuada administración. Los estándares generalmente platean una administración cualitativa. Esta investigación estará limitada a la gestión de los riesgos operativos en el ámbito la administración cuantitativa.

1. CAPITULO 1 - Generalidades

En el Perú a través de la Resolución SBS N° 37-2008 del 10 de enero de 2008, se aprobó el Reglamento de la Gestión Integral de Riesgos, que establece que las empresas supervisadas deben contar con una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios y Que, mediante la Resolución SBS N° 2116-2009 del 02 de abril del 2009, se aprobó el Reglamento para la Gestión del Riesgo Operacional, la cual es de aplicación para todo el sistema financiero peruano.

Todas las instituciones supervisadas por la SBS, se encuentra inmersa en el cumplimiento de las normativas emitidas por el regulador, y entre los riesgos que enfrenta como parte del desarrollo de sus actividades se encuentra el riesgo operacional, el cual puede generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos.

Las instituciones Financieras, al incorporar una herramienta software, debe permitirles incorporar un conjunto importante de mejores prácticas para gestionar este tipo de riesgo, tomando en consideración lo establecido en la normativa peruana y los criterios difundidos por el ente regulador.

La herramienta software además de aportarle directamente a la gestión del riesgo operacional y de permitirle integrar a sus demás riesgos financieros, debe permitirle integrar los requerimientos del Sistema de Control Interno, lo cual ha sido dispuesto por la Contraloría General de la República a través de su Resolución CGR N° 320-2006 y cuyo reglamento se indica en la Resolución CGR N° 458-2008, logrando una reducción de esfuerzo y desgaste en las Unidades de Control para dicha implementación y permitiendo una integración más natural de las áreas de negocio hacia un gestión integrada de riesgos, tal como lo indica la Resolución SBS N° 037-2008.

Finalmente, una adecuada gestión de riesgos en una Institución financiera, le permitirá en un futuro optar por un método de cálculo para el requerimiento patrimonial más adecuado y acorde con sus expectativas de crecimiento institucional.
El proyecto parte precisamente de la búsqueda y requerimiento de una herramienta en el mercado, que cumpliera con la normativa peruana en cuanto la gestión de los riesgos operacionales en el año 2006, cuyas características debían ser la facilidad de uso

principalmente para personal que no integra la Unidad de Riesgos, que esté basada en el uso de herramientas del tipo Open Source, y principalmente la flexibilidad que debía tener la herramienta ante cambios normativos, con un adecuado soporte técnico a nivel país y de costos accesibles, al no existir dicha herramienta con tales características es que se inició la construcción de SIRO.

SIRO, debe soportar la metodología Australiana Neocelandesa 4360, y el estándar COSO/ERM, debe contar con el detalle funcional que se indican en las normativas peruanas.

1.1. Definición del Problema

En esta sección se describirá el problema que se quiere abordar con el proyecto, estableciendo un marco de referencia para su correcto entendimiento así como el plan que se tendrá en cuenta durante su desarrollo.

1.2. Objetivo General

El propósito del proyecto de tesis es Diseñar e implementar el Sistema de Riesgo Operacional, incluyendo el modulo de gestión de eventos de perdida, basado en la continuidad de la plataforma creada de riesgo operacional, que es la base para poder llegar a la gestión cuantitativa, con el objetivo de poder realizar una gestión integral del Riesgo para el sector financiero del Perú tal como se muestra en la Figura 1.

Figura 1: Gestión Integrada de Riesgo Según Normativa Peruana

En la Actualidad algunas instituciones financieras (CAJAS MUNICIPALES, EDPYMES, CAJAS RURALES, COOPAC, Entre otras) gestionan sus riesgos sin

la utilización de un software de riesgo operacional. Esto hace que la gestión del riesgo tenga un carácter esporádico y no se tome el riesgo operacional como una cultura organizacional, debido a que para el manejo de los riesgos se necesita información de múltiples fuentes la gestión se hace tediosa y muchas veces no se toma en serio en las organizaciones. Un inconveniente más a la gestión de riesgos es que el no contar con un sistema informático que gestione el riesgo la consolidación de la información se realiza de manera manual, lo cual conlleva a trabajos mecánicos no deseados por los profesionales en la gestión de riesgos debido a la complejidad del tratamiento de la información, y todo esto hace que la participación de las diferentes áreas y dueños de los procesos sea insuficiente y tengan poco compromiso en la participación de la gestión del riesgo operacional, trayendo como consecuencia un falta de internalización de la metodología, entre las áreas de auditoría, logística, negocios, sistemas, organización y métodos, y así mismo trayendo como consecuencia un mayor incremento de la provisión que se tiene por riesgo operacional (requerimiento patrimonial); Ver Figura 2

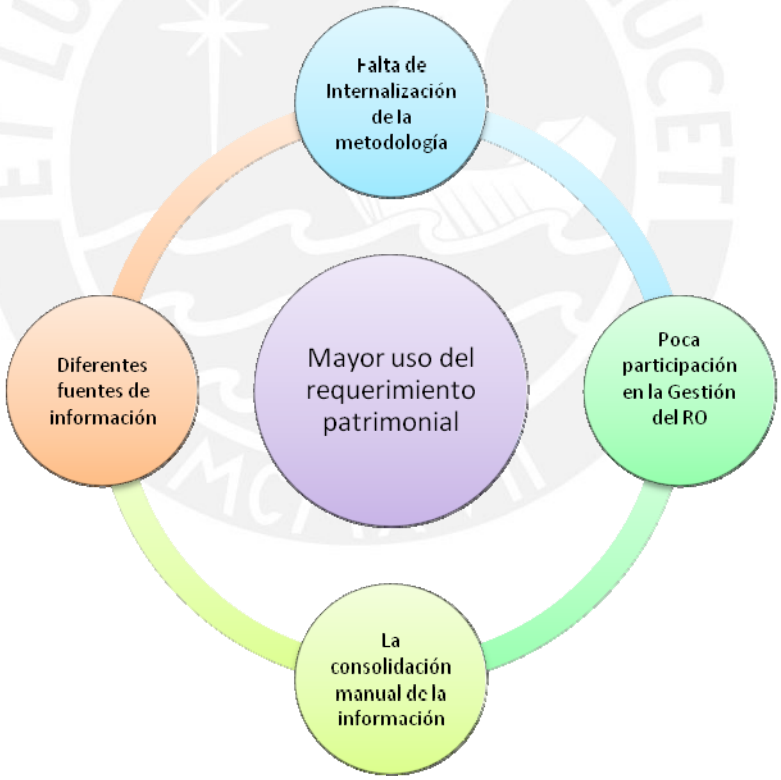


Figura 2 Problemática de la Gestión del Riesgo Operacional

Para el desarrollo del presente proyecto se debe tener en cuenta el diseño en multicapas, y no requiriéndose más que un navegador para poder conectarse al sistema.

Las entidades bancarias y financieras tienen muchas sucursales ubicadas dentro del territorio nacional por lo que es necesaria la utilización de ancho de banda (Internet - Segura) para enviar información, la herramienta a desarrollarse permitirá la conectividad por medio del browser sobre la arquitectura de las herramientas del mercado.

La plataforma de desarrollo se basara en Open Source siendo este un estándar acordado por la necesidad de no contar con licencias para el desarrollo ni la necesidad de contar con licencias para las entidades que requieran del Software. Es importante hacer mención que se realizar un análisis de las herramientas utilizadas para el desarrollo de software.

1.3. Objetivos Específicos

Los Objetivos que busca este proyecto de Tesis son:

1. Definir las principales necesidades del manejo de la Información y de la Integración de la Gestión de Riesgos Operacionales en la Instituciones financieras.

2. Aplicar la metodología COSO/ERM para la gestión del Riesgo Operacional.

3. Diseñar la Estructura de Datos de Acuerdo a la Normativa peruana Vigente de la Superintendencia de Banca y Seguros para la Gestión del Riesgo Operacional en el tiempo.

4. Desarrollar los Módulos Principales del Sistema Integral de Riesgo Operacional para Entidades Financieras.

1.4. La Realidad Peruana En El Riesgo Operacional.

La SBS con el fin de introducir en Perú la gestión de los riesgos operacionales dispuso la emisión de normas entre las que se puede mencionar:

- Resolución SBS N° 037-2008: Gestión Integral de Riesgos
- Resolución SBS N° 2116-2009: Reglamento de Riesgo Operacional
- Resolución SBS N° 2115-2009: Reglamento para el Requerimiento de Patrimonio Efectivo por R.O.
- Resolución CGR 320-2006: Normas de Control Interno

- Resolución CGR 458-2008: Guía para la Implementación del SCI

SIRO es una iniciativa para la realización de un software de riesgo operacional que de cumplimiento al marco normativo y a la realidad peruana teniendo como objetivo poder desarrollar mediante el software la cuantificación de los riesgos operacionales.

Luego de una búsqueda mediática de software en el mercado nacional que sean reconocidos por las distintas instituciones financieras del medio se ha podido identificar algunas opciones que están comercializándose en el mercado, las cuales tienen orígenes extranjeros y que no tienen embebidas las normativas peruanas que difieren de las normativas internacionales. Los Software identificados brindan una adecuación a las de las normas peruanas en muchos casos no reflejan la realidad de la gestión del riesgo operacional según la normatividad de la Superintendencia de Banca y Seguros. Este software se explicara de manera más detallada en la sección del estado del arte.

1.5. Metodología Elegida

Se ha adoptado la utilización de RUP porque he trabajado siempre con esa metodología en proyectos anteriores, así mismo se basa en casos de uso, los cuales me permiten modelar el negocio, para conocer más a fondo la problemática que aqueja a la organización.

Así mismo es iterativa pues se podrá avanzar paso a paso, es incremental pues se podrá ampliar el proyecto en caso sea necesario.

Además la utilización de RUP es una restricción del proyecto por ser una metodología de desarrollo de software que el equipo de trabajo conoce y ha utilizado en proyectos anteriores.

En conclusión se utilizará la metodología RUP como base para la implementación de este Proyecto, por ser dirigida por casos de uso para tener una visión precisa del negocio, por ser incremental e iterativa y fácil de comprender.

2. CAPITULO 2 - MARCO TEÓRICO

2.1 El Riesgo Operacional en las Entidades Financieras

La preocupación tradicional de las entidades financieras esta, centrada en los riesgos de crédito (incertidumbre acerca de la recuperación de los préstamos concedidos) y mercado alteraciones en los precios que afectan a las carteras de la entidad), se ha desplazado hacia otro tipo de problemas bancarios de múltiples causas englobados bajo el término riesgo operacional. A partir de la década de los noventa, estas incertidumbres pasan de referirse a eventos pequeños, predecibles y frecuentes (errores de procesos, fallos técnicos...) a protagonizar las quiebras bancarias más significativas y copar las páginas de los periódicos, motivando una creciente preocupación en el sector y suscitando la atención de los reguladores. Estas grandes pérdidas se deben a problemas legales, deficiencias de control interno, débil supervisión de los empleados, fraude, falsificación de cuentas o contabilidad creativa, factores en muchos casos motivados por el desarrollo tecnológico, la creciente complejidad de las operaciones, la diversificación de productos, los nuevos canales de distribución, outsourcing, entre otras.

En el Nuevo Acuerdo de Capitales de Basilea (Basilea-II), aprobado en el mes de junio de 2004. La definición tomada actualmente como referente para el riesgo operacional es: “el riesgo de pérdida directa debido a la inadecuación o a fallos en los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación”

2.2 Cuantificación y Medida Del Riesgo Operacional

La identificación del riesgo operacional conlleva todo un proceso de auto evaluación y diagnóstico al que puede contribuir la labor de la auditoría interna. En cualquier caso, se suele establecer un mapa de riesgos, en base a la combinación de dos variables: la frecuencia o probabilidad de que acontezca una pérdida operacional y la severidad o cuantía de dicha pérdida.

Dado que los riesgos menos significativos se asumen como parte del negocio y ya se han considerado al fijar el precio de los productos y servicios financieros, y los menos frecuentes y de mayor impacto representan circunstancias muy anómalas, el interés de la gestión se centra en los riesgos medios, distintos entre sí. La entidad dispone de información suficiente sobre los eventos frecuentes y de pequeña cuantía, lo que permite modelizar su distribución de pérdidas, aplicando herramientas estadísticas.

