Universidad Ricardo Palma

Facultad de Ingeniería

Escuela Profesional de Ingeniería Informática

Sistema para el Análisis y Gestión de Riesgos

Tesis Para optar el Título Profesional de Ingeniero Informático

Presentado por:

Antton Deyke Cavalcanti Garay

LIMA – PERU

2012

INDICE

ANEXOS

CAPITULO I: TEMA

1.1 Título del Tema

Sistema para Análisis y Gestión de Riesgos

1.2 Planteamiento del Problema

1.2.1 Antecedentes

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 - ahora ISO 9001
- 1992 Publicación BS 7750 - ahora ISO 14001
- 1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

En el Perú, se ha implementado con éxito el uso y buenas prácticas de este modelo y se cuenta actualmente con profesionales certificados en Auditoria, Analistas de Riesgos y Calidad de Procesos.

1.2.2 Introducción al Análisis y Gestión de Riesgos

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

Riesgo:

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Análisis de riesgos:

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Sabiendo lo que podría pasar, hay que tomar decisiones.

Gestión de riesgos:

Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Nótese que una opción legítima es aceptar el riesgo. Es frecuente oír que la seguridad absoluta no existe; en efecto, siempre hay que aceptar un riesgo que, eso sí, debe ser conocido y sometido al umbral de calidad que se requiere del servicio.

Como todo esto es muy delicado, no es meramente técnico, e incluye la decisión de aceptar un cierto nivel de riesgo, deviene imprescindible saber en qué condiciones se trabaja y así poder ajustar la confianza que merece el sistema. Para ello qué mejor que una aproximación

metódica que permita tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

1.2.3 Importancia

1.2.3.1 Justificación Práctica

Establecer el proceso para la identificación, análisis, evaluación y tratamiento de riesgos, considerando la seguridad de la información del negocio, los requisitos legales y reglamentarios.

Poder agilizar la toma de decisiones por parte de la gerencia de proyectos, realizando un adecuado seguimiento y control de riesgos que evite un impacto negativo en los objetivos de la organización.

Desarrollar un sistema para mejorar los procesos de gestión de riesgos, obteniendo resultados positivos para el aseguramiento de la información.

1.2.3.2 Justificación Académica

Agregar nuevo material que refleje el crecimiento de los conocimientos y prácticas en el manejo de gestión de riesgos, documentando esas prácticas, herramientas, técnicas y otros elementos pertinentes generalmente reconocidos como buenas prácticas.

Ampliar el tratamiento en el proceso de planificación de la gestión de riesgos y transmitir su importancia al grupo de trabajo.

Ampliar el conocimiento y uso de técnicas de recopilación y evaluación de información dirigidas a proyectos y sus sistemas.

1.2.4 Línea de Investigación

Ingeniería de Software – Gestión de Riesgos

1.3 Objetivo

1.3.1 Análisis del Problema

Uno de los principales problemas en la gestión de riesgos es la implementación adecuada, considerando la percepción y realidad de los riesgos que podrían afectar a la empresa. A continuación veremos un diseño de los problemas principales y las relaciones de causa – efecto, utilizando diagramas de árbol de problemas y árbol de objetivos, para mejor entendimiento.

1.3.1.1 Árbol de Problemas

Problema en la Empresa GMD SA.

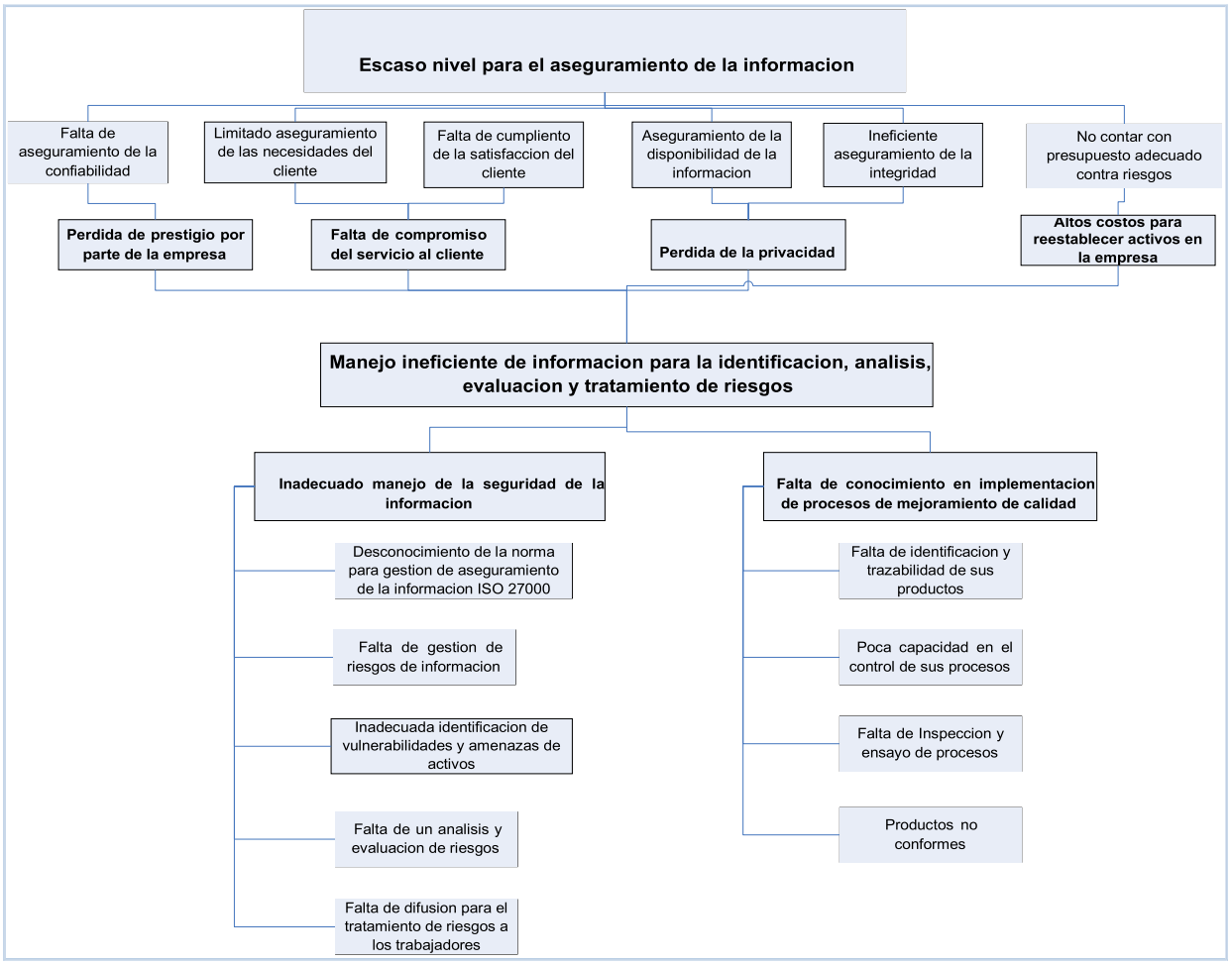


Fig. 1 Árbol de Problemas; Fuente: Propia

1.3.1.2 Árbol de Objetivos

Solución para la Empresa GMD SA.

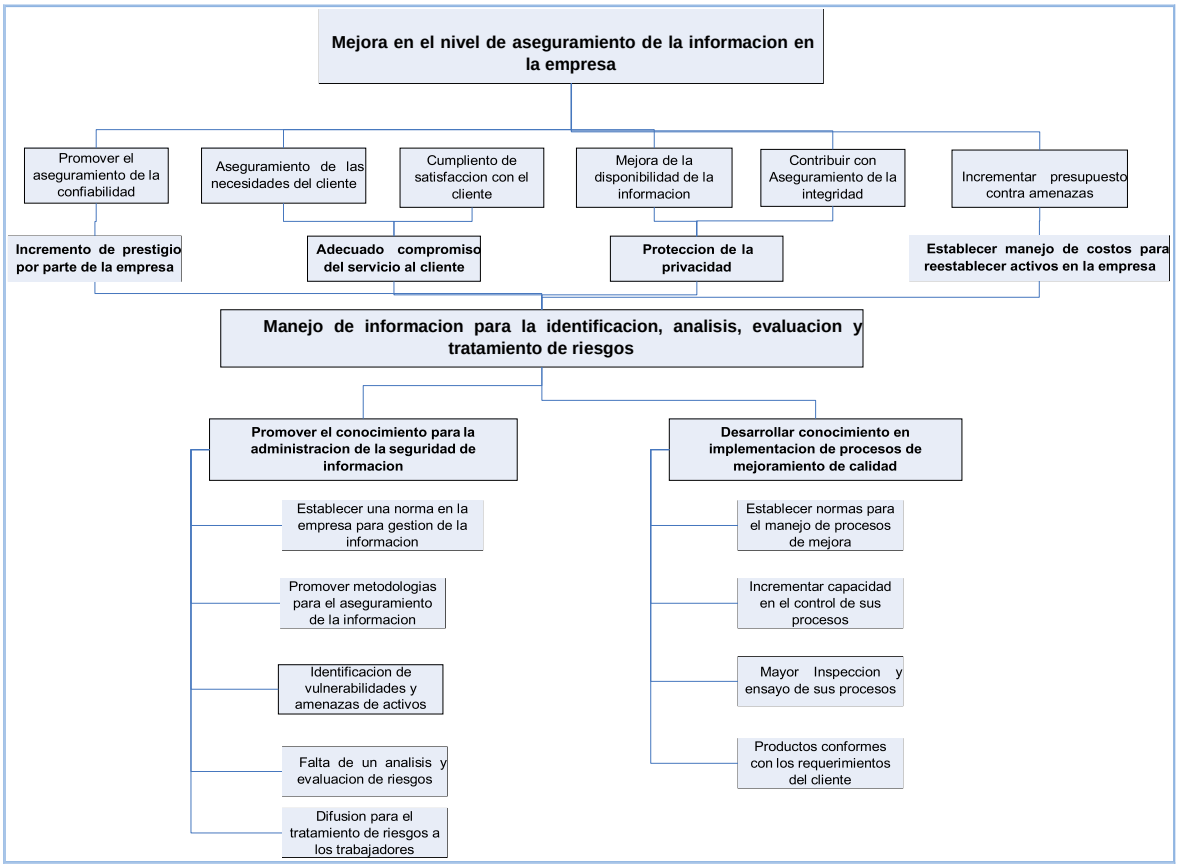


Fig. 2. Árbol de Objetivos; Fuente: Propia

1.3.2 Objetivo General

El objetivo general es la mejora en el manejo de riesgos, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando un seguimiento y control de riesgos. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Además se diseñó un nuevo material que refleja el crecimiento de los conocimientos y prácticas en el manejo de gestión de riesgos en seguridad de la información, se documentó esas prácticas, herramientas, técnicas y otros elementos pertinentes generalmente reconocidos como buenas prácticas.

El beneficio por parte de la empresa GMD fue obtener una evaluación de riesgos mediante un sistema Web, manteniendo las técnicas y prácticas que se realizan en este momento de forma manual. Generando así los medios para evaluar las amenazas existentes de una forma adecuada y eficiente.

1.4 Hipótesis

Toda hipótesis de causalidad involucra un efecto y una presente causa, que en teoría debe predecirlo el tiempo, sobretodo tratándose de una investigación relacionada a la evaluación de riesgos, que pueden o no hacer un daño a nuestra empresa.

En estos casos es imposible saber cuándo sucederá y qué impacto tendrá. Para ello se investigó las metodologías más importantes del rubro, diseño un modelo con los procesos adecuados para la evaluación y elaboró una herramienta capaz de identificar, cuantificar, planificar una contramedida y realizar un seguimiento, con el cual se busca prevenir o reducir el daño a la empresa.

1.5 Alcances

1.5.1 Análisis y Diseño

Se realizó un detallado análisis para la gestión de riesgos en un proyecto entre los que se encuentra los siguientes procesos, basados en metodologías establecidas en la guía de fundamentos de la dirección de proyectos:

Planificación de la Gestión de Riesgos: Decidir cómo enfocar, planificar y ejecutar las actividades de gestión de riesgos para un proyecto.

Identificación de Riesgos: Determinar que riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.

Análisis Cualitativo de Riesgos: Priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.

Análisis Cuantitativo de Riesgos: Analizar numéricamente el efecto de los riesgos identificados en los objetivos generales del proyecto.

Planificación de la Respuesta a los Riesgos: Desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

Seguimiento y Control de Riesgos: Realizar el seguimiento de los riesgos identificados, supervisar los riesgos residuales, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos evaluar su efectividad a lo largo del ciclo de vida del proyecto.

1.5.2 Desarrollo

Se implementó un sistema web para el seguimiento y control de riesgos informáticos, siguiendo los procesos establecidos en la parte de análisis y diseño.

Se generó un reporte como solución, para la correcta toma de decisiones que podrá verificar la alta gerencia en base al análisis expuesto. También se contó con un proceso de mantenimiento, que realiza un monitoreo a los responsables a cargo de los controles, tareas y salvaguardas a implementar, comunicando al área responsable y jefe a cargo.

1.5.3 Innovación

Se implementó una herramienta de evaluación para información o Focus Group. La cual tendrá como función principal la de obtener información sobre las opiniones, actitudes y experiencias de los riesgos posibles en un proyecto informático, siendo el evaluador el Gerente o Encargado del Proyecto.

Cabe resaltar que el focus group es una herramienta interesante para la evaluación de proyectos o de programas, sobre todo sirve para recopilar información rápida, así como puntos de vista y discusión para nuestro proyecto. (Ver Anexo 12).

Se realizó la documentación de los procesos establecidos anteriormente y debidamente modelados en el lenguaje UML (Unified Modeling Language) utilizando la metodología RUP (Rational Unifed Process). (Ver capítulo 5).

CAPITULO II: MARCO TEÓRICO

2.1 Introducción a las Tecnologías Básicas

En este ensayo se desarrolla un marco teórico conceptual para la Tecnología de la Información, el cual incluye la buena práctica de metodologías, herramientas y soluciones software que permitan una buena Gestión de Proyectos. Se dan las características básicas de las prácticas tecnológicas a la Ingeniería del Software. Se analizan las diferentes actividades para una buena Toma de Decisiones, colaborando con el alcance de objetivos principales en un proyecto.

Análogamente se estudian las diferentes metodologías de modelado de negocios, así como en programación orientada a objetos y uso de herramientas tecnológicas para el manejo de riesgos en un proyecto. Se discutirá los métodos de extracción de información como: Focus Group, para ayuda en el proceso de Planificación de Riesgos en un Proyecto.

Para la elaboración de esta tesis, se deberán manejar términos como:

Internet [1]: Internet es la red global. Es la red más grande que tiene el palmo físico más ancho posible. El Internet puede, quizás, ser asociado a la frase" la red de todas las redes". Entre algunos de los servicios que el Internet proporciona son:

- E-mail – (SMTP, POP3/IMAP, MIME).
- DNS – Domain Name Service.
- FTP – File Transfer Protocol.
- Telnet.
- Web, entre otros.

Web [2]: El Web consiste en un sistema de computadoras conectadas con el Internet (Internet hosts), funcionando un pedazo de web server llamado del software. Por ejemplo, detrás de cualquier URL del tipo http://www.ordererntry-example.de hay software del web server. La Web es apenas una de los servicios que el Internet proporciona - probablemente el más popular que brinda.

Web Server [3]: El termino web server representa un sistema de los módulos de programación, que se deben instalar sobre un ordenador huésped del Internet (Internet host) de modo que puedan participar en la Web; Web server maneja peticiones de HTTP, recupera

y entrega los documentos del HTML como respuesta. El término es ambiguo; refiere al paquete de programas informáticos y a la computadora dedicada (Internet host) en donde el software está instalado, y a veces la combinación de ambos.

Aplicación Web [4]: Llamada a aquellas aplicaciones que los usuarios pueden utilizar accediendo a un servidor web a través de Internet o de una intranet mediante un navegador. En otras palabras, es una aplicación software que se codifica en un lenguaje soportado por los navegadores web (HTML, JavaScript, Java, etc.) en la que se confía la ejecución al navegador.

Las aplicaciones web son populares debido a lo práctico del navegador web como cliente ligero, así como a la facilidad para actualizar y mantener aplicaciones web sin distribuir e instalar software a miles de usuarios potenciales. Existen aplicaciones como los webmails, wikis, weblogs, tiendas en línea que son ejemplos bien conocidos de aplicaciones web.

2.1.1 Definición de Riesgo

El riesgo en un proyecto es un evento incierto o condición incierta que si ocurre, tiene un efecto positivo o negativo sobre el proyecto.

Podemos afirmar que un riesgo está presente en todos los proyectos. Se conoce como factor de riesgo a cada aspecto particular del riesgo en el proyecto, el cual tiene causas y consecuencias que pueden ser analizadas con diferente profundidad y detalle.

Riesgos en proyectos son aquellos que pueden ser identificados, analizados, y que es posible encontrar una minimización de su probabilidad de ocurrencia o de su impacto.

Los riesgos que son una amenaza para el proyecto deben ser asumidos, si la recompensa que se obtiene al asumirlos es positiva.

Las organizaciones deben saber aceptar el hecho de que hay riesgos en todos los proyectos y deben tener una metodología para administrarlos. El gerente de cada proyecto es el impulsor de esta metodología, y debe actuar con trasparencia y realismo al tratar el riesgo con los patrocinadores.

2.2 Marco Normativo

El estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution.

2.3 Introducción a la Empresa o Institución

Se contó con el apoyo en el proceso de levantamiento de información, de la Empresa Privada GMD, empresa líder en la provisión de soluciones de Tecnología de Información. Además, GMD recibió la certificación Internacional de calidad ISO 9001 de la Prestigiosa firma LLoyd´s Register Quality Assurance, organización que recomendó esta certificación en mérito a la calidad de los servicios que provee a sus clientes. A su vez, la certificación CMMI-3 (Capability Maturity Model Integration), estándar internacional otorgado por el European Software Institute (ESI) a GMD, es un modelo integrado creado por el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon (CMU) que garantiza la capacidad, madurez y calidad en los procesos de producción de software, asegurando a su vez la aplicación de las mejores prácticas para el desarrollo de dicho producto.

Esta certificación marca un hito en la historia de las empresas peruanas de TI y además permite afianzar la calidad de productos y servicios, ampliar la atención del mercado corporativo local y regional, incrementar en 100% los puestos de trabajo en la fábrica de software, competir con menores costos pero igual calidad con los países del BRIC (nombre como se conoce a las naciones con mayor crecimiento comercial en TI como Brasil, Rusia, India y China).

El activo más importante de GMD es su personal altamente calificado, compuesto por más de 900 profesionales de primer nivel, comprometidos con la organización y dotados con capacidades innovadoras, los cuales se encuentran en permanente especialización y garantizan el máximo nivel de satisfacción en la atención a sus clientes. Siendo distribuida a continuación en el siguiente cuadro organizacional.

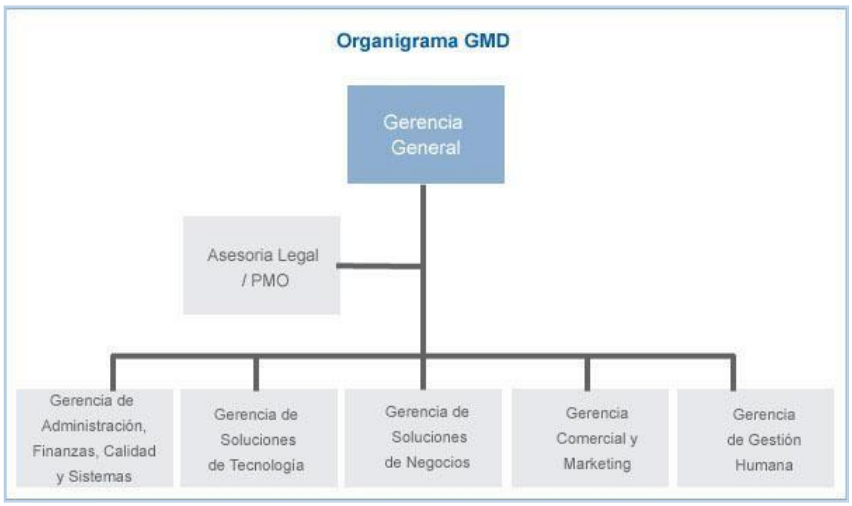


Fig. 3. Organigrama de la Empresa Peruana GMD; Fuente: GMD SA.

Así también se dispondrá con el apoyo de Ing. PMP José Luis Sandoval, Jefe del Área de Calidad, en dicha empresa, así como el personal a su cargo.

2.3.1 Estrategia Metodológica

La estrategia metodológica para la extracción de información de manos de expertos, fue la de entrevistas, la cual será de beneficio para la obtención y uso de información de personal laboral en acción. En la cual se detallaran puntos específicos acerca de la gestión de proyectos, así como experiencia del encuestado (útil para medir la calidad de información), herramientas de desarrollo, análisis y gestión, así como metodologías que se están usando para la evaluación de gestión de riesgos del proyecto, también se mencionara la opinión de los encuestados acerca del método que deberían tomar las empresas para mejorar su gestión.

Esta estrategia será complementada con la de encuestas a personal experto en el tema, ya que vemos que en la anterior, por ser implementada en una empresa de prestigio, no será efectiva en su totalidad, a causa de beneficio personal o de la empresa.

El total de entrevistas que se realizaran en el proceso de extracción de información, serán de 3. Los puntos que deberán cumplir los entrevistados serán:

- Ser un Profesional a nombre de la Nación o haber obtenido algún grado académico Superior.
- Tener conocimiento acerca de Gestión de Proyectos.
- Haber participado o ser participante de algún proyecto, en el cual se realice una Gestión de Proyectos o Control Interno.

El total de entrevistas que se realizaran en el proceso de extracción de información, serán de 20. El Punto de verificación con los que contaran los encuestados será:

Haber participado o ser participante de algún proyecto, en el cual se realice una Gestión de Proyectos.

2.4 Glosario de Términos

Actividad: Un componente del trabajo realizado en el transcurso del proyecto.

Activo: Cualquier cosa que tenga valor para la organización. (ISO/IEC 13335-1:2004).

Actividad Crítica: Cualquier actividad del cronograma en un camino crítico del proyecto. Se determina más comúnmente con el método de la ruta crítica. Aunque algunas actividades son críticas en su sentido literal, sin estar en la ruta crítica, este significado se utiliza raramente en el contexto del proyecto.

Amenaza: Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización. (ISO/IEC 13335-1:2004).

Análisis Monte Carlo: Una Técnica que calcula, o permite, el costo del proyecto o el cronograma del proyecto muchas veces, utilizando valores de datos iníciales seleccionados al azar a partir de distribuciones de probabilidades de costos o duraciones posibles, para calcular una distribución de los costos totales del proyecto o fechas de conclusiones posibles. También conocido como: Análisis de Monte Carlo.

Análisis Cuantitativo: El proceso de analizar numéricamente el efecto de los riesgos identificados sobre los objetivos generales del proyecto.

Análisis Cualitativo: El proceso de priorizar riesgos para mayor análisis o acción, al evaluar y combinar la probabilidad de ocurrencia e impacto de dichos riesgos.

Árbol de Decisiones: Análisis mediante Árbol de Decisiones; El árbol de decisiones es un diagrama que describe una decisión que se está considerando y las consecuencias de seleccionar una u otra de las alternativas disponibles. Se usa cuando algunos escenarios futuros o resultados de acciones son inciertos. Incorpora las probabilidades y los costos o recompensas de cada camino lógico de eventos y decisiones futuras, y usa el análisis del valor monetario esperado para ayudar a la organización a identificar los valores relativos de las acciones alternativas.

CCTA: La Agencia Central de Informática y Telecomunicaciones (CCTA) era un organismo de gobierno del Reino Unido proporcionando apoyo informático y de telecomunicaciones a los departamentos del Gobierno.

Contrato: Un contrato es un acuerdo vinculante para las partes en virtud del cual el vendedor se obliga a proveer el producto, servicio o resultado especificado y el comprador a pagar por él.

Control: Controlar, comparar el rendimiento real con el rendimiento planificado, analizar las variaciones, calcular las tendencias para realizar mejoras en los procesos, evaluar las alternativas posibles y recomendar las acciones correctivas apropiadas según sea necesario.

Controlar Costos: El proceso de monitorear la situación del proyecto para actualizar el presupuesto del mismo y gestionar cambios a la línea base de costo. También conocida como Controlar costos.

Controlar el cronograma: El proceso de monitorear la situación del proyecto para actualizar el avance del mismo y gestionar cambios a la línea base del cronograma.

Controlar el Avance: El proceso de monitorear la situación del proyecto y del alcance del producto, y de gestionar cambios a la línea base del alcance.

CRAMM: Cramm (Análisis de Riesgo de la ACTC y el Método de Gestión) fue creado en 1987 por el Centro de Informática y la Agencia Nacional de Telecomunicaciones (CCTA) del gobierno del Reino Unido. Cramm se encuentra actualmente en su quinta versión, CRAMM la versión 5.0. Se compone de tres etapas, cada una con el apoyo de cuestionarios objetivos y directrices. Las dos primeras etapas identificar y analizar los riesgos para el sistema. La tercera etapa recomienda cómo estos riesgos deben ser manejados.

Diagrama de Gantt: Representación gráfica de información relativa al cronograma. En el típico diagrama de barras, las actividades del cronograma o los componentes de la estructura de desglose de trabajo se enumeran en la parte izquierda del diagrama, los datos se presentan en la parte superior y la duración de las actividades se muestra como barras horizontales ubicadas según su fecha.

Diagrama de Flujo: La representación en formato de diagrama de los datos iníciales, medidas de un proceso y resultados de uno o más proceso dentro de un sistema.

Degradación: Medida de la pérdida de valor de un activo cuando ocurre una amenaza.

EDT (Estructura de Desglose del Trabajo): El proceso de subdividir los entregables del proyecto y el trabajo del proyecto en componentes más pequeños y más fáciles de manejar. También conocido: Crear EDT(Estructura de Desagregación del Trabajo);

Crear EDT (Estructura de Descomposición del Trabajo); Crear EDT(Estructura de División del Trabajo); Crear EDT(Estructura de Detallada del Trabajo).

Evaluación del riesgo: Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar importancia del riesgo. (ISO/IEC Guía 73: 2002).

Estimación Ascendente: Un método de estimación de un componente del trabajo. El trabajo se descompone más detalladamente. Se prepara un estimado de lo que se necesita para cumplir con los requisitos de cada una de las partes del trabajo inferiores y más detalladas, y estas estimaciones se suman luego a la cantidad total del componente del trabajo. La exactitud de la estimación ascendente se basa en el tamaño y la complejidad del trabajo identificado en los niveles anteriores.

Frecuencia: Medida de la probabilidad de ocurrencia de una amenaza.

Gerente Funcional: Alguien con autoridad de dirección sobre una unidad de la organización dentro de una organización funcional. El gerente de cualquier grupo que efectivamente realiza un producto o presta un servicio. A veces se le denomina gerente de línea.

Gestionar el equipo del proyecto: El proceso de monitorear el rendimiento de los miembros del equipo, proporcionar comentarios, resolver problemas y gestionar cambios para optimizar el rendimiento del proyecto. También conocido como administrar el equipo de proyecto; Dirigir el equipo del proyecto; o gerenciar el equipo del proyecto.

GMD: Empresa peruana perteneciente al Grupo Grana y Montero, brinda servicios de Outsourcing de tecnología, procesos, software factory e infraestructura de hardware y software.

Identificar Riesgos: El proceso de determinar los riesgos que pueden afectar al proyecto y documentar sus características.

IEC: La Comisión Electrotécnica Internacional (CEI o IEC International Electrotechnical Commission) es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas. Se desarrollan conjuntamente con la ISO (normas ISO/IEC).

Impacto: Medida del daño sobre el activo, derivado de la materialización de una amenaza.

ISO: ISO es la Organización Internacional para la Estandarización, que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales. Se conoce por ISO tanto a la Organización como a las normas establecidas por la misma para estandarizar los procesos de producción y control en empresas y organizaciones internacionales.

IT: Tecnología de la información y comunicación. Son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.

ITSEC: Las Tecnologías de la Información Criterios de Evaluación de Seguridad (ITSEC) es un conjunto estructurado de criterios para la evaluación de la seguridad informática dentro de los productos y sistemas. El ITSEC fue publicado en 1990. Después de una extensa revisión internacional, la versión 1.2 fue publicada en junio de 1991 por la Comisión de las Comunidades Europeas para el uso operacional dentro de los esquemas de evaluación y certificación.

Desde el lanzamiento de la ITSEC en 1990, una serie de otros países europeos han puesto de acuerdo para reconocer la validez de las evaluaciones ITSEC.

Juicio de Expertos: Un juicio que se brinda sobre la base de la experiencia en un área de aplicación, área de conocimiento, disciplina, industria, etc. Según resulte apropiado para la actividad que se está llevando a cabo. Dicha experiencia puede ser proporcionada por cualquier grupo o persona con educación, conocimiento, habilidad, experiencia o capacitación especializada.

MAGERIT: La Metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Metodología: Un sistema de prácticas, técnicas, procedimientos y normas utilizado por quienes trabajan en una disciplina.

Monitorear: Recolectar datos de rendimiento del proyecto con respecto a un plan, producir medidas de rendimiento, e informar y difundir la información sobre rendimiento. También conocido como: Supervisar.

Monitorear y Controlar el Trabajo del Proyecto: El proceso de monitorear, analizar y regular el avance a fin de cumplir con los objetivos de rendimiento definidos en el plan para la dirección del proyecto. También conocido como Supervisar y controlar el Trabajo del Proyecto.

Monitorear y Controlar los Riesgos: El proceso de implementar los planes de respuesta a los riesgos, monitorear los riesgos identificados, monitorear los riesgos residuales, identificar nuevos riesgos y evaluar el proceso de los riesgos a través del proyecto.

PAE: PAE, es un nuevo canal de difusión de la Administración Pública que unifica y centraliza toda la información sobre administración electrónica en España.

PMI: PMI es una organización Internacional sin fines de lucro fundada en 1969 en Estados Unidos, cuyo objetivo es la profesionalización del gerenciamiento de proyectos. Cuenta actualmente con 200.000 miembros en 125 países.

Presupuesto: La estimación aprobada para el proyecto o cualquier otro componente de la estructura de desglose del trabajo u otra actividad del cronograma.

Procedimiento de Monitoreo y Control: Aquellos procesos requeridos para monitorear, analizar y regular el progreso y el rendimiento del proyecto, para identificar aéreas en las que sean necesarios cambios al plan y para iniciar los cambios correspondientes. También conocido como: Proceso de Seguimiento y control.

Project Charter: Acta de constitución. Acta de Constitución del Proyecto.

Plan de Gestión de Costos: El documento que fija el formato y establece las actividades y los criterios necesarios para planificar, estructurara y controlar los costos del proyecto. El plan de gestión de costos del proyecto es un plan subsidiario del plan para la dirección del

proyecto o una parte de él. También conocido como: Plan de Administración de Costos; Plan de Gerencia de Costos; Plan de Gerenciamiento de Costos o Gestión de Costes.

Planificar la gestión de Riesgos: El proceso de definir como realizar actividades de gestión de riesgos para un proyecto.

Planificar la respuesta a los Riesgos: El proceso de desarrollar opciones y medidas para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

Riesgo Intrínseco: Combinación de la probabilidad de un evento y su ocurrencia. (ISO/IEC Guía 73:2002).

Riesgo Residual: Resultado de la selección e implementación de medidas para modificar el riesgo. (ISO/IEC Guía 73:2002).

Salvaguarda: Medios para contrarrestar las amenazas. Los objetivos de control y los controles (Ver Anexos) son seleccionados para el tratamiento de riesgos.

Solicitud de Cambio: Solicitud para ampliar o reducir el alcance de un proyecto, modificar políticas, procesos, planes o procedimientos, modificar costos o presupuestos, o revisar cronogramas.

Solicitud de Cambio Aprobada: Una solicitud de cambio que se ha aprobado a través del proceso de control de cambio integrado y que ha sido aprobada.

SGSI: Sistema de Gestión de Seguridad de la Información.

SSITAD: El Comité de Seguridad de los Sistemas de Información y Protección de Datos Personalizados Automatizados (SSITAD). Fue creado el 15 de Diciembre de 1995 por acuerdo de la Comisión Permanente del Consejo Superior de Informática (en la actualidad Consejo Superior de Administración Electrónica, CSAE). La creación de SSITAD obedeció al desarrollo de sus competencias en materia de protección de los datos informáticos, con el fin de proponer, impulsar, vertebrar y ejecutar políticas y actuaciones en materia de seguridad de los sistemas de información, tanto de medidas técnicas, como de orden administrativo-organizativo y legislativo, en los ámbitos nacional, europeo e internacional.

Tormenta de Ideas: Una técnica general de recolección de datos y creatividad que puede usarse para identificar riesgos, ideas o soluciones a problemas mediante el uso de un grupo de miembros del equipo o expertos del tema. También conocido como: Lluvia de Ideas.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo. (ISO/IEC Guía 73: 2002).

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 13335-1:2004).

2.5 Cronograma

Diagrama de Gantt

	EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**1**	**Proyecto de Tesis**	**134 días**	**jue 06/05/10**	**mar 09/11/10**	
2	**1.1**	**Inicio**	**134 días**	**jue 06/05/10**	**mar 09/11/10**	
3	**1.1.0**	**Plan de Proyecto**	**2 días**	**jue 06/05/10**	**vie 07/05/10**	
4	1.1.0.1	Elaborar Plan de Proyecto	1 día	jue 06/05/10	jue 06/05/10	
5	1.1.0.2	Realizar Reunion de Aprobacion	1 día	vie 07/05/10	vie 07/05/10	4
6	**1.1.1**	**Investigar y Documentar Tema**	**10 días**	**lun 10/05/10**	**vie 21/05/10**	
7	1.1.1.1	Investigar Libros	2 días	lun 10/05/10	mar 11/05/10	3
8	1.1.1.2	Investigar Tema	2 días	mié 12/05/10	jue 13/05/10	7
9	1.1.1.3	Investigar Papers	2 días	vie 14/05/10	lun 17/05/10	8
10	1.1.1.4	Investigar portales cientificos	2 días	mar 18/05/10	mié 19/05/10	9
11	1.1.1.5	Analizar libros, papers y tesis relacionadas	2 días	jue 20/05/10	vie 21/05/10	10
12	**1.1.2**	**Analizar Informacion obtenida de expertos**	**22 días**	**lun 24/05/10**	**mar 22/06/10**	
13	1.1.2.5	Llevar a cabo entrevistas a personal especializado	10 días	lun 24/05/10	vie 04/06/10	6
14	1.1.2.6	Evaluar el funcionamiento de Proyecto	5 días	lun 07/06/10	vie 11/06/10	13
15	1.1.2.7	Analizar los resultados de las Entrevistas	5 días	lun 14/06/10	vie 18/06/10	14
16	1.1.2.8	Analizar los resultados de la Evaluacion	2 días	lun 21/06/10	mar 22/06/10	15
17	**1.1.3**	**Analisis y Diseno**	**20 días**	**mié 23/06/10**	**mar 20/07/10**	
18	1.1.3.4	Modelo del Negocio	5 días	mié 23/06/10	mar 29/06/10	12
19	1.1.3.5	Modelo del Sistema	5 días	mié 30/06/10	mar 06/07/10	18
20	1.1.3.6	Modelo de la BD	10 días	mié 07/07/10	mar 20/07/10	19
21	**1.1.4**	**Implementacion de Sistema**	**51 días**	**mié 21/07/10**	**mié 29/09/10**	
22	**1.1.4.2**	**Programacion del Sistema**	**51 días**	**mié 21/07/10**	**mié 29/09/10**	
23	1.1.4.2.1	CUS:Valoracion de Activo	10 días	mié 21/07/10	mar 03/08/10	17
24	1.1.4.2.2	CUS: Identificacion de Amenaza y Vulnerabilida	10 días	mié 04/08/10	mar 17/08/10	23
25	1.1.4.2.3	CUS: Identificar Frecuencia y Degradacion	10 días	mié 18/08/10	mar 31/08/10	24
26	1.1.4.2.4	CUS: Identificar Salvaguarda	10 días	mié 01/09/10	mar 14/09/10	25
27	1.1.4.2.5	CUS: Identificar Riesgo Intrinseco y Residual	5 días	mié 15/09/10	mar 21/09/10	26
28	1.1.4.2.6	CUS: Toma de decisiones	3 días	mié 22/09/10	vie 24/09/10	27
29	1.1.4.2.7	CUS: Tratamiento de Riesgo	3 días	lun 27/09/10	mié 29/09/10	28
30	**1.1.5**	**Evaluacion y Pruebas del Sistema**	**25 días**	**jue 30/09/10**	**mié 03/11/10**	
31	1.1.5.3	Realizar Pruebas del Sistema	10 días	jue 30/09/10	mié 13/10/10	21
32	1.1.5.4	Corregir errores del Sistema	15 días	jue 14/10/10	mié 03/11/10	31
33	**1.1.6**	**Cierre del Proyecto**	**3 días**	**jue 04/11/10**	**lun 08/11/10**	
34	1.1.6.5	Recopilar documentación del proyecto	1 día	jue 04/11/10	jue 04/11/10	30
35	1.1.6.6	Calcular métricas del proyecto	1 día	vie 05/11/10	vie 05/11/10	34
36	1.1.6.7	Realizar reunión de cierre del proyecto	1 día	lun 08/11/10	lun 08/11/10	35
37	**1.1.7**	**Presentacion**	**1 día**	**mar 09/11/10**	**mar 09/11/10**	
38	1.1.7.2	Presentacion de Proyecto de Tesis	1 día	mar 09/11/10	mar 09/11/10	36
39	1.2	Fin	0 días	mar 09/11/10	mar 09/11/10	37

Fig. 4. Cronograma de Proyecto de Tesis; Fuente: Propia.

2.6 Lista de Evaluación de Amenazas

Categorias de Riesgos
1. Del Tamaño del Producto (TP)
2. Del Impacto en el Negocio (IN)
3. Relacionados con el Cliente (RC)
4. Del Proceso (PS)
5. Tecnológicos (TC)
6. Del Entorno de Desarrollo (ED)
7. Asociados con el Tamaño de la Plantilla de Personal y su Experiencia (PP)

Valores de Impacto
1. Catastrófico
2. Crítica
3. Marginal
4. Despreciable

Cuadro 1 para de Categoría de Riesgos;
Fuente: Propia.

Nro.	Amenazas	Categoría	Probabilidad	Impacto
1	Falta de equipos y herramientas(PC, laptop, internet, etc.) para trabajar el proyecto	ED	10%	3
2	No tener las habilidades en programación o diseño	PP	40%	1
3	No contar con la información del negocio	IN	10%	4
4	No contar con el apoyo de asesoría externa	PP	10%	4
5	No contar con un ambiento para el desarrollo del sistema	ED	20%	3
6	No poder realizar las actividades establecidas dentro del cronograma a tiempo.	PS	40%	2
7	No haber desarrollado el alcance para el sistema		20%	3
8	Nivel de satisfacción del usuario final	RC	30%	2
9	Cambios significativos en los requerimientos	IN	20%	3
10	Falta de disponibilidad para herramientas de análisis, diseño y Programación	TC	10%	4
11	Aplazamientos en el Cronograma de Trabajo.	PS	40%	3

Cuadro 2 para Cuantificar Amenazas;
Fuente: Propia.

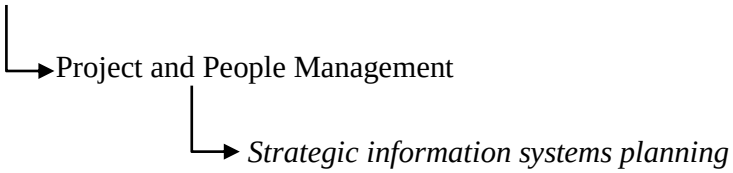
Valores de Impacto:

0. **Catastrófico:** Es la valoración para aquellos riesgos, que tendrían un impacto capaz de parar el proyecto y se pensaría en la forma de evitar el problema, ampliando el problema o reducir el alcance del proyecto.
1. **Crítico:** Es la valoración que pongo a aquellos riesgos que pueden transferidos o que requieren un nivel significativo para su evaluación.
2. **Marginal:** Es la valoración que asigno a los riesgos que pueden ser asumidos, realizando una valoración temprana o no adoptando técnicas demasiado complejas, tendrían una valoración despreciable en el proyecto.
3. **Despreciable:** Es la valoración que se da a los riesgos que causan un impacto menor en mi proyecto.

CAPITULO III: ESTADO DEL ARTE

3.1. Taxonomía

MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS



MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS o Dirección de Sistemas de Información y Cómputo, se puede decir que Dirección es planear, organizar, dirigir y controlar todos los recursos de un ente económico para alcanzar unos fines claramente determinados. Se apoya en otras ciencias como la economía, el derecho y la contabilidad para poder ejercer sus funciones.

Project Management o dirección de Proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades de un proyecto para satisfacer los requisitos del proyecto. La dirección de Proyectos se logra mediante la aplicación e integración de los procesos de dirección de proyectos de inicio, planificación, ejecución, seguimiento y control y cierre. Mientras que un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. Temporal significa que cada proyecto tiene un comienzo y un final definido. Un proyecto crea productos entregables únicos. Productos entregables son productos, servicios o resultados.

Strategic information systems planning o Planeamiento Estratégico de Sistemas de Información es una estrategia para la evaluación de los diferentes procesos de un proyecto en donde la Gestión de Riesgos esta inmersa. Gestión de Riesgos es el acto o practica de tratamiento de riesgos. Se incluye el planeamiento de riesgos, determinando (identificando y analizando) tema de riesgos, desarrollando estrategias de manejo de riesgos, y control y monitoreo de riesgos, para determinar cómo han ido cambiando.

3.2. Revisión de Métodos

3.2.1. Metodologías para Gestión de Riesgos

3.2.1.1. MAGERIT

La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

MAGERIT ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática, en España.

Objetivos de MAGERIT

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.
- Como objetivo a más largo plazo, MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información (ITSEC, Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información).

La Aplicación de MAGERIT permite:

- Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad.

- Ayudar a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- La incrustación de mecanismos de seguridad en el corazón mismo de los sistemas de información:
    - Para aminorar las insuficiencias de los sistemas vigentes;
    - Para asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento.

El Análisis y Gestión de Riesgos es el centro de toda actuación organizada en materia de seguridad y, por tanto, de la gestión global de la seguridad. Influye en las Fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento).

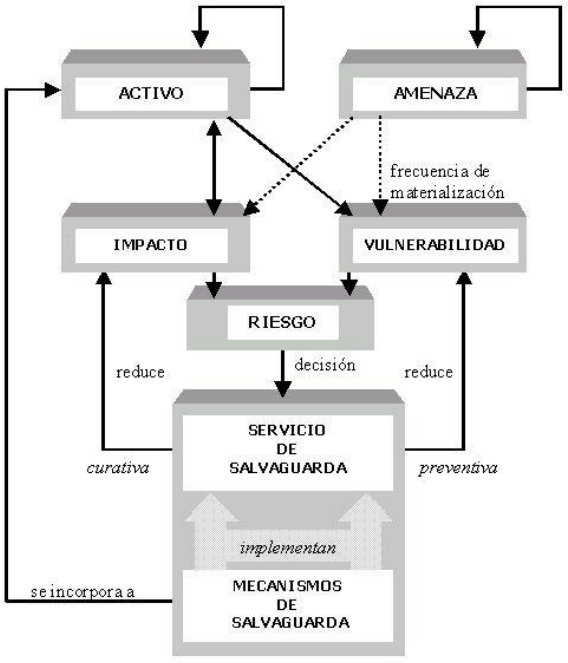


Fig. 7 Mapeo de MAGERIT frente a amenazas;

Fuente: [19] PAE Portal Administración Electrónica de España.

Tipos de proyectos

MAGERIT responde a las necesidades de un espectro amplio de intereses de usuarios con un enfoque de adaptación a cada organización y a sensibilidades diferentes en Seguridad de los Sistemas de Información. Las diferencias residen en tres cuestiones fundamentales:

- Situación dentro del "ciclo de estudio": marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- Envergadura: complejidad e incertidumbre relativas del Dominio estudiado, tipo de estudio más adecuado a la situación (corto, simplificado, etc.), granularidad adoptada.
- Problemas específicos que se desee solventar: Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para homologación de sistemas o productos, Auditorías de seguridad.

Estructura de MAGERIT

El modelo normativo de MAGERIT se apoya en tres sub modelos: El sub modelo de Elementos proporciona los "componentes" que el sub modelo de Eventos va a relacionar entre sí y con el tiempo, mientras que el sub modelo de Procesos será la descripción funcional ("el esquema explicativo") del proyecto de seguridad a construir.

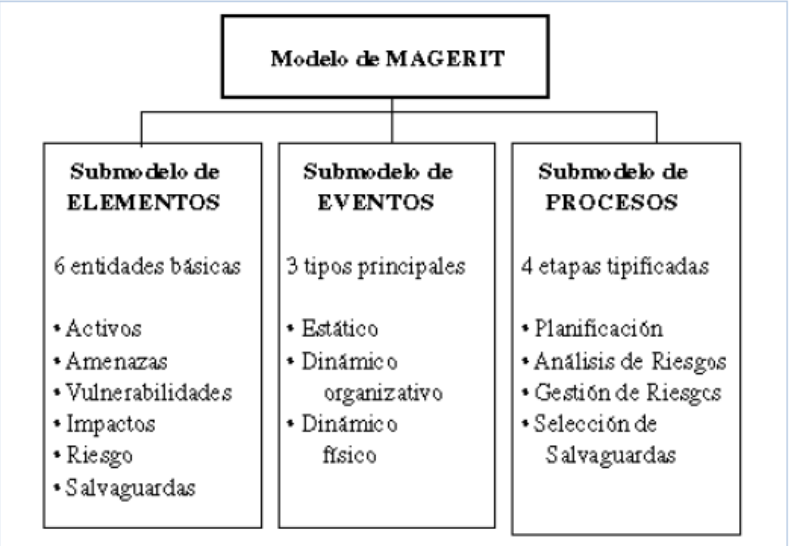


Fig. 8 Modelo de MAGERIT;

Fuente: [19] PAE Portal Administración Electrónica de España.

El sub modelo de Procesos de MAGERIT comprende 4 Etapas:

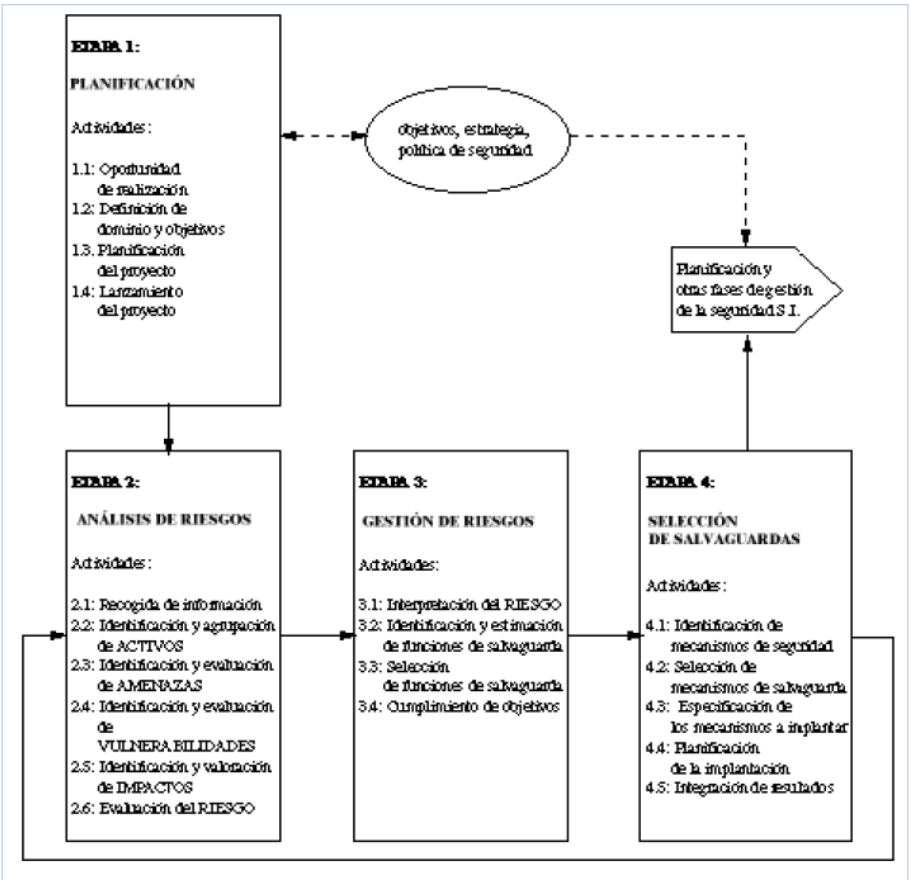


Fig. 9 Sub modelo de procesos de MAGERIT;

Fuente: [19] PAE Portal Administración Electrónica de España.

1. [12] Planificación del Proyecto de Riesgos. Como consideraciones iníciales para arrancar el proyecto de Análisis y Gestión de Riesgos (AGR), se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.
2. Análisis de riesgos. Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.
3. Gestión de riesgos. Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

Selección de salvaguardas. Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del Análisis y Gestión de Riesgos (AGR), para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

3.2.1.2. CRAMM

[13]CRAMM (CCTA Risk Analysis and Management Method) fue creado en 1987 por la Central Computing and Telecommunications Agency (CCTA) del gobierno de Reino Unido. CRAMM está actualmente en su quinta versión, versión 5.0 de CRAMM. Abarca tres etapas, cada uno apoyada por los cuestionarios objetivos y pautas. Las primeras dos etapas identifican y analizan los riesgos al sistema. La tercera etapa recomienda cómo estos riesgos deben ser manejados. Las tres etapas de CRAMM son como sigue:

Etapa 1 el establecimiento de los objetivos para la seguridad:

- Definición del límite para el estudio;
- La identificación y la valoración de los activos físicos esos forman la parte del sistema;
- La determinación del valor de los datos celebró entrevistándose con a usuarios sobre los impactos potenciales del negocio que podrían presentarse de la indisponibilidad, de la destrucción, del acceso o de la modificación;
- La identificación y la valoración de los activos del software esos forman la parte del sistema.

Etapa 2 La evaluación de los riesgos al sistema propuesto y de los requisitos para la seguridad cerca:

- Identificando y determinando el tipo y el nivel de amenazas que pueden afectar al sistema;
- Determinación del grado de vulnerabilidades del sistema y las amenazas identificadas;
- Combinar cálculos de la amenaza y de la vulnerabilidad con valores de activo para calcular medidas de riesgos.

Etapa 3 La identificación y la selección de contramedidas que sean conmensuradas con las medidas de riesgos calculados en la etapa 2. CRAMM contiene una biblioteca muy grande de las contramedidas que consiste en sobre 3000 contramedidas detalladas organizadas en sobre 70 agrupaciones lógicas.

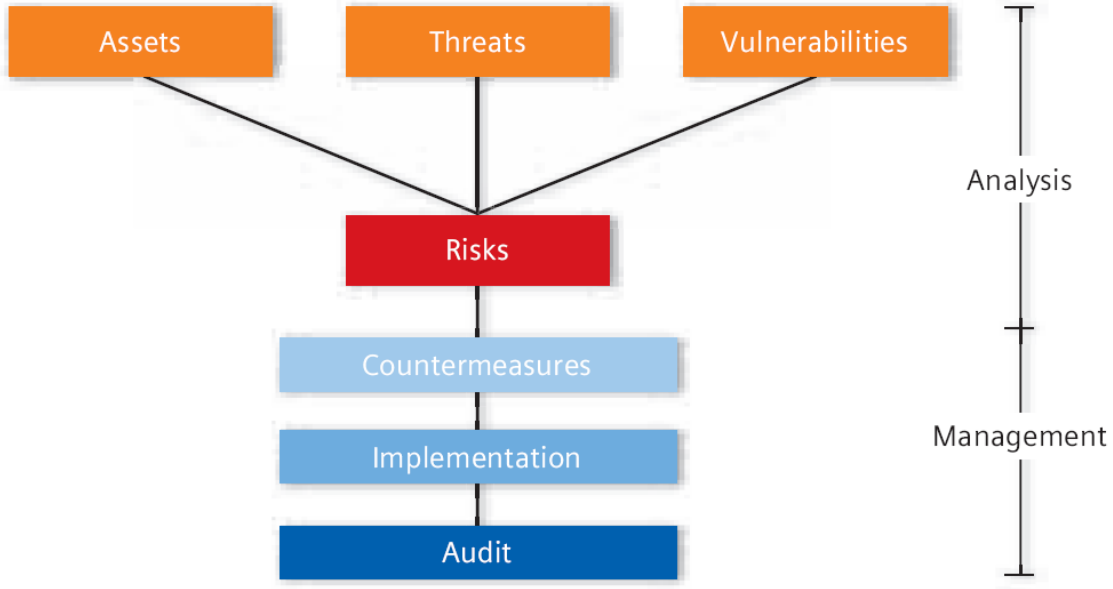


Fig. 10 Modelo de la Metodología CRAMM;
Fuente: [13] CCTA (Central Computing and Telecommunications Agency)

3.2.1.3. Modelo de Gestión de Riesgos PMI

La metodología de análisis y gestión de proyectos centran sus objetivos en aumentar la probabilidad y el impacto de los eventos positivos y disminuir la probabilidad de impacto de eventos adversos para el proyecto.

Los Procesos de Gestión de los Riesgos son:

Planificación de la Gestión de Riesgos: Decidir cómo enfocar, planificar y ejecutar las actividades de gestión de riesgos para un proyecto.

Identificación de Riesgos: Determinar que riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.

Análisis Cualitativo de Riesgos: Priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.

Análisis Cuantitativo de Riesgos: Analizar numéricamente el efecto de los riesgos identificados en los objetivos generales del proyecto.

Planificación de la Respuesta a los Riesgos: Desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

Seguimiento y Control de Riesgos: Realizar el seguimiento de los riesgos identificados, supervisar los riesgos residuales, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos evaluar su efectividad a lo largo del ciclo de vida del proyecto. **[2]**

La siguiente figura muestra la descripción de los procesos de gestión de proyectos.

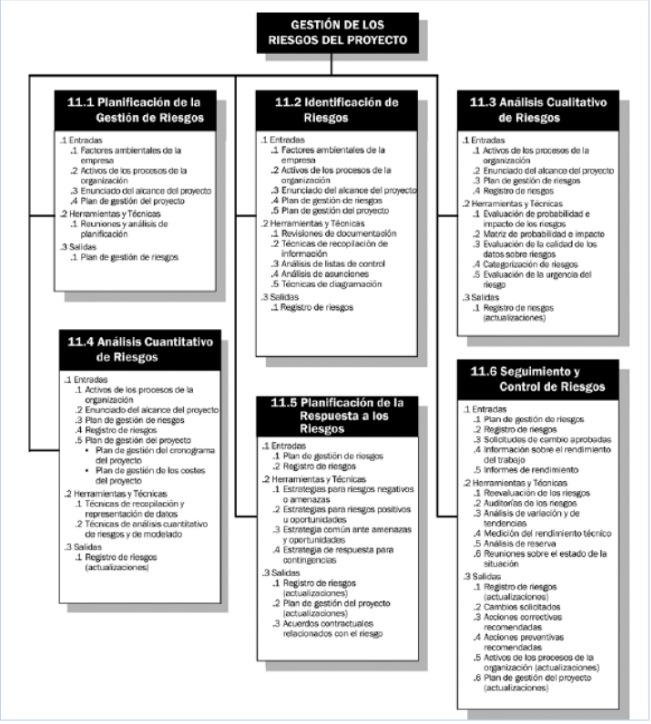


Fig. 5 Descripción General de la Gestión de los Riesgos en Procesos;
Fuente: [2] PMBOK guía de fundamentos de la dirección de proyectos.

[5]La siguiente figura muestra un diagrama de flujo de esos procesos y de sus entradas y salidas y procesos de otras áreas de conocimiento relacionadas.

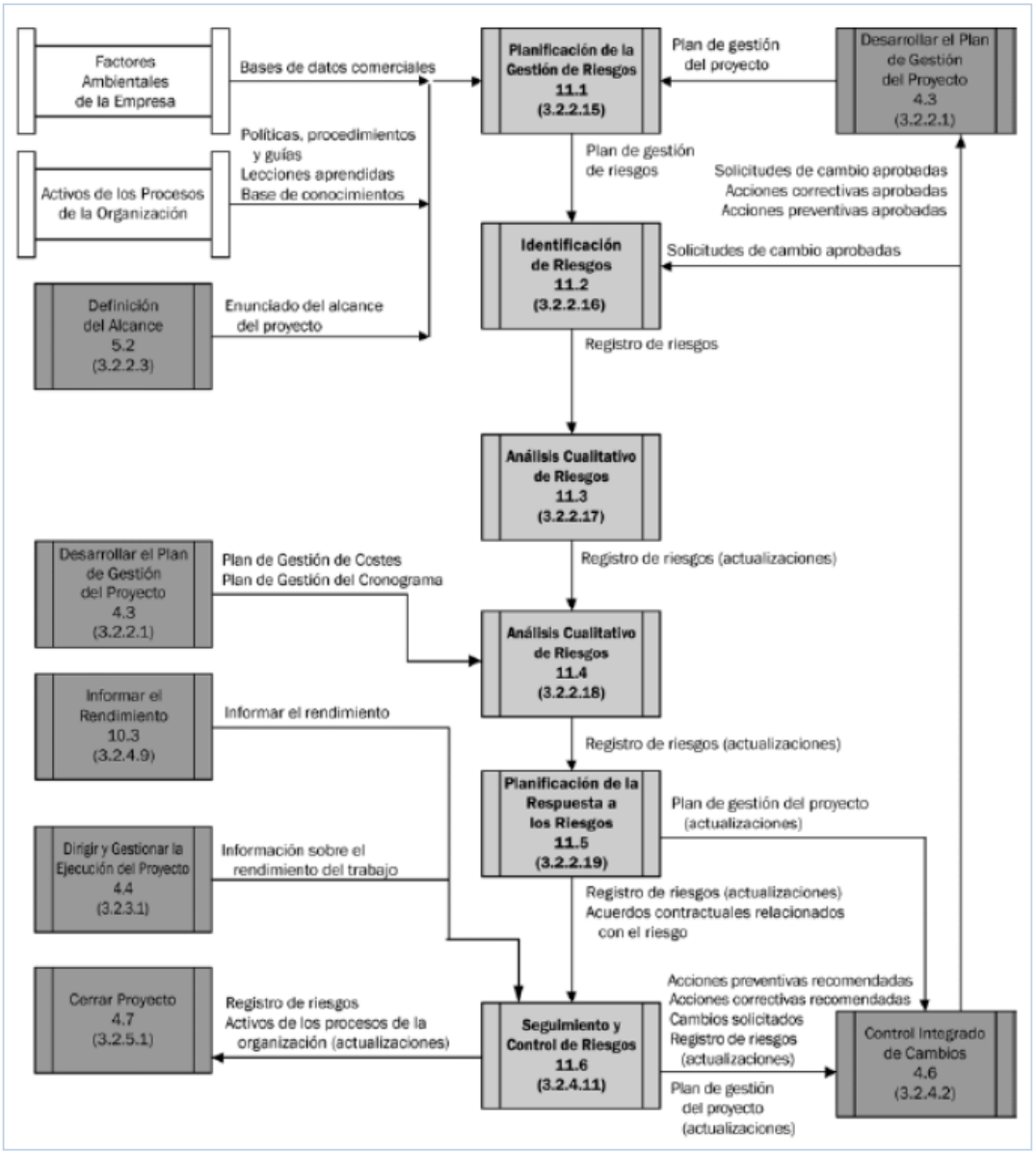


Fig. 6 Diagrama de Flujo de procesos de Gestión de los Riesgos en Proyectos.
Fuente: [2] PMBOK guía de fundamentos de la dirección de proyectos.

3.2.1.4. **Metodología de Riesgos en RUP**

El propósito de la Planificación de Proyectos de Software es establecer planes razonables para la ejecución de ingeniería de software y para la administración de proyectos de software. Estos planes, son lo necesario para administrar el proyecto de software. Sin planes realistas, no se puede implementar un proyecto efectivo de administración.

Uno de los objetivos de RUP es asegurar que las expectativas de todas las partes son sincronizadas y consistentes. Esto es asegurado a través de evaluaciones periódicas durante el ciclo de vida del proyecto, y es documentado en el Reporte de Evaluación de Status. Este reporte es utilizado para hacer un seguimiento a información acerca de recursos (humano y financiero), mayores riesgos, progreso técnico medido a través de métricas y resultados de hitos principales.

Con RUP hacemos uso de las siguientes clases de métricas:

- Progreso (líneas de código, número de clases, puntos de función por iteración, rehacer).
- Estabilidad (tipo de rehacer, volatilidad de requerimientos o implementación).
- Adaptabilidad (costo de rehacer).
- Modularidad (extensión del impacto de rehacer).
- Calidad (velocidad de descubrimiento de defectos, densidad, profundidad e indicador de rehacer).
- Madurez (horas de prueba por falla).
- Perfil de desembolso de recursos (planeados versus actuales).

Los documentos RUP que contienen los planes y compromisos son:

- Casos de Negocio
- Plan de Desarrollo de Software
- Plan de Medición
- Lista de Riesgos
- Plan del Proyecto
- Plan(es) de Iteración
- Evaluación(es) de Iteración, y
- Evaluación(es) de Status

[14] La Lista de Riesgos es un artefacto de RUP que nos provee una visión de todos los riesgos conocidos en el proyecto, y sirve como entrada para la planificación y evaluación del proyecto. Cada riesgo es descrito en función de su impacto, y un plan de contingencia será desarrollado para mitigar el riesgo en cuestión.

La Lista de Riesgos es desarrollada junto con los Casos de Negocio, los cuales formarán la base para la decisión de continuar o no con el proyecto. La Lista de Riesgos es mantenida a través de todo el ciclo de vida del proyecto.

3.2.1.5. Comparación de Metodologías

[14]Tanto en MAGERIT, CRAMM desarrollan metodologías similares para la gestión de riesgos, además se hace mención del modelo que presenta PMI siendo las más efectivas en el mercado y por esa razón tomada en cuenta para nuestro ensayo.

Notamos que MAGERIT es una metodología que busca simplificar los costos y aminorar los tiempos, por lo siguiente: los procesos de Análisis Cualitativo y Cuantitativo, que son manejados por PMI con tal nombre, son simplificados y simplemente llamados: Análisis de Riesgo, siendo estos dos procesos críticos para la búsqueda a las respuestas para la prevención y buena gestión del proyecto. Siendo mas ágil el proceso de análisis de riesgo pero difícil de diferenciar al momento de controlar en siguientes oportunidades.

También se denota que tanto MAGERIT y CRAMM tiene la particularidad de identificar sus riesgos y a la vez estar tomando medidas de salvaguardas, siendo una técnica hábil para aminorar los tiempos, pero teniendo la deficiencia de solo hacer esa gestión lideres o gerentes de proyectos con años de experiencia, ya que no se puede identificar riesgos sin antes no haberlos sufrido y haber tomado respuestas y haber obtenido éxito.

En conclusión, podemos afirmar que cualquier metodología de análisis de riesgos conlleva de forma implícita una identificación, inventario de activos, una reflexión sobre el posible catálogo de amenazas que pueden afectar a los mismos, la medición de su impacto y probabilidad de ocurrencia, así como una recomendación final sobre las salvaguardas más apropiados para minimizar el riesgo.

3.2.1.6. Cuadro Comparativo de Metodologías

	Valoración
0	No Cumple
1	Cumple Parcialmente
2	Cumple Plenamente

	Pesos para nuestro proyecto
1	Bajo
2	Moderado
3	Alto

0. **No Cumple**: Es la valoración que se da si la metodología no cumple con la característica que se necesita para nuestro proyecto.
1. **Cumple Parcialmente**: Es la valoración que se le da a la metodología que cumple con ciertas características, pero no siendo la más adecuada.
2. **Cumple Plenamente**: Es la valoración que se da a la metodología que cumple del todo y mejora los procesos en nuestro proyecto.