El fraude cometido con tarjetas de crédito, errores contables, errores en liquidaciones, figura entre los ejemplos más habituales. Suelen reflejar pérdidas esperadas, que se cubren a través de provisiones, Por el contrario, la escasa frecuencia de riesgos externos (desastres naturales, incendios...), fraudes o pleitos, dificulta su tratamiento Por esa razón, las entidades deben recurrir a datos externos (bases de datos del sector), la participación en consorcios de datos o el diseño de escenarios por parte de expertos, completando así la escasez de información interna. Dado su carácter inesperado, es para la cobertura de este tipo de riesgos para lo que se precisa capital y, en ocasiones, la contratación de seguros.

2.3 Transferencia del Riesgo Mediante Seguros

Los seguros permiten transferir el riesgo a un tercero (el asegurador) y mitigar la pérdida financiera, en lugar de gestionar internamente esa incertidumbre. Los riesgos tradicionalmente asegurados se asocian a activos físicos, personal o tecnología. Sin embargo, no todos los riesgos son asegurables y la decisión de contratar un seguro depende, en definitiva, del valor añadido que suponga para el asegurado. La contratación de un seguro puede generar valor añadido para los accionistas a través de la estabilidad de los flujos de caja, prevención de catástrofes financieras, mayor supervisión y control, así como la gestión del riesgo a menor coste. La entidad optará por contratar un seguro para financiar sus pérdidas operacionales cuando su coste (la prima) sea inferior al uso de recursos propios con idéntica finalidad. El seguro es, en este caso, un sustituto del capital.

2.4 Herramientas para el Control del Riesgo Operacional

Superados los intentos iniciales por adaptar los modelos de gestión antes aplicados a otros riesgos, el esfuerzo se centra ahora en desarrollar herramientas cuantitativas y cualitativas de medición y control del riesgo operacional. Mientras

que las técnicas cuantitativas pretenden reflejar estadísticamente el comportamiento de las pérdidas, situando la pérdida esperada, inesperada y excepcional (la cola de la distribución, que refleja los riesgos extremos), la utilidad de los instrumentos cualitativos radica en identificar y vigilar estos riesgos, pudiendo contribuir al desarrollo de metodologías de gestión interna que colaboren en el desarrollo de modelos avanzados. Entre ellos destacan los indicadores de riesgo y las redes causales.

a) Indicadores de Riesgo:

Se identifican variables representativas del funcionamiento de la entidad en aquellos puntos que puedan derivar en pérdidas operacionales, permitiendo la identificación, control y seguimiento del riesgo. En consecuencia, al diseño de un Cuadro de Mando en entidades financieras tradicional debería incorporarse un conjunto de indicadores de riesgo. Para ello, a las cuatro perspectivas tradicionales (pero no necesariamente las únicas) propuestas por Kaplan y Norton (clientes, proceso interno, aprendizaje y crecimiento y financiera) debe sumarse una más referida al riesgo o, alternativamente, incluir indicadores al respecto en las ya existentes, pudiendo identificarlos para los cuatro drivers citados en Basilea-II.

b) Redes causales

Son representaciones gráficas de relaciones causales entre variables. Partiendo del conocimiento previo, se trabaja con probabilidades a priori que podrán modificarse a través del análisis para definir probabilidades a posteriori.

2.5 La Regulación del nuevo acuerdo de Basilea

El Acuerdo de Capitales de Basilea (BCBS, 1988), destinado a la cobertura del riesgo de crédito mediante capital y modificado en 1996 para incorporar el riesgo de mercado, se había quedado obsoleto por no responder al nuevo entorno financiero, su escala sensibilidad real al riesgo y el olvido de los riesgos operacionales. Basilea-II ha incorporado esta categoría para el cálculo del capital regulatorio, aunque éste se cuestione como el mejor instrumento para su cobertura. El Acuerdo se estructura en tres pilares [B2], y en todos ellos se hace referencia al riesgo operacional.

El pilar 1 (requisitos mínimos de capital) al determinar los recursos propios

El pilar 2 (revisión supervisora) al verificar que el capital calculado es apropiado y responde al perfil de riesgos de la entidad
El pilar 3 (disciplina de mercado) exigiendo que se revele la información relativa a la carga de capital y método aplicado.
Los métodos para el cálculo de requerimiento de capital son:

a) Método del Indicador Básico: el capital a mantener se calcula como un porcentaje predefinido (15%) sobre la media de los ingresos brutos de los tres últimos años (si son negativos o cero no se consideran).

b) Método Estándar: el capital se obtiene agregando la cifra calculada a partir de porcentajes predefinidos para las ocho líneas de negocio prestablecidas, a las que cada entidad debe adaptar su propia estructura. Los ingresos brutos se mantienen como indicador (importe medio anual obtenido en los tres últimos años en cada línea), siendo posible la compensación de cifras positivas y negativas entre distintas líneas (no así en la Directiva Europea).

c) Métodos de Medición Avanzada: permiten determinar el capital regulatorio por riesgo operacional a partir de los modelos desarrollados por cada entidad, partiendo de sus datos internos. Basilea-II alude expresamente a dos enfoques: el método de medición interna y el enfoque de distribución de pérdidas, aunque en documentos consultivos anteriores también se hacía referencia a la elaboración de scorecards. A partir de las ocho líneas de negocio y siete categorías de riesgos, los cálculos se realizan para cada combinación de ambas categorías.

2.6 Estado del Arte

Cuando no hay información acerca del riesgo operacional en las entidades financieras el trabajo es incierto, es por ello que el requerimiento de capital para estas instituciones se hace necesario pues se debe asegurar la continuidad del negocio y la protección de los capitales en las entidades financieras, las probabilidades sin información actualizada no se pueden predecir, en la actualidad esto se basa en las experiencias, no se tiene recolección de datos para definir si la cualificación proporcionada por las áreas de negocio o dueños de los procesos de negocio se producen en la realidad con la frecuencia y el impacto que indican pues las herramientas de recolección de información no son las adecuadas.

Con El Software de Riesgo operacional Como herramienta se permite cumplir con uno de los requerimientos que permite gestionar el RO de modo más eficiente y permite la contribución de la cultura de la gestión del RO en la Organización.

En la actualidad los bancos tienen base de datos de pérdidas que permiten recopilar eventos de pérdidas que son desarrollos de Empresas internacionales y uno que otro software desarrollado de manera interna que no está certificado por la SBS.

Los principales Sistemas en riesgo operacional que se encuentran en el mercado nacional son:

- Power Risk de la Empresa Escalar Consulting. Ver Anexo Power Risk.
- ERA – de la Empresa Method Ware. Ver anexo Metod WAre
- TeamRisk – de la Empresa PriceWaterhouse. Ver anexo TeamRisk
- MEYCORCOSO AG – de la Empresa MeyorCoso. ver anexo Meyor coso

Esta información es obtenida de las propias páginas web de las compañías que brindan software de Riesgo Operacional, la información manejada por estos software tiene carácter de confidencial por las entidades financieras por tratarse de riesgos operativos que no deben salir del entorno organizacional, es por ello que el software debe tener niveles de seguridad que aseguren la privacidad de la información, esto es algo que las compañías no muestran en la información de sus producto.

En resumen las empresas que hay en el mercado brindan una serie de herramientas que pueden manejar el riesgo operacional y lo que hacen es adecuar las políticas de las organizaciones al uso de la herramienta, no tienen embebidas la normativa peruana dentro del core del software, lo que hacen es adecuar el software a la normativa peruana con ciertos problemas que pasan a ser problemas de la organización.

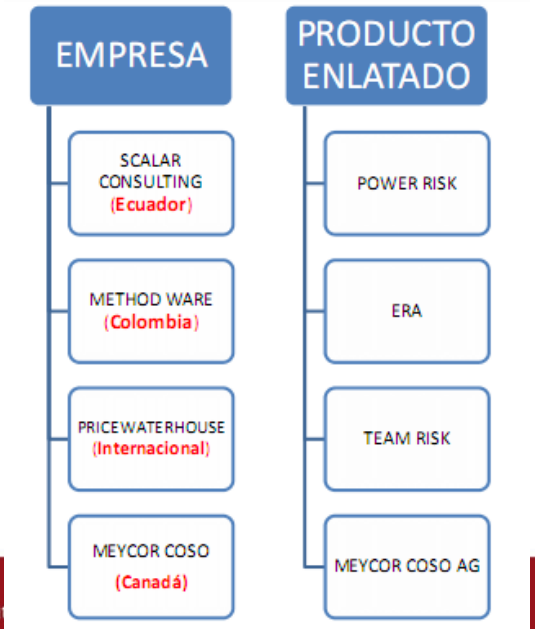


Figura 3 : Principales Software Existentes en el Mercado Nacional

3. CAPITULO 3 - IDENTIFICACIÓN DE REQUERIMIENTOS

A continuación, se describen los requerimientos funcionales y no funcionales del sistema que se desarrollara, los cuales fueron identificados luego de realizar entrevistas con distintas personas ligadas a las áreas de riesgo operacional (en unas 10 reuniones de trabajo) de entidades financieras, además de contar con la ayuda contante de un especialista en riesgo operacional que es quien brinda el conocimiento y experiencia volcada en el presente software, siendo además algunos requerimientos identificados por la naturaleza del propio sistema.

3.1 Obtención de requerimientos

En esta sección se detallaran los tanto los requisitos funcionales y no funcionales del sistema de Riesgo Operacional, en el **anexo** Catalogo de Requisitos se muestran con más detalle estos requerimientos.

3.2 Requerimientos funcionales

Los Requisitos Funcionales se han agrupado dela siguiente manera:

- Parámetros.
- Módulo Riesgos/Controles (COSO – ERM).
- Modulo de Eventos de Pérdida.
- Indicadores.
- Ayuda.
- Seguridad.
- Reportes.
- Reportes Estadísticos.

3.3 Requerimientos no funcionales

Algunos de los requisitos no funcionales que se han tomado en cuenta para el presente proyecto son:

- Se utilizara la Metodología RUP para el Desarrollo de Software
- El sistema permitirá alternar entre el teclado y el Mouse.
- El sistema correrá en plataformas Windows 2000/Windows XP y superiores.
- El sistema deberá contribuir en el ahorro de tiempo en los registros y búsquedas.
- El sistema deberá ser portable, tanto la aplicación como la base de datos para su uso conveniente.
- Se utilizará como gestor de base de datos PostgreSQL, con licencia libre
- Para el manejo de la seguridad, el sistema contará con niveles y roles de usuario para el manejo al sistema.
- El sistema deberá ser portable, tanto la aplicación como la base de datos para su uso conveniente.

Además de la descripción de los requerimientos tanto funcionales como no funcionales se ha realizado una evaluación según la prioridad y la exigencia de acuerdo a la necesidad tal y como se muestra a continuación.

Prioridad
B: baja
M: media
A: alta

Exigencia
E: exigible
D: deseable

Para mas detalle de los Requerimientos ver el Anexo Catalogo de requisitos y el anexo de Especificación de Requisitos de Software ERS v2.

3.4 Análisis de la solución

3.4.1 Viabilidad del sistema

Para Definir la viabilidad del proyecto de tesis, se ha decido tomar en cuenta 2 criterios que son:

- Viabilidad Económica:

  En cuanto a la viabilidad económica se ha tomado en cuenta para la realización del presente proyecto de tesis los costos de las herramientas de desarrollo (Software Libre) y el personal que se contara para el desarrollo (Especialistas en Riesgo Operacional, Analistas Funcionales,

Desarrolladores, Líder del Proyecto entre otros) y el tesista que es el responsable de toda su elaboración con el apoyo de un asesor, el cual es brindado por la Pontificia Universidad Católica del Perú.

- Viabilidad Técnica:

  Con Referencia a los requerimientos técnicos para la elaboración del proyecto de tesis, se cuenta con las herramientas necesarias para su desarrollo, como son: IDE Netbeans 6.8, motor de Base de Datos PostgreSQL 8.4 y 03 computadoras, 01 servidor desarrollo, 02 lap top y como generador de reportes IReports for Jasper Report 3.7.2, para el encriptamiento de la información en la base de datos se utiliza el Sistema de Algoritmo de Encriptamiento Matemático AES 128 bits, para la realización del diseño grafico se utilizara el EXTJs, para la visualización de gráficos y formularios se utiliza la librería SexyLightbox 2.3, Como servidor web se utilizará el Apache Tomcat 5.5.28. Con respecto a los posibles problemas que surjan por el uso de estas herramientas, estas son de usos generales y muy difundidos, por los que se cuenta con amplia información para solucionar cualquier inconveniente que ocurra durante el desarrollo del proyecto de tesis.

3.4.2 Análisis técnico y económico

- Análisis Económico: Los costos Considerados para el desarrollo del presente proyecto de tesis son los siguientes:

Nombre del Recurso	Costo xMes	Cantidad (Mes)	Total
Consultor (Asesor)	S/. 1,500.00	12	S/. 18,000.00
Analista Programador	S/. 5,000.00	12	S/. 60,000.00
Profesional Riesgo operacional	S/. 1,500.00	12	S/. 18,000.00
Líder Proyecto (Tesista)	S/. 1,500.00	12	S/. 18,000.00
Luz, internet	S/. 500.00	12	S/. 6,000.00
Alquiler de equipos	S/. 350.00	12	S/. 4,200.00
Alquiler de hosting	S/. 50.00	12	S/. 600.00
Total			S/. 124,800.00

Tabla 6: Costo del Proyecto de Tesis

De la Tabla Anterior se puede observar que el costo para la realización del presente proyecto es de alto, gran parte de estos costos han sido asumidos por el tesista y un socio que es el profesional de riesgo operacional; Adicionalmente se ha realizado una valorización de del trabajo realizado por lo que no se ha realizado el desembolso total del dinero para este proyecto, el desarrollo en la totalidad se ha realizado en la ciudad de Piura, para el proceso de implantación y puesta en marcha del proyecto se detallara en la sección correspondiente a implantación.

- Análisis Técnico: La instalación del componente servidor se realizara en un Servidor virtual alquilado en internet y el componente por el lado del cliente no será necesario la adquisición de licencias pues el cliente solo accederá al servidor con un navegador web de preferencia Mozilla Firefox 5.0 como mínimo.

Para definir la calidad del software se analizara las siguientes características:

1. Disponibilidad:
   El sistema estará disponible cada vez que un usuario lo requiera en el lugar que lo requiera (Internet).

2. Robustez:
   El sistema tendrá capacidad para funcionar correctamente utilizando poco ancho de banda para enviar y/o recibir información, debe funcionar de manera correcta en caso se realicen entradas de información erróneas, debe funcionar correctamente ante múltiples accesos de usuarios validado en el sistema.

3. Utilidad:
   El sistema será fácil de utilizar y tendrá un entorno de trabajo amigable con referencias para los usuarios de riesgo operacional, además será apropiado para cualquier usuario que tenga autorización de hacer uso de él.

4. Capacidad de Configuración:

El sistema será capaz de ser configurable, parametrizado según la normativa de la SBS de acuerdo a la complejidad y estructura de las operaciones de las entidades financieras lo cual permitirá extender su plazo de vida útil antes de su próximo mantenimiento.

5. Capacidad de Mantenimiento:
   El diseño de este sistema permitirá dar mantenimiento sin complicaciones, respetando el diseño de la interfaz lo más que se pueda.

6. Seguridad:
   El sistema mantendrá segura la información, realizando algunos ingresos de datos a las bases de datos de manera encriptado además el sistema trabaja en base a perfiles y roles de usuario permitiendo solo el acceso a usuarios autorizados, lo cual evitará de manera eficiente cualquier infiltración por parte de personas ajenas al sistema, Además se tiene seguridad web basado en sesiones de acceso al sistema lo cual no permite acceder al sistema sin antes haberse identificado en el sistema.

3.4.3 Restricciones de costo y tiempo

El desarrollo del proyecto de tesis está sujeto a las siguientes restricciones:

- El costo máximo deseable es que no se exceda en más 3 veces de lo que tiene en la Tabla 6 costos de proyecto de Tesis.
- Se deberá seguir los tiempos de cada fase del proyecto definida en el diagrama de Gantt (ver anexo Diagrama de Gantt).
- El desarrollo del proyecto no debe de exceder a los 02 ciclos académicos de la PUCP (1 año).

3.4.4 Definición del sistema

El Sistema de Información deberá cumplir con la normativa peruana en cuanto la gestión de los riesgos operacionales, debe ser fácil de usar de usar principalmente para personal que no integra la Unidad de Riesgos, estará basada en el uso de herramientas del tipo Open Source, de manera que no agregue más costo sobre el costo total de propiedad (TCO) y principalmente es adaptable ante cambios normativos, se puede indicar que El sistema, soportara la metodología Australiana Neocelandesa 4360, y el estándar COSO/ERM. Deberá contar con el detalle funcional que se indican en las normativas peruanas, permitiendo integrar la gestión del riesgo

operacional, gestión de controles y la gestión de los eventos de pérdida, con usuarios ilimitados, además permitirá gestionar los riesgos operacionales utilizando las mejores prácticas del mercado, tales como COSO/ERM y AS/NZS 4360:2004. Deberá ser una herramienta creada en un entorno Web logrando que la gestión de riesgos sea una experiencia sencilla, agradable y productiva.

4. CAPITULO 4 - DISEÑO

En esta sección se describirá los casos de uso y las especificaciones de requerimientos del software del sistema de riesgo operacional para entidades financieras de manera general pudiendo encontrar información más detallada en el Anexo ERS .

4.1 Arquitectura de la solución

4.1.1 Especificación de Requisitos de Software (ERS)

En esta sección se presentara a los actores que participan el sistema de Riesgo Operacional.

Figura 10: Catalogo de Actores

Casos de Uso por Paquete

En esta sección se Describirá los paquetes que se tendrán en el sistema de riesgo operacional.

Paquete General

El paquete General contiene los casos de uso que corresponden a la administración de los parámetros que se utilizan para la gestión de los riesgos, la administración del sistema, administración de los riesgos, el registro de los controles que actúan como mitigadores de los riesgos, el registro de los eventos de pérdida, el registro de los indicadores por riesgo identificado, la gestión de seguridad y gestión de alertas.

Los casos de uso incluidos en este paquete son:

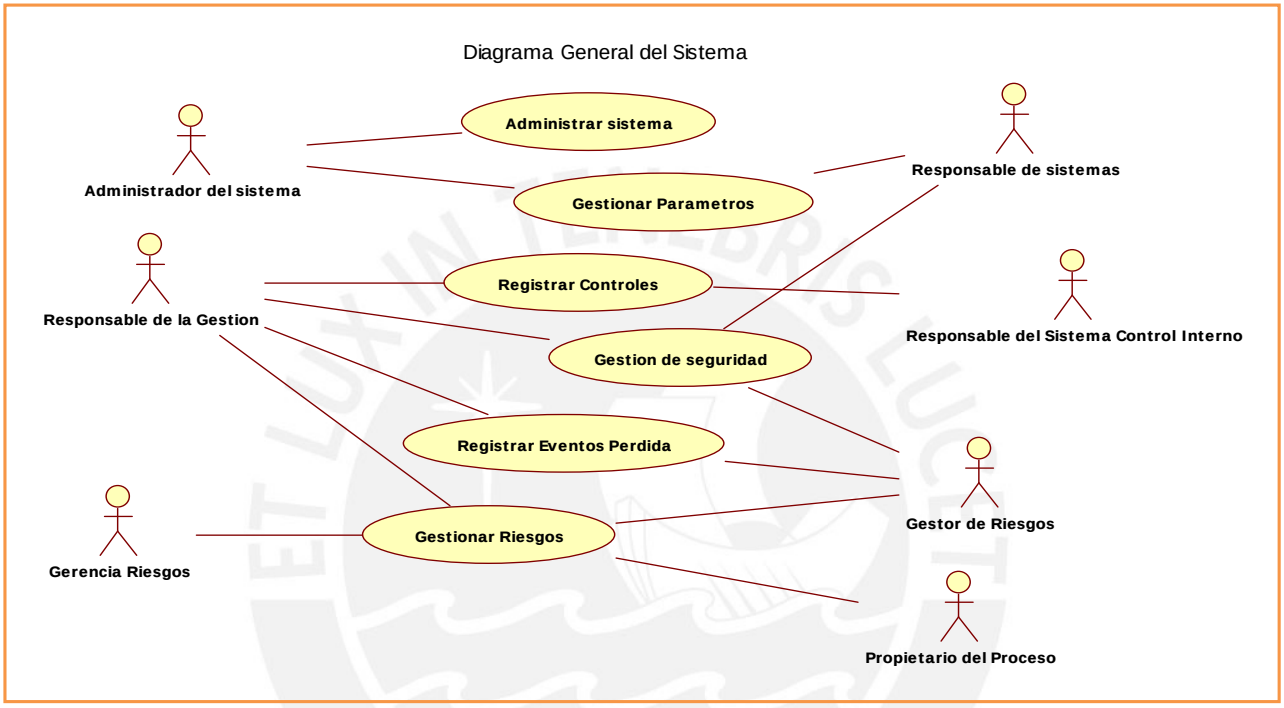


Figura 11: Casos de Uso Paquete General

Paquete Administrar Seguridad

El paquete de Gestión de Riesgos contiene los casos de uso que corresponden al registro de riesgos a través de las matrices previamente definidas y que estas son realizadas por los respectivos actores (Gestor de riesgos, Propietario del proceso, Responsable de la Gestión y Gerencia de Riesgos).

Los casos de uso incluidos en este paquete son:

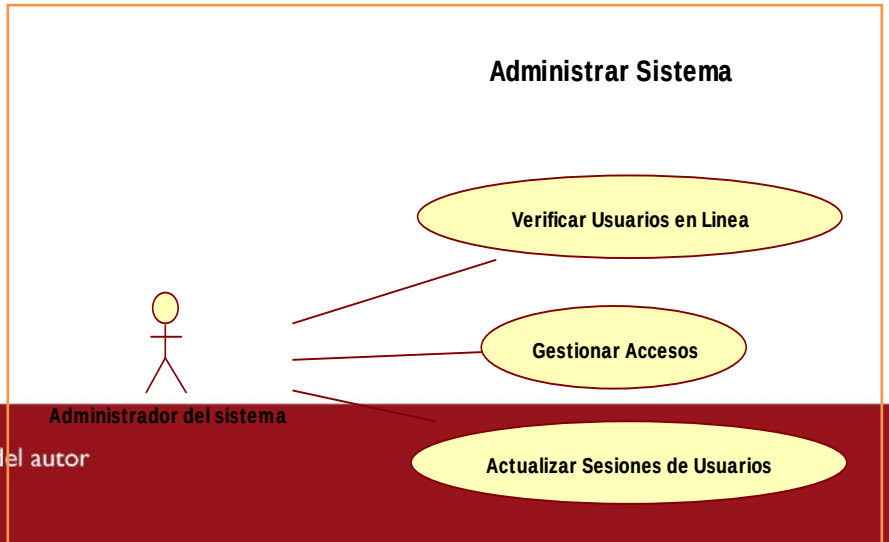


Figura 12: Diagrama de Casos de Uso del Administrar Seguridad

Paquete Gestión de Riesgos

El paquete de Gestión de Riesgos contiene los casos de uso que corresponden al registro de riesgos a través de las matrices previamente definidas y que estas son realizadas por los respectivos actores (Gestor de riesgos, Propietario del proceso, Responsable de la Gestión y Gerencia de Riesgos).

Los casos de uso incluidos en este paquete son:

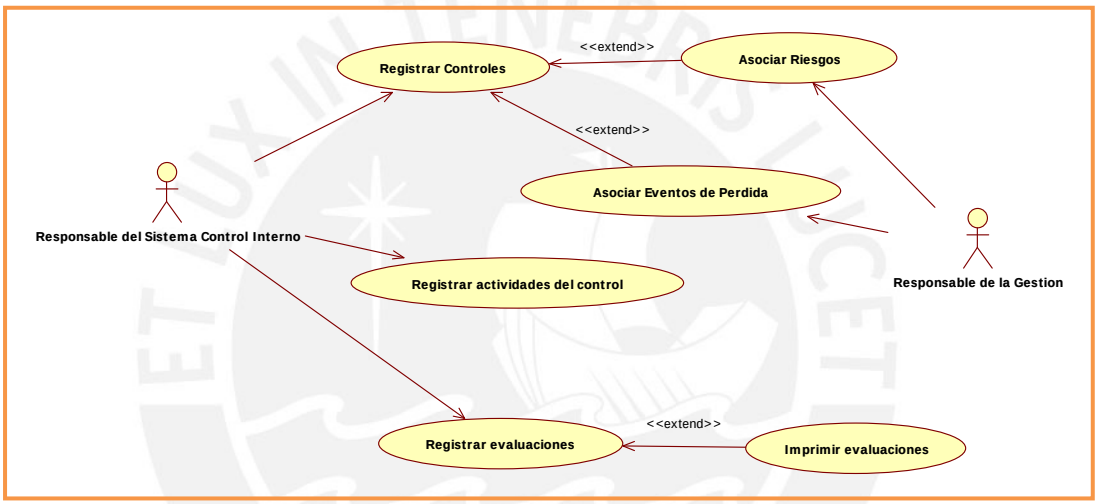


Figura 13: Diagrama de Casos de Uso del Paquete Gestión de Riesgos

Paquete Registro de Controles

El paquete Registro de controles contiene los casos de uso que corresponden al registro de los controles que actúan como mitigadores de los riesgos, y estos son realizados por el actor (Responsable del sistema de control interno, Gestor de riesgos).