VALOR		PMI	MAGERIT	CRAMM
	Dirigido a:			
2	Gerentes de Proyectos	2	2	2
3	Auditores	2	2	2
3	Analistas de Riesgos	2	2	2
2	Integrantes de Proyectos	2	2	1
	Procesos:			
2	Planificación de Gestión de Riesgos	2	2	2
2	Identificación de Riesgos	2	2	2
2	Análisis Cualitativo	2	2	1
2	Análisis Cuantitativo	2	2	1
3	Planificación de la Respuesta a los Riesgos	2	2	2
3	Seguimiento y Control de Riesgos	1	2	1
	Funcionalidades			
	Activos			
1	Descripción Funcional del Sistema	2	2	1
2	Identificación de Datos, SW y Activos	1	2	1
3	Valorar Activos en términos de Impacto en el negocio	2	2	1
3	Valorar Activos físicos en términos de coste de reemplazo	1	2	1

3	Valorar activos SW en términos de Disponibilidad, Confidencialidad e Integridad	1	2	0
3	Cálculos del Riesgo	1	2	2
	Identificar Amenazas			
1	Estimar probabilidad de ocurrencia	2	2	0
2	Estimar extensión(Probabilidad vs Impacto)	2	2	0
3	Calcular Riesgos según matriz que incorpora amenazas	2	2	1
	Salvaguardas			
3	Identificar contramedidas para disminuir los riesgos detectados	2	2	2
3	Evaluar salvaguardas existentes para evitar detectar áreas existentes o de debilidad	2	2	0
3	Hacer recomendaciones sobre salvaguardas apropiadas	2	2	1
Total		94	108	66

Cuadro 3. Comparación de metodologías PMI, MAGERIT y CRAMM;

Fuente: Propia

Vemos que la alternativa elegida sería la de MAGERIT, debido al valor aportado para el proyecto. En cuanto a las otras opciones, son tomadas en cuenta como referencia, obteniendo una mayor información a la hora de realizar la evaluación del riesgo.

3.3. Aplicaciones Varias

3.3.1. Gestión de Riesgos Financieros

[15]La administración de riesgos financieros es una rama especializada de las finanzas corporativas, que se dedica al manejo o cobertura de los riesgos financieros. Por esta razón, un administrador de riesgos financieros se encarga del asesoramiento y manejo de la exposición ante el riesgo de corporativos o empresas a través del uso de instrumentos financieros derivados.

El riesgo financiero hace referencia a la incertidumbre asociada al rendimiento de la inversión debida a la posibilidad de que la empresa no pueda hacer frente a sus obligaciones financieras (principalmente, al pago de los intereses y la amortización de las deudas). Es decir, el riesgo financiero es debido a un único factor: las obligaciones financieras fijas en las que se incurre.

Cuanto mayor sea la suma de dinero que una organización pública o privada debe en relación con su tamaño, y cuanto más alta sea la tasa de interés que debe pagar por ella, con mayor probabilidad la suma de intereses y amortización del principal llegará a ser un problema para la empresa y con mayor probabilidad el valor de mercado de sus inversiones (el valor de mercado de la compañía) fluctuará.

3.3.2. Gestión de Riesgos Económicos

[15]El riesgo económico hace referencia a la incertidumbre producida en el rendimiento de la inversión debida a los cambios producidos en la situación económica del sector en el que opera la empresa. Así a modo de ejemplo, dicho riesgo puede provenir de la política de gestión de la empresa, la política de distribución de productos o servicios, la aparición de nuevos competidores, la alteración en los gustos de los consumidores.

El riesgo económico es una consecuencia directa de las decisiones de inversión. De manera que la estructura de los activos de la empresa es responsable del nivel y de la variabilidad de los beneficios de explotación. Este es un tipo de riesgo específico o no sistemático puesto que sólo atañe a cada inversión, o empresa, en particular. Como es único, la exposición al mismo varía según sea la inversión o la empresa en la que se invierta, lo que influirá en la política de selección de activos de cada inversor en particular. Hay que tener en cuenta que este tipo de riesgo puede producir grandes pérdidas en un corto espacio de tiempo; por ejemplo, la aparición en el mercado de un producto más avanzado y barato que el nuestro puede hacer descender las ventas de nuestros productos de una forma realmente grande provocando grandes pérdidas en la empresa. Además, si se produce una recesión económica, al reducirse los beneficios de las empresas también se reducen sus impuestos provocando con ello que los gobiernos central, autonómico y local vean reducida su capacidad financiera para servir a la comunidad. Así, pues, el riesgo económico afecta a las instituciones gubernamentales de forma indirecta.

El riesgo económico tiende a reducirse a través de la propiedad de inversiones a corto plazo. Cuanto antes se recupere la inversión menor será el plazo de tiempo para que las condiciones cambien de forma que afecten sustancialmente al rendimiento esperado del proyecto. Por ello, muchos inversores adoptan el criterio del plazo de recuperación para valorar los proyectos de inversión puesto que dicho método prima la liquidez del proyecto al jerarquizar las inversiones con arreglo a su menor plazo de recuperación.

3.4. Software Existentes

3.4.1. @RISK

[16]Instituciones líderes en todo el mundo (Procter & Gamble, Merck entre otros) confían en Palisade y su producto @RISK para la gestión de riesgos y análisis de toma de decisiones. El motivo por el cual las Empresas confían en el @RISK es que tienen la seguridad que obtendrán no solo una herramienta capaz de realizar una buena gestión de riesgos sino también un software que sea reconocido por diferentes organizaciones líderes en el análisis de riesgos tales como PMI, lo cual les permitirá permanecer un paso delante frente a sus competidoras.

El @RISK para Project utiliza la simulación Monte Carlo para mostrarle todos los posibles resultados en su proyecto y qué tan probable es de que los mismos ocurran. Esto significa que finalmente posee el panorama más completo posible. También puede determinar qué tareas son más importantes y luego administrar los riesgos apropiadamente. El @RISK para Project le muestra la mejor estrategia basada en la información disponible.

Fig. 11 Imagen Promocional del Producto;
Fuente: [18] Portal de Palisade Corp.

Al ejecutar una simulación, el @RISK para Project lleva a su modelo de proyecto desde la representación de justamente un único posible resultado a la representación de miles de ellos. Con el @RISK para Project, se podrán contestar preguntas como ¿Cuál es la probabilidad de completar determinado punto de control intermedio a tiempo y bajo control presupuestario? O bien, ¿cuáles son las probabilidades de que determinada fase de un proyecto sea completada antes de un día en particular?

El @RISK para Project provee un amplio rango de gráficos para poder interpretar y presentar sus resultados a otros. El Gráfico de Gantt de @RISK le permite visualizar los resultados de simulación directamente en el gráfico de Gantt nativo de Project. Las curvas de histograma y acumulativas muestran la probabilidad de ocurrencia de distintos resultados. Utilizando gráficos sobrepuestos y de resumen para comparaciones más avanzadas.

Características

- Monte Carlo RISKOptimizer 5.0: Combina la simulación de Monte Carlo con optimización basada en algoritmos genéticos para encontrar la mejor combinación de factores que cumplen con un resultado deseado bajo condiciones inciertas.
- Acelerado Integrado de @RISK: Acelera la velocidad de simulaciones múltiples por medio de procesamiento en paralelo, utilizando procesadores multi-core y hasta cuatro CPUs.
- Ajuste integrado de distribuciones: Adapta funciones de distribución a sus datos históricos.
- Librería de @RISK: una base de datos SQL para guardar y compartir con otros usuarios funciones de distribución, componentes de modelos, y resultados de simulaciones.
- Excel Developer Kit (XDK): Automatiza y adapta @RISK a su Excel por medio de librerías completas de comandos y funciones que le permiten controlar cada aspecto de @RISK en su hoja de cálculo. Añade @RISK a cualquier aplicación que quiera personalizar.
- Análisis de Estrés: Le permite controlar el rango que se muestrea de una función de distribución, permitiéndole apreciar cómo diferentes escenarios afectan sus conclusiones son necesidad de cambiar su modelo.
- Análisis Avanzado de Sensibilidad: Le permite apreciar cómo los cambios en cualquier entrada, ya sea distribución de probabilidad o valores fijos, afectan los resultados de la simulación.
- Búsqueda Objetivo (Goal Seek) de @RISK: Utiliza simulaciones múltiples para encontrar un valor de entrada que cumple una meta que usted especifica.

Precio del Producto: $ 1995.00

Plataforma de Soporte: Windows 2000, 2003, XP, Vista.

Software Adicional: Excel, Project.

3.4.2. Crystal Ball

[17]Crystal Ball constituye el método más simple para realizar simulaciones mediante el método de Monte Carlo en su hoja de cálculo. Crystal Ball calcula automáticamente miles de casos del tipo "¿qué pasaría si…?" grabando las entradas y los resultados obtenidos de cada cálculo como escenarios individuales. El análisis de estos escenarios revelará el rango de posibles resultados, la probabilidad de que estos ocurran, la entrada que ha tenido más efecto en su modelo y donde deberían enfocarse, a partir de ahí, sus esfuerzos.

Entre algunas de sus funcionalidades ayudan a mejorar procesos como: incrementar las ventas, reducir los costes, ahorrar tiempo de desarrollo, mejorar la calidad de los productos. Cada día

se enfrenta a estos objetivos, y con cada decisión que toma el éxito está más próximo. Como ayuda a la toma de decisiones, es frecuente crear modelos de hojas de cálculo basados en los datos disponibles, su conocimiento del mercado y sus años de experiencia.

Es una herramienta para hacer sus predicciones; una herramienta que le ayuda a planificar lo inesperado y que refuerce la calidad de las decisiones críticas para su negocio. Es una herramienta dinámica que muestre aquello que más impacta en su negocio, y que le permita experimentar y visualizar todo el rango de posibles resultados.

Características:

- Simulación de Monte Carlo: Calcula múltiples escenarios de un modelo de hoja de cálculo automáticamente. Libera al usuario de las restricciones propias de las estimaciones y de los valores puntuales.
- Galería de Distribuciones: Ofrece una interfaz intuitiva para seleccionar las variables de entrada del modelo. Incluye 16 distribuciones discretas y continuas, así como distribuciones propias. Simplifica la cuantificación del riesgo, sin que sea necesario introducir la fórmula de la distribución en Excel.
- Funciones de Capacidad de Procesos: Defina especificaciones (Inferior, Superior y Deseada) en sus predicciones, calcule las métricas de capacidad y observe los resultados de la simulación y las métricas juntas en una gráfica dividida. Con las métricas de capacidad de Crystal Ball se simplifica el flujo de trabajo y se integra la simulación en su metodología Six Sigma y de Calidad.
- Gráficas de Predicción: Muestre gráficamente los resultados de la simulación junto con las estadísticas. Observe y analice miles de posibles resultados gracias a las gráficas interactivas.
- Análisis de Sensibilidad y Tornado: Dispone de dos métodos para identificar las variables de entrada más críticas de su modelo. De esta manera, podrá centrarse en las variables del modelo con un mayor riesgo.

Precio del Producto: $ 2018.99

Plataforma de Soporte: Windows 2000, 2003, XP, Vista.

Software Adicional: Excel.

3.4.3. Risk Simulator

[18]Es un software para toma de decisiones de negocios críticas. Considera todos los riesgos de sus proyectos y decisiones y se encuentra enfocado en resultados. Le ayuda a entender lo que es un riesgo y como cuantificarlo y valor el riesgo en sus proyectos y decisiones.

Además, Risk Simulator está integrado con el software Real Options Super Lattice Solver, el cual puede utilizar para resolver opciones estratégicas, financieras y de recursos humanos.

Características:

- Simulación Monte Carlo

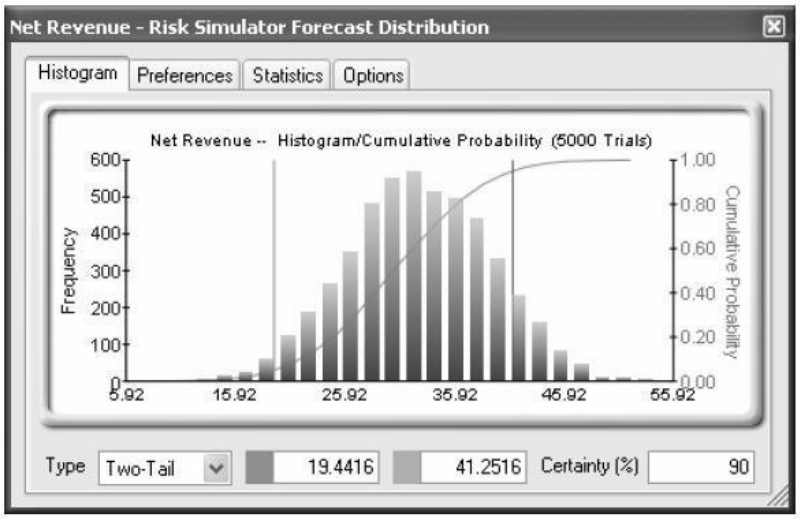


Fig. 12 Simulación de Montecarlo vista en Risk Simulator;

Fuente: [17] Real Option Software Corp.

- Integración completa con Microsoft Excel (conexión dinámica, macros VBA y mucho más).
- Simulación comprensiva y reportes analíticos para cada funcionalidad.
- Simulación correlacionada con truncamiento distribucional.
- Perfil de simulaciones para análisis de escenarios en simulación.
- Métodos de Monte Carlo tradicionales.
- Análisis de múltiples regresiones (series ed tiempo, cross-sectional y panel).
- Predicción de series de tiempo.
- Diagnósticos de datos (Auto-correlación, Correlación, Distributiva Lags, Heteroestadisticidad, Micronumerosity, Multi-colinealidad, No-linealidad, No-Estacionariedad, Normalidad, Outliers y Estimaciones de Parametros Estocasticos)
- Extracción de datos y predicciones

- Análisis de escenarios.
- Análisis de sensibilidad.
- Análisis Estadístico (Auto-correlación, ajustamiento de datos, Estadística Descriptiva, Pruebas de Hipótesis, Extrapolación No -Lineal, Normalidad, Estimación de Parámetros Estocásticos, predicción de series de tiempo).

Precio del Producto: $ 1925.00

Plataforma de Soporte: Windows 2000, 2003, XP, Vista.

Software Adicional: Excel.

3.4.4. Cuadro Comparativo de Aplicativos

	@Risk	Risk Simulator	Cristal Ball	SGSI
Gestión de Usuarios	√			√
Perfil de Usuario	√			√
Registro de Activos	√	√	√	√
Registro de Riesgos	√	√	√	√
Registro de Amenazas	√	√	√	√
Registro de Controles	√	√	√	√
Consulta de Parametros				√
Valorización de Activos	√	√	√	√
Valorización deNiveles de Activos	√	√	√	√
Identificación de Frecuencia y Degradacion	√	√	√	√
Matriz de Impacto	√	√	√	√
Administración de Controles	√			√
Tratamiento de Riesgos	√	√	√	√
Seguimiento de Riesgo		√		√
Asignación de responsable				√
Alerta de Riesgo a correo				√
Total	12	10	9	16

Cuadro 4. Comparación de aplicativos @risk, risk simulator, cristal ball y SGSI;

Fuente: Propia

CAPITULO IV: ANÁLISIS DE FACTIBILIDAD

4.1. Factibilidad Técnica

4.1.1. Propuesta Técnica utilizando Software Propietario 1

- Oracle 10g Enterprise Edition.
- Sistema Operativo Windows 2000.
- Visual .NET 2005
- .Net Framework.
- Microsoft Office 2003

4.1.2. Propuesta Técnica utilizando Software Propietario 2

- SQL Server 2005.
- Visual .NET 2005
- .Net Framework.
- Sistema Operativo Windows XP Profesional Edition.
- Microsoft Office 2003

4.1.3. Propuesta Técnica utilizando Software Propietario/Libre

- MySql
- J2SDK.
- Sistema Operativo Windows XP Profesional Edition.
- OpenOffice.org 2.4.2

*Nota: Debido a que la empresa ya posee y realiza mantenimiento a otros usuarios y propios. Se opta por la opción de la propuesta 4.1.2 Propuesta Técnica utilizando Software Propietario 2. Con ello abreviamos el tiempo y aminoramos coste de capacitación para los usuarios que, por ya tener estos aplicativos se tendrá un mejor desempeño.

4.2. Factibilidad Económica

4.2.1. Propuesta Económica utilizando Hardware/Software Propietario 1

Oracle 10g Enterprise Edition	$. 0.00
.Net Framework	$. 0.00
Visual .NET Professional 2005	$. 0.00
Sistema Operativo Windows 2000	$. 0.00
Computadora HP (Hewlett-Packard) Pavilion s3330f (2.8GHz AMD Athlon 64 X2Quad, Ram 2GB DDR2, HD 500GB)	$. 0.00
Costo de Desarrollo Analista Programador (S/.68.18 por día, trabajando 8h diarias,5 días a la semana, 22 días al mes por 6 meses)	$. 3000.00
Costo Total	**$. 3000.00**

4.2.2. Propuesta Económica utilizando Hardware/Software Propietario 2

SQL Server 2005	$. 0.00
.Net Framework	$. 0.00
Visual .NET Professional 2005	$. 0.00
Sistema Operativo Windows XP Profesional Edition	$. 0.00
Computadora HP (Hewlett-Packard) Pavilion s3330f (2.8GHz AMD Athlon 64 X2Quad, Ram 2GB DDR2, HD 500GB)	$.0.00
Costo de Desarrollo Analista Programador (S/.68.18 por día, trabajando 8h diarias, 5 días a la semana, 22 días al mes por 6 meses)	$.3000.00
Costo Total	**$. 3000.00**

4.2.3. Propuesta Económica utilizando Hardware/Software Libre

MySql	$. 0.00
J2SDK.	$. 0.00
Sistema Operativo Windows XP Profesional Edition	$. 0.00
OpenOffice.org 2.4.2	$. 0.00
Computadora HP (Hewlett-Packard) Pavilion s3330f (3.0 GHz Core Quad, Ram 4GB DDR2, HD 500GB)	$. 0.00
Costo de Desarrollo Analista Programador (S/.68.18 por día, trabajando 8h diarias, 5 días a la semana, 22 días al mes por 6 meses)	$. 3000.00
Costo Total	**$. 3000.00**

4.2.4. Propuesta Económica para el mantenimiento del Sistema

Única vez	
Capacitación (2 personas, 16h)	$. 250.00
Analista de Riesgos(S./ 207.00 por día, trabajando 8h diarias, 5 días a la semana, 22 días al mes por 1 mes)	$. 1520.00
Programador(S./ 204.5 por día, trabajando 8h diarias, 5 días a la semana, 22 días al mes por 1 mes)	$. 1500.00
Semanal	
Backups de Información (Realizado por el analista de riesgos. 1 vez por semana, en toda la etapa de ejecución de Proyecto). Reportes de progreso y estadísticas.	$. 40.00
Anual	
Soporte Online. (S./ 54.50 por día, trabajando 8h diarias, 5 días a la semana al año, durante 2 años)	$. 8600.00
Costo Total	**$. 11910.00**

4.2.5. Otros

2 Paquetes de Hoja Bond, formato A4 (500 hojas)	S/. 40.00
2 Cartuchos de Tinta Negra para Impresora HP	S/. 120.00
1 Cartucho de Tinta a Color para Impresora HP	S/. 70.00
Costo total	S/. 230.00

*Nota: Debido a que se cuenta con el sponsor GMD S.A. el proyecto se podrá implementar en un módulo de Mejoras de Procesos en dicha compañía. No se hará gastos en compras de equipos nuevos. Además el software producido, cumple con las expectativas exigidas por el cliente.

4.3. Alternativa seleccionada

A continuación mostraremos un cuadro comparativo entre los requerimientos de la empresa en contraposición con las alternativas técnicas y económicas para nuestro proyecto.

		Factibilidad Técnica			Factibilidad Económica		
Valor	Requerimientos Funcionales	4.1.1 Soft. Propietario 1	4.1.2 Soft. Propietario 2	4.1.3 Soft. Libre	4.2.1 Soft/Hard Propietario 1	4.2.2 Soft/Hard Propietario 2	4.2.3 Soft/Hard Libre
2	R1: El sistema contara con un esquema de gestión de accesos para la seguridad de la información (usuario y contraseña).	2	2	2	2	2	2
3	R2: El Sistema podrá ser accedido para consultas, por otros usuarios que considere conveniente tenga acceso, otorgándosele un perfil de usuario. De acuerdo a este perfil dicho usuario podrá tener ciertas restricciones de acceso.	2	2	2	2	2	2
3	R3: El usuario será el encargado de ingresar información sobre los datos de los diferentes riesgos que se dan comúnmente (retardos en el cronograma establecido, no cumplir con los objetivos del proyecto, costo variable de producto, entre otros).	2	2	2	2	2	2
1	R4: La información se obtendrá de fuentes de información del sistema obtenidas de los diferentes especialistas en el tema. En donde se tienen datos específicos de cada riesgo.	2	2	1	2	2	1
3	R5: Mediante el Sistema también podrán realizar medidas a tomar para reducir los riesgos en su proyecto (Mitigar, Evitar, Aceptar, Trasladar).	2	2	2	2	2	2
3	R6: El Sistema será capaz realizar un proceso de seguimiento de controles de riesgos. El cual enviara automáticamente y con un tiempo determinado las fechas correspondientes para terminar las tareas por proceso.	1	2	2	1	2	2
3	R7: El usuario podrá generar reportes para poder estar al tanto de las medidas usadas y, obtener como resultado el poder prevenirlas en otra posible oportunidad o en otro proyecto similar evaluando el coste del proyecto.	2	2	2	2	2	2
	Requerimientos No Funcionales						
3	Interfaz de Usuario	1	2	1	1	2	1
1	Documentación	2	2	1	2	2	1
3	Caract. de Rendimiento	2	2	2	2	2	2

3	Seguridad	2	2	0	2	2	0
2	Desempeño	2	2	2	2	2	2
	Total	54	60	49	54	60	49

Cuadro 5. Comparación de Propuestas Técnicas y Económicas;
Fuente: Propia
*Nota: Valores de referencia ver pág. 50.

	Valoración para Proyecto
1	Bajo
2	Moderado
3	Alto

	Valoración Factores
0	No Cumple
1	Cumple Parcialmente
2	Cumple Plenamente

Luego de analizar las distintas alternativas considerando factores técnicos y económicos, se considera conveniente optar por la propuesta Software Propietario 2. Las razones por dicha alternativa son las siguientes:

- La opción del administrador de Base de Datos SQL Server 2005, es considerada como una herramienta potente y de fácil implementación, debido a que está muy difundida en el mercado laboral Peruano. No se vio la necesidad de ejecutarlo en otro administrador más potente (ORACLE), ya que la cantidad de usuarios requerida aun es baja.
- Como herramienta de desarrollo se escogió a Visual.NET 2005 Professional Edition, debido a que es la herramienta con menor riesgo de error en la compatibilidad, adaptabilidad y alto acoplamiento al SGBD utilizado, brindando los métodos para la reutilización de código, facilitando la programación y reduciendo los tiempos del proyecto.
- Se considera al Sistema Operativo Windows XP Professional Edition como el sistema más usado en el mercado, facilitando la implementación y evitando los problemas de adaptación a otros usuarios.

CAPITULO V: Contribución Teórica y Práctica

5.1. Requerimientos Funcionales

El sistema propuesto reúne una serie de requerimientos captados en las reuniones llevadas a cabo por parte del cliente GMD. Mediante una serie de entrevistas se concluyó realizar un sistema capaz de poder manejar las actividades pertenecientes al manejo de riesgos, implementación de salvaguardas y seguimiento de contramedidas.

La información requerida para la toma de requerimientos funcionales y no funcionales partieron del área de Mejoramiento de Procesos y Gestión de calidad, se procedió a realizar encuestas a personal experto en el tema de manejo de riesgos y reuniones con José Luis Sandoval, jefe de gestión de calidad y a la vez jefe del proyecto: Sistema de Gestión de Seguridad de la Información para el COT.

Luego mediante reuniones con Iván Hilarión, jefe del área de sistemas y tecnologías, se pudo captar los requerimientos y estándares utilizados para los sistemas de GMD y adaptarlos en nuestro sistema.

Requerimiento 1: El sistema contara con un esquema de gestión de accesos para la seguridad de la información (usuario y contraseña).

Requerimiento 2: El Sistema podrá ser accedido para consultas, por otros usuarios que considere conveniente tenga acceso, otorgándosele un perfil de usuario. De acuerdo a este perfil dicho usuario podrá tener ciertas restricciones de acceso.

Requerimiento 3: El usuario será el encargado de ingresar información sobre los datos de los diferentes riesgos que se dan comúnmente (retardos en el cronograma establecido, no cumplir con los objetivos del proyecto, costo variable de producto, entre otros).

Requerimiento 4: La información se obtendrá de fuentes de información del sistema obtenidas de los diferentes especialistas en el tema. En donde se tienen datos específicos de cada riesgo.

Requerimiento 5: Mediante el Sistema también podrán realizar medidas a tomar para reducir los riesgos en su proyecto (Mitigar, Evitar, Aceptar, Trasladar).

Requerimiento 6: El Sistema será capaz realizar un proceso de seguimiento de controles de riesgos. El cual enviara automáticamente y con un tiempo determinado las fechas correspondientes para terminar las tareas por proceso.

Requerimiento 7: El usuario podrá generar reportes para poder estar al tanto de las medidas usadas y, obtener como resultado el poder prevenirlas en otra posible oportunidad o en otro proyecto similar evaluando el coste del proyecto.

5.2. Requerimientos No Funcionales

5.2.1. Interface de Usuario

La interfaz debe ser clara, sencilla y amigable, tanto para el registro de la información como para realizar las consultas, de tal forma que pueda ser comprensible para usuarios que no cuenten con mucha experiencia en la evaluación de riesgos en proyectos de Sistemas Informáticos.

5.2.2. Documentación

En cuanto a la documentación se le brindara al Usuario un manual en donde se explicara detalladamente el funcionamiento del Sistema, así como también contará con una sección de asistencia para posibles problemas que puedan presentarse.

5.2.3. Características de Rendimiento

El tiempo de respuesta por cada solicitud estará fluctuando aproximadamente 0.5 segundos, los tiempos de respuesta mayores con un máximo de 2 segundos.

5.2.4. Seguridad

Para que los datos no puedan ser accedidos o modificados por usuarios no autorizados, se deberá identificar con el nombre de usuario y una clave para tener acceso al Sistema.

5.2.5. Desempeño

Dado a que el sistema es una aplicación web, existe la posibilidad de caídas, debido al Hardware del cliente o al Servidor, esto puede hacer que se pierdan datos, ante esta posibilidad el sistema hará respaldos, para la mantención y protección de los datos.

5.3. Modelado del Sistema

5.3.1. Diagrama de Actores

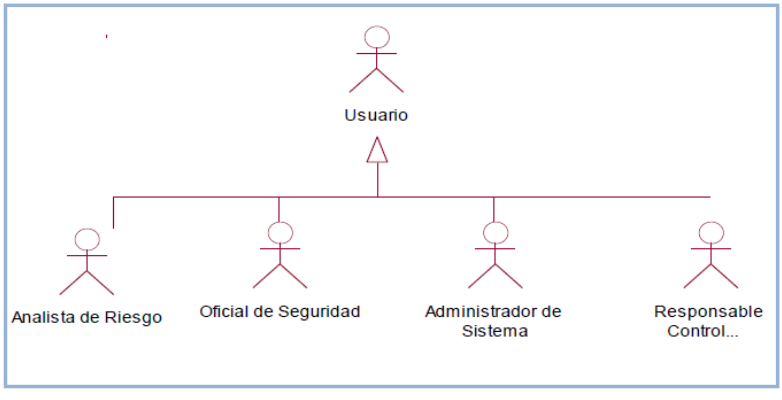


Fig 13. Diagrama de Actores;

Fuente: Propia.

5.3.2. Diagrama de Paquetes

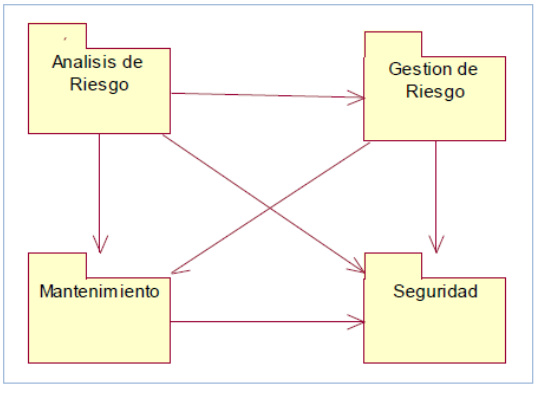


Fig 14. Diagrama de Paquetes;

Fuente: Propia.

5.3.3. Casos de Uso por Paquetes

5.3.3.1 Casos de Uso por Paquetes: Análisis de Riesgo

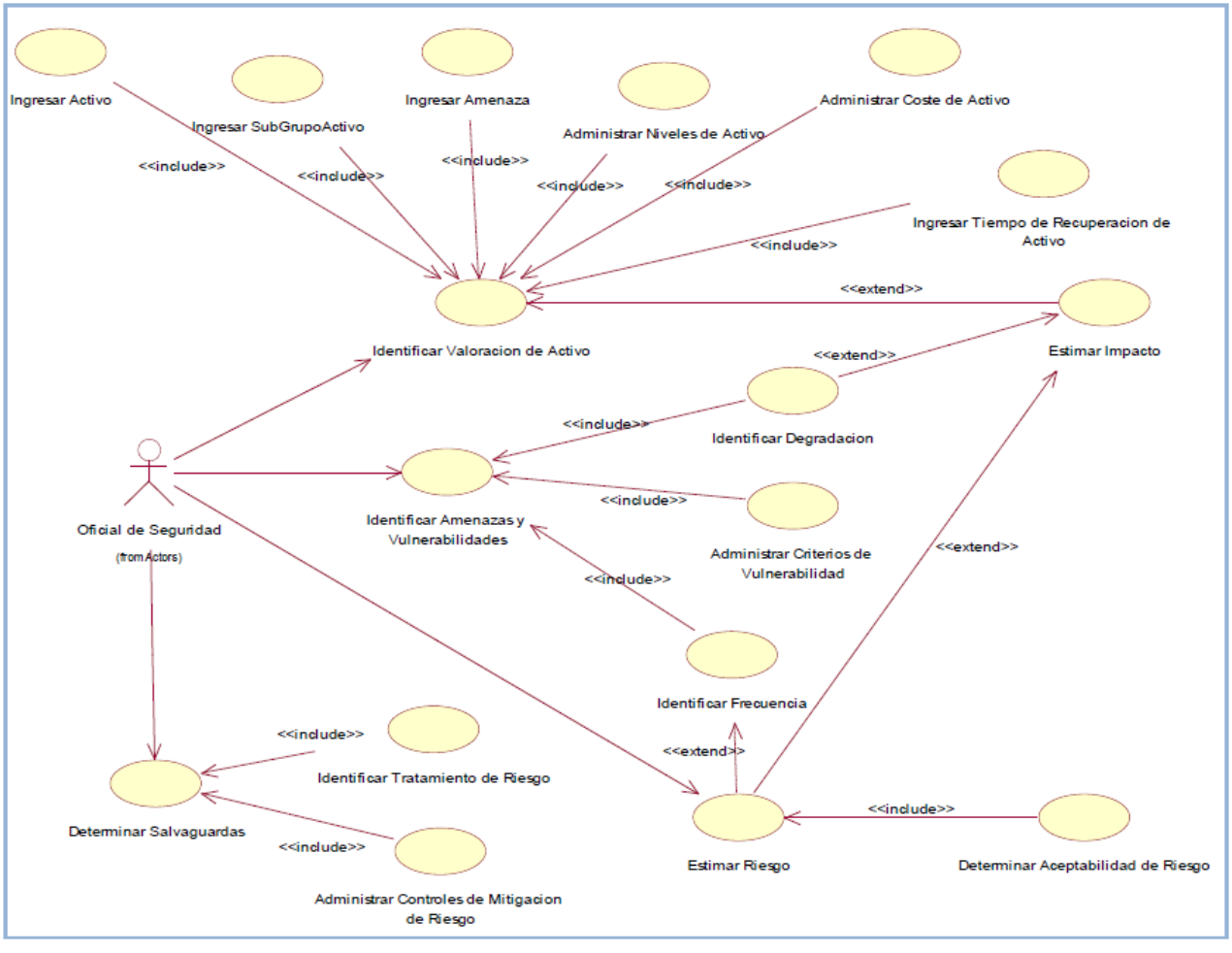


Fig. 15. Diagrama CUS. Análisis de Riesgo;

Fuente: Propia.