Los casos de uso incluidos en este paquete son:

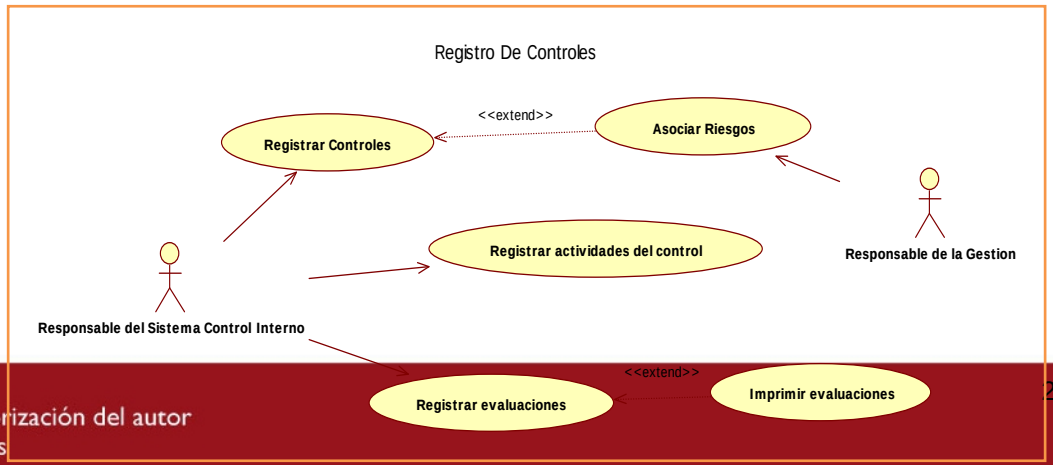


Figura 14: Diagrama de Casos de Uso del Paquete Registro de Controles

Paquete Registro de Eventos de Pérdida

El paquete Registro de Eventos de Pérdida contiene los casos de uso que corresponden al registro de los eventos de pérdida, siendo realizado por el actor (Responsable de la gestión, Gestor de riesgos).

Los casos de uso incluidos en este paquete son:

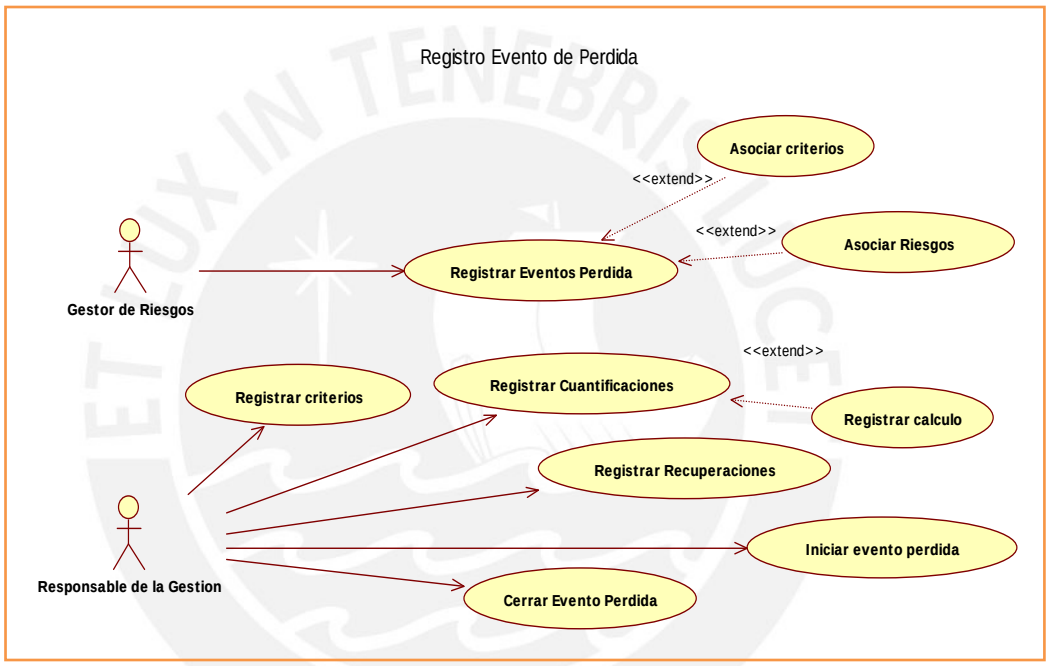


Figura 15: Diagrama de Casos de Uso del Paquete Registro de Eventos de Pérdida

Paquete Gestión de Seguridad

El paquete Gestión de Seguridad contiene los casos de uso que corresponden a la administración de usuarios y perfiles de usuarios para la integridad del sistema.

Los casos de uso incluidos en este paquete son:

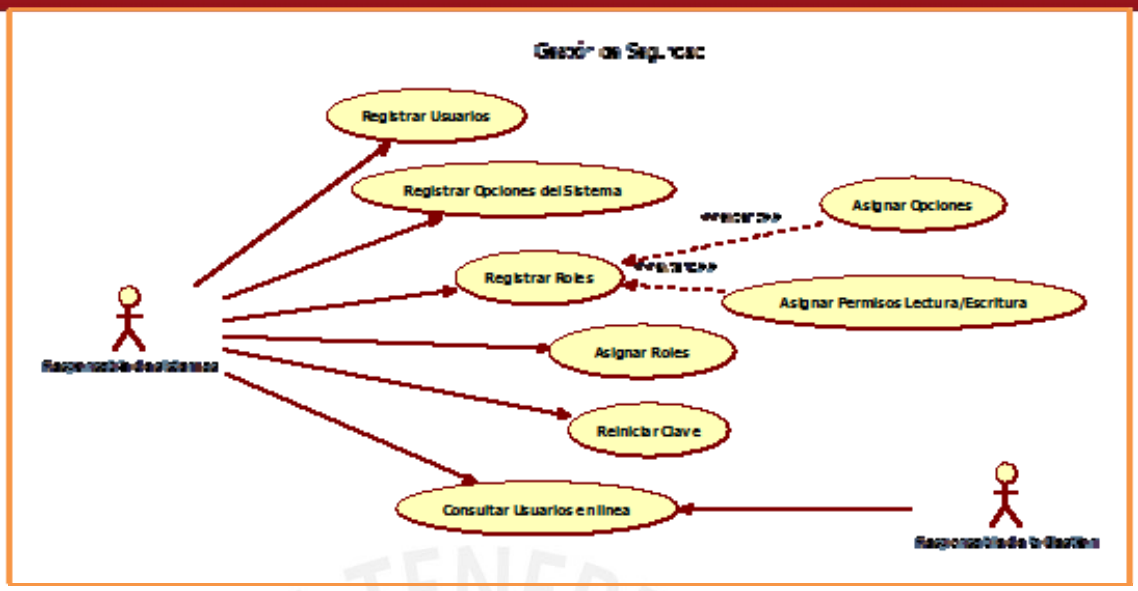


Figura 15: Diagrama de Casos de Uso del Paquete Gestión de Seguridad

4.2 Arquitectura del Software

En los siguientes puntos se detallará la arquitectura del software a desarrollar.

Arquitectura 3 Capas

En general, para el presente proyecto se planteara una arquitectura en 3 capas o niveles:

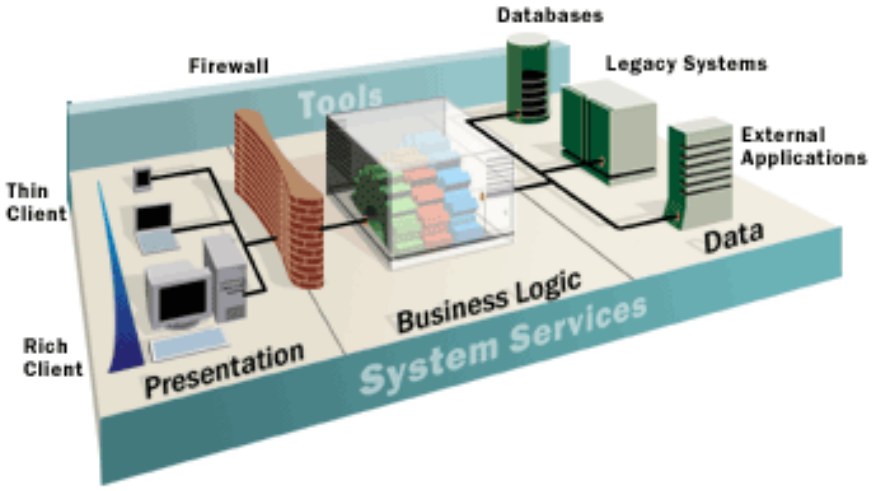


Figura 16: Arquitectura 3 Capas

4.3 La Arquitectura Model View Controler (MVC)

La arquitectura Model-View-Controller surgió como patrón arquitectónico para el desarrollo de interfaces gráficas de usuario en entornos Smalltalk. Su concepto se basaba en separar el modelo de datos de la aplicación de su representación de cara al usuario y de la interacción de éste con la aplicación, mediante la división de la aplicación en tres partes fundamentales:

- El modelo, que contiene la lógica de negocio de la aplicación
- La vista, que muestra al usuario la información que éste necesita.
- El controlador, que recibe e interpreta la interacción del usuario, actuando sobre modelo y vista de manera adecuada para provocar cambios de estado en la representación interna de los datos, así como en su visualización.

Esta arquitectura ha demostrado ser muy apropiada para las aplicaciones web y especialmente adaptarse bien a las tecnologías proporcionadas por la plataforma J2EE.

4.4 Especificación de Herramientas a Usar

4.4.1 Lenguaje de programación Java

Sun Microsystems es la empresa que ha inventado el lenguaje Java, en un intento de resolver simultáneamente todos los problemas que se planteaban a los desarrolladores de software por la proliferación de arquitecturas incompatibles en los siguientes aspectos:

- Diferentes máquinas desde el punto de vista del hardware.
- Diferentes sistemas operativos.
- Diferentes sistemas de ventanas que funcionan sobre una misma máquina.

Estos problemas se han agravado aún más con la expansión de Internet en la cual debe comunicarse plataformas heterogéneas, y dónde las aplicaciones distribuidas son el corazón del sistema.

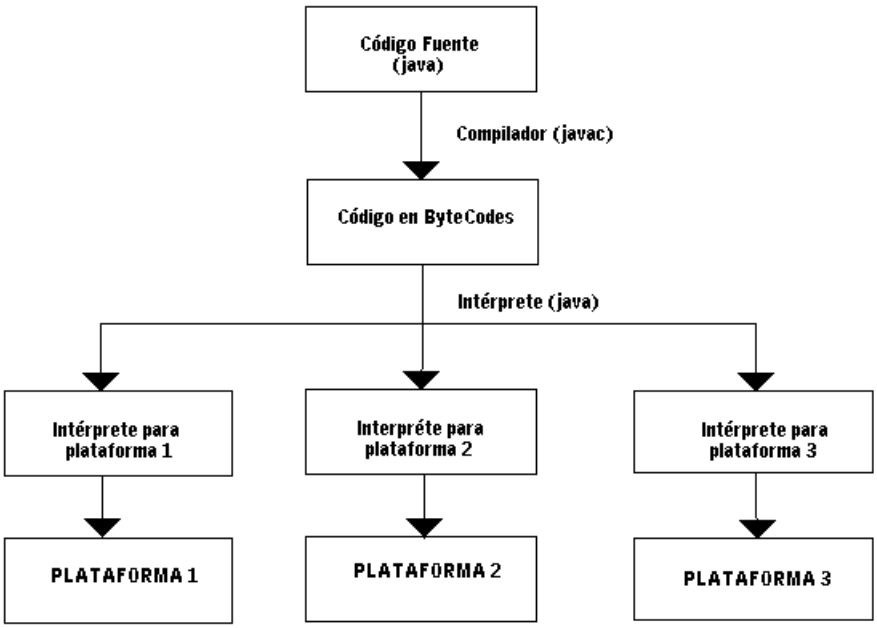


Figura 17: Arquitectura Java

- Los programas se compilan a un fichero (*.class) intermedio, en un lenguaje creado por Sun (bytecodes). Este fichero luego es interpretado por una máquina virtual java (JVM). Por tanto, java es compilable-interpretable.