5.3.3.2 Casos de Uso por Paquetes: Gestión de Riesgo

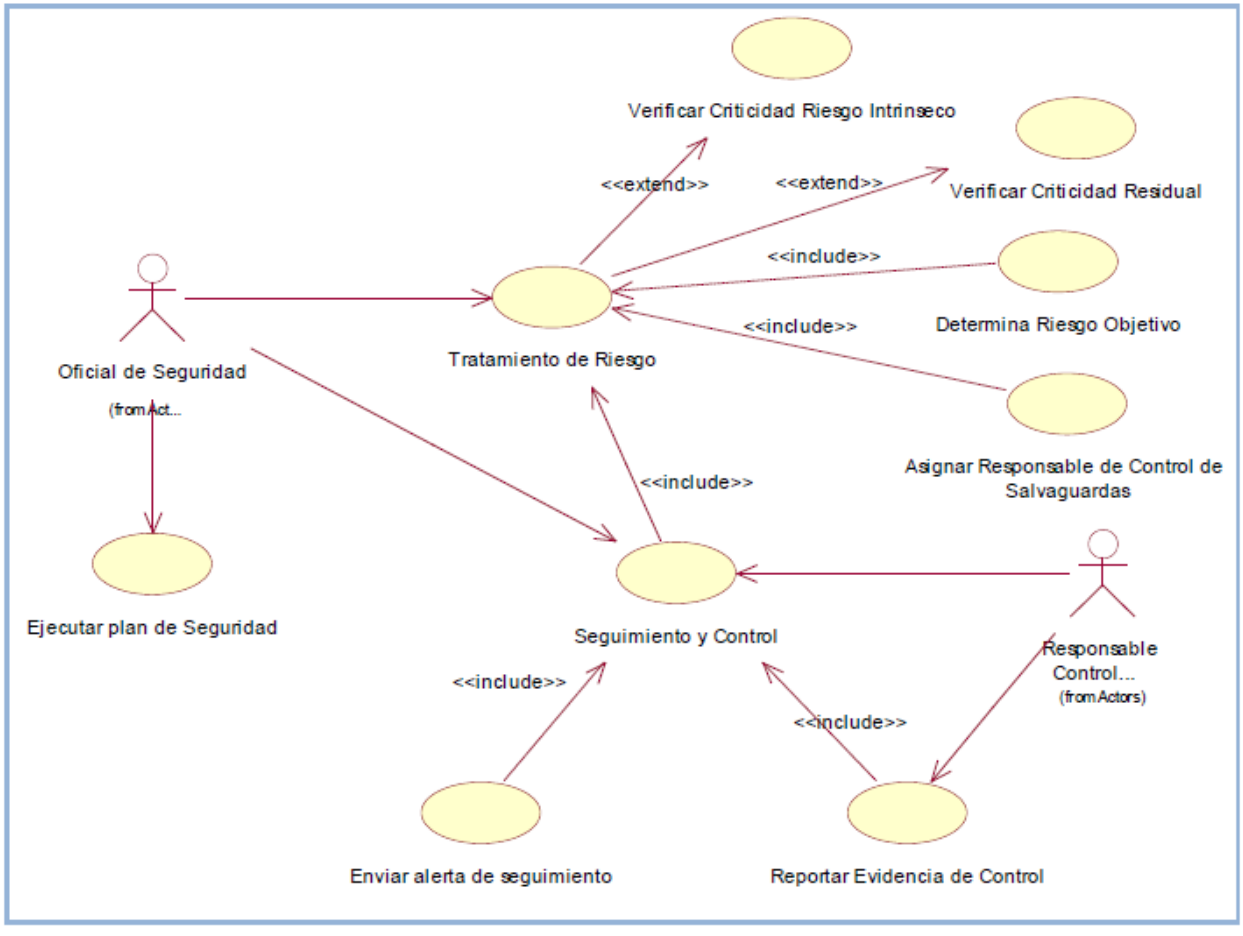


Fig 16. Diagrama de CUS. Gestión de Riesgo;

Fuente: Propia

5.3.3.3 Casos de Uso por Paquetes: Mantenimiento

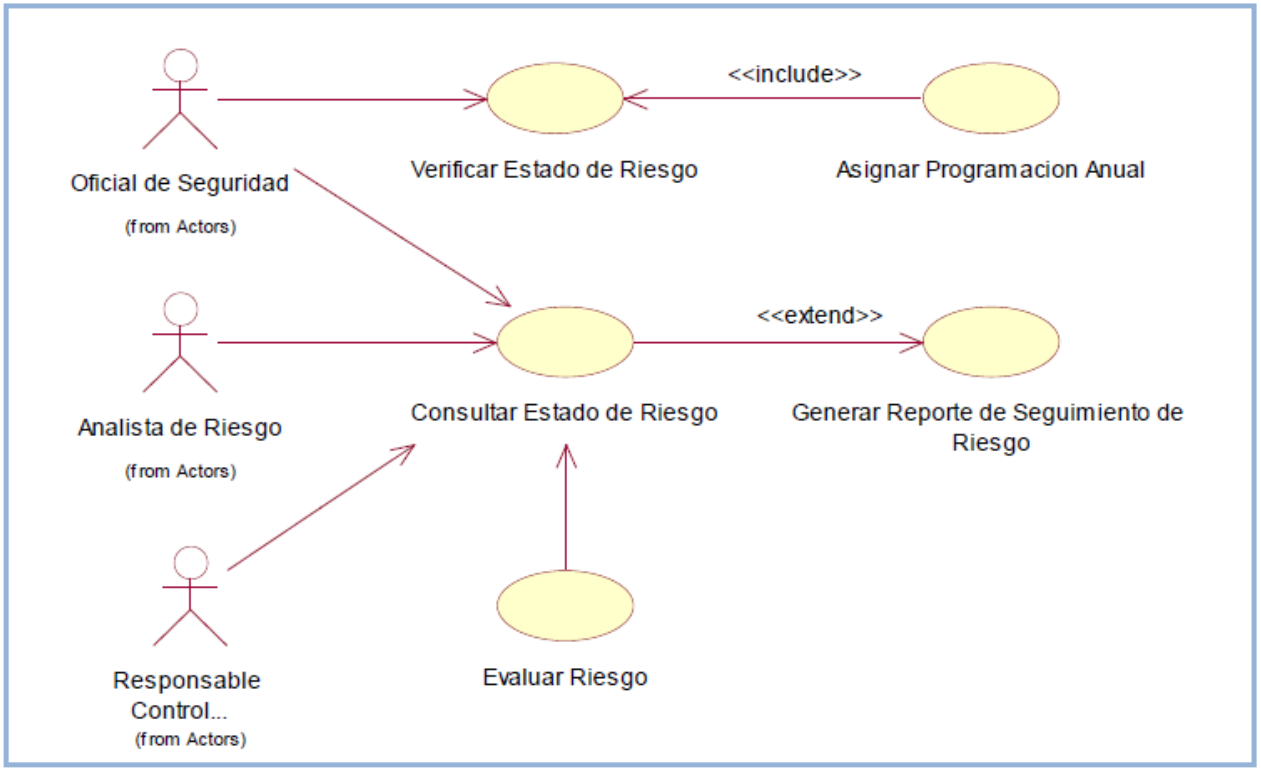


Fig 17. Diagrama de CUS. Mantenimiento;

Fuente: Propia.

5.3.3.4 Casos de Uso por Paquetes: Seguridad

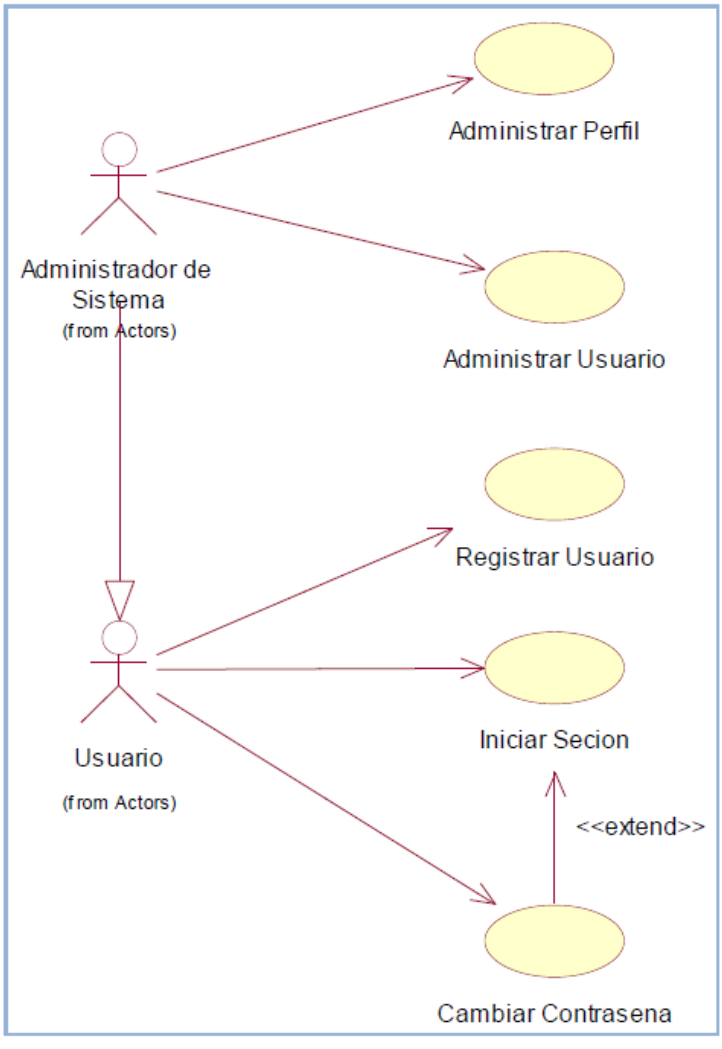


Fig. 18. Seguridad;

Fuente: Propia

5.3.4. Diagramas de Actividad

5.3.4.1 Diagramas de Actividad: Identificación de valoración de Activo

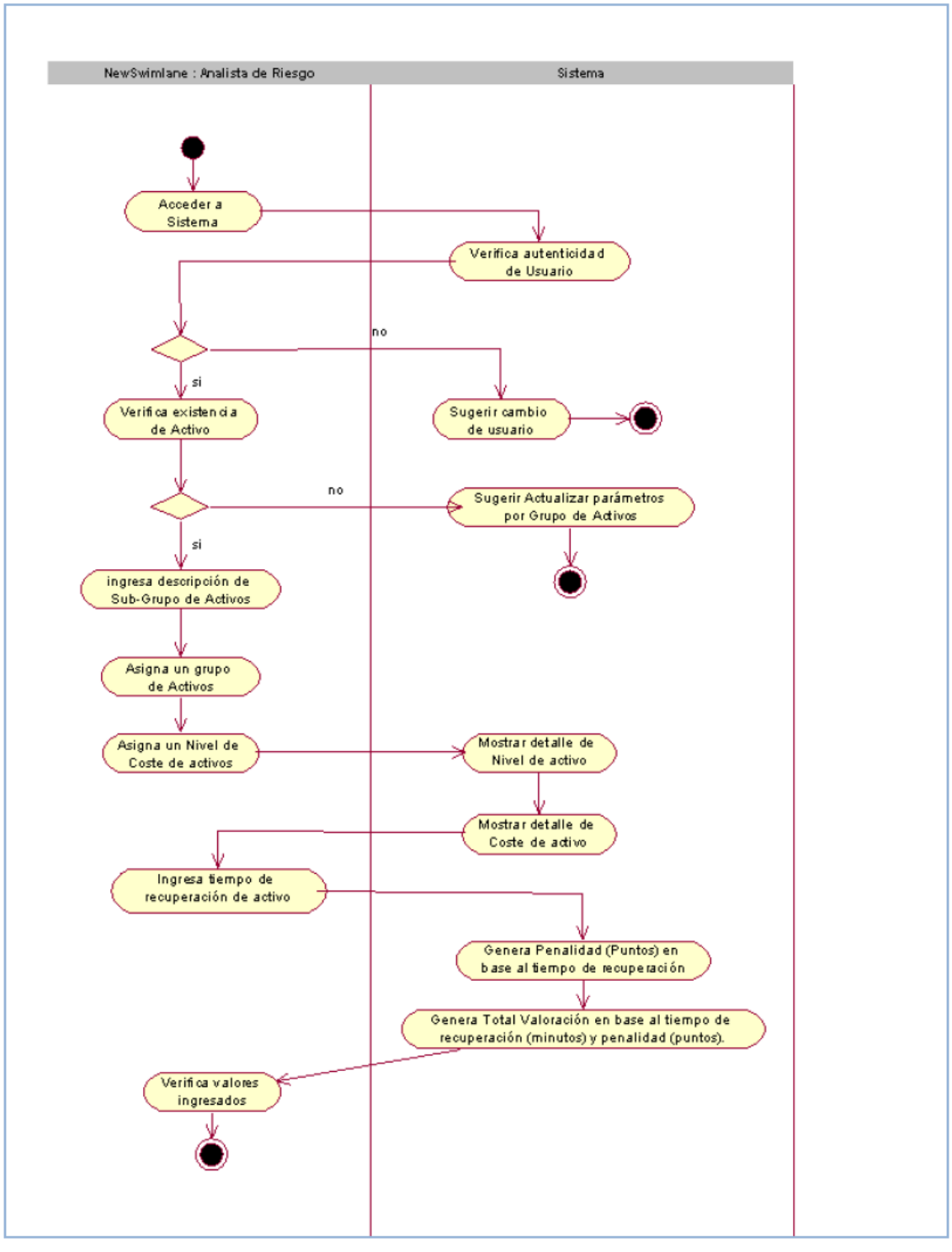


Fig 19. Diagrama de Actividad. Identificación de Activo;

Fuente: Propia.

5.3.4.2 Diagramas de Actividad: Registrar Salvaguardas

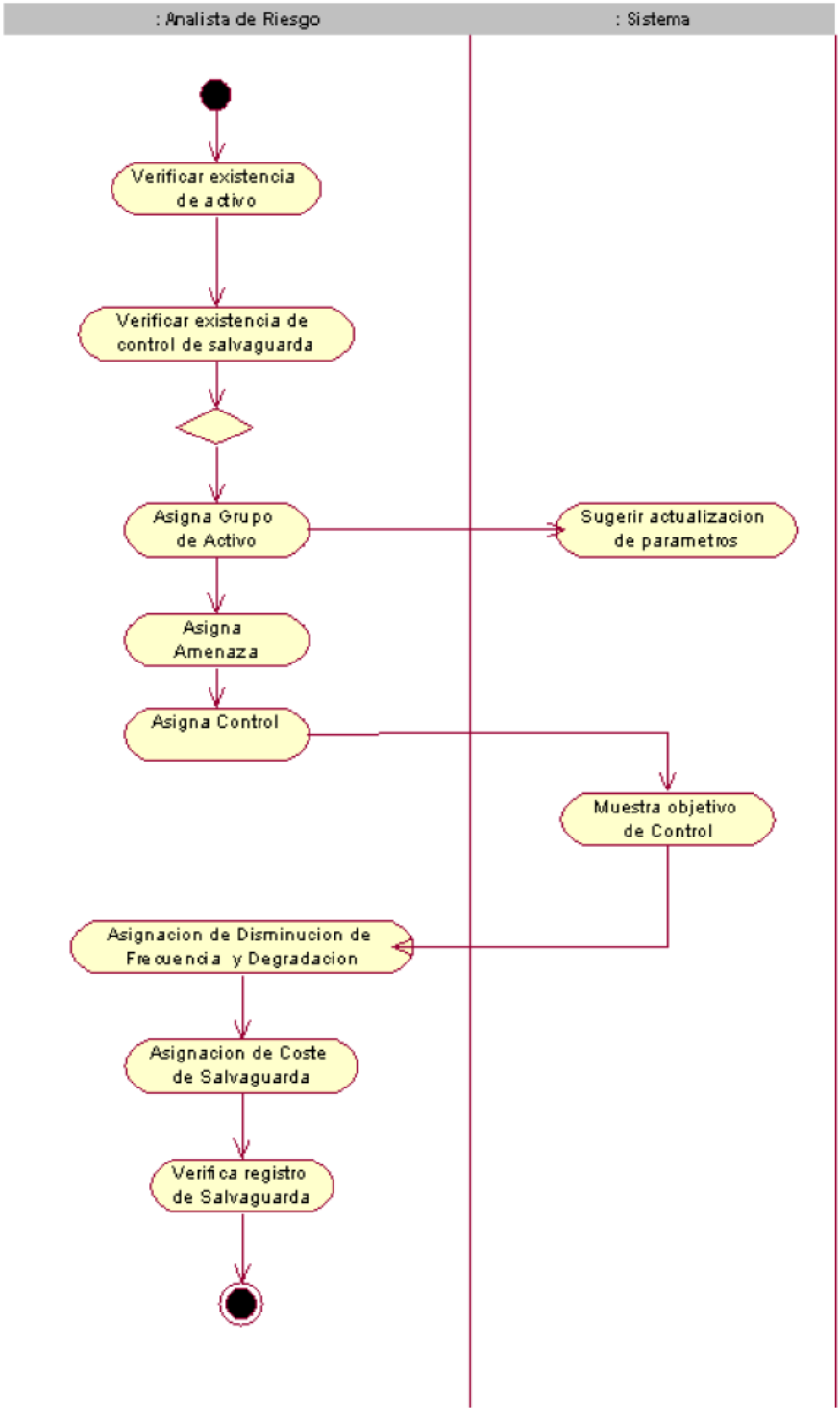


Fig. 20. Diagrama de Actividad. Registrar Salvaguardas;

Fuente: Propia.

5.3.4.3 Diagramas de Actividad: Tomar Decisiones

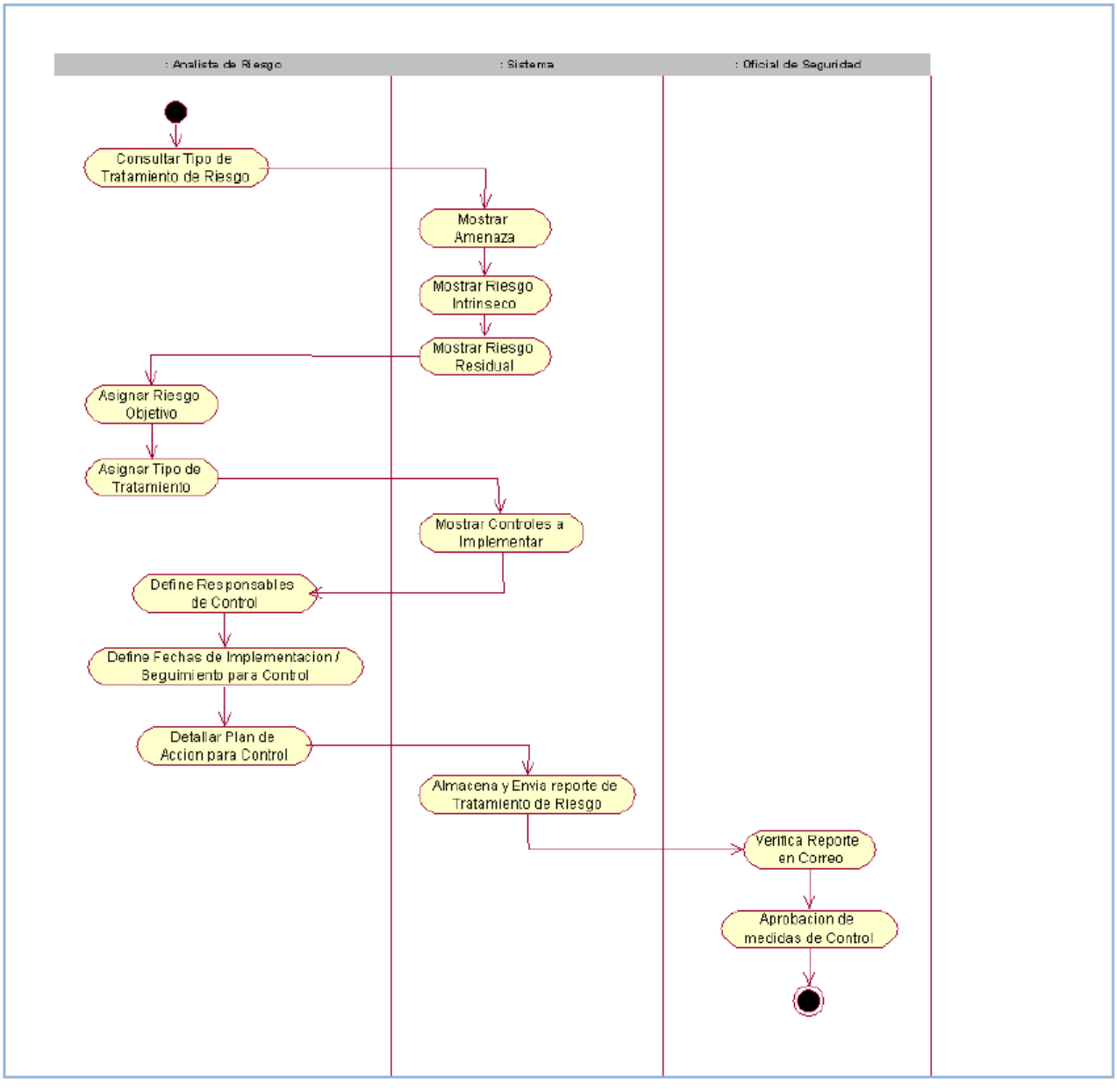


Fig. 21. Diagrama de Actividad. Tomar Decisiones;

Fuente: Propia.

5.3.5. Diagrama Secuencias

5.3.5.1 Diagrama Secuencias: Iniciar Sesión

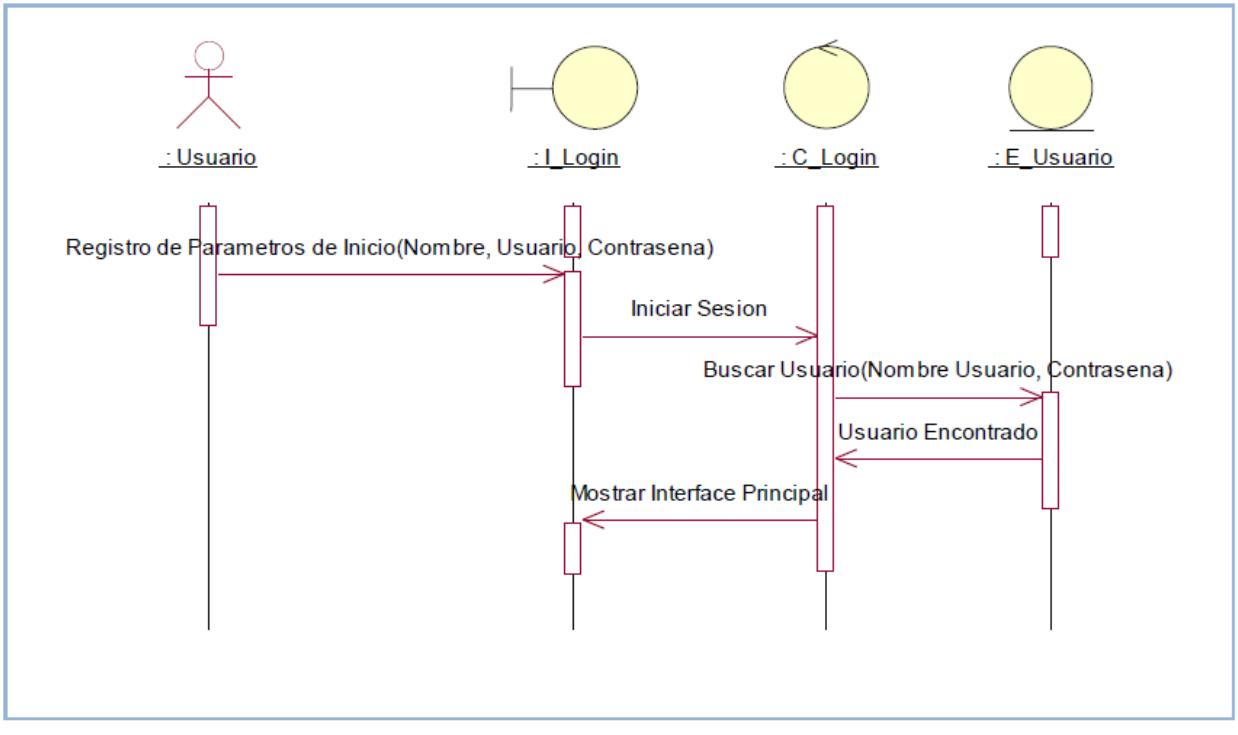


Fig. 22. Diagrama de Secuencia. Iniciar Sesión;

Fuente: Propia.

5.3.5.2 Diagrama Secuencias: Registrar Usuario

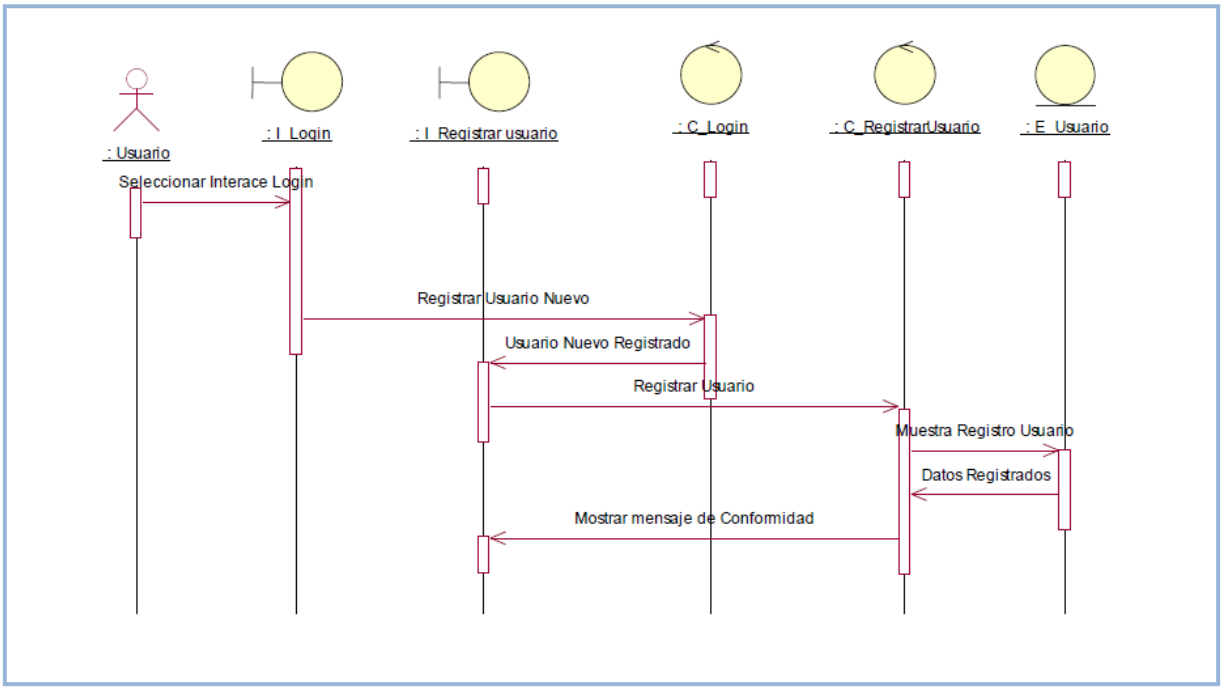


Fig. 23. Diagrama de Secuencia. Registrar Usuario;

Fuente: Propia.

5.3.5.3 Diagrama Secuencias: Identificar Valoración de Activo

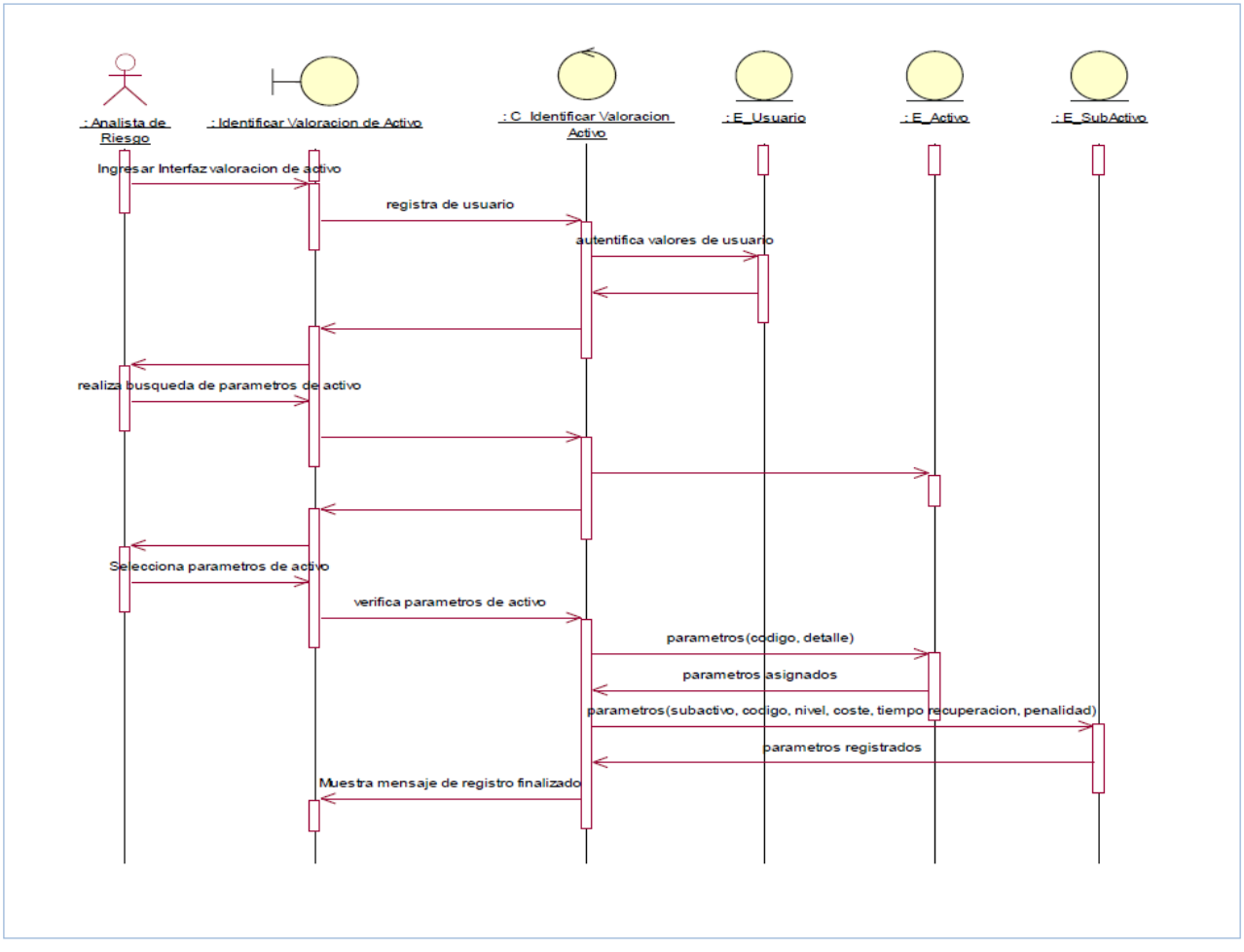


Fig. 24 CUS Identificar Valoración de Activo;

Fuente: Propia.

5.3.6. Diagrama Clases

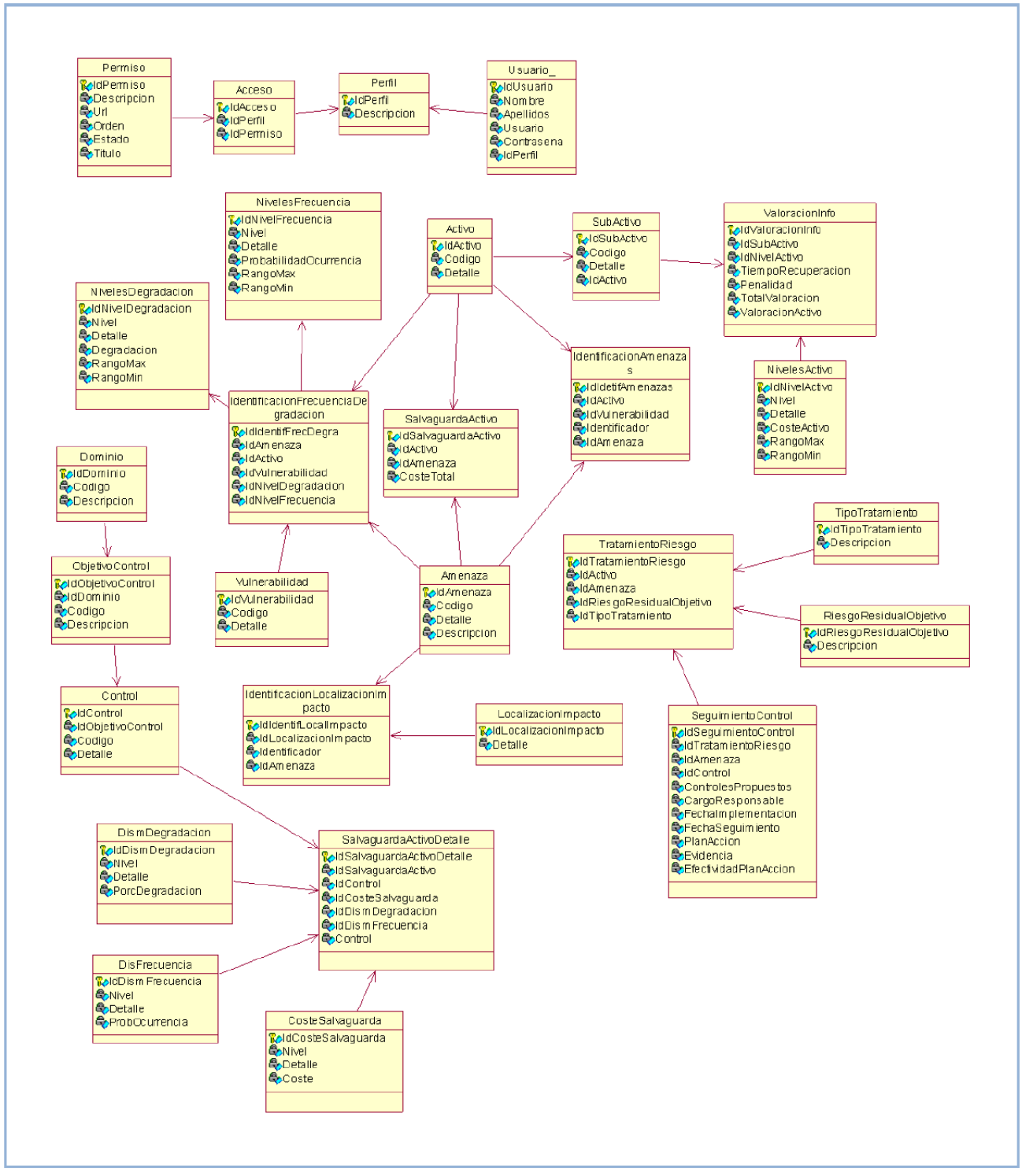


Fig. 25. Diagrama de Clases;

Fuente: Propia.