4.4.2 NebBeans 6.8:

NetBeans IDE es un entorno de desarrollo integrado (IDE) modular y basado en estándares, escrito con el lenguaje de programación Java. El proyecto de NetBeans consta de un IDE de código abierto con gran variedad de funciones escrito con el lenguaje de programación Java y una plataforma para aplicaciones de cliente enriquecidas que se puede utilizar como marco genérico para crear cualquier tipo de aplicación.

NetBeans IDE es un reconocido entorno de desarrollo integrado disponible para Windows, Mac, Linux y Solaris. El proyecto de NetBeans está formado por un IDE de código abierto y una plataforma de aplicación que permite a los desarrolladores crear con rapidez aplicaciones web, empresariales, de escritorio y móviles utilizando la plataforma Java, así como JavaFX, PHP, JavaScript y Ajax, Ruby y Ruby on Rails, Groovy and Grails y C/C++.

4.4.3 Postgres Sql

El sistema de gestión de base de datos PostgreSQL nace en la universidad de Berkeley - California, en los años 80, como un proyecto académico y actualmente se encuentra en la versión 8.1, siendo permanentemente mantenido por la comunidad Open Source. La coordinación del desarrollo del PostgreSQL es realizada por el Global Development Group, que está formada por un amplio grupo de desarrolladores alrededor del mundo, que permite al PostgreSQL evolucionar constantemente en cuanto a la corrección de errores y la implementación de nuevas funcionalidades.

4.4.4 Apache Tomcat:

Tomcat (también llamado Jakarta Tomcat o Apache Tomcat) funciona como un contenedor de servlets desarrollado bajo el proyecto Jakarta en la Apache Software Foundation. Tomcat implementa las especificaciones de los servlets y de JavaServer Pages (JSP) de Sun Microsystems.

4.4.5 Ireport

iReport es un diseñador visual de código libre para JasperReports escrito en Java. Es un programa que ayuda a los usuarios y desarrolladores que usan la librería JasperReports para diseñar reportes visualmente. A través de una interfaz rica y simple de usar, iReport provee las funciones más importantes para crear reportes amenos en poco tiempo

iReport puede ayudar a la gente que no conoce la sintaxis XML para generar reportes de JasperReports.
Funcionamiento de iReport
iReport provee a los usuarios de JasperReports una interfaz visual para construir reportes, generar archivos “jasper” y “print” de prueba. iReport nació como una herramienta de desarrollo, pero puede utilizarse como una herramienta de oficina para adquirir datos almacenados en una base de datos, sin pasar a través de alguna otra aplicación

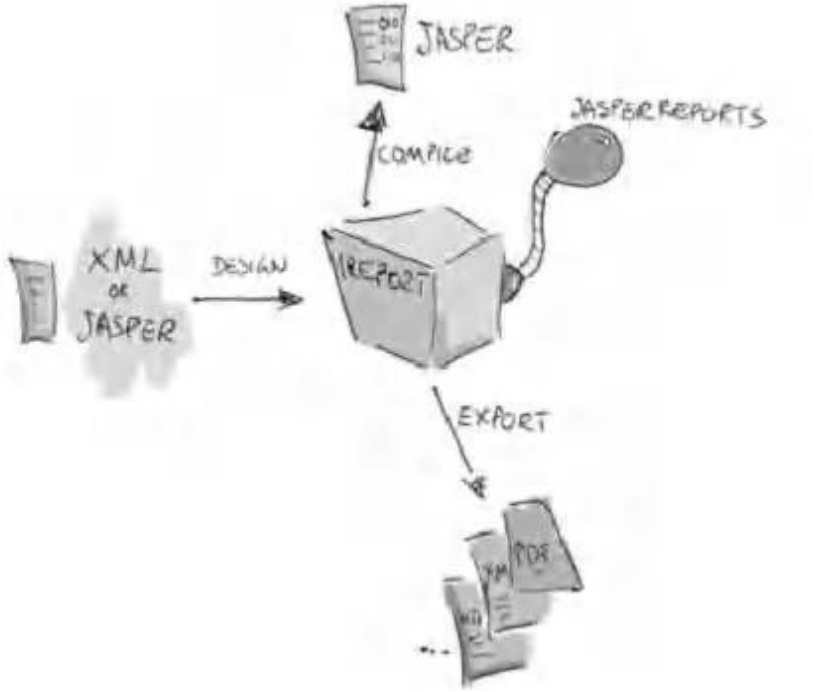


Figura 18: Gestión de Reportes con Ireport

4.5 Diagramas de Secuencia

En esta sección se mostrara uno de los diagramas que se pueden encontrar con mayor detalle en el Documento Reporte de Diseño de Software. (_RDS_Tesis Siro)

4.5.1 Diagrama de Secuencia Registrar Riesgos

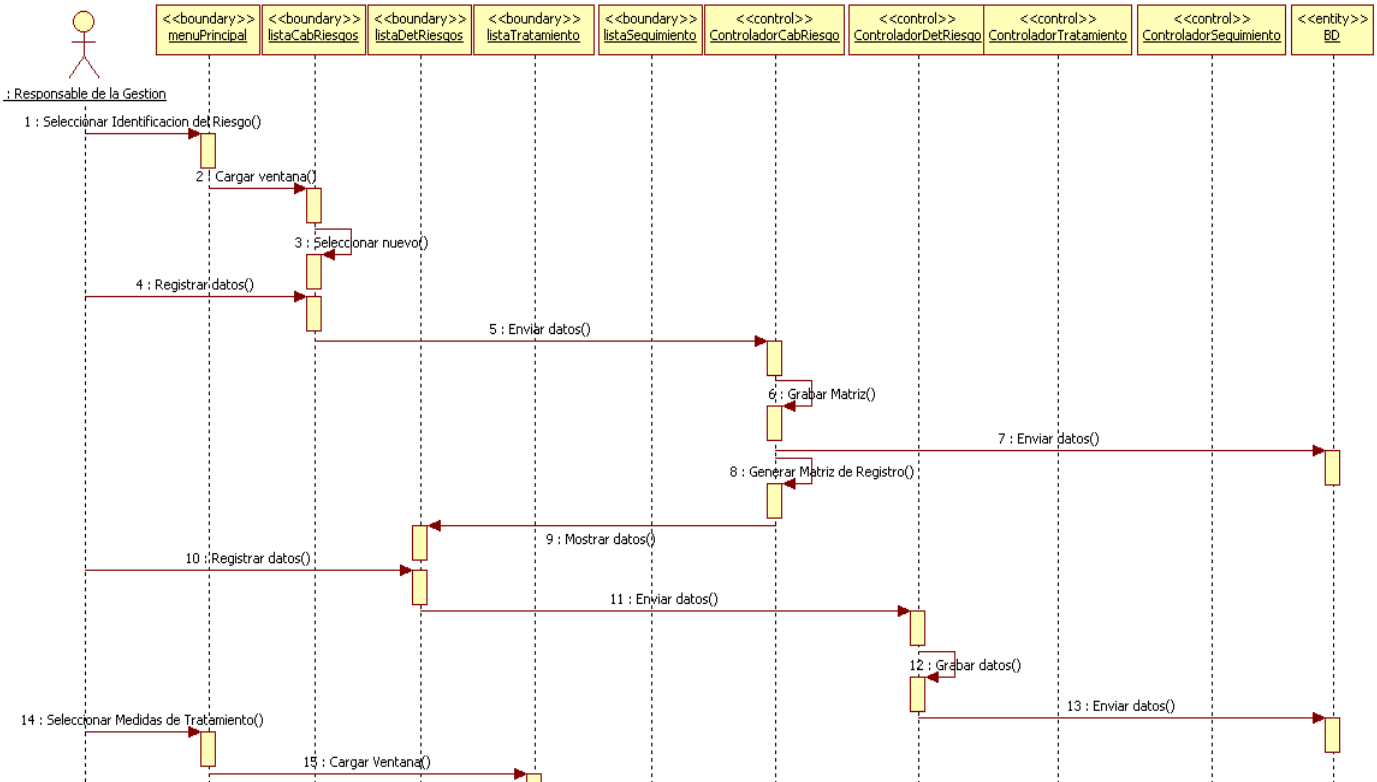


Figura 19: Diagrama de Secuencia Registrar Riesgo

4.6 Diagrama de Componentes

El Presente Diagrama de componentes muestra los distintos componentes que se utilizan desde las distintas capas implementadas en el proyecto de desarrollo de Software

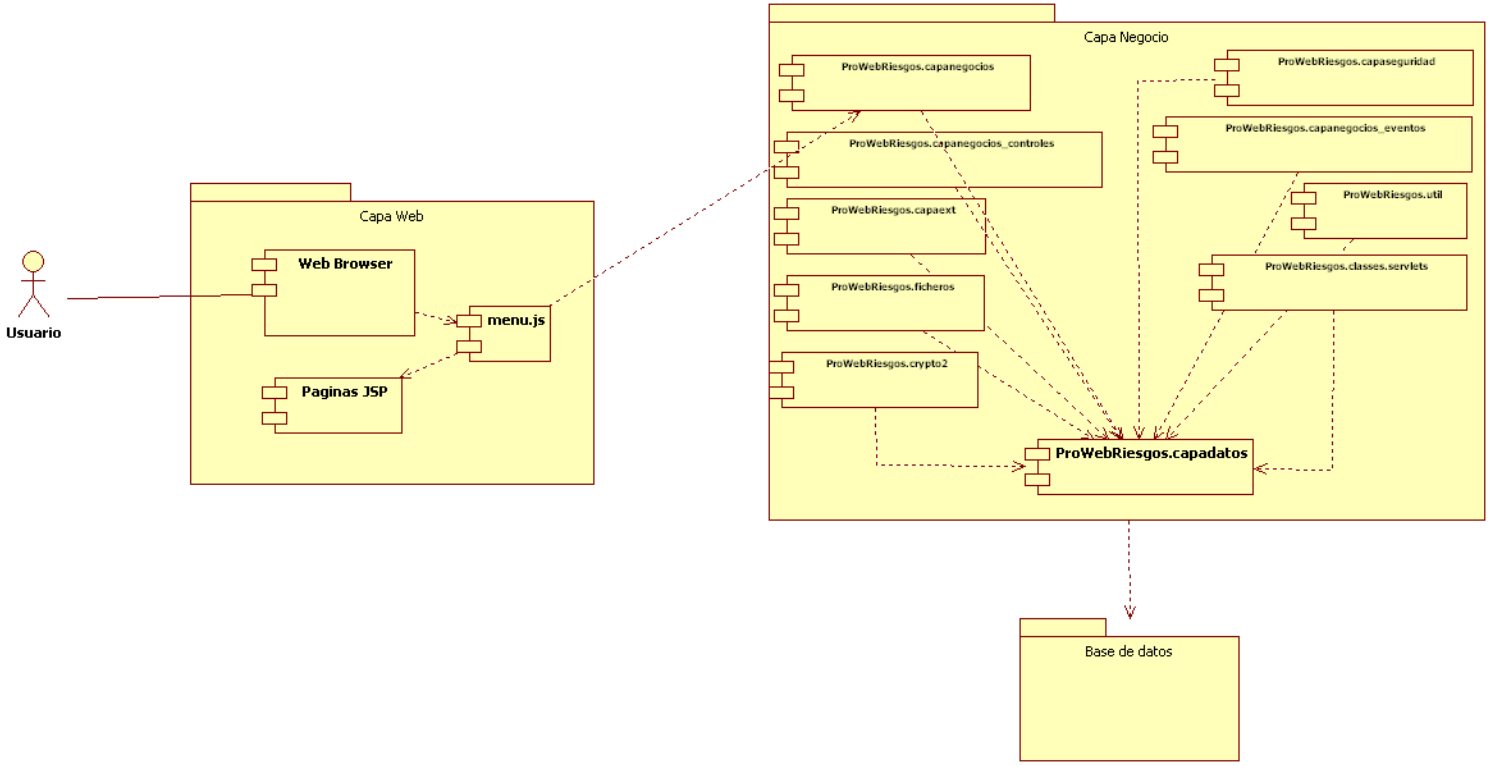


Figura 25: Diagrama de Componentes

4.7 Diagrama de Despliegue

Este diagrama muestra la infraestructura en donde se realizara la implantación del Software que se ha desarrollado

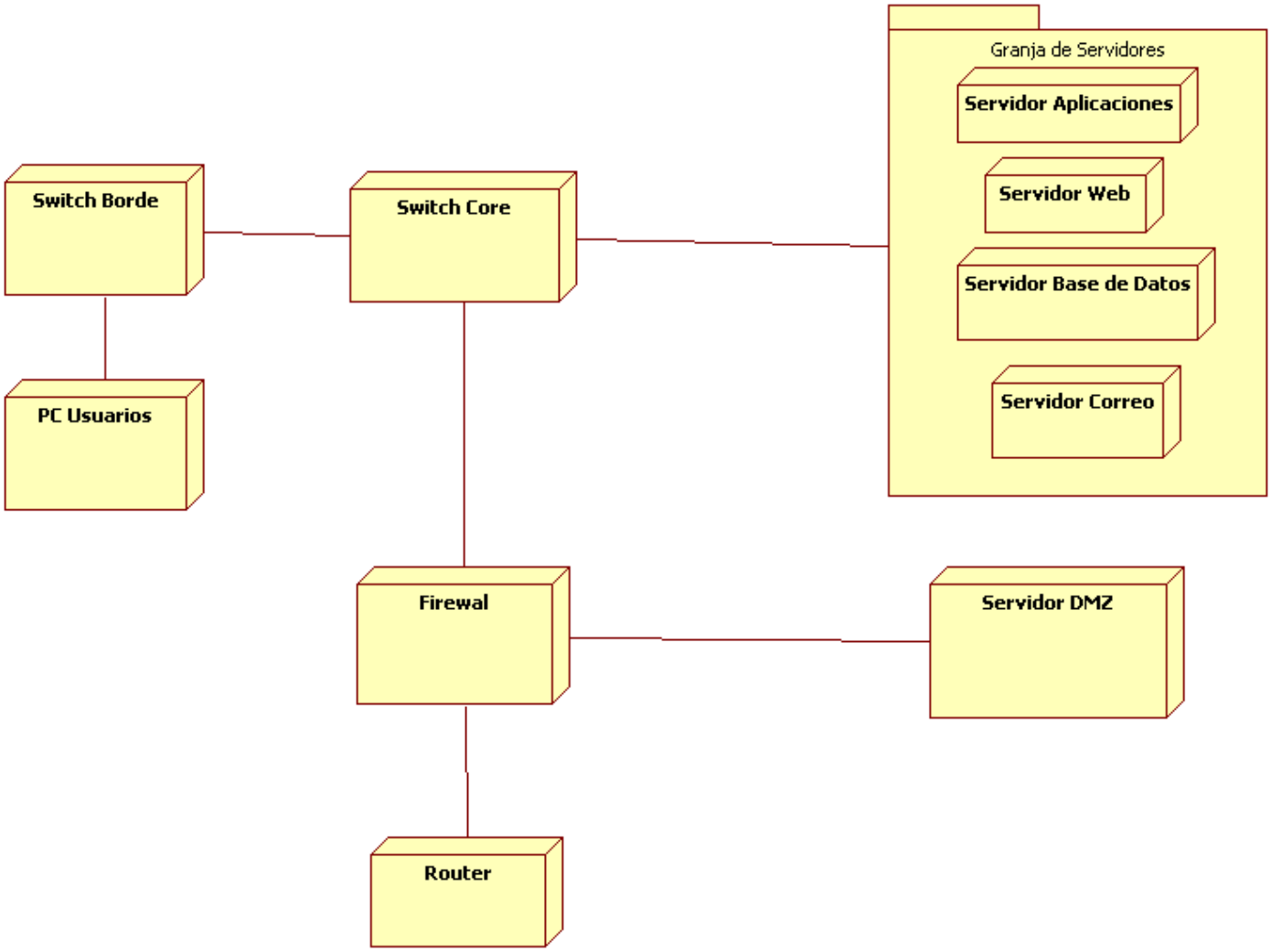


Figura 26: Diagrama de Despliegue

4.8 Diseño de interfaz gráfica

En esta sección mostraremos algunas pantallas principales del sistema de riesgo operacional pueden ver más detalle en el Anexo _Pantallas.

4.8.1 Ventanas del sistema

En la Figura 28 se muestra la interfaz de ingreso al sistema integral del riesgo operacional

Figura 28: Formulario de Acceso de la Institución para el Acceso al Sistema

En la Figura 29 se muestra el menú de los módulos de parámetros

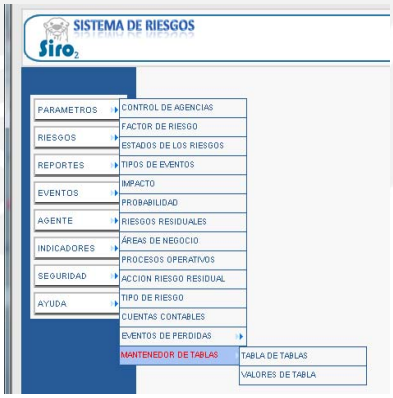


Figura 29: Menú del módulo de Parámetros

Para Mayor detalle de la Parte de Diseño revisar el **Anexo** _RDS_Tesis_Siro donde también se podrá ver el modelo lógico y el modelo físico de la base de datos

5. CAPITULO 5 – IMPLEMENTACIÓN Y DESPLIEGUE

5.1 Estándares de Programación

A continuación se presenta un resumen de estos estándares mediante una plantilla base de los 2 módulos básicos de programación, un clase Java, y un página JSP, estas plantillas servirán a la sección de Control de Calidad para verificar que la claridad de los programas y que se ciñen al estándar Java.

Los ejemplos muestran en las plantillas la forma de comentar el código fuente, para que se pueda obtener el JavaDoc correspondiente (documentación automática de Java). Esta Información la encontrara con mayor detalle en el anexo Estándares de Programación.

5.2 Plantilla De Codificación Java.

Esta plantilla Java se puede extender a otras clases como Servlets.
Para una clase Java tiene el siguiente orden:

Comentarios de Inicio
Definición Package
Declaraciones de Import
Declaraciones de la Clase
Comentario Documentación de la Clase
Estamento class
Atributos o Variables Estáticas
    public
    protected
    private
Atributos
    public
    protected

private

Constructores

Métodos

La siguiente plantilla resume los principales estándares de codificación propuestos por Sun y tomados para el proyecto

.

```
/*
* @(#)Plantilla.java version 1.01 2007/01/01
* Copyright (c) 2007 SOA Sistema de Riesgos.
*/
package com.soariesgos.ejemplos;
import com.soariesgos.librerias.*; //import de librerías y clases a utilizar
/**
* Descripción de la Clase, ejemplo: Plantilla que muestra los
* principales estándares de codificación.
*
* @versión 1.01 01 Ene 2007
* @author SOA Team
*/
public class Plantilla extends ClasePadre {
/* Comentario de implementación, ejemplo: Esta clase no tiene funcionalidades.
*/
/** atributo1 comentario documentación atributo
* puede ser de mas de una línea
*/
public static int atributo1; //comentario línea: primero las variables estáticas,
    //en orden 1.-public, 2.-protected, 3.-private
/** atributo2 comentario documentación */
public Integer atributo2; //luego var de instancia, mismo orden 1.-public, 2.-protected, 3.-private
/** atributo3 comentario documentación */
protected Integer atributo3;
/**
* Descripción para el constructor.
*/
```

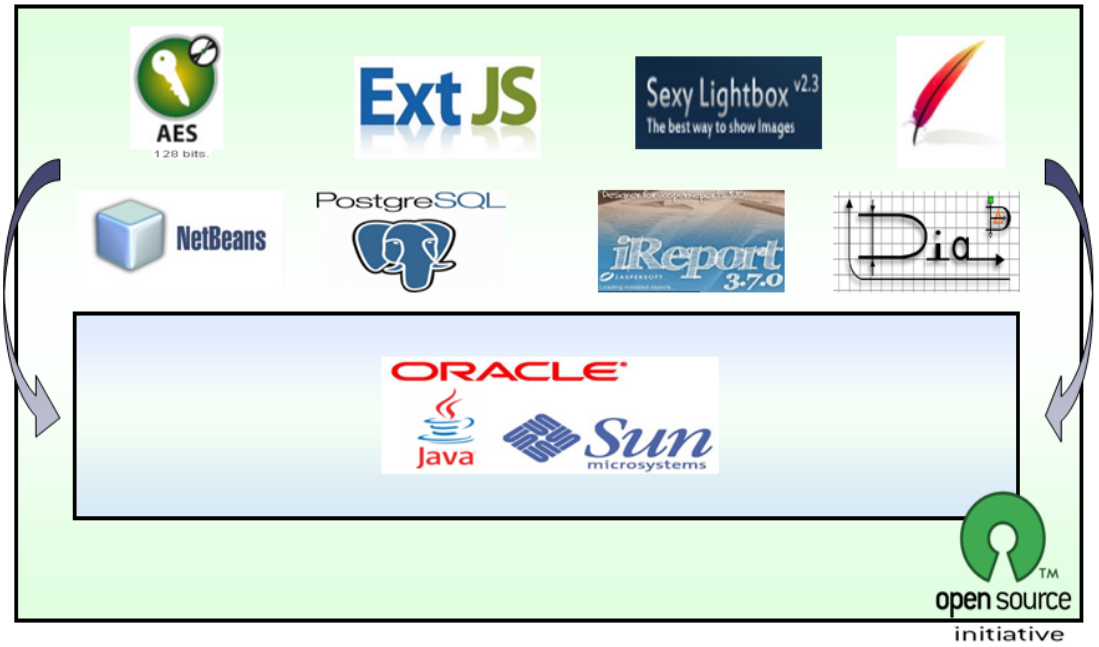
```
public Plantilla() {
// … implementación …
}
```

5.3 Despliegue.

El proceso de implantación se desarrolla siguiendo 2 procesos principales:

5.3.1 Instalación del Software en la Entidad

5.3.2 Nuestra Plataforma



5.4 COMPONENTES

Los componentes que se utilizaran para la instalación del software en alguna entidad financiera son:

Nº	Descripción	Versión	Link de descarga	Lado
1	Java Runtime Environment JRE	JAVA 6 actualización 22	http://www.oracle.com/technetwork/java/javase/downloads/index.html#need https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_Developer-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=jre-6u22-oth-JPR@CDS-CDS_Developer	Servidor
2	Adobe Flash Player 10 Activex	10.1.82.76	http://get.adobe.com/es/flashplayer/ http://www.adobe.com/support/flashplayer/downloads.html	Cliente
3	Apache Tomcat	5.5.28	http://tomcat.apache.org/download-55.cgi http://rapidshare.com/files/360833847/apache-tomcat-5.5.28.exe	Servidor

4	PostgreSQL	8.4	http://www.postgresql.org/download/	Servidor

5.5 Puesta en Marcha del Software

Para la Puesta en marcha del Software se necesitara realizar los siguientes procesos que deben realizarse para poder ingresar la información al Software de Gestión Integral de Riesgo Operacional.

5.5.1 Identificación de Procesos

En este punto se realizara una identificación de procesos para poder identificar los riesgos por procesos de acuerdo a las mejores practicas de gestión de riesgos.

5.5.2 Mapeo de Procesos

El mapeo de los procesos se realiza considerando la identificación de aquellos procesos que ocurren en tres grandes rubros: los procesos Estratégicos, los de Negocios y los procesos de Soporte.

Esta actividad se realiza la revisión de la documentación normativa de La Entidad a fin de esbozar los procesos que se realizan, los cuales deben ser validados posteriormente por los dueños del proceso y complementados con la identificación de las actividades que se realizan en cada proceso.

5.5.3 Identificación del alcance de los Procesos

Se debe Realizar el planteamiento de la gestión por procesos, la identificación de los mismos considera que debe existir una clasificación y la definición del alcance de cada uno de ellos para que sea un referente al momento de la identificación de los riesgos operacionales.

5.5.4 Inducción al Personal

Realizar jornadas de capacitación al personal, en los siguientes puntos:

a) Inducción para adoptar la gestión por procesos.

b) Jornada de capacitación en aplicación de la metodología de Riesgos Operacionales.