5.3.7. Modelo Conceptual

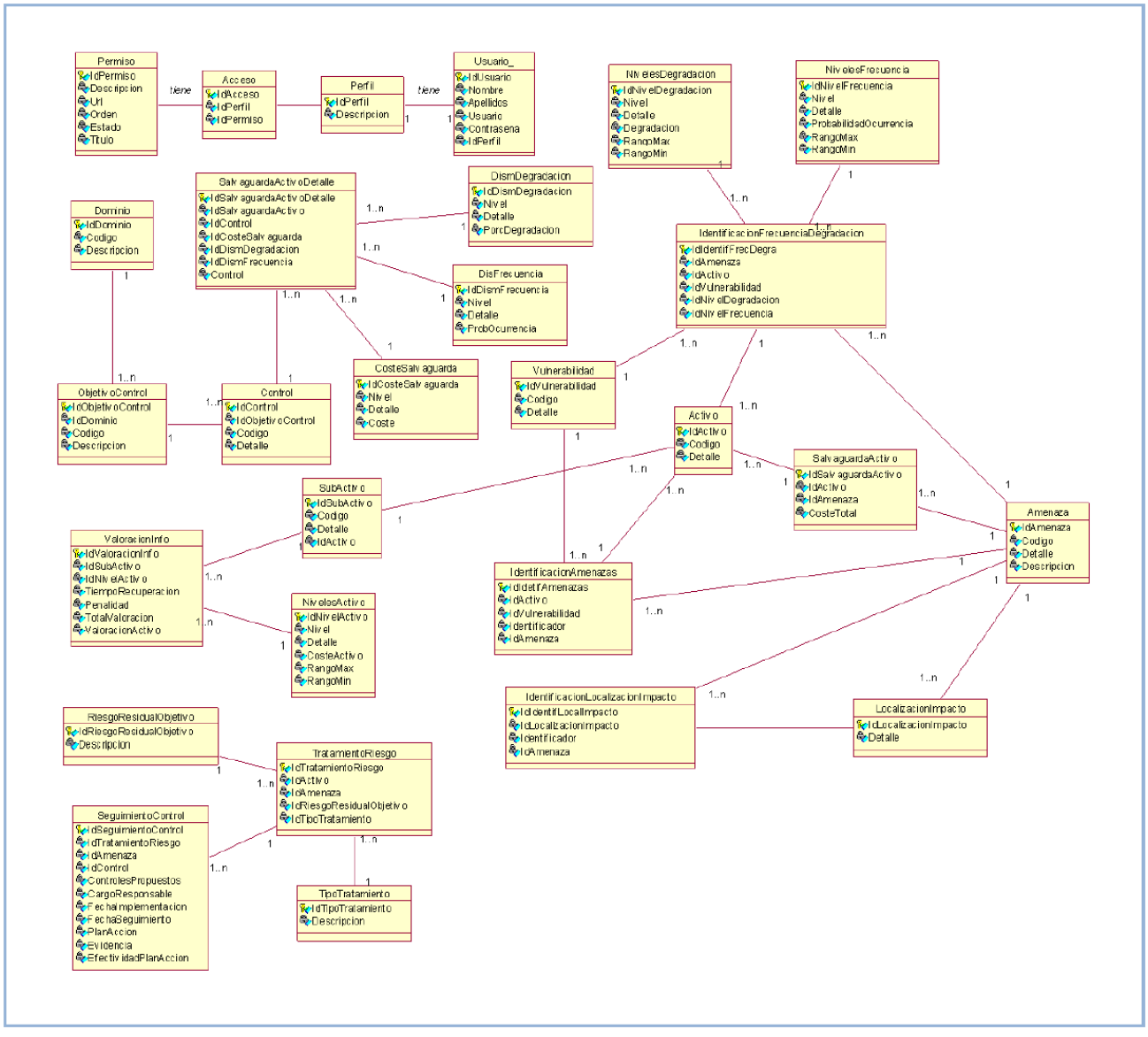


Fig. 26. Modelo Conceptual;

Fuente: Propia.

5.3.8. Diagrama de Componentes

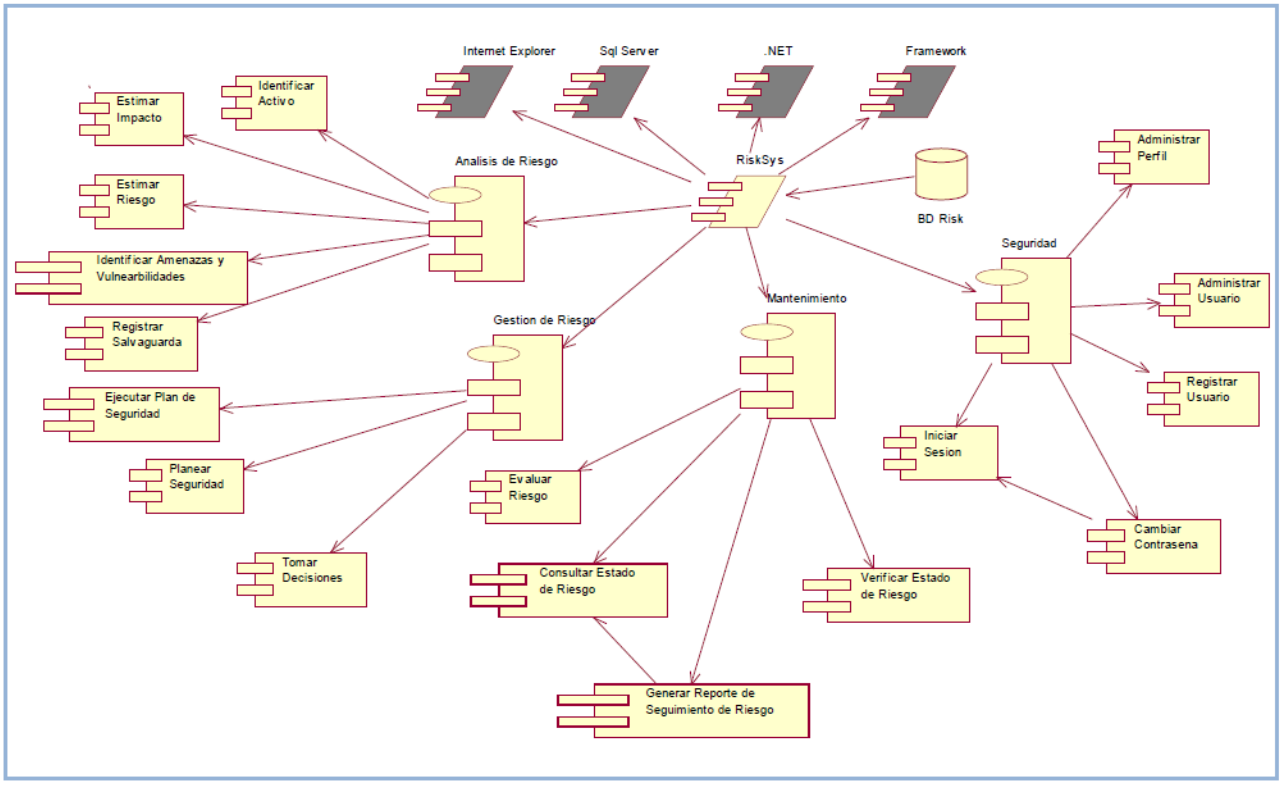


Fig. 27. Diagrama de Componentes;

Fuente: Propia.

5.3.9. Diagrama de Despliegue

Un Diagrama de Despliegue modela la arquitectura en tiempo de ejecución de un sistema. Esto muestra la configuración de los elementos de hardware (nodos) y muestra cómo los elementos y artefactos del software se trazan en esos nodos.

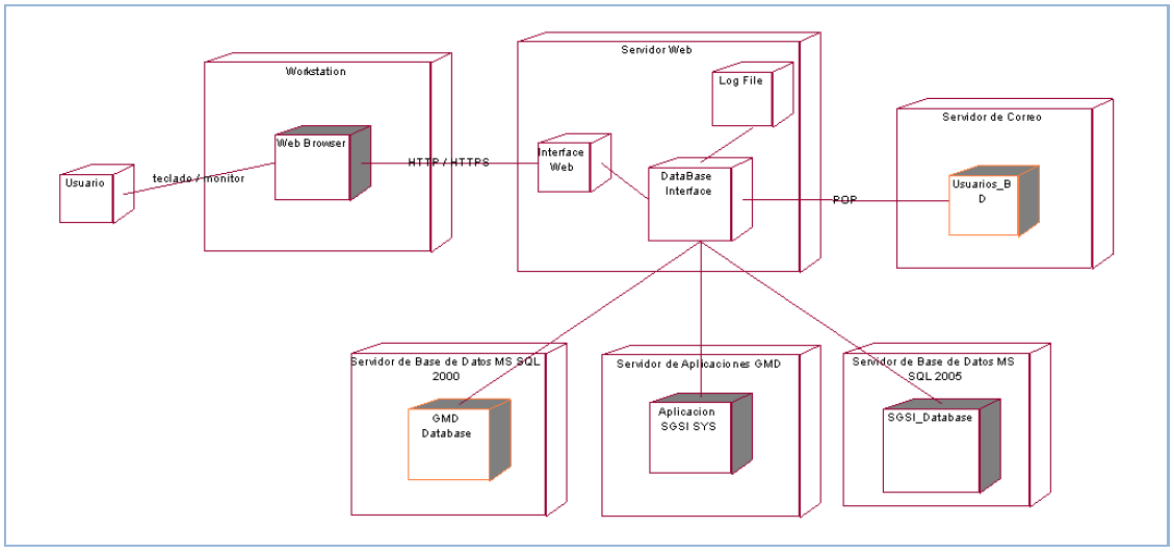


Fig. 28. Diagrama de Despliegue. Muestra el desempeño del sistema en ejecución;
Fuente: Propia.

1. Usuario: Este elemento al desear hacer uso de nuestra aplicación WEB, mediante el acceso desde su PC.
2. Workstation: Este elemento sirve como herramienta para intercambiar datos de tipo información entre el usuario y aplicaciones tales como nuestra aplicación Web.
3. IIS Web Server: Este elemento es un programa que está diseñado para transferir hipertextos, páginas web o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música. El programa implementa el protocolo HTTP (HyperText Transfer Protocol). El término también se emplea para referirse al ordenador que ejecuta el programa.
4. Web Browser: Es un programa que permite visualizar la información que contiene una página web (ya esté alojada en un servidor dentro de la World Wide Web o en uno local). El navegador interpreta el código, HTML generalmente, en el que está escrita la página web y lo presenta en pantalla permitiendo al usuario interactuar con su contenido y navegar hacia otros lugares de la red mediante enlaces o hipervínculos.
5. SGSI_SYS: Es el programa que sirve como herramienta para el gestión de riesgos y base de nuestro proyecto de tesis.
6. Database Interface: Describe el modelo de base de datos y muestra el camino de cómo comunicar, modificar y recuperar la información contenida en ella.
7. Log file: Datos en el computador, que se almacenan los eventos, así como accesos a la información y manipulación de ella.
8. Database Server: Un servidor de base de datos es un programa que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor.
9. SGSI_Database: En el cual estaría ubicada la información relacionada a nuestra aplicación para la gestión de riesgos.

CAPITULO VI: EVALUACIÓN DEL SISTEMA

6.1. Epílogo

Las pruebas se presentaron a lo largo de todo el ciclo de vida de nuestro desarrollo de software, pasando por requerimientos, análisis y diseño, programación, puesta en marcha y mantenimiento.

El esquema de pruebas de requerimientos se muestra de manera general, mientras que del esquema de pruebas de análisis y diseño, de puesta en marcha y de mantenimiento se presentan en los casos más representativos de nuestro producto.

6.2. Introducción

En el mundo de la computación tan cambiante de hoy en día, y sobre todo de gran evolución tecnológica, y en vista de las exigencias que ha traído la globalización, se ha hecho necesario desarrollar metodologías para asegurar la calidad de los productos de software y obtener un mejoramiento continuo de todos los procesos relacionados con el desarrollo de software. Entre tantas metodologías, se pueden mencionar: CMMI (Capability Maturity Model Integration). Vale la pena aclarar que CMMI es un esquema de diagnóstico y de evaluación de la madurez del proceso de desarrollo de software, más que un esquema de mejoramiento de procesos.

A continuación, se presenta el proceso de diseño y ejecución de pruebas de software (básicamente pruebas de programación) que se ha definido para nuestro proyecto de tesis.

6.3. ¿Cómo llegar a la definición del esquema de Pruebas de Software?

CMMI, provee una guía de cómo obtener el control del proceso de desarrollo y mantenimiento de software, de cómo llevar nuestros procesos. La Figura 28 muestra el esquema general de cinco niveles de madurez del proceso de software propuesto por CMMI, y la Figura 29 revela la estructura de cada nivel de madurez.

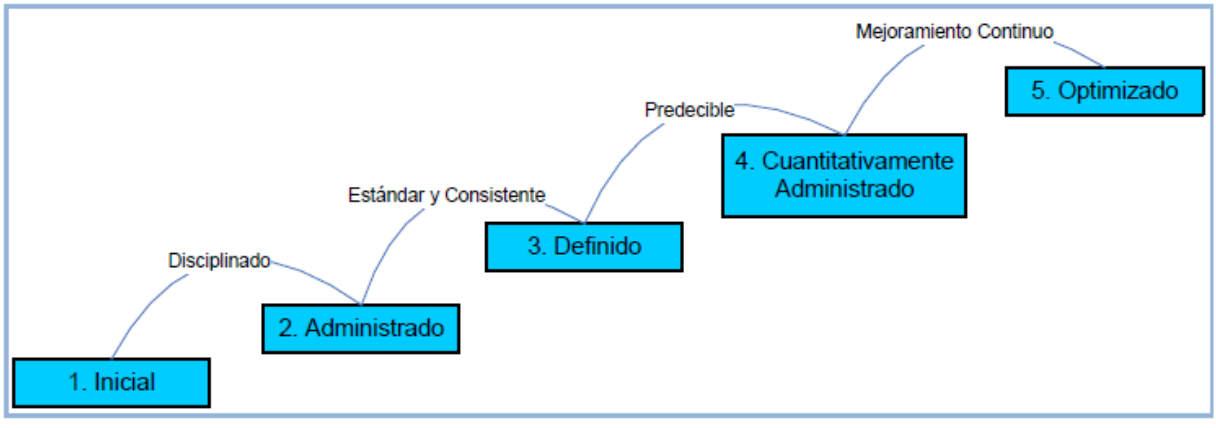


Fig. 28. Niveles de madurez del proceso de software;

Fuente: [3] Software Engineering Institute.

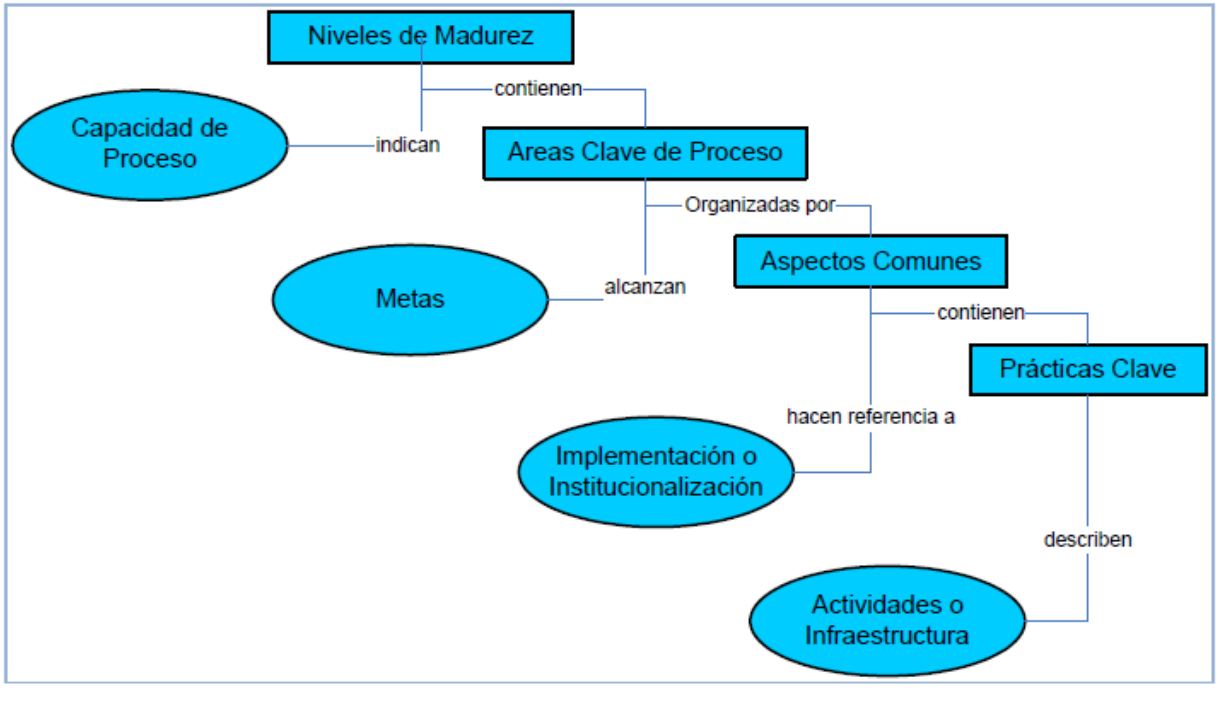


Fig. 29. Estructura de los niveles de madurez de CMM;

Fuente: [3] Software Engineering Institute.

Como se ha mencionado anteriormente, se ha revisado el esquema propuesto por CMMI para determinar el estado actual de nuestro proceso de desarrollo de software, y establecer las acciones a tomar en búsqueda de alcanzar un mayor nivel de madurez en nuestro proceso.

6.4. Diseño y ejecución de las pruebas de software

El sistema propuesto es una herramienta para obtener medidas de salvaguardas para posibles riesgos en proyectos informáticos y qué medidas se tomaron a consecuencia de ese análisis y así sobrellevar las posibles amenazas, basadas en la información acumulada de proyectos de trabajos anteriores.

La prueba es un elemento crítico para la calidad del software en nuestro sistema.

Las pruebas que se consideró, dentro del plan de pruebas, son las siguientes:

- Pruebas de requerimientos.
- Pruebas de análisis.
- Pruebas de diseño.
- Pruebas de unidad.
- Inspecciones.
- Pruebas de información no periódica.

La Figura 30 muestra, gráficamente, las pruebas de software realizadas.

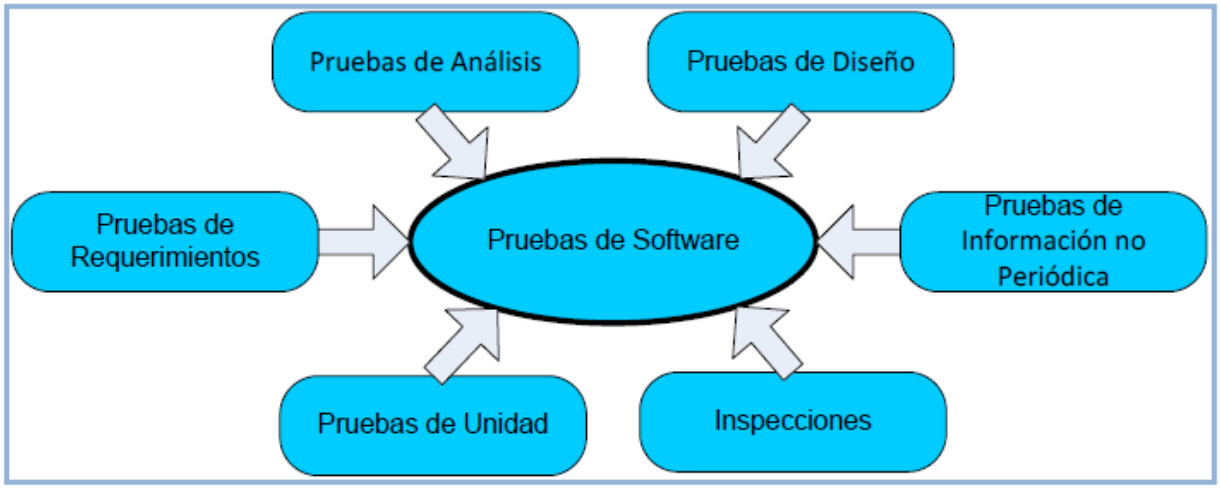


Fig. 30. Pruebas de software consideradas;
Fuente: [3] Software Engineering Institute.

6.4.1. Pruebas de Requerimientos

Los requerimientos de software en nuestro sistema tienen una explicación clara, precisa y completa del problema, que facilitó el análisis de errores y la generación de casos de prueba. Un asunto de gran importancia fue asegurar la corrección, coherencia y exactitud de los requerimientos del usuario.

Durante el proceso de provisión de requerimientos, una persona, revisó el documento de especificación de requerimientos, con la lista de chequeo general del documento y la lista de chequeo de requerimientos.

La corrección del contenido del documento fue responsabilidad del analista y el líder de proyecto, quienes son los encargados de aprobar los requerimientos definidos en el documento.

El diagrama del proceso de provisión de requerimientos se muestra en la Figura 31, y el detalle del mismo en la Cuadro 4, que se presentan a continuación.

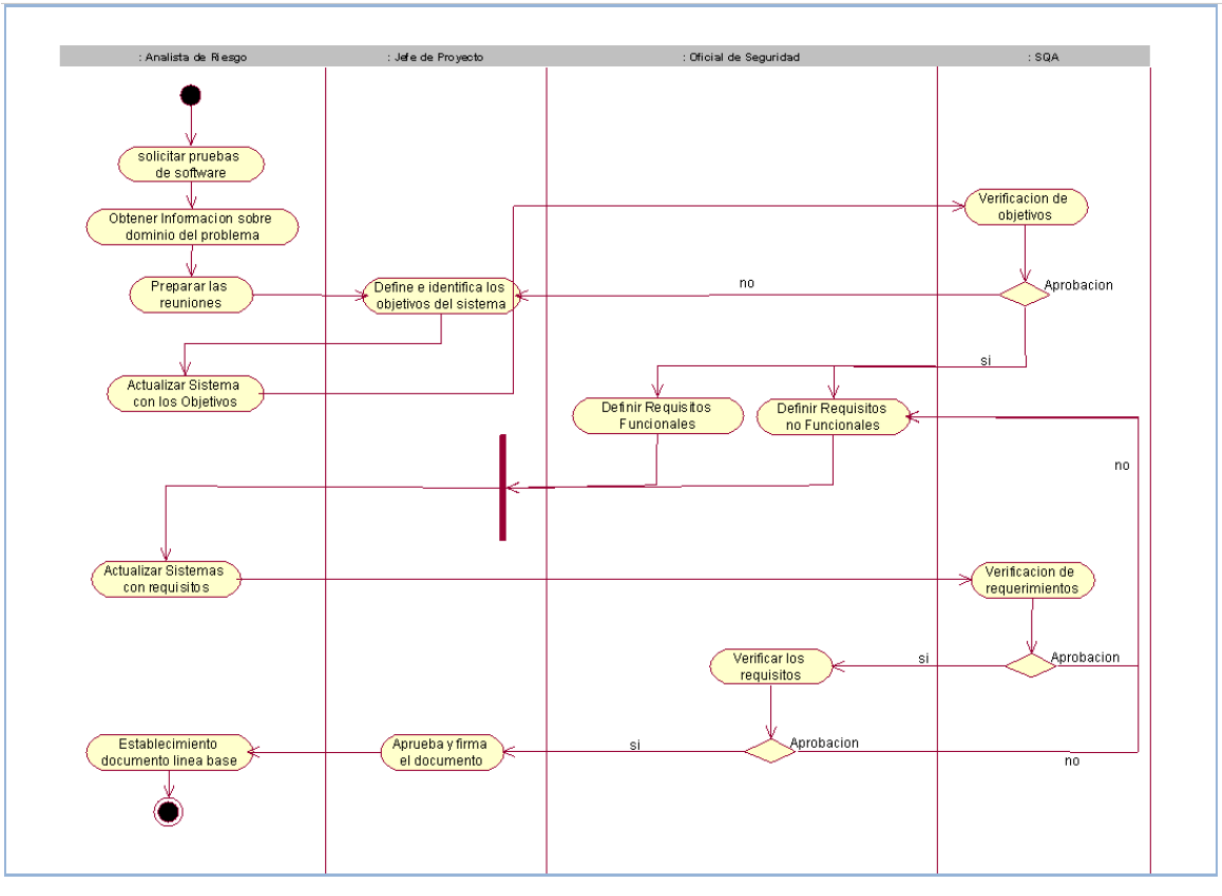


Fig. 31. Proceso de provisión de requerimientos;
Fuente: Propia

Detalle	Encargado	Recursos
Se determinó si los objetivos son claros, verificables y necesarios (entre otros). El resultado de esta revisión se consigna en la lista de chequeo de objetivos.	Revisor SQA	Lista de chequeo de objetivos
Mediante un proceso iterativo se definió la funcionalidad esperada del software, y se consignó usando el documento de requerimientos del sistema.	Especificador de requerimientos	Requerimientos del sistema
Se verificó el documento de requerimientos, usando la lista de chequeo general del documento de especificación de requerimientos lista de chequeo general del documento de provisión y análisis de requerimientos.	Revisor SQA	Lista de chequeo general del documento de provisión y análisis de requerimientos
Revisan cada requerimiento (consistencia, ambigüedad, etc.), usando para ello la lista de chequeo de requerimientos.	Revisor SQA	Lista de chequeo de Requerimientos.

Cuadro 6. Detalle del proceso de provisión de requerimientos;

Fuente: Propia.

6.4.2. Pruebas de Unidad

El proceso de pruebas de unidad se describe en el siguiente diagrama de la Figura 32, así como el detalle del mismo en la Cuadro 5.

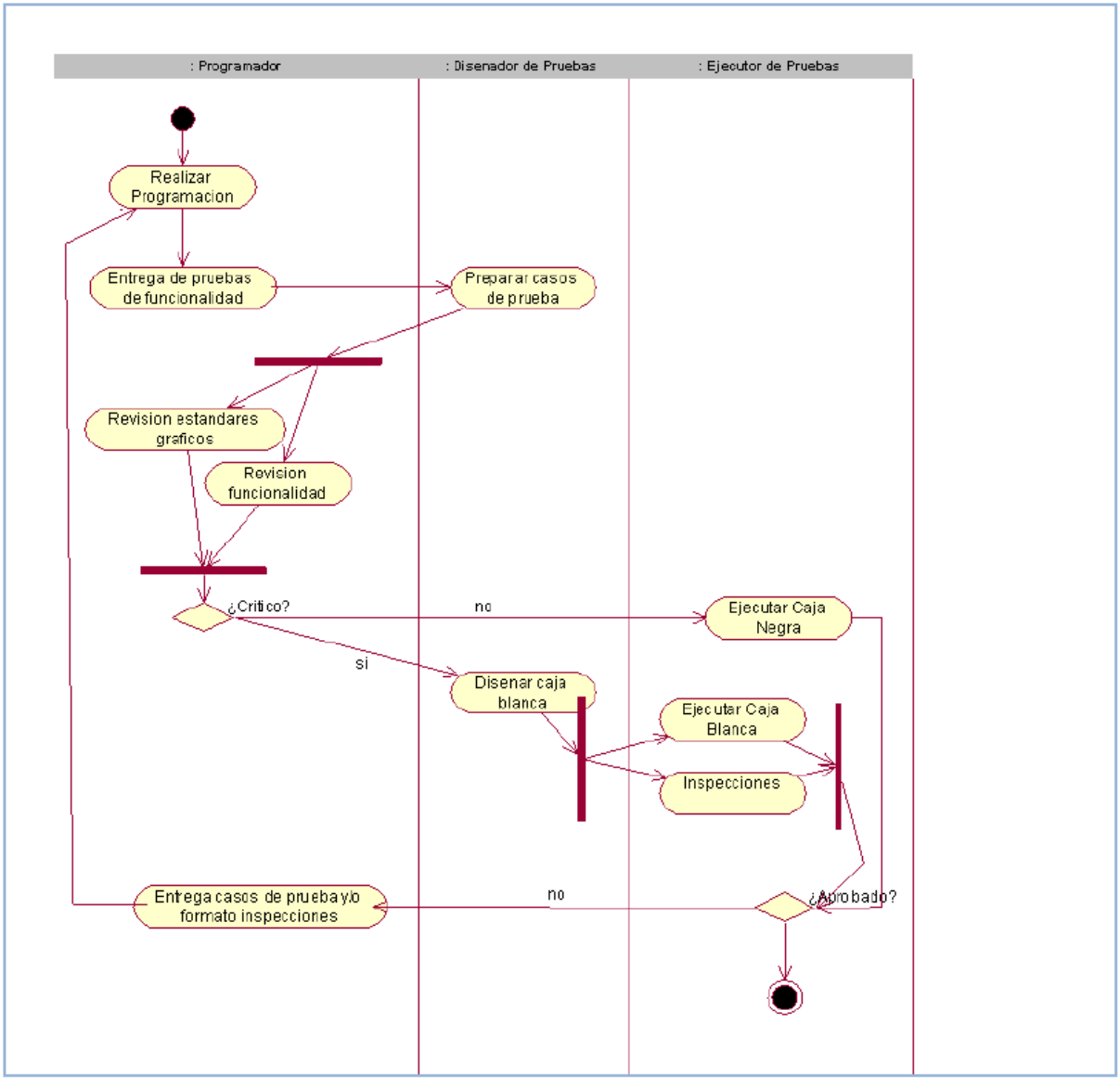


Fig. 32. Proceso de pruebas de unidad;

Fuente: Propia.