Cabe indicar que la realización de dichas jornadas permitirá difundir la metodología de la gestión del riesgo operacional a los diferentes niveles de la institución, permitiendo fortalecer la cultura de la gestión del riesgo y principalmente para el reporte de eventos que se suscitan en el día a día como parte del desarrollo de las operaciones que realiza La Entidad.

5.5.5 Identificación de Riesgos

La identificación de los riesgos operacionales se debe realizar tomando en consideración la metodología establecida en el Manual de Control del Riesgo Operacional de La Entidad. La aplicación de dicha metodología se complementa con la que incorpora SIRO, la cual recoge las mejores prácticas y demanda recoger más información para poder procesar y emitir sus reportes.

El personal que participará en los talleres de autoevaluación serán aquellos colaboradores que sean los más experimentados y conocedores del negocio, a fin de que la información que sea recogida adopte la característica de criterio experto"

La evaluación de la *Probabilidad* e *Impacto* que realizan los responsables y/o expertos de los procesos, son enteramente cualitativa, es decir que se evalúa sobre la base de la experiencia y de los eventos que han ocurrido en La Entidad.

5.5.6 Identificación de Controles

La identificación de los controles frente a los riesgo identificados, se realiza a través del análisis de la documentación y/o normativa con que cuenta La Entidad, tales como Políticas, Reglamentos, Manuales, Procedimientos.

Es importante indicar que el proceso de levantamiento de controles es un proceso cíclico y al y este proceso no puede darse por concluido o finalizado, y por el contrario, debe continuarse y fortalecerse de la mano con la interacción del Órgano de Control Interno y el Sistema de Control Interno,

del cual forma parte todo el personal de La Entidad, a fin de dar cumplimiento a lo indicado en la Resolución SBS Nº 037-2008 del 10/01/2008.

5.5.7 Identificación de las Medidas de Tratamiento

La identificación de las medidas de tratamiento debe realizar en parte durante la identificación de los riesgos operacionales, en los talleres de autoevaluación y las entrevistas realizadas a los funcionarios de la Entidad.

Cabe indicar que esta identificación de las medidas de tratamiento son propuestas y deberán ser analizadas y discutidas con los dueños de los procesos, a efecto de determinar quienes serán los responsables de su implementación, asimismo se deberá establecer los plazos en el cual serán implementadas dichas medidas de tratamiento, con la finalidad de que se pueda realizar un adecuado monitoreo de las mismas.

5.5.8 Designación de los Gestores de Riesgo Operacional

Se deberá designar gestores de Riesgo Operacional, asimismo, es importante indicar que para los colaboradores que recién se inician como gestores del riesgo operacional, podría resultar un tanto complicado entender ¿el porqué? Del rol que deberán cumplir, por lo que se debe entender que las capacitaciones deben ser en forma continua. Esto permitirá que el personal gradualmente entienda y se comprometa para con la gestión del riesgo operacional.

Otro ámbito sobre el cual tendrá incidencia el trabajo de los gestores del riesgo operacional será precisamente en el área donde labora, por lo que las Gerencias de líneas, deberán comunicar oficialmente a todo el personal del establecimiento y asignación del rol de un Gestor de Riesgo Operacional.

6. CAPITULO 6 - PRUEBAS

6.1 Estrategia de pruebas

En esta sección se hace referencia a las pruebas realizadas al Sistema Integral de Riesgo Operacional, se han realizado las pruebas de integración y las pruebas de sistema no realizándose las pruebas de aceptación pues estas deben realizar cuando el sistema se ponga en producción.

Con referencia a las pruebas de aceptación estas serán realizadas por las entidades que adquieran el software de acuerdo a los estándares de pruebas y de acuerdo a los criterios propios de cada institución, se espera que el Sistema SIRO cumpla con los requisitos de la Normativa de la Superintendencia de Banca y Seguros.

En el Anexo – _Pruebas_de_Siro se presentan pruebas que se han realizado mediante el cual se redactarán los pasos importantes para aplicar de manera efectiva el control de calidad a través de las técnicas de pruebas de caja negra, a fin de obtener el listado de deficiencias para el producto analizado; con el objetivo de realizar las correcciones necesarias para que este sea fiable y efectivo.

6.2 Casos de prueba

Propósito:	Una o dos oraciones cortas sobre el aspecto del sistema que está siendo probado. Si esto toma mucho tiempo, rompa el caso de prueba o ponga más información en las descripciones de las características.
Prerrequisitos:	Suposiciones que deben cumplirse antes de que correr el caso de prueba. Por ejemplo, "registrado", "inicio de sesión como invitado permitido", "el usuario testuser existe".
Datos de Prueba:	Lista de variables y sus posibles valores usados en el caso de prueba. Ud. puede enlistar valores específicos o describir

	rangos de valores. El caso de prueba deberá ser ejecutado una vez por cada combinación de valores. Estos valores se escriben notación de asignación, uno por línea. Por ejemplo: loginID = {loginID válido, loginID inválido, email válido, email inválido , vacío} password = {válido, inválido, vacío}
Pasos:	Pasos a ejecutar la prueba. Vea las reglas de formateo para pasos abajo. visitar LoginPage teclear usernameOrEmail teclear password hacer click en Entrar ver: la página de los términos de uso hacer click hasta el fondo de la página hacer en click Aceptar ver: PersonalPage verificar el mensaje de bienvenida si el inicio de sesión es correcto
Suceso / Alternativa.	Se listan una serie de sucesos, los cuales contienen los pasos a seguir, los que determinan una situación de la cual se tomará la alternativa más adecuada. Suceso 1: 1…… n……. Alternativa: …….. Suceso n: 1……. n……. Alternativa n:……
Opciones	Muestra la lista de posibles acciones que se pueden realizar en el sistema.
Resultado Esperado	Muestra el resultado óptimo del caso de prueba.
Evaluación de la Prueba	Muestra si la prueba resultó fallida o si se realizó con éxito.
Notas y Preguntas:	NOTA

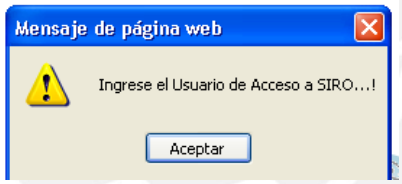
PREGUNTA

A continuación presentaremos un ejemplo de un caso de pruebas si desea ver mas casos de pruebas podrá referirse al anexo _Pruebas_de_Siro.

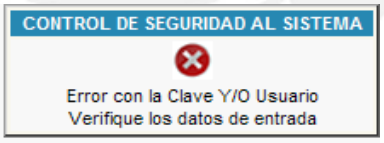
6.3 Caso de Prueba: Inicio de Sesión

Propósito:	Acceder al sistema, mediante el "logeo" respectivo del usuario autorizado. (Fig. 1)
Pre-requisitos:	Acceder al icono del escritorio, correspondiente al sistema, haciendo doble clic. Suponer que el usuario ya se encuentra registrado.
Datos de Prueba:	loginID = {loginID válido, loginID inválido, vacío} clave = {válido, inválido, vacío}
Pasos:	1. Ejecutar el sistema SIRO 2. teclear el Login 3. teclear clave 4. hacer click en Aceptar 5. ver: Pagina de Información Personal 6. verificar el mensaje de bienvenida si el inicio de sesión es correcto.
Notas y Preguntas:	Debe permitir como máximo hasta 3 intentos para el inicio de sesión, en caso contrario recomendarse comunicarse con el encargado del servidor.
Suceso / Alternativa.	**Suceso 1:** 1. Repetir la secuencia principal hasta el Ítem 2. 2. Clic en el botón "Aceptar" **Alternativa:** Emitir mensaje de Alerta información:"Ingrese la Clave de Acceso a Siro" (Fig. 2) 3. Repetir Ítem del 3 al 6. **Suceso 2:** 1. Repetir la secuencia principal hasta el ítem 4. 2. Si la clave de acceso, es incorrecta. **Alternativa:** Emitir mensaje de advertencia: "Usuario o clave incorrecta" (Fig. 3) Repetir Ítem del 2 al 4

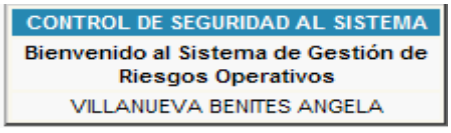
	Suceso 3: 1. Repetir la secuencia principal hasta el ítem 4. 2. Si la clave de acceso, es correcta. **Alternativa:** Emitir mensaje de bienvenida al sistema. (Fig. 4) Repetir ítem del 5 al 6.
Opciones	El sistema no permite el acceso del usuario, porque no ingreso contraseña. El sistema no permite el acceso del usuario, porque no ingreso la contraseña es invalida. El sistema permite el ingreso del usuario, logeado.
Resultado Esperado	El sistema validó el logeo de usuario.
Evaluación de la Prueba	Prueba fallida.
Notas	El logeo de usuario no se realiza si no se ingresan los respectivos valores de los campos.



(Fig. 2)



(Fig. 3)



(Fig. 4)

7. CAPITULO 7 - GESTIÓN Y CONFIGURACIÓN DEL CAMBIO.

La gestión de configuración del Software (GCS) es el arte de identificar, organizar y controlar las modificaciones que sufre el software que construye un equipo de programación. Así mismo se puede decir que la GCS, es un conjunto de actividades desarrolladas para gestionar los cambios a lo largo del ciclo de vida del software de computadora.

Los cambios dentro del desarrollo del software pueden ocurrir en cualquier momento por lo tanto debemos estar preparados, las actividades de CGS sirven para:

- Identificar el cambio de nuestro software.
- Controlar ese cambio.
- Garantizar que el cambio quede bien implantado.
- Informar el cambio.

Actividades

a. Identificación de los elementos de configuración y líneas base

Se han identificado las siguientes líneas bases.

Etapas del Ciclo de Vida	Líneas base	Elementos de configuración (EC)
Planificación	Línea Base de planificación	Plan del proyecto
Análisis	Línea Base de Análisis	Definición, estructuración de la metodología Definición de los requerimientos funcionales y no funcionales. Análisis de la Solución Definiciones y alcances del sistema
Diseño	Línea Base de Diseño	Arquitectura de solución Arquitectura del Software Modelo Lógico Modelo Físico Implementación de Producto
Pruebas	Línea Base de Pruebas	Estrategias de Pruebas Diagramas de Pruebas

b. Control de cambios

Para el control de cambios se tiene que considerar como objetivos, establecer versiones básicas del proyecto y del producto, así como proveer formas para controlar los requerimientos de cambio externo e interno que

afectan estas versiones básicas, y finalmente asegurar que los cambios requeridos son actualmente hechos a las versiones básicas de los productos una vez se han aprobado.

Ante cualquier cambio que se realice al software se debe de tener en cuenta lo siguiente:

1. Petición de cambio
2. Evaluación del cambio: Esfuerzo técnico, efectos secundarios, impacto sobre otros componentes, costos.
3. Informe de Cambios (resultados evaluación) a la ACC (Autoridad de Control de Cambios).
4. Se genera una OCI (Orden de Cambio de Ingeniería) para cada cambio: qué se cambiará; restricciones, criterios de revisión y auditoría.
5. Objeto dado de baja
6. Realización del cambio
7. Revisión del cambio.
8. Objeto dado de alta aplicando mecanismos de control de versión.

El Formato de esta sección la pueden verificar en el anexo Formato de GyCC SIRO

c. Control de versiones

El control de versiones combina procedimientos y herramientas para gestionar las versiones de los objetos de configuración creadas durante el proceso de ingeniería del software. Se ha definido como metodología de desarrollo a RUP, en el cual se describe el ciclo de desarrollo de software, y el mismo que contempla los procedimientos para poder realizar cualquier cambio de requerimiento de usuario.

El Formato de esta sección la puede verificar en el anexo Formato de GyCC SIRO

d. Informe de estado

El informe de estado mantiene como objetivo, registrar y reportar los cambios a los componentes de configuración.

Se debe de registrar cuales son los cambios que se han realizado a los requerimientos ya establecidos en el sistema, así mismo indicar si algunos de los componentes fueron afectados debidos a estos cambios.

El Formato de esta sección la puede verificar en el anexo Formato de GyCC SIRO

e. Auditorias y revisiones

Como objetivo principal para las auditorias y revisiones, se ha definido lo siguiente:
Verificar que el producto de SW integrado satisface los requerimientos estándares o acuerdos contractuales y que los componentes que se integran corresponden con las versiones vigentes.