1. Preparación de Casos de Prueba				
	Detalle	Restricciones	Encargados	Recursos
	El encargado de elaborar los casos de prueba recibe del analista el diseño de la forma/reporte y una descripción de la funcionalidad, usando el formato de pruebas de funcionalidad. Así mismo, el diseñador de los casos de prueba debe recibir las listas de chequeo de programación ya revisadas por el analista/ Programador (Ver Anexos 4, 5, 6, y 8).	Formato de pruebas de funcionalidad (Ver Anexo 9).	Analista diseñador de casos de prueba.	Antton Cavalcanti
	Si el módulo es nuevo, se elabora el árbol de clases equivalentes, la tabla de particiones y un listado de casos de prueba. Si el módulo no es nuevo, deben revisarse los documentos de caja negra para establecer los cambios, que pueden ser: i. Eliminación de entradas, lo cual significa que se deben revisar todos los casos de prueba que incluyan estas entradas para modificarlos apropiadamente. También es posible que se eliminen algunos casos de prueba. ii. Inclusión de entradas, lo cual significa revisar los casos de prueba existentes y adicionar nuevos casos. iii. Eliminación/Inclusión de salidas: implica revisar los casos de prueba para establecer los cambios.	Formato de pruebas de funcionalidad (Ver Anexo 9).	Diseñador de casos de prueba.	Antton Cavalcanti
	Cada caso de prueba debe dejarse documentado y se debe ingresar esta información en el sistema.	Formato de pruebas de funcionalidad (Ver Anexo 9).	Diseñador de casos de prueba.	Antton Cavalcanti
2. Revisión de Estándares gráficos				
	Se Realizó la revisión indicada en la lista de chequeo de estándares, y dejar consignados los resultados y la fecha de la revisión en el sistema.	Lista de chequeo de presentación de formas (Ver Anexo 7)	Analista	Antton Cavalcanti
3. Revisión de funcionalidad				
	Se comprobó que se cumpla lo establecido en la lista de chequeo de funcionalidad de formas o reportes, según corresponda. Dejar documentado el resultado y la fecha de realización de esta actividad en el sistema.	Lista de chequeo de funcionalidad de aplicaciones formas (Ver Anexo 2) Lista de chequeo de funcionalidad de aplicaciones – reportes (Ver Anexo 3)	Analista	Antton Cavalcanti

4. Ejecución de pruebas de caja negra				
	Detalle	Restricciones	Encargados	Recursos
	El ejecutor debió contar con el módulo desarrollado y tener todos los permisos que tendría el usuario final. Además, debe contar con los casos de pruebas diseñados.		Ejecutor de pruebas.	Antton Cavalcanti
	Se deben ejecutar todos los casos de prueba y consignar los resultados obtenidos en el formato.	Formato de resultados de ejecución de pruebas.	Ejecutor de pruebas.	Antton Cavalcanti
5. Diseño y ejecución de pruebas de caja blanca [opcional]				
	Preparación de los casos de prueba. El analista proporciono el código de la función y el cálculo de la complejidad.		Diseñador de pruebas.	Antton Cavalcanti
	Se estableció la lista de casos de prueba y se documenta cada uno.		Diseñador de pruebas.	Antton Cavalcanti
	Se ejecutó las pruebas para cada caso encontrado y se obtuvo los resultados.		Ejecutor de pruebas.	Antton Cavalcanti
6. Inspecciones [opcional]				
	Se realizó la inspección siguiendo la lista de chequeo y anotando los errores encontrados en el formato.	Inspecciones-Registro de defectos.	Revisor Moderador Analista	Antton Cavalcanti
	Se realizó la reunión de inspección, orientada por el moderador. El revisor y el moderador exponen los errores hallados.		Revisor Moderador	Antton Cavalcanti
	El analista aclara las dudas o indica si hubo un error de apreciación		Analista	Antton Cavalcanti
	Se consignan los resultados consolidados de la inspección y se entregan al analista.		Moderador	Antton Cavalcanti

Cuadro 7. Detalle del proceso de pruebas de unidad;

Fuente: Propia

6.4.3. Inspecciones

El objetivo de las inspecciones fue implementar un proceso formal de revisión detallada del producto por parte de pares (Analistas y programadores del área) y un moderador (Jefe de Calidad GMD), con el propósito de encontrar defectos en una etapa muy temprana del desarrollo del producto. El diagrama de la Figura 33 muestra el proceso de inspecciones.

El detalle de dicho proceso se encuentra en la Cuadro 5.

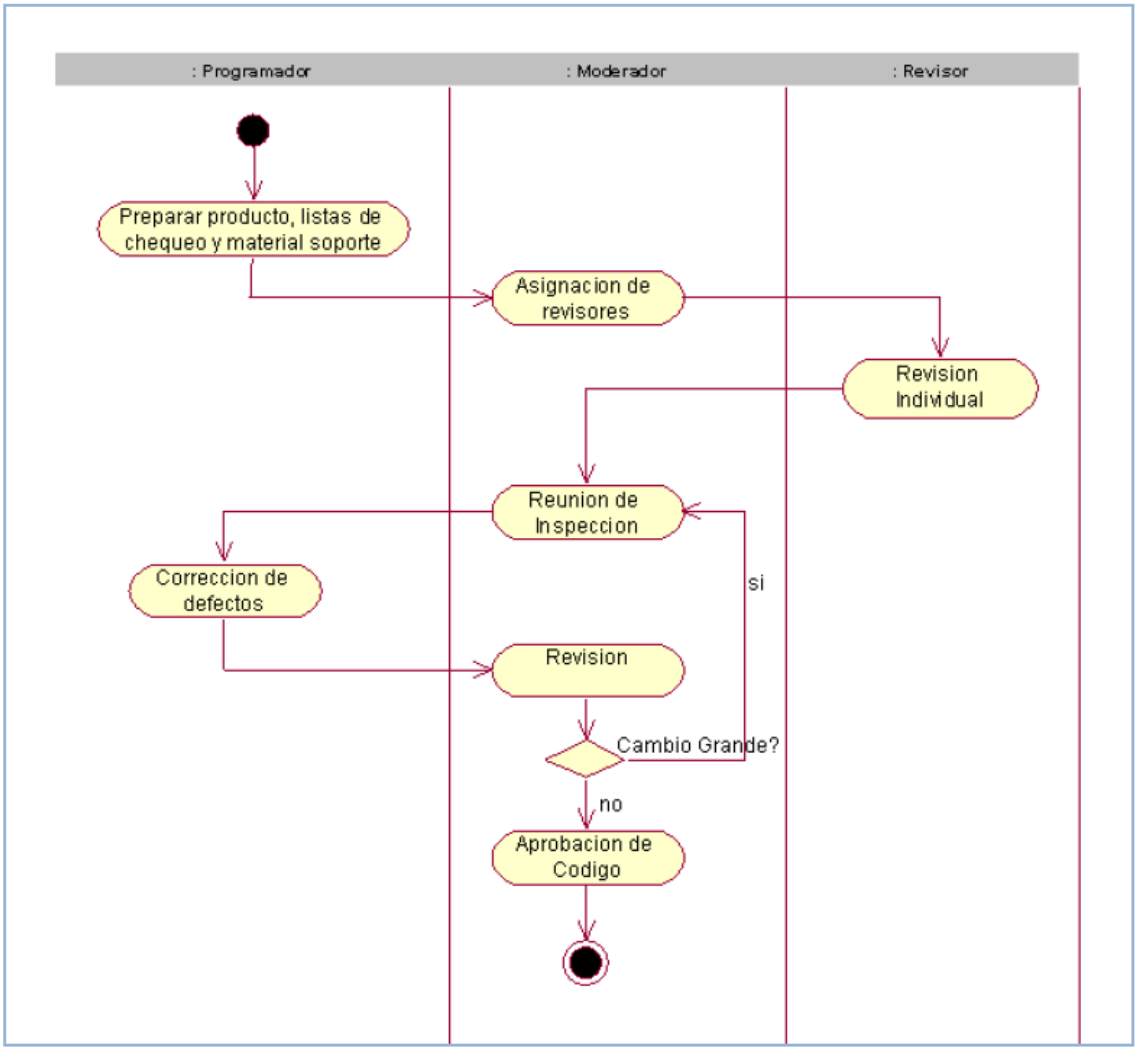


Fig. 33. Proceso de inspecciones.

Fuente: Propia.

1. Elaborar documentos para inspección				
	Detalle	Restricciones	Encargados	Recursos
	El analista preparó los siguientes elementos para la inspección: — Código fuente (líneas numeradas o identificación de cada sub-módulo). — Material de soporte, como descripción de la funcionalidad. — Lista de chequeo para inspecciones.	Formato de inspecciones– Registro de defectos.	Analista	Antton Cavalcanti
	2. Asignación de revisores			
	El moderador asignó revisor para este módulo, con experiencia en desarrollo de programas en el lenguaje en el cual se elaboró el módulo a evaluar o, si esto no es posible, con en programación en general.	Uno de los revisores debe de ser de un proyecto diferente al del producto inspeccionado.	Moderador	Antton Cavalcanti
	Una vez asignados los revisores, se les entrega una copia del material que presentó el analista y el formato para consignar los resultados de la inspección.		Moderador	Antton Cavalcanti
	Se estableció una fecha de reunión y se indica esta fecha a los revisores y al analista.		Moderador	Antton Cavalcanti
	3. Revisión individual			
	Se realizó la inspección siguiendo la lista de chequeo y anotando los errores encontrados en el formato.	Formato de inspecciones. Registro de defectos.	Revisor Moderador	José Luis Sandoval Antton Cavalcanti
	4. Reunión de Inspección			
	El moderador dirigió esta reunión, haciendo que el revisor (y él mismo) expongan brevemente los errores encontrados.		Moderador Revisor	José Luis Sandoval
	El analista aclara dudas o indica si hay un error de apreciación por parte de los revisores, pero no puede tratar de dar explicaciones sobre algún error o indicar formas de corregirlo.		Analista	Antton Cavalcanti
	El moderador consigna en el formato los resultados consolidados de la inspección y los pasa el analista.		Moderador	José Luis Sandoval

Cuadro 8. Detalle del proceso de inspección;

Fuente: Propia

6.4.4. Pruebas de Información no periódica

La Figura 34 muestra el diagrama del proceso de pruebas de información no periódica. El detalle del proceso se encuentra en la Cuadro 7.

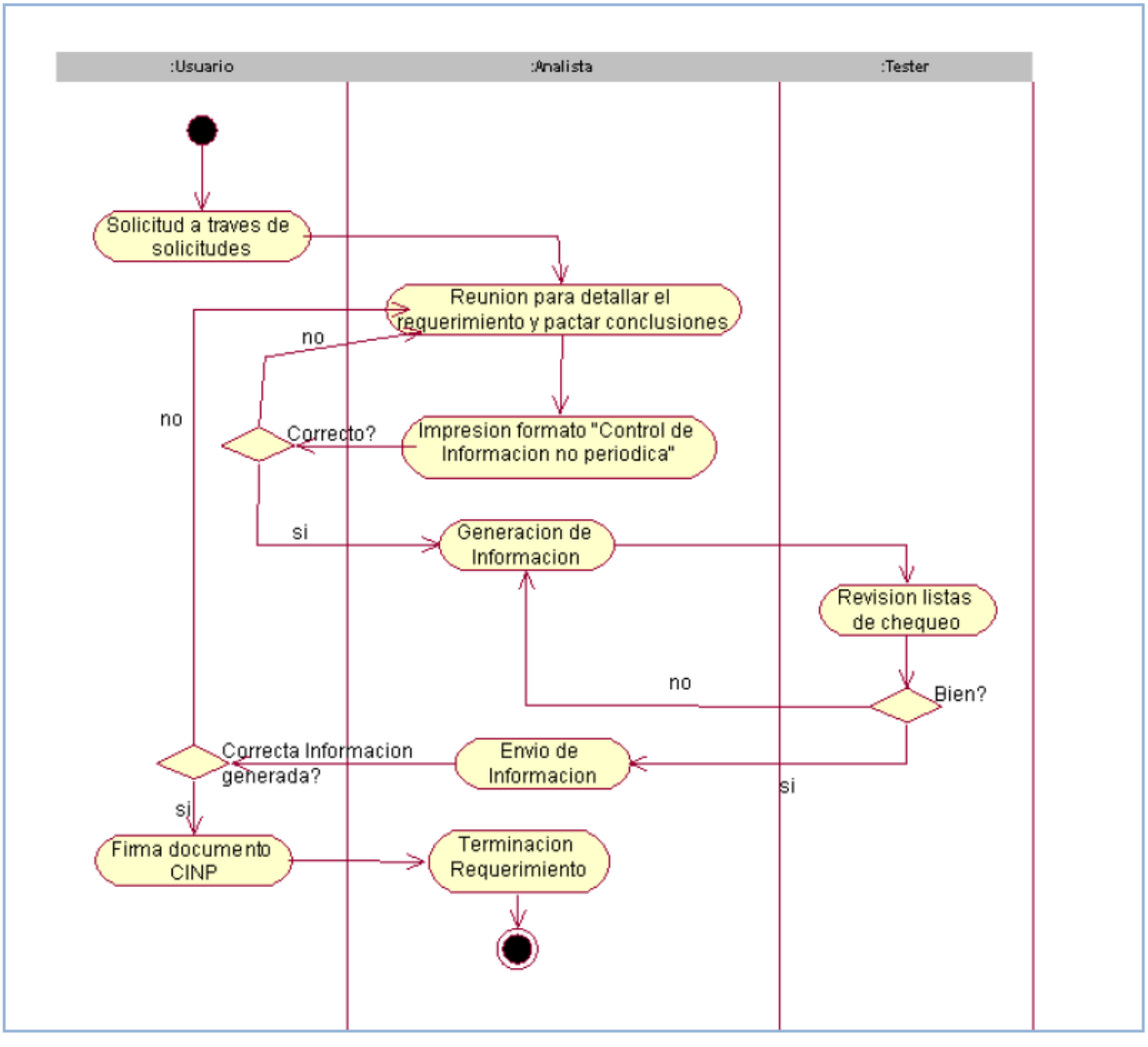


Fig. 34. Proceso de pruebas de información no periódica.

Fuente: Propia

1. Pruebas e inspecciones para información no periódica				
	Detalle	Restricciones	Encargados	Recursos
	Ingreso de la solicitud a través del correo.		Usuario	Antton Cavalcanti
	Reunión para detallar el requerimiento y pactar conclusiones.		Analista Usuario	Antton Cavalcanti
	Se imprime el formato de control de información no periódica:		Analista	Antton Cavalcanti
	El usuario verifica la información en el formato.		Usuario	
	Comprobado el formato, se genera la información pedida.		Analista	Antton Cavalcanti
	Revisión de las listas de chequeo.		SQA	Antton Cavalcanti
	Aprobada la información, se envía al usuario.		Analista	Antton Cavalcanti
	El usuario corrobora la información generada.		Usuario	Antton Cavalcanti
	Si la información es correcta, firma aprobación de documento.		Usuario	Antton Cavalcanti José Luis Sandoval
	Finaliza el requerimiento.		Analista	Antton Cavalcanti

Cuadro 9. Detalle del proceso de Pruebas para información no periódica.

Fuente: Propia

6.5. Autoevaluación en el proceso de pruebas

Las encuestas y evaluaciones son una herramienta de gran valor para medir la percepción y el conocimiento de las personas envueltas en el tema de evaluación de riesgos. Como parte de un proceso de concientización, evaluación y aprendizaje por mi parte, diseñe un formato de autoevaluación que permite determinar, en alguna medida, el conocimiento que se obtuvo del proceso de pruebas. Los resultados de mi autoevaluación sirven de retroalimentación dentro de mi proceso de pruebas de software, y son utilizados para direccionar las medidas que se tengan que tomar para solucionar los problemas identificados.

Determine si las siguientes afirmaciones fueron realizadas o no. En el caso de no haberlas verificado explique la razón		
Colocar (V) verificado o (x) no verificado, según sea conveniente.	(□)	(X)
1. ¿Se realizaron inspecciones verificando el cumplimiento de los requerimientos Funcionales?	✓	
2. ¿Antes de programar un módulo, se buscó conciliar la problemática del usuario?	✓	
3. ¿Al terminar de programar el modulo se buscó la verificación del usuario?	✓	
4. El analista, además de programar, estuvo involucrado en las siguientes actividades de pruebas: revisiones de funcionalidad, revisiones de estándares gráficos y aprobación del diseño gráfico por parte del usuario.	✓	
5. Cuando se modifica un módulo debe realizarse de nuevo la prueba de caja negra completa (incluir todos los casos de prueba).	✓	

Cuadro 10. Detalla la autoevaluación del proceso de pruebas;

Fuente: Propia

6.6. Evaluación del cliente

Para la mejora continua de nuestro proceso de pruebas, se utilizaron diferentes tipos de herramientas capaces de medir y evaluar la opinión de nuestros clientes.

Entre alguna de ellas tenemos la del focus group, que busco ahondar en la problemática de la empresa, y el por qué? necesaria una mejora en la gestión de activos. (Ver Anexo 11)

Otra herramienta interesante fueron las encuestas, realizadas a los diferentes tipos de trabajadores de la empresa, las cuales nos dejaron entre ver la experiencia de los usuarios con otro tipo de software de gestión de riesgos. También la apreciación a nuestro producto y su saldo positivo en el proceso de mejora continua.(Ver Anexo 9 y 10)

Además las reuniones nos sirvieron para ver el interés del usuario y los cambios solicitados por ellos. Hasta llegar al producto final.

6.7. Resumen

El aseguramiento de calidad de software se trabajó dentro de cada una de las actividades de desarrollo del proyecto, de la siguiente manera:

- Se realizó una revisión por pares para el proyecto.
- Haciendo seguimiento formal al proyecto, no sólo en tiempos y costos, sino en cumplimiento con estándares y metodología de desarrollo de software.
- Se consolida la metodología de gestión de riesgos y la de desarrollo de software en busca de alcanzar niveles superiores de madurez.

Los objetivos básicos de las inspecciones son:

- Encontrar errores lo más temprano posible en el ciclo de desarrollo.
- Asegurar que los usuarios están de acuerdo en la parte técnica del trabajo.
- Verificar que el trabajo cumple con los criterios preestablecidos.

Para toda prueba debe haber un plan que incluye:

- Objetivos para cada fase de prueba.
- Procedimientos y estándares a ser utilizados para planear y llevar a cabo las pruebas y reportar los resultados.
- Criterios para determinar si la prueba está completa, como también el éxito de cada prueba.

Cada caso de prueba se debe ejecutar y al final debe quedar un reporte de las pruebas con la siguiente información:

- Proyecto y programas que se están probando, objetivo de la prueba y el plan de pruebas.
- Responsables y participantes de las pruebas.
- Casos de prueba.
- Resultados de las pruebas.
- Firma de los responsables de las pruebas y certificación de que se siguió el procedimiento apropiado.

Las pruebas fueron analizadas teniendo en cuenta:

- Los errores graves encontrados fueron analizados en grupo, para hallar soluciones y maneras de que no vuelvan a suceder.
- Se Revisó la efectividad de las pruebas y reforzó aquellas que más errores detectadas.
- Uno de los beneficios de la autoevaluación fue que los moderadores pudieron sugerir mejoras dentro del proceso de desarrollo de software, y así se incrementó la calidad del sistema.

CAPITULO VII: CONCLUSIONES

Podemos afirmar que se cumple con los objetivos generales y específicos del proyecto ya que se obtiene una herramienta capaz de manejar los riesgos y hacerles un seguimiento, cumpliendo la estructura de la metodología aplicada y la aceptación de nuestro cliente.

Podemos decir que el análisis de riesgos nos permitió determinar qué tiene la Organización, en este caso la empresa GMD, y estimar lo que podría suceder. El análisis de riesgos también permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y obtener resultados positivos.

Con esta nueva gestión de riesgos, permitirá a la empresa GMD organizar la defensa concienzuda y prudente, previniendo sucesos perjudiciales y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la dirección asume.

En nuestro sistema de gestión de riesgos se buscó asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la empresa GMD, minimizando así las amenazas de seguridad de la información.

CAPITULO VIII: RECOMENDACIONES

Podemos recomendar que la empresa GMD, deberá crear un área de seguridad informática, capaz de gestionar técnicas y metodologías, para aplicar la solución más efectiva posible contra las amenazas de sus activos.

La empresa GMD deberá definir una estructura del estándar ISO 27000, definiciones, descripciones e indicaciones como evaluar y tratar los riesgos de seguridad de la información.

Además, aplicar el mejoramiento en la Gestión de activos, responsabilidad sobre los activos y clasificación de la información.

Adquisición, desarrollo y mantenimiento de los sistemas de información, requisitos de seguridad de los sistemas de información, tratamiento correcto de las aplicaciones, controles de acceso, seguridad en los procesos de desarrollo y soporte, gestión de la vulnerabilidad.

GMD deberá realizar la gestión de los incidentes de seguridad de la información, notación de eventos y puntos débiles de seguridad de la información, gestión de incidentes de la seguridad de información y mejoras.

La empresa también deberá realizar el cumplimiento en los requisitos legales y normas de seguridad, consideraciones sobre las auditorias de la seguridad de la información.

Una compañía experta en seguridad informática propone una política de seguridad y recomendaciones para que sus usuarios puedan proteger sus equipos e información contra amenazas.

CAPITULO IX: REFERENCIAS BIBLIOGRÁFICAS

1. HAROLD KERZNER. Project Management “A Systems Approach to Planning, Scheduling, and Controlling”. JHON WILEY & SONS, INC. Novena edición, 2006.
2. PROJECT MANAGEMENT INSTITUTE, INC. Guía del PMBOK “Guía de los Fundamentos de la dirección de proyectos”, PMI GLOBAL STANDARD, Cuarta Edición, 2008.
3. THE SOFTWARE ENGINEERING INSTITUTE, CMMI for Development version 1.2. CARNEGI MELLON UNIVERSITY. 2006.
4. SARY REGEV, AVRAHAM SHTUB, YAKOV BEN-HAIM, Managing Project Risks as Knowledge Gaps, Project Management Journal, ABI/INFORM Global, Dic 2006.
5. KEVIN M. CURRAN, MICHAEL W. CURRAN, Handling the Truth in Risk Management, Cost Engenineering. Morgantown, Oct 2008. Vol. 50; Pg. 19, 6 pag.
6. JANE SEYMOUR, GARY BELLAMY, MERRYN GOTT, SAM H. AHMEDZAI, DAVID CLARK, Using focus Groups to Explore older people’s Attitudes to End of Life Care, PROQUEST Social Science Journals, Jul 2002, pag 517.
7. HANZEL TAYLOR, Risk Management and Problem Resolution Strategies for IT Projects: Prescription and Practice, PROQUEST Social Science Journals Dic 2006, pag 49.
8. VAROUJAN K MINASSIAN, GEORGE F JERGEAS, A Prototype Risk Analysis for Determining Contingency Using Approximate Reasoning Method, Cost Engenineering. Morgantown, Jan 2009. Vol. 51; Pg. 26 pag.
9. KHALID KHANFAR, ABED ELZAMLY, WALID AL-AHMAD, ELLAS EL-QAWASMEH, KHALID ALSAMARA, SALEEM ABULEIL, Managing Software Project Risks with the Chi-Square Technique, International Management Review, Jan 2008, Vol. 4, 2
10. LONECK, BARRY; WAY, BRUCE, Using a Focus Group of Clinicians to Develop a Research Project on Therapeutic Process for Clients with Dual Diagnoses, PROQUEST Social Science Journals Dic 1997, 42, 1 pg. 107.
11. JABLONSKI STEFAB, Guide to web application and plataform, Springuer, 2004, pag. 19 – 21.

12. MINISTERIO DE ADMINISTRACIONES PUBLICAS, Magerit versión 1.2: metodología de análisis y gestión de riesgos de los sistemas de información. Publicado por Ministerio de Administraciones públicas de España, 2007.
13. Andy Jones, Debi Ashenden, Risk management for computer security: Protecting your network and information assets, Publicado por Butterworth-Heinemann,July 2005.
14. PHILIPPE KRUCHTEN, The rational unified process: an introduction, Addison-Wesley, Feb 2003.
15. EUGENE F. BRIGHMAN, JOEL F. HOUSTON. Fundamentos de administración financiera por. Cengage Learning Editores, April 2005.

En Internet

16. Página Oficial de @Risk en: http://www.palisade-lta.com/risk/ (accesado: 25 Mayo 2012)
17. Página Oficial de Crystal Ball en: http://www.aertia.com/ (accesado: 24 Mayo 2012)
18. Página Oficial de Crystal Ball en: http://www.realoptionsvaluation.com/risksimulator.html (accesado: 24 Mayo 2012).
19. Portal de Administración Electrónica en: http://www.realoptionsvaluation.com/risksimulator.html (accesado: 1 Mayo 2012).

Anexo 1

Lista de chequeo de aseguramiento de calidad

Analista: Antton Cavalcanti

Fecha: 01/05/2010

Revisión de aseguramiento de calidad

Actividad	Si	No	No aplica	Información Adicional
¿Existe alguien en su organización responsable por los procesos de pruebas?	X			
¿Tiene y usa un estándar para el plan de pruebas?	X			
¿Tiene y usa un estándar para las pruebas de unidad?	X			
¿Tiene y usa un estándar para el reporte de la ejecución de las pruebas?	X			
¿La planeación y ejecución de pruebas se realiza en paralelo con el proceso de desarrollo de software?	X			
¿Se verifica que las especificaciones estén correctamente implementadas?	X			
¿Se verifica que las expectativas del cliente sean satisfechas?	X			
¿Los probadores reportan los defectos al equipo de desarrollo de software para corrección?	X			
¿Los probadores identifican la prioridad de los riesgos del negocio para el desarrollo del plan de pruebas?	X			
¿Existen objetivos de pruebas medibles para cada sistema de software que está siendo probado?			x	
¿Se usan métricas para mejorar el proceso de aseguramiento de la calidad?	X			
¿Los probadores han definido pronósticos de defectos basándose en datos y experiencias previos?	X			
¿Existe un proceso de mejoramiento continuo para su proceso de pruebas?	X			
¿Los tipos de defectos están identificados?	X			
¿Se usan métricas para planear y evaluar el proceso de pruebas?	X			
¿Tiene un proceso de entrenamiento de probadores?	X			
¿El uso de una herramienta automatizada de pruebas es parte significativa de su proceso?		x		

Anexo 2

Lista de chequeo de estándares de presentación y funcionalidad de la aplicación para formas

Fecha: 01/05/2010

Forma: **Descripción: Estándares de Funcionalidad**

Analista: Antton Cavalcanti **Revisor: José L. Sandoval**

Revisión de estándares de presentación

Actividad	Si	No	No aplica	Información Adicional
¿Están claramente definidos los bloques de información (Frames)?	X			
¿Tiene los encabezados de título y nombre de aplicación correctos?	X			
¿Las etiquetas de los campos son claras y representativas?	X			
¿Los campos de despliegue están completamente inhabilitados y del color respectivo?	X			
¿Los campos de solamente despliegue están claramente identificados?	X			
¿Tiene los colores estándar?	X			
¿Los campos fecha tienen el formato DD-MON-RRRR y se puede ingresar los datos como Ej: 12ago2001?		X		Necesariamente los campos son ingresados con un estándar.
Cuando se tiene una forma con múltiples tabs, ¿se conoce cuál es el registro padre de los tabs?	X			
¿La forma tiene la dimensión correcta?	X			
¿Los Radio Groups tienen un frame que los abarca?			X	No presentamos radiogroups
¿Los campos están alineados en forma correcta?	X			
¿Los campos requieren y tienen Tooltip?			X	No presentamos tooltip
¿Los LOVs tienen el tamaño y la posición adecuados (que no requieran ser movidos)?	X			
¿Los LOV's están heredados?	X			
¿Los barras de Scroll son blancas y de ancho 15?		X		Se moldeo a un estándar menor debido a la capacidad de

				información en las tableview
¿Están habilitados los botones del toolbar de manera adecuada y corresponden con las teclas de función?	x			

Revisión de funcionalidad				
Actividad	**Si**	**No**	**No aplica**	**Información Adicional**
¿La forma realiza la función que se necesita?	X			
¿La forma ha sido ingresada a SGSI_BD con todas las funciones, tablas y roles asociados?	X			
¿Los datos de la forma cambian en forma sincronizada?	X			
¿Es rápido y fácil el manejo de la forma?	X			
Cuando se cambia el valor de un campo de entrada, ¿se modifica también el campo de despliegue?	X			
¿Los bloques hijos están coordinados con el bloque padre en consulta, borrado y cuando se limpia la forma?	X			
Los campos que hacen referencia a datos de otras tablas ¿tienen cada uno su lista de valores?	X			
¿Las listas de valores son lentas para recuperar la información?	X			Se logro corregir el problema de respuesta por búsqueda.
¿El tiempo de respuesta es adecuado?	X			Menos de 1 segundo por respuesta.
¿El orden de navegación de los campos es el correcto?	X			
¿Los mensajes graves son manejados adecuadamente?	X			
¿Los campos Validate from LOV funcionan adecuadamente?	X			
¿Si el reporte requiere mucho tiempo, esto le es notificado al usuario?		X		La mayoría de de los reportes contienen información no pesada.
¿Está la forma documentada?	X			
¿Si llama reportes, la extensión de los reportes es la correcta?	X			

Revisión del código y los datos que retorna

Actividad	Si	No	No aplica	Información Adicional
¿Se ha realizado el proceso de prueba formal?	X			
¿Está la mayor cantidad de código en la base de datos?	X			
¿Se ha realizado el proceso de afinamiento Sql?	X			

Anexo 3

Lista de chequeo de estándares de presentación y funcionalidad de la aplicación para reportes

Fecha: 01/05/2010

Forma: **Descripción: Estándares de Presentación**

Analista: Antton Cavalcanti **Revisor: José L. Sandoval**

Revisión de estándares de presentación

Actividad	Si	No	No aplica	Información Adicional
¿El reporte tiene el nombre del sistema correcto?	x			
¿El reporte tiene los encabezados de título y nombre de aplicación correctos?	X			
¿El reporte tiene la fecha de generación?	X			
¿El reporte tiene el número de página y el total de páginas?	X			
¿El reporte tiene los colores estándares? Naranja y Azul.	X			
¿Los campos fecha tienen el formato DD-MON-YYYY?	X			
¿Los campos están alineados en forma correcta?	X			
¿El reporte tiene subtotales y totales de control?	X			
¿El reporte tiene, en la parte superior, las condiciones de generación del listado?		X		
¿El reporte tiene el visto bueno del usuario?	X			
¿Se ha hecho revisión por pares?	X			
¿Se ha realizado el proceso de afinamiento sql?	X			
¿Está la mayor cantidad de código en la base de datos?	X			
¿El código cumple con los estándares?	X			
¿Está el reporte registrado en SGSI_BD?	X			

Anexo 4

Lista de chequeo de estándares de tablas

Fecha: 05/05/2010

Forma: **Descripción: Estándares de Tablas de Datos**

Analista: Antton Cavalcanti **Revisor: José L. Sandoval**

Revisión de las tablas

Actividad	**Si**	**No**	**No aplica**	**Información Adicional**
¿El nombre de la tabla es correcto según los estándares?	x			
¿Tiene las descripciones de la columna en la base de datos?		x		
¿Tiene las llaves e índices adecuados?	x			
¿La tabla ha sido recreada teniendo en cuenta su uso?	x			

Anexo 5

Lista de chequeo de estándares de funciones y procedimientos

Fecha: 05/05/2010

Func/Proc: **Descripción: Estándares de Funciones**

Analista: Antton Cavalcanti **Revisor: José L. Sandoval**

Revisión de estándares

Actividad	Si	No	No aplica	Información Adicional
¿El nombre cumple con los estándares?	X			
¿El código cumple con los estándares?	X			
¿Está la función/procedimiento documentado?	X			
¿Se ha realizado el proceso de afinamiento sql?	X			
¿Se ha registrado en SGSI_BD?	X			
¿Se usan todas las variables, constantes y parámetros?	X			
¿La asignación de valores a las variables, constantes y parámetros tiene un propósito?	X			
¿Son correctas las validaciones de condiciones?	X			
Por ejemplo: código no alcanzable, ciclos infinitos, división por cero, verificación de rangos, redondeos.	X			
¿Faltan validaciones?	x			
¿Se manejan todas las posibles excepciones?	X			
¿Las variables que guardan datos de columnas de tablas se han definido de acuerdo con esto? Tabla.columna%type	X			
Si se llaman otras funciones y/o procedimientos, ¿tienen el número de parámetros y el tipo de datos adecuado?	X			

Anexo 6

Lista de chequeo de estándares de programación-Código

Objeto	
Fecha de revisión	**05/05/2010**
Revisado por	**José L. Sandoval**

	si	**No**
Aprobado	**x**	

.

Elemento a revisar

Actividad	**Si**	**No**	**No aplica**	**Información Adicional**
Código en general	X			
¿Está el código indentado a, por lo menos dos espacios?	X			
¿Están ordenados alfabéticamente las constantes, variables y cursores?	X			
¿Están alineados a la izquierda las constantes, variables y cursores?	X			
¿Están alineados a la izquierda la definición del tipo de dato de las constantes, variables y cursores?	X			
¿Está definida sola una constante, variable o cursor por línea?	X			
Documentación ¿Está toda la documentación en una línea diferente al código que se está documentando?	X			
¿Comprende la documentación de funciones/ procedimiento tres partes: una descripción general de lo que hace la función o procedimiento, la descripción de los parámetros de entrada y la descripción de los posibles valores y/o parámetros de salida?	X			
Parámetros ¿El nombre de los parámetros empieza con la letra minúscula y es significativo?	X			
Constantes ¿El nombre de las constantes empieza con la letra minúscula y es significativo?	X			
Variables ¿El nombre de las variables empieza con la letra minúscula y es significativo?	X			
Cursores ¿El nombre de los cursores empieza con las letras minúsculas y es significativo?	X			

¿Están los nombres de los cursores alineados a la izquierda junto con la definición del tipo de dato de las constantes y variables?	X			
Instrucciones Select, Insert, Update y Delete ¿Están todas las instrucciones Select, Insert, Update y Delete escritas en minúsculas, a excepción de variables que hagan referencia a campos de las formas?	X			
Instrucciones Select ¿Están las cláusulas Select, Into, From, Where, Order BY, Group BY y Having escritas en líneas diferentes?	X			
Instrucciones Insert ¿Están las cláusulas Insert Into y Values escritas en líneas diferentes?	X			
Instrucciones Update ¿Están las cláusulas Update, SET y Where escritas en líneas diferentes?	X			
¿Está cada columna que se actualice en una línea diferente?	X			
¿Están todas las columnas que se actualicen alineadas a la izquierda?	X			
Instrucciones Delete ¿Están las cláusulas Delete y Where escritas en líneas diferentes?	X			

Anexo 7

Lista de chequeo de estándares de Formas

Objeto	
Fecha de revisión	**05/05/2010**
Revisado por	**José L. Sandoval**

	si	**No**
Aprobado	**x**	

.

Elemento a revisar				
Actividad	**Si**	**No**	**No aplica**	**Información Adicional**
Forma ¿Tiene la forma la descripción y su título de acuerdo con los estándares?	X			
¿Tiene la forma la dimensión correcta?	X			
Cuando se tiene una forma con múltiples tabs, ¿se conoce cuál es el registro padre de los tabs?	X			
Título del frame ¿Está el título en mayúscula inicial?	X			
Si el frame es de un solo registro, ¿está su título en singular?	X			
Si el frame es multirregistro, ¿está su título en plural?	X			
¿Está localizado el título en la parte superior izquierda del frame?	X			
Campos ¿Tiene el contenido del campo la alineación adecuada, de acuerdo con su tipo de dato?	X			
Si existen varios campos organizados verticalmente, ¿están alineados todos a la izquierda?	X			
Etiquetas Si la organización NO es tabular, ¿están situadas las etiquetas a la izquierda del campo al que pertenecen?	X			
Si la organización SÍ es tabular, ¿están situadas las etiquetas en la parte superior del campo al que pertenecen?	X			
Etiquetas Si la organización SÍ es tabular, ¿están las etiquetas centradas?	X			
¿Están las etiquetas en mayúscula inicial?	X			
¿Están las etiquetas sin los dos puntos al final?	X			

Si existen varios campos organizados verticalmente, ¿están alineadas todas las etiquetas a la derecha?	X			
¿Están las etiquetas formadas de manera que no utilicen abreviaturas ni expresiones de solicitud?	X			
Radio Buttons y Check Box ¿Emplean mayúscula inicial?	X			
En cuanto a su estructura, ¿emplean orientación en forma de columna?	X			
En cuanto a su estructura, ¿emplean alineamiento a la izquierda?	X			
¿Están organizadas las opciones en el orden esperado, de mayor a menor frecuencia de ocurrencia?	X			
¿Están enmarcados dentro de un frame?	X			
Listas de valores ¿Están organizados los descriptores alineados a la izquierda en forma de columna?	X			
¿Están organizados los descriptores en orden alfabético o numérico, según sea el caso?	X			
¿Están los descriptores en mayúscula inicial?	X			
¿El ancho es suficiente para evitar el uso de scroll horizontal?	X			
¿Tienen las listas de valores la posición adecuada, de forma que no requieran ser movidas?	X			
Scroll ¿Están las barras de scroll vertical ubicadas a la derecha?	X			
¿Están las barras de scroll vertical iguales a la altura de sus campos asociados?	X			
¿Están las barras de scroll horizontal ubicadas en la parte inferior?	X			
¿Están las barras de scroll horizontal iguales al ancho de sus campos asociados?	X			
¿Son las barras de scroll blancas?	X			
Botones Si están ubicados horizontalmente, ¿están en la parte inferior de la pantalla?	X			
Si están ubicados verticalmente, ¿están a la derecha de la pantalla?	X			
Los botones organizados horizontalmente, ¿tienen la misma altura?	X			
Los botones organizados verticalmente, ¿tienen el mismo ancho?	X			
¿Está colocada la opción más frecuente a la izquierda o en el tope, según corresponda?	X			
¿Usan los botones mayúscula inicial?	X			
¿Incluye puntos suspensivos (...) si la acción despliega otra ventana?	X			

Anexo 8

Formato de pruebas de funcionalidad

Fecha: 20/05/2010

Analista: Antton Cavalcanti **Tipo de Prueba: Funcional**

Ejecución	**Si**	
Aprobado	**Si**	
Revisado por	**José L. Sandoval**	

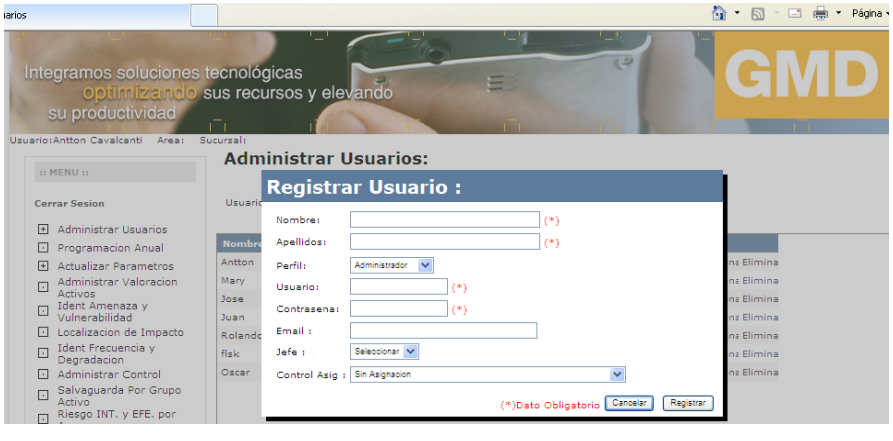
Caso de Uso: Registro de Usuario

Descripción

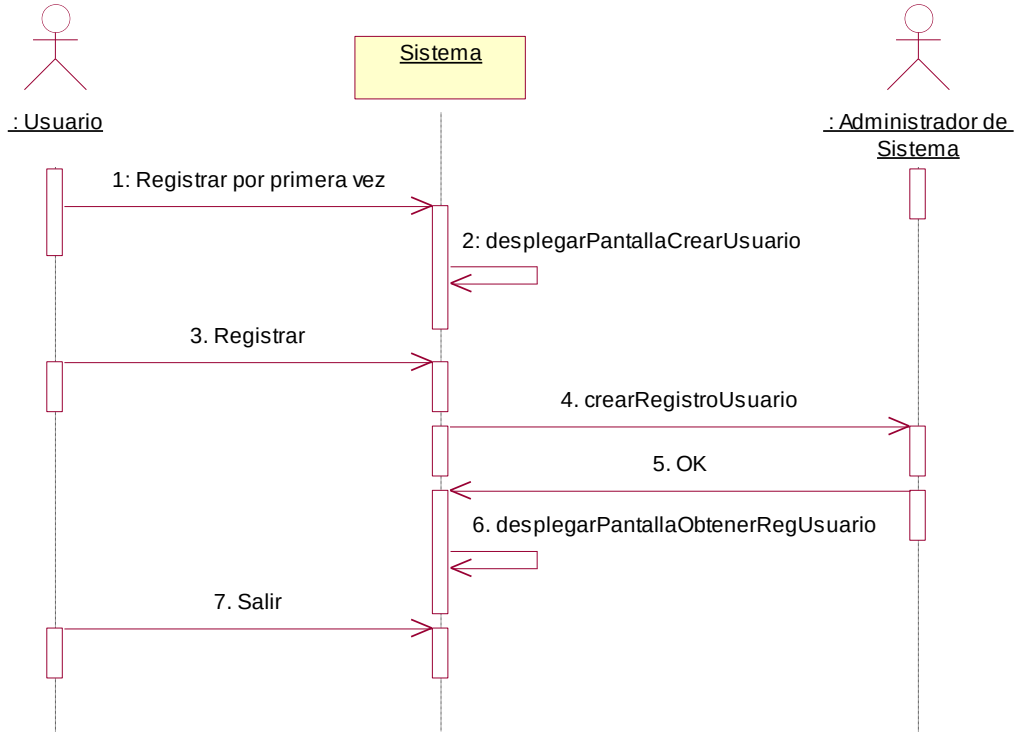
Este caso de uso podrá realizar el registro de cualquier usuario dentro de la red intranet de la compañía.

Entradas:	**Salidas**:
Nombre, Apellidos, Perfil, Usuario, Contraseña, Email, Jefe.	Antton, Cavalcanti, Administrador, Usu, Con, antton1414@gmail.com, Sandoval.

Pantalla



Secuencia de Caso de Uso: Registro de Usuario



Caso de Uso: Administrar Valoración de Activo

Descripción

Este caso de uso podrá determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de que perjuicio (coste) supondría su degradación.

De esta forma el caso de uso permitirá al Oficial de Seguridad: Identificar los activos y realizar la valoración de activos.

Entradas

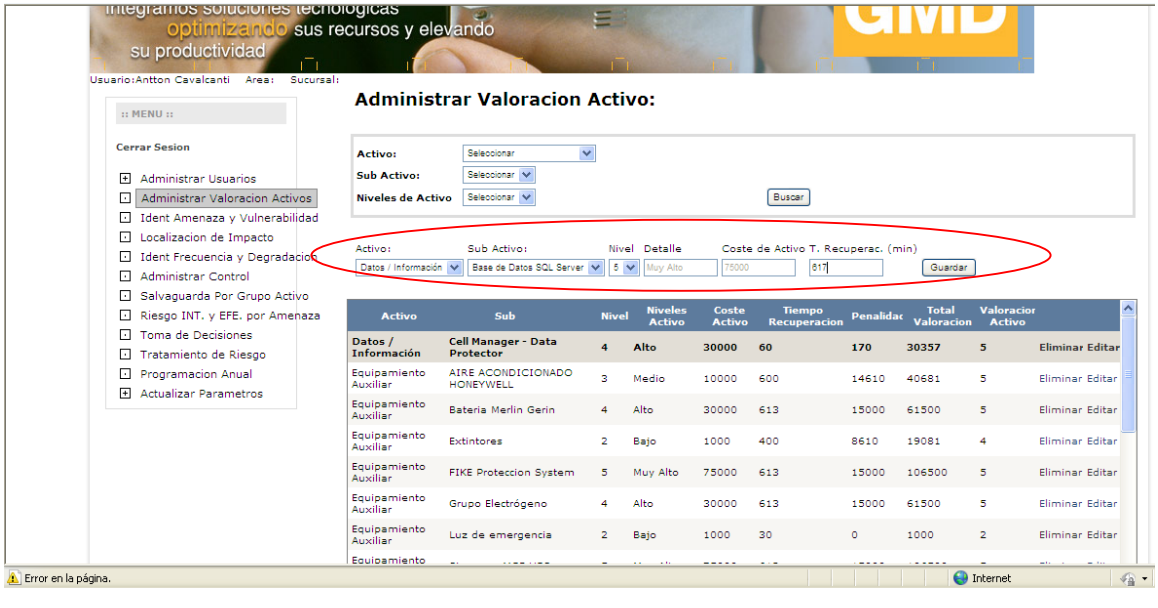
1. Oficial de Seguridad: Inicia el caso de uso cuando ingresa descripción de grupo de Activos. **Ej.: Datos e Información**
2. Oficial de Seguridad: Asigna un Sub-Grupo de Activos. **Ej.: Base de Datos SQL Server 2000**
3. Oficial de Seguridad: Asigna un Nivel de Coste de activos. **Ej.: 5**
4. Sistema: Muestra Nivel de Detalle de Coste de Activos. **Ej.: Alto**

5. Oficial de Seguridad: Ingresa tiempo de recuperación correspondiente (Valoración de Información). **Ej.: 75000**
6. Sistema: Genera Penalidad (Puntos) en base al tiempo de recuperación. **Ej.: 15120**
7. Sistema: Genera Total Valoración en base a el tiempo de recuperación (minutos) y penalidad (puntos). **Ej.: 106752**
8. Sistema: Finaliza el caso de uso cuando muestra la valoración del Activo en base al Total Valoración. **Ej.: 5**

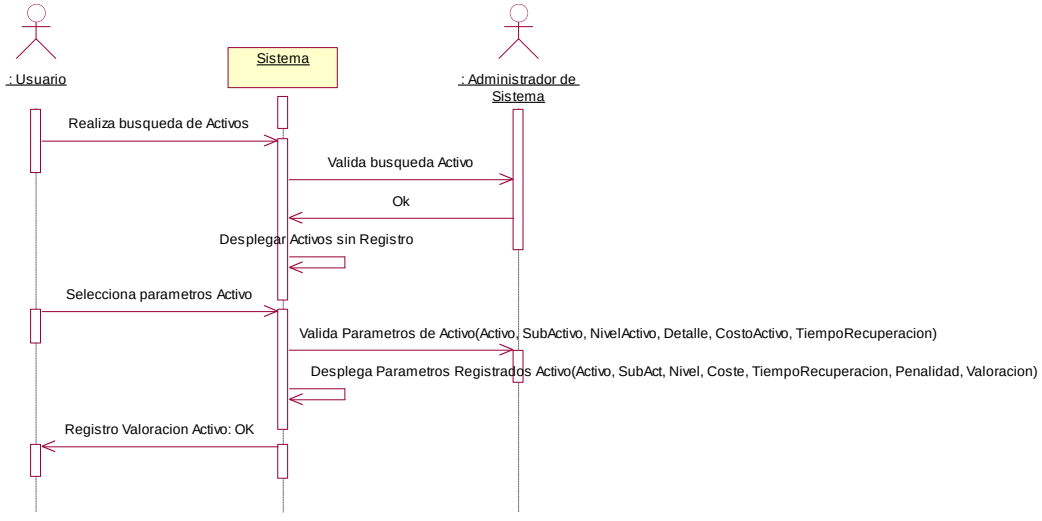
Salidas Esperadas

1. Se determino el grupo de activo según corresponda.
2. Se obtuvo el nivel de coste y detalle por cada activo expuesto.
3. Se determino la penalidad que se obtiene por tiempo de recuperación que corresponde a cada activo.
4. Se obtiene el total de valoración para la organización.
5. Se obtiene la valoración del activo.

Pantallas



Secuencia de Caso de Uso: Valoración de Activos



Caso de Uso: Administrar Salvaguarda

Descripción

Este caso de uso identificar las alternativas para el administrar una contramedida para reducir el riesgo. Luego se procederá a la identificación de controles, determinación de controles a implementar y la implementación de controles para poder mitigar la posible amenaza.

Entradas

Determinar Salvaguardas

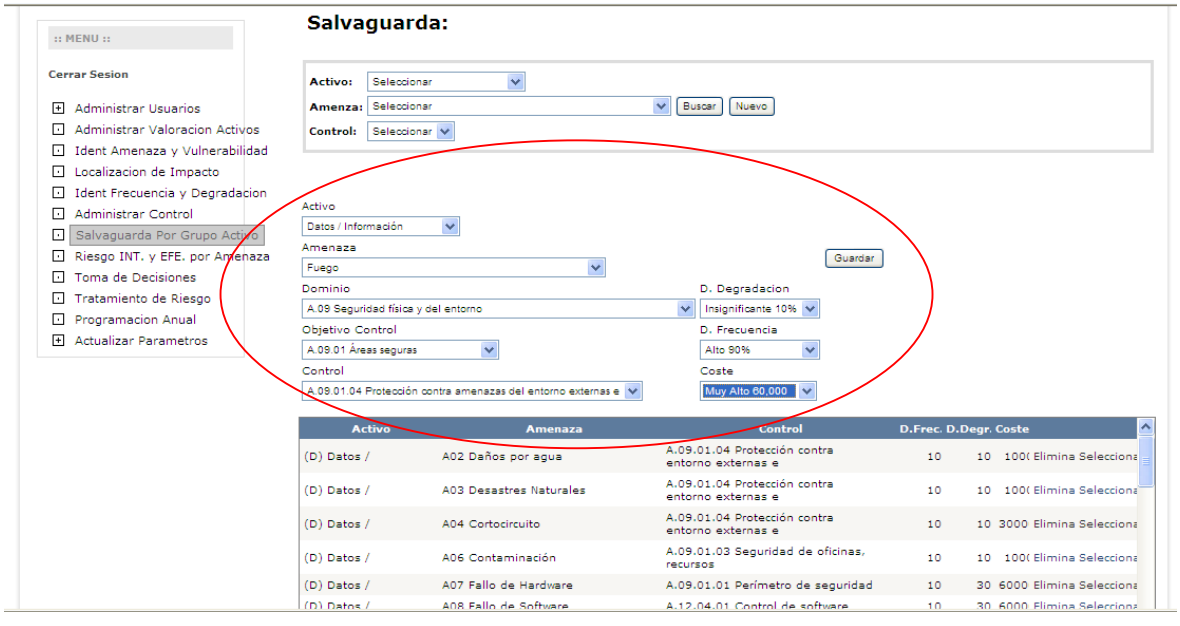
1. Oficial de Seguridad: Inicia el caso de uso cuando ingresa descripción de grupo de Activos. **Ej.: Datos e Información**
2. Oficial de Seguridad: Asigna una amenaza de Activos. **Ej.: Fuego**
3. Oficial de Seguridad: Asigna un Dominio de Control de Activos. **Ej.: A.09 Seguridad Física y del Entorno.**
4. Oficial de Seguridad: Asigna un Objetivo control de Amenaza. **Ej.: A.09.01 Áreas Seguras.**
5. Oficial de Seguridad: Asigna un control de Amenaza. **Ej.: A.09.01.04 Protección contra amenazas del entorno externas.**
6. Oficial de Seguridad: Asigna una Disminución de la degradación. **Ej.: Insignificante 10%**
7. Oficial de Seguridad: Asigna una Disminución de la frecuencia. **Ej.: Alto 90%**

8. Oficial de Seguridad: Asigna un Coste de Amenaza. **Ej.: Muy Alto 60000**

Salidas Esperadas

1. Se identifica el Control de Riesgo a tomar. Ej.: A.09.01.04 Protección contra amenazas del entorno externas.

Pantallas



Caso de Uso: Tratamiento de Riesgo

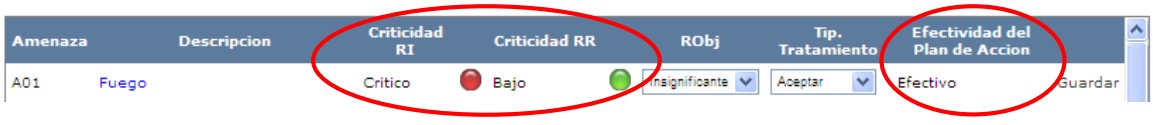
Descripción

Este caso de uso identificar las alternativas para el tratamiento de riesgos, así como la alternativa para reducir el riesgo. Luego se verificara la efectividad del plan de acción realizado.

Entradas:	**Salidas:**
Código Amenaza, Descripción Amenaza, Criticidad Riesgo Intrínseco, Criticidad Riesgo Residual.	A01, Fuego, Critico, Bajo. Riesgo Objetivo: Insignificante Tipo de Tratamiento: Reducir Efectividad: Efectivo.

Pantalla:

Tratamiento de Riesgo:



Nota: Se puede verificar el análisis comparando el estado en el que se encontraba la criticidad del riesgo Intrínseco (Antes) vs la Criticidad Riesgo Residual (después). Estado CRITICO (ROJO) vs Estado Bajo (Verde).

Ej. FUEGO vs Grupo de Activos

Riesgo Intrínseco=

=+SI(Frecuencia="","",Frecuencia*Impacto*Coste por Grupo de Activo) =

=+SI(Frecuencia="","",5%*90%*152021) =

= 6841

Riesgo Residual

=+SI(Frecuencia ="","", Frecuencia * Impacto * Coste por Grupo de Activo *(100%-Disminución de la frecuencia)*(100%-Disminución de la Degradación))=

= 0

Criticidad del Riesgo Cuantitativo		
5	30000 a más	Crítico
4	(20000 - 30000)	Alto
3	(7000-20000)	Moderado
2	(1000-7000)	Bajo
1	(0-1000)	Insignificante

Total Riesgo Intrínseco=SUMA RI(Servicios + Datos e Información + Software + Hardware + Redes de Comunicaciones + Soporte de Información + Equipamiento Auxiliar + Instalaciones +Personal)

= 81301

Total Riesgo Residual=SUMA RR(Servicios + Datos e Información + Software + Hardware + Redes de Comunicaciones + Soporte de Información + Equipamiento Auxiliar + Instalaciones +Personal)

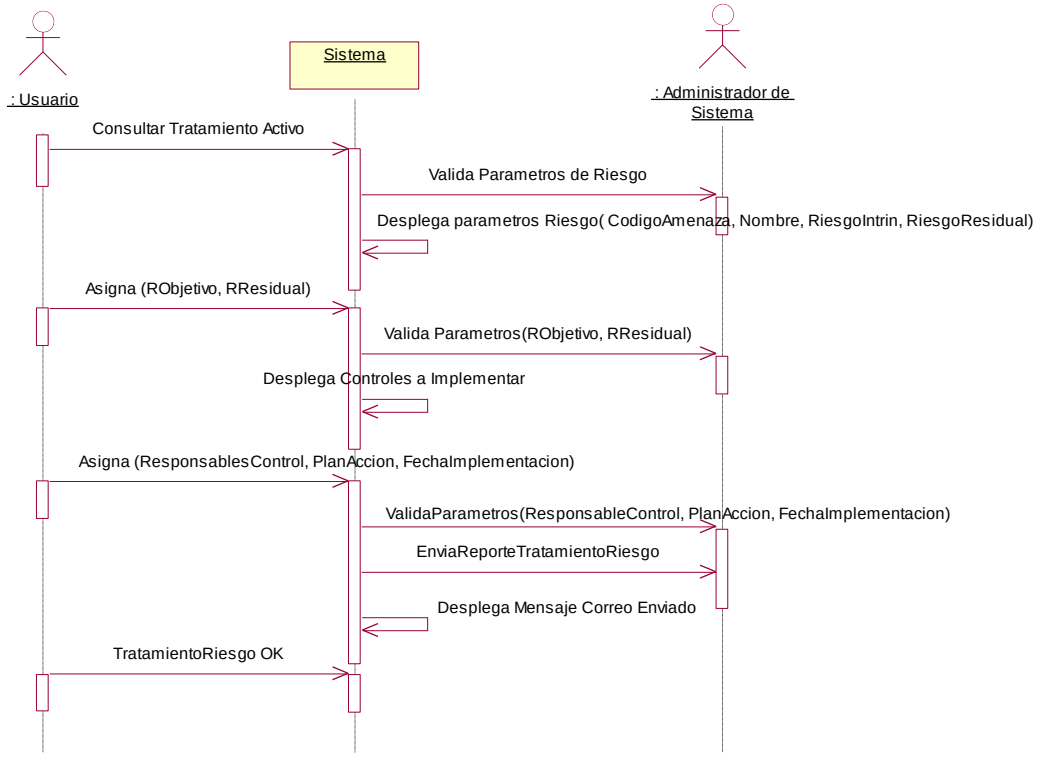
=26

Nivel Criticidad Riesgo Intrínseco= CRITICO

Nivel Criticidad Riesgo Residual= INSIGNIFICANTE

Conclusión: Podemos concluir que el estado y tratamiento para el ejemplo con la amenaza: FUEGO, ha sido mitigado y el plan de acción es EFECTIVO.

Secuencia de Caso de Uso: Tratamiento de Riesgo



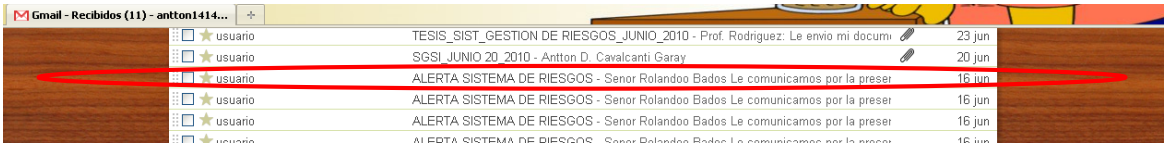
Caso de Uso: Seguimiento de Riesgo

Entradas:	**Salidas**:
Amenaza, Control, Actividades Propuestas, Responsable Fecha de Implementación del control	Fuego, A.09.01.04, Actividades Propuestas: Implementar sistema contra incendios F200, Responsable: Rolando Bados, Fecha de Implementación del control: 02/11/2010.

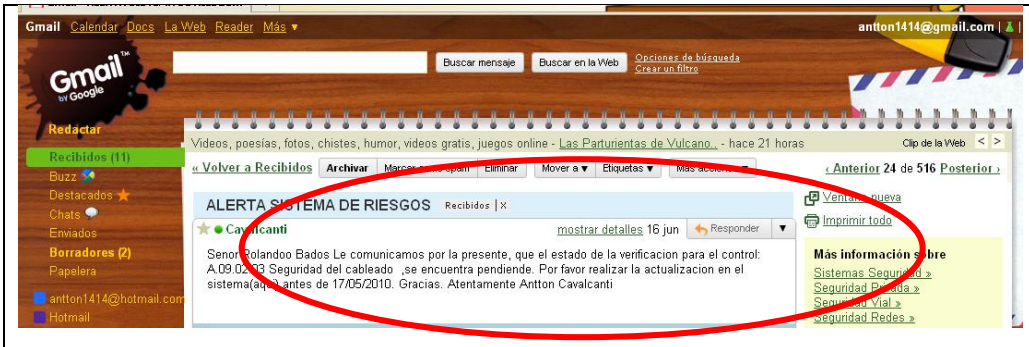
Pantalla:

Nota: Una vez realizado el análisis se podrá asignar al responsable de las actividades propuestas para hacer el seguimiento de la efectividad de nuestro análisis.

Las alertas a los Expertos técnicos responsables, se les hará llegar a sus respectivos correos en donde ellos podrán actualizar la información para dicho seguimiento.



Las alertas llegaran al correo del responsable indicándoles la fecha límite para poder hacer la actualización de su actividad.


Gmail
Calendar
Docs
La Web
Reader
Más
antton1414@gmail.com
Buscar mensaje
Buscar en la Web
Opciones de búsqueda
Crear un filtro
Redactar
Recibidos (11)
Buzz
Destacados
Chats
Enviados
Borradores (2)
Papelera
antton1414@hotmail.com
Hotmail
Videos, poesías, fotos, chistes, humor, videos gratis, juegos online - Las Parturientas de Vulcano.. - hace 21 horas
Clip de la Web
« Volver a Recibidos
Archivar
Eliminar
Mover a
Etiquetas
‹ Anterior 24 de 516 Posterior ›
ALERTA SISTEMA DE RIESGOS
Recibidos
Cavalcanti
mostrar detalles 16 jun
Responder
Imprimir todo
Más información sobre
Sistemas Seguridad »
Seguridad Privada »
Seguridad Vial »
Seguridad Redes »

Anexo 9

Modelo de Encuesta

Fecha: 05/05/2010

Analista: Antton Cavalcanti **Revisor: José L. Sandoval**

Información brindada de Clientes

Preguntas				

1. ¿Ha participado en Proyectos de TI?

   Si.

2. **¿Aproximadamente cuantos años de experiencia en Proyectos Informáticos tiene?**

   Más de 5 años.

3. **¿En cuántos proyectos a participado en su trayectoria laboral?**

   Más de 5.

4. **¿Ha realizado las labores de Gerente de Proyectos?**

   Si.

5. **¿Cree usted que el manejo de riesgos es necesario en Proyectos Informáticos?**

   Si. Porque permite mitigar los efectos deseados en cualquier etapa del proyecto y evitar poner en riesgo la operación y/o resultados que los accionistas esperan del proyecto.

6. **¿Ha utilizado algún software para el manejo y seguimiento de Riesgos en Proyectos?**

   Si. En GMD se utiliza la metodología PASCO, la cual contempla en una de sus fases el relevamiento de los riesgos del proyecto y la forma como se deben mitigar previamente, a través de controles de seguimiento en el calendario.

7. **¿Cree usted que la gestión de Proyectos en empresas Peruanas es eficiente?**

   No. Porque actualmente es una necesidad gerenciar un proyecto a través de mejoras practicas, sea porque empresas con mayor background en el manejo de proyectos han llegado al mercado peruano como competidores, utilizando culturalmente metodologías de atenuar las incertidumbres de un proyecto a través de su proceso normal de gestión, con el uso obligatorio de herramientas las cuales enriquecen con la experiencia de cada gente y que queda en la empresa como parte de su "Know how".

8. **¿De qué forma mejoraría la gestión de proyectos en empresas peruanas?**

   Difundiendo el uso de base de datos de conocimiento (knowledge Warehouse) estandarización de herramientas de gestión que permitan homogenizar el procedimiento de gestión, haciéndolo medible y/o comparable, implementando tableros de control, task forcé para el seguimiento de hitos.

9. **¿Cuál es el mayor riesgo que se le ha presentado en algún proyecto?**

   El no establecer límites de algunas clausulas en el contrato, el no acotar responsabilidades del cliente en algún entregable, el mismo que es pre-requisito para desarrollar una actividad del proyecto.

10. **¿Estaría de acuerdo en la implementación de un Focus Group, para la planificación de riesgos en proyectos informáticos?**

Si. En GMD se estableció “El comité de ideas” que es un hito anterior al comité de cierre, en el cual se convocan a los gerentes de proyectos y a través de este comité de expertos, se evalua la factibilidad, pros y riesgos. Esto tiene como resultado no desgastar a toda la organización y evitar problemas ulteriores.

Anexo 10

Pruebas de Efectividad

Fecha: 05/05/2010

Analista: Antton Cavalcanti **Revisor: José L. Sandoval**

Preguntas realizadas a Usuario Final

Preguntas				

1. ¿Identificas los Activos mejor que antes de tener el sistema?

   Si. Hay un mejor orden para identificar los activos. Y se pueden buscar a sus similares con mayor facilidad.

2. **¿Identificas y/o clasificas los riesgos mejor que antes de tener el nuevo sistema?**

   Si. Se puede detectar mejor los riesgos y existe una mejor clasificación para su búsqueda.

3. **¿Identificas medidas para minimizar los riesgos mejor que sin el nuevo sistema?**

   Si. Ahora puedo tener una idea de que tratamiento tomar para alguna incidencia, pero creo que faltarían agregar algunas nuevas.

4. **¿Sugieres medidas para mitigar los riesgos si se materializan (mejor que sin el software)?**

   Si. Se puede ver que existen contramedidas para minimizar los riesgos en mis proyectos a cargo. Pero debería existir algún proceso dentro del sistema para poder indicar on time a los responsables a cargo de implementar estas medidas.

5. **¿Identificas los procedimientos y las responsabilidades a cargo para la mitigación de riesgos?**

   No creo que sea factible delegar las responsabilidades mediante un software, debería ser tratado mediante reuniones previas y hacerle un seguimiento coordinado entre el área de calidad y los responsables.

6. **¿Mejoraron los procedimientos para la identificación de amenazas para los activos con el nuevo sistema?**

   Si existe una mejora definitivamente, pero es un sistema demasiado orientado a dar responsabilidades y no genera respuestas inmediatas.

7. **¿Se facilita la identificación de los impactos por cada vulnerabilidad de los activos con el nuevo sistema?**

   Si existe un manejo en el manejo de impactos. Pero la valorización por cada activo afectado no necesariamente es el que se ve en la realidad.

8. **¿El sistema logra integrar con otro tipo de sistema de gestión?**

   El proceso de Gestión de Riesgos debería tener un producto el cual debería ser expuesto ante todos sus trabajadores, para que estén al tanto de donde es impactada la empresa.

9. **¿Qué tareas fueron reforzadas al implementar este sistema?**

   Asignación de responsabilidades, revisión de activos, riesgos, etc.

10. ¿Se logro mejorar el análisis y evaluación de los riesgos con el nuevo sistema?

Si existe una mejora en cuanto a la evaluación y análisis de incidencias. Mejorando la productividad de los trabajadores y ahorro de tiempo, alargamiento de calendarios y horas de trabajo.

11. ¿En qué área cree Ud., el sistema de gestión de riesgos obtuvo un impacto económico al ser implementado?

Área de Gestión de Procesos.