Así mismo de han tenido que considerar que todos los productos de SW hayan sido producidos descritos e identificados correctamente y que todas las solicitudes de cambio han sido procesadas, tal y como se han definido.

Para asegurar que el cambio de los requerimientos en la arquitectura del software se ha implementado correctamente, se debe de tener en cuenta lo siguiente:

a. Revisiones técnicas formales: basada en la corrección técnica del elemento de configuración que ha sido modificado.

b. Auditorias de configuración del software: complementa la revisión técnica formal

El Formato de esta sección la puede verificar en el **anexo** Formato de GyCC SIRO

8. CAPITULO 8 - PLAN DE PROYECTO

Se describirá el plan que se utilizará para el proyecto, mayor detalle se puede encontrar en el anexo “Diagrama de Gantt”.

8.1 Metodología

Se utilizará como metodología de gestión del proyecto una disciplina de la metodología RUP (Rational Unified Process) que se muestra en la figura 3, esta disciplina se llama Administración del Proyecto, que se utilizará como base para la gestión de este proyecto aprovechando la equivalencia que RUP plantea con el Project Management Body of Knowledge (PMBOK).

Figura 3: Disciplinas de soporte de RUP

Al no ser un proyecto de gran escala, no se requieren de todas las actividades que se plantean en esta disciplina. Producto de las actividades descritas anteriormente, la metodología define para la disciplina encargada de la administración del proyecto varios documentos resultantes (artefactos), en este proyecto se producirán los siguientes:

- Plan de desarrollo de software.
- Lista de riesgos.

Solo se tendrán los artefactos mencionados, teniendo en cuenta que el Plan de desarrollo de software tiene incluido la organización del proyecto, por fases, así como el plan de gestión de riesgos y calidad.

8.2 Fases del Plan

El desarrollo del sistema será conducido por un enfoque de fases, siendo estas descritas en la tabla 1

Tabla 1: Fases del proyecto

Fase	Inicio	Fin
Fase de Concepción	03/03/2010	01/06/2010
Fase de Elaboración	03/06/2007	01/09/2010
Fase de Construcción	02/09/2008	30/12/2010

Cada fase constará de las actividades que se muestran en la tabla 2:

Tabla 2: Actividades del proyecto

Fase	Descripción	Misión
Fase de Concepción	Elaboración del plan de proyecto. Elaboración de lista de riesgos. Levantamiento de información. Identificación del problema. Definición del problema. Desarrollo de la visión. Identificación de requerimientos. Identificación de actores y casos de uso.	La identificación del problema a resolver así como la obtención de los requisitos que servirán para definir las funcionalidades que presentará el sistema.
Fase de Elaboración	Especificación de requerimientos de software. Evaluación de soluciones existentes. Definición de metodología de solución. Evaluación de viabilidad. Análisis técnico y económico. Identificación de restricciones de costo y tiempo. Identificación de indicadores.	El desarrollo del diseño del sistema, de forma que cumpla con los requisitos establecidos en la fase anterior, que servirán de base para el proceso de construcción.

	Identificación de reportes. Elaboración del diagrama de clases. Diseño de la arquitectura. Diseño de la interfaz gráfica. Ampliación del diagrama de clases. Diseño de la Base de Datos.	
Fase de Construcción	Selección de tecnologías. Construcción de la aplicación. Construcción de los reportes. Elaboración del plan de pruebas. Elaboración de casos de prueba. Evaluación de casos de prueba. Elaboración de resultados de pruebas.	La finalización del proyecto obteniendo el sistema y la base de datos probados y listos para su uso por el usuario.

1.5.1. Estructura de Descomposición del Trabajo

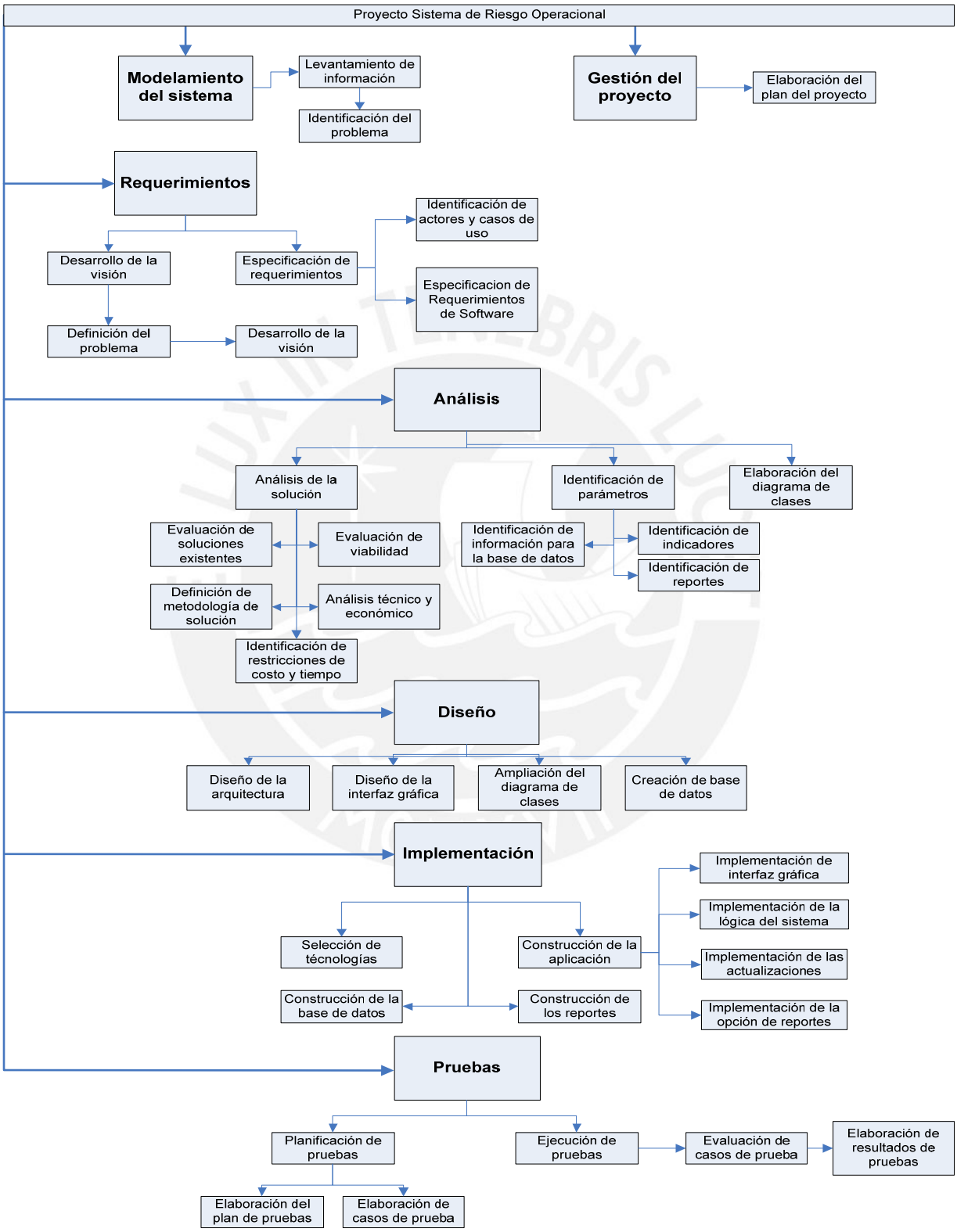


Figura 4: Figura Estructura de Descomposición de Trabajo [EDT]

9. CAPITULO 9 - CONCLUSIONES Y RECOMENDACIONES

Se han realizado reuniones con especialistas en Riesgo operacional que manejan la metodología de Coso/Enterprice Risk Manager quienes ayudaron a definir los requisitos de un sistema de Riesgo operacional y priorizarlos según normativa peruana.

Con respecto al uso de un software libre para el desarrollo este es un requerimiento de los especialistas en manejo de riesgo operacional para evitar los costes excesivos en la adquisición de licencias y el servicio de implantación del sistema.

La utilización del sistema de riesgo operacional en las entidades financieras integra las distintas aéreas de negocio y procesos de gestión de la organización ayudando y automatizando a la gestión del riesgo operacional por parte del área de Gestión del Riesgo.

9.1 Conclusiones

Para el desarrollo del presente proyecto se ha utilizado la metodología Rational Unified Process enfatizando en los documentos principales para la mejor comprensión del proyecto si hubiese algún cambio por parte de los usuarios o nuevos requisitos.

El Sistema de Riesgo Operacional (SIRO), soporta la metodología Australiana Neocelandesa 4360, y el estándar COSO/ERM.

El Sistema de Riesgo Operacional (SIRO), Cuenta con el detalle funcional que se indican en las normativas peruanas.

El Sistema de Riesgo Operacional (SIRO), Permite integrar la gestión del Riesgo Operacional en las diferentes áreas de su institución, impulsando el establecimiento de una cultura adecuada y reduce el esfuerzo para lograr una adecuada gestión del riesgo operacional.

El Desarrollo del plan de pruebas, ha permitido validar que el sistema de riesgo operacional cumple con los requerimientos planteados por la gestión de riesgos para entidades financieras.

9.2 Recomendaciones y trabajos futuro

Se debe evaluar la posibilidad de programar jornadas semestrales de difusión de la metodología (COSO/ERM) para la gestión del riesgo operacional con los dueños de los procesos, de manera adaptada a la realidad de la entidad Financieras,.

Se debe programar la implementación de un sistema de incentivos por la gestión del riesgo operacional, de manera que se estimule al personal a asumir su rol frente a dicha gestión, de modo que se tenga un creciente compromiso frente a este objetivo.

El personal de la Unidad de Riesgos, específicamente el analista de Riesgo Operacional debe interactuar más con el personal de las agencias, de modo que se proyecte el conocimiento sobre la gestión que realiza con este riesgo.

Se deben programar jornadas de capacitación a todo el personal de la entidad Financiera que implemente el Sistema de Riesgo Operacional y en especial a los Gestores de Riesgos para motivarlos a integrarse en la gestión del riesgo operacional como parte de la adopción de la cultura del riesgo operacional que necesitará expandirse.

Se debe establecer un responsable de impulsar el uso sistemático de la gestión del riesgo operacional, de manera que facilite la consolidación de la información, así como el monitoreo y los demás componentes de la metodología COSO/ERM.

10. Bibliografía

FONTNOUVELLE, P., E. ROSENGREN y J. JORDAN
2004 International Convergence of Capital Measurement and Capital Standards: a Revised Framework
http://www.bis.org/publ/bcbs107.htm

FONTNOUVELLE, P., V. DE JESUS-RUEFF, E. ROSENGREN y J. JORDAN, Reserva Federal de Boston.
2003 Implications of Alternative Operational Risk Modelling Techniques
Boston 20 noviembre 2004 pp.22
Consulta: 10 enero 2010
http://riskregforum.org/data/pdf/BASEL%20II%20Presentation%20BICA%202004.pdf

PROJECT MANAGMENT INSTITUTE
(2008) *Guía de los Fundamentos de la Dirección de Proyectos PMBOK*. Cuarta Edición 2008 Project Managment Institute.

JACOBSON IVAN; BOOCH GRADY, RUMBAUGH JAMES.
2000 El proceso Unificado de Desarrollo de Software.
España: Addison Wesley

ESCALAR CONSULTINGMÓDULO
2010 Modulo de Riesgo Operativo de Power Risk de la empresa Escalar Consulting
Consulta: Diciembre 2010
http://www.grupoescalar.com/software/riesgo_operativo.htm

METHOD WARE
2010 MeSoftware ERA – de la Empresa Method Ware obtenido noviembre
Consulta : Noviembre
http://www.methodware.com/era/

AGUILAR, G. Y CAMARGO G.
2004 *Análisis de la Morosidad en las instituciones microfinancieras del Perú*. En Mercado y Gestión del microcrédito en el Perú.
Lima: Consorcio de Investigación Económica y Social. Serie: Diagnóstico y Propuestas No 12.

ALEXANDER, C.

2003 The present and future of financial Risk Management, ISMA Centre.

Oxford University

Consulta: Marzo 2010

http://jfec.oxfordjournals.org/content/3/1/3.short

CEMLA.ORG

2004 Comité de Basilea y Comité Técnico de la Organización Internacional Comisiones de Valores, (1997), Boletín del Cemla. http://www.cemla.org/newsletters/newsletter-0103-basilea.htm

Jorion, Philippe.

2008 Valor en Riesgo. El nuevo paradigma para el control de riesgos con Colombia: Editorial Limusa.