Área de Gestión de Calidad

Área Aseguramiento de Calidad

Área de Seguridad de Información

Anexo 11

Resultados de Focus Group

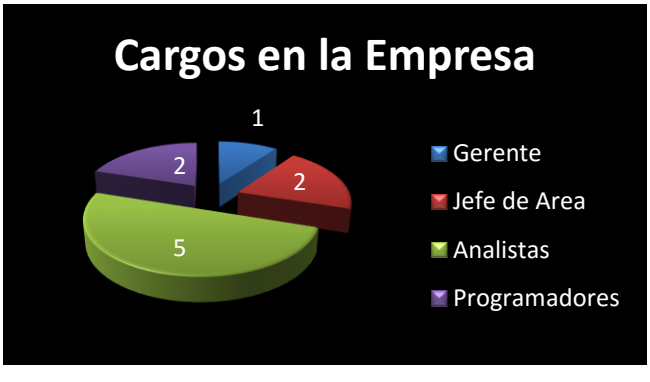
Fecha: 05/05/2010

Analista: Antton Cavalcanti **Revisor: Glen Rodríguez**

Preguntas realizadas a Usuario Final				
Preguntas				

1. ¿Ha participado en Proyectos de TI?

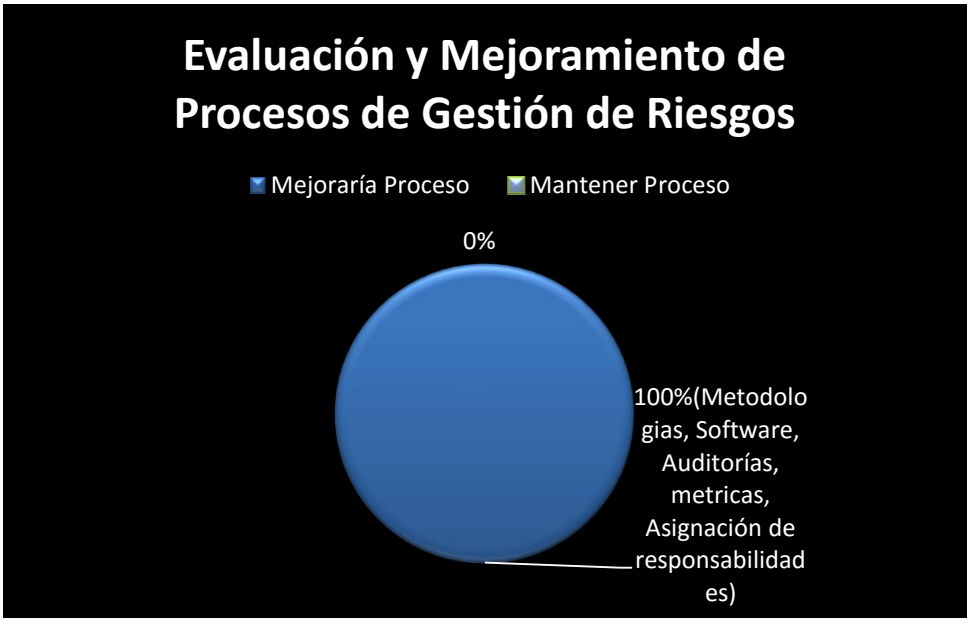
2. ¿Qué cargo ocupas en la empresa?



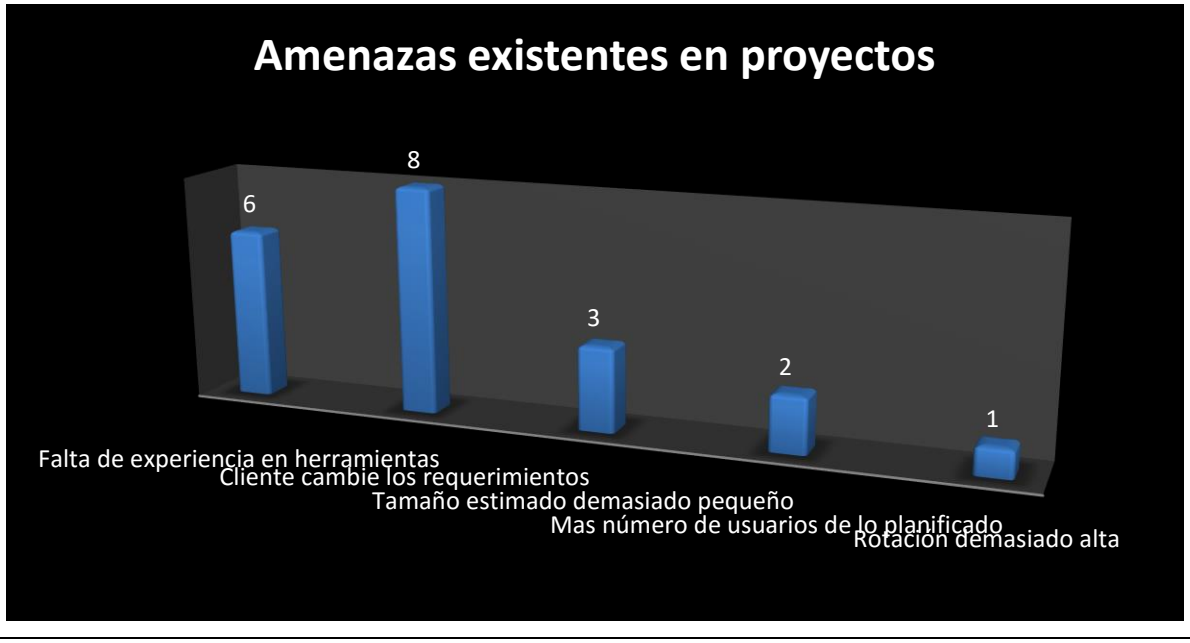
3. **¿Tienes alguna experiencia con software de Evaluación de Riesgos?**

4. **¿Tienes alguna experiencia con metodologías de Evaluación de Riesgos?**

5. **¿Mejorarías los métodos para la gestión de riesgos en la empresa?**



6. **¿Cuáles son las amenazas más comunes con las que se ha enfrentado en Proyectos?**



Anexo 12

Manual de Sistema

Sistema de Gestion de Riesgos SGSI

Realizado por: Antton Cavalcanti Garay

1 de Julio de 2012

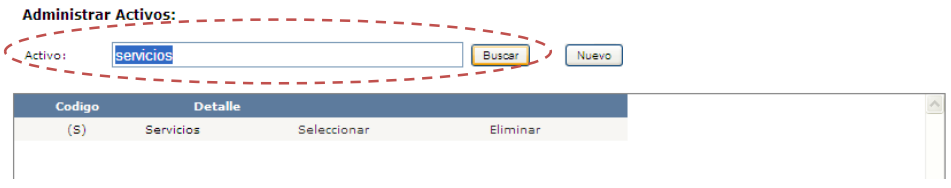
Pantalla Login

El Cliente podrá hacer ingreso mediante un usuario y clave asignada por el administrador.

Pantalla Menu

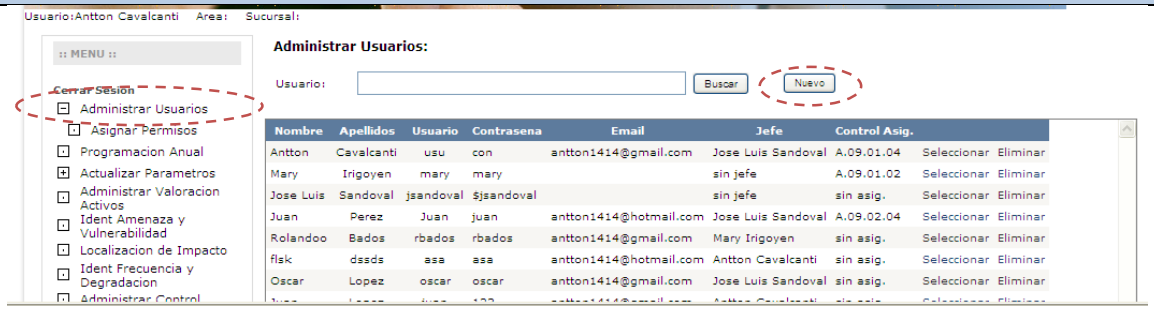
A continuación se presenta la pantalla en el cual el usuario podrá acceder a las opciones asignadas según sea su perfil.

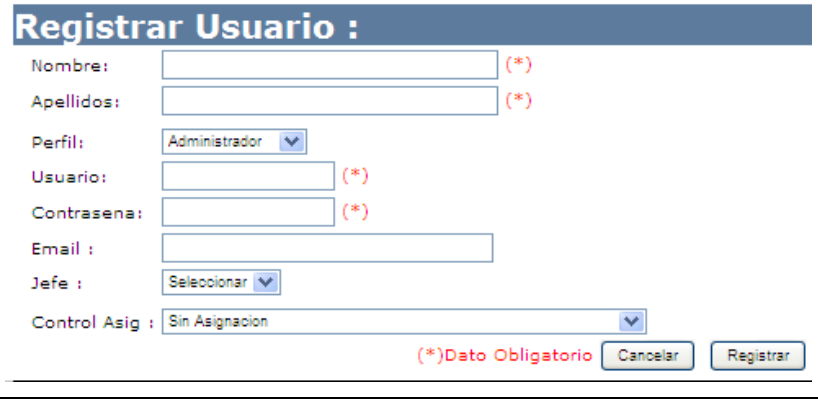
Motor de Búsqueda de Sistema



El motor de búsqueda fue un requerimiento por parte del cliente para ayudar al usuario del sistema a realizar una búsqueda con mayor rapidez. Debido al gran contenido y verificación de activos, se tuvo que manejar de esta manera. Esta herramienta está presente en casi todas las pestanas, debido a que el administrador también requiere verificar al detalle los datos ya ingresados.

Pantalla Administrar Usuario

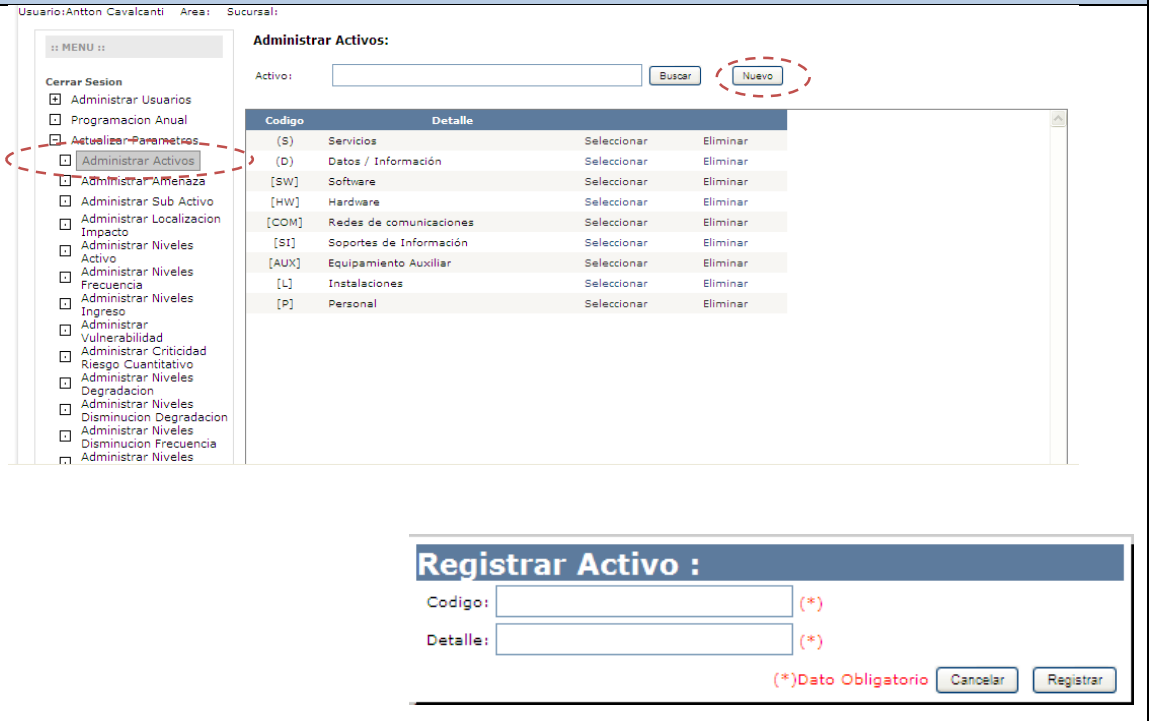




A continuación se presenta la pantalla en el cual el Administrador de Sistema podrá gestionar el acceso a los usuarios.

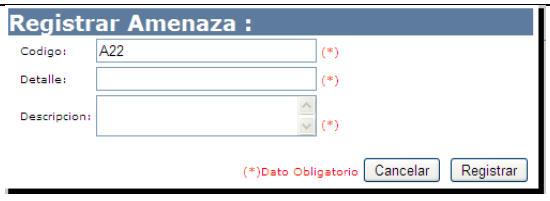
Una vez dándole clic al botón: Nuevo, aparecerá una pantalla para poder ingresar los datos relativos al usuario nuevo.

Pantalla Registro de Activo



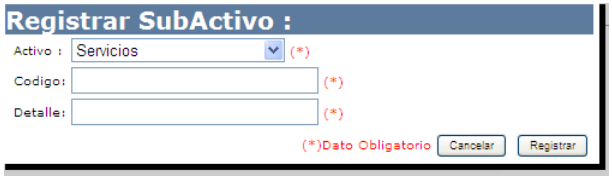
En la siguiente opción del Menu>> Actualizar Parametros>> Administrar Activos. Se aprecia el registro de activos, que también será llenada por el Administrador de Sistema.

Pantalla Registro de Amenaza



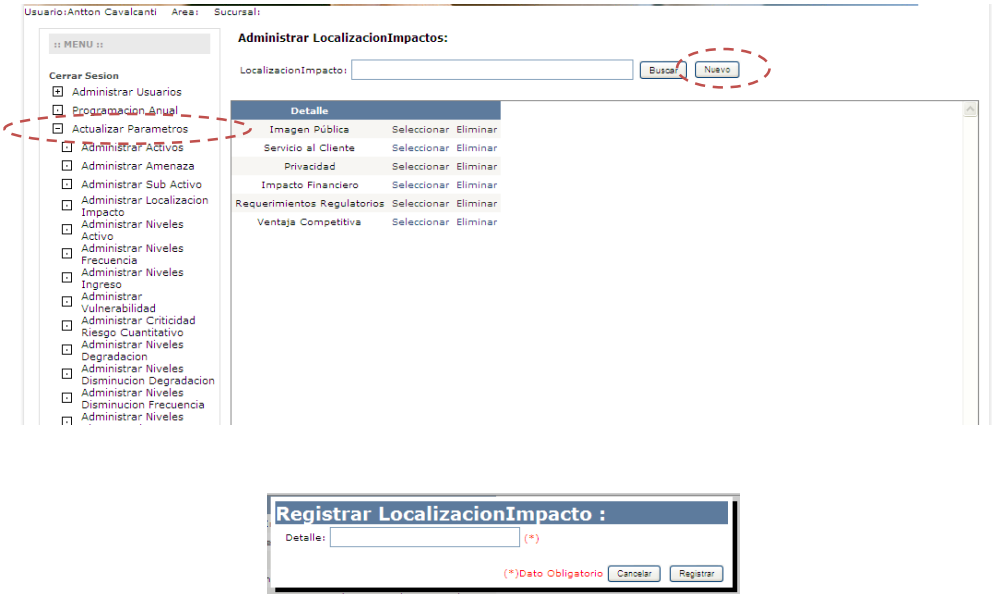
En la siguiente pantalla del Menú>> Actualizar Parámetros, tenemos la opción Administrar Amenaza. En el cual se realizara el Registro de la amenaza. Esta pantalla solo será gestionada por el Administrador de Sistema. Sera importante recalcar el código y la descripción de cada amenaza.

Pantalla Registro Sub Activo



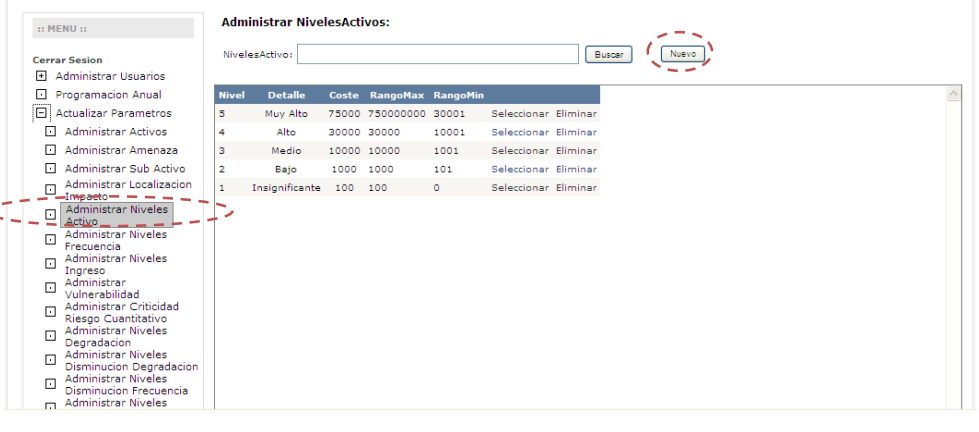
En la siguiente pantalla el administrador realizara el registro de Sub Activos, previamente deberá asignar el tipo de Activo al que se encuentra.

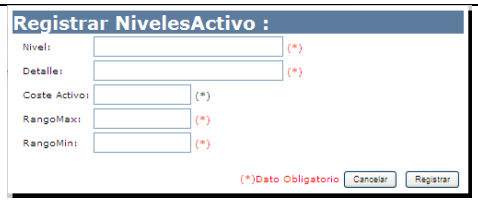
Pantalla Localización de Impacto



En la siguiente pantalla el administrador realizara el registro de la localización del impacto según la empresa.

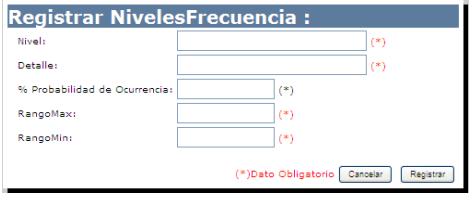
Pantalla Niveles de Activo





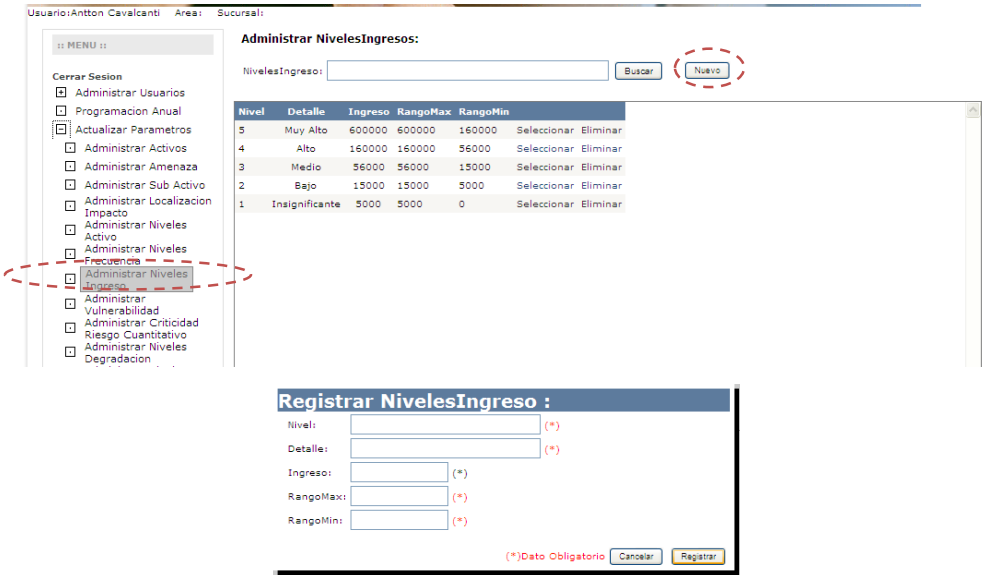
En la siguiente pantalla el administrador realizara el registro de los niveles de Activos. Se podrá apreciar cuando un usuario realice el mantenimiento, en qué nivel se encuentra.

Pantalla Niveles de Frecuencia



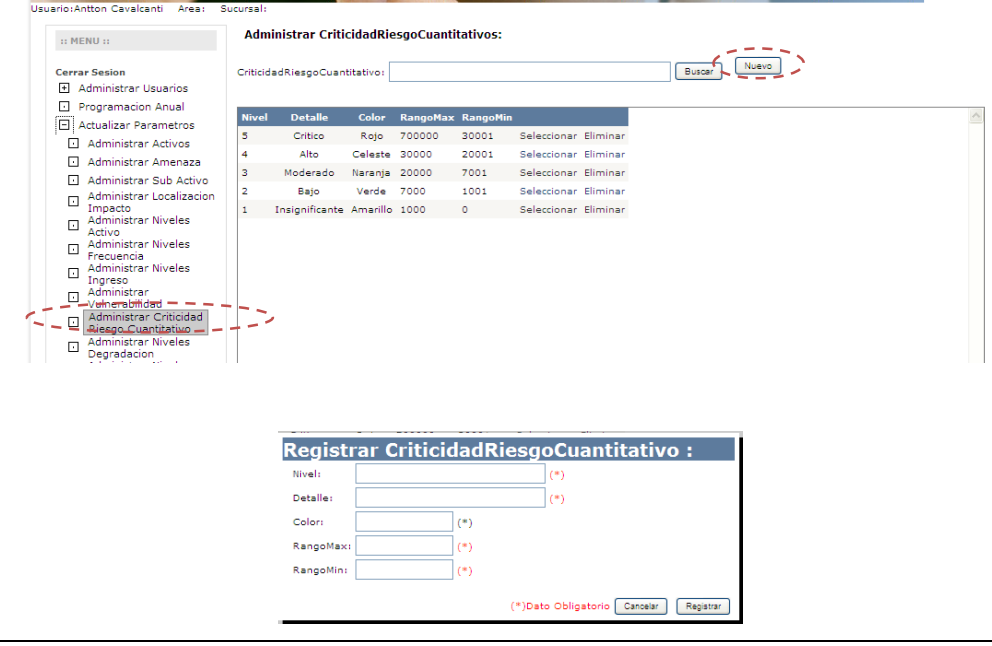
En la siguiente pantalla el administrador realizara el registro de los niveles de Frecuencia. Actualmente existen 5 descritos por la empresa: Muy frecuente, frecuente, normal, poco frecuente, raramente.

Pantalla Niveles de Ingreso



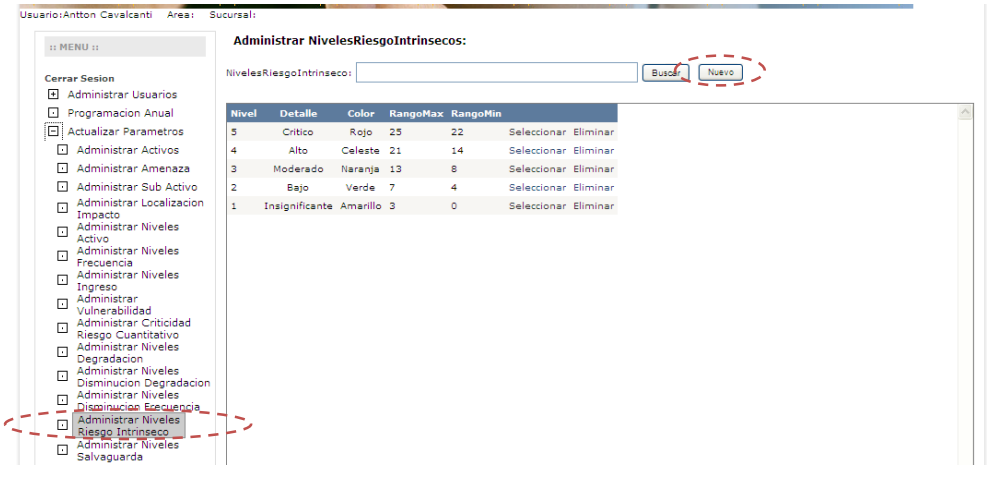
En la siguiente pantalla el administrador realizara el registro de los niveles de Ingreso, presentes en la empresa. Actualmente existen 5 niveles descritos por la empresa: muy Alto, alto, medio, bajo, insignificante.

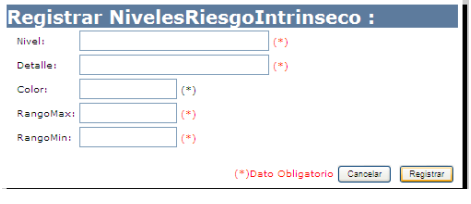
Pantalla Criticidad de Riesgo Cuantitativo



En la siguiente pantalla el administrador realizara el registro de los niveles de criticidad de riesgo cuantitativo. Actualmente existen 5 niveles descritos por la empresa: Crítico, Alto, Moderado, Bajo, Insignificante.

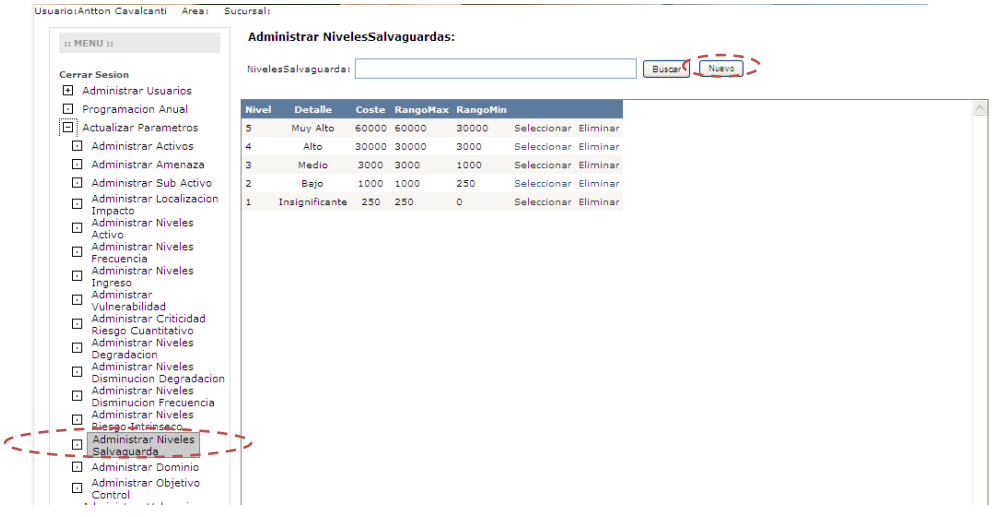
Pantalla Criticidad de Riesgo Intrínseco

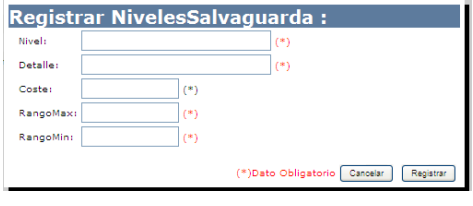




En la siguiente pantalla el administrador realizara el registro de los niveles de criticidad de riesgo Intrínseco. Actualmente existen 5 niveles descritos por la empresa: Crítico, Alto, Moderado, Bajo, Insignificante. A diferencia del riesgo cuantitativo, los valores de los rangos son menores ya que son referenciales y ya debió pasar por un plan de salvaguardas.

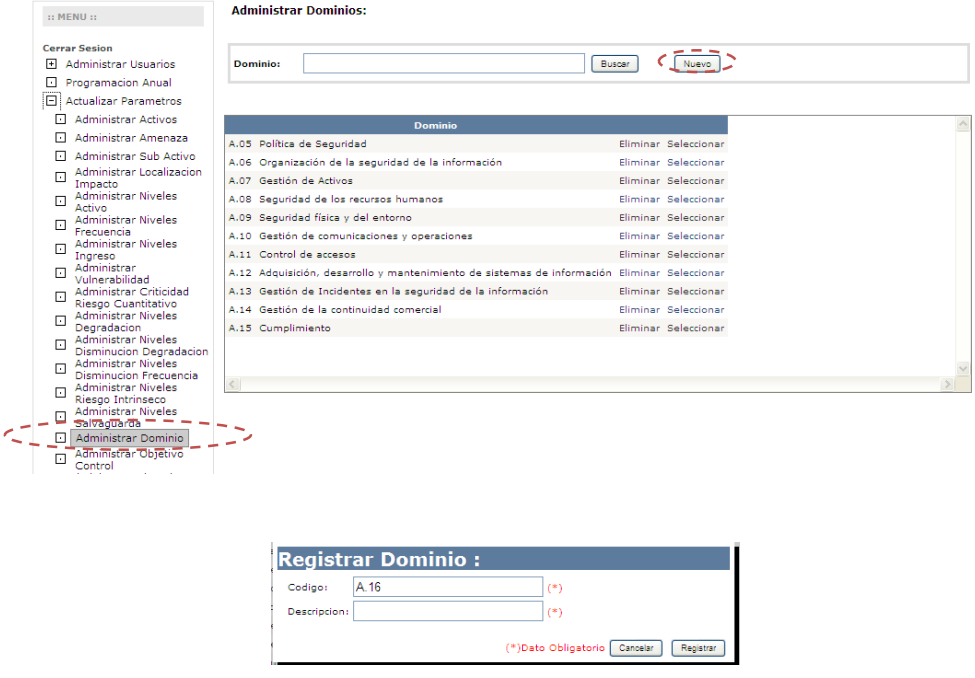
Pantalla Niveles de Salvaguarda





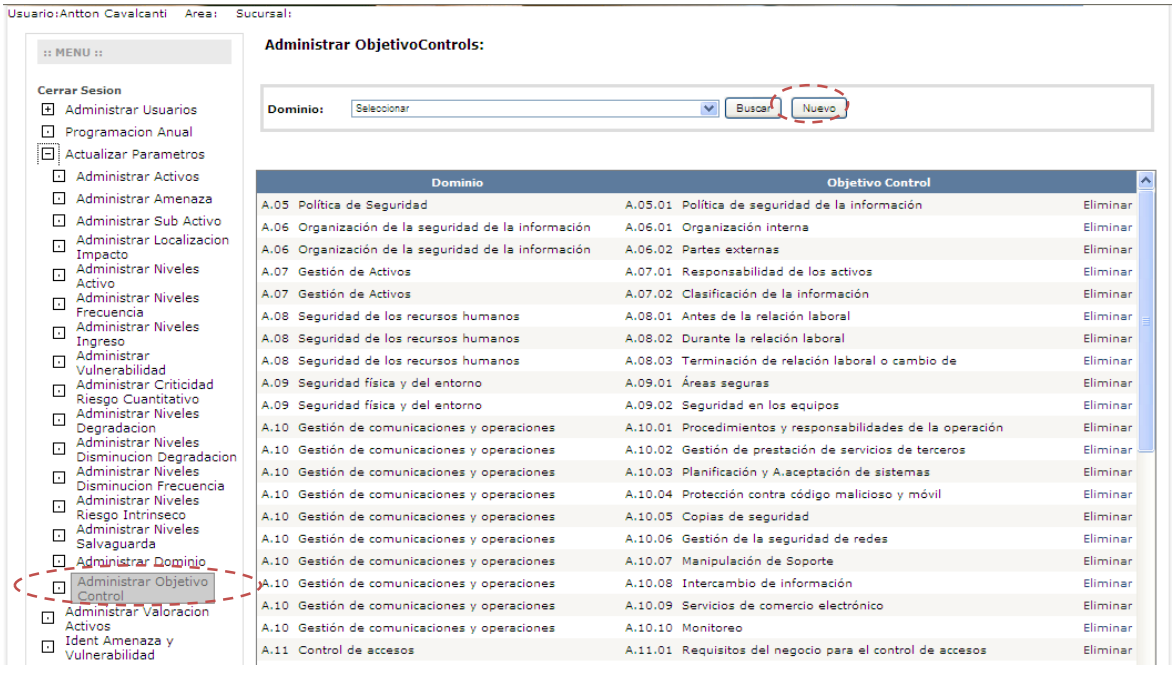
En la siguiente pantalla el administrador realizara el registro de los niveles de salvaguarda. Actualmente existen 5 niveles descritos por la empresa: Muy Alto, alto, medio, bajo, insignificante. Los niveles se ajustan al coste de la salvaguarda utilizada.

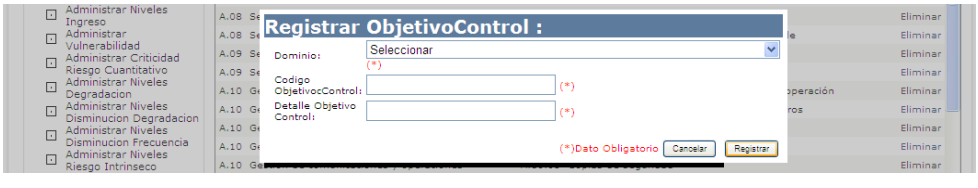
Pantalla Dominio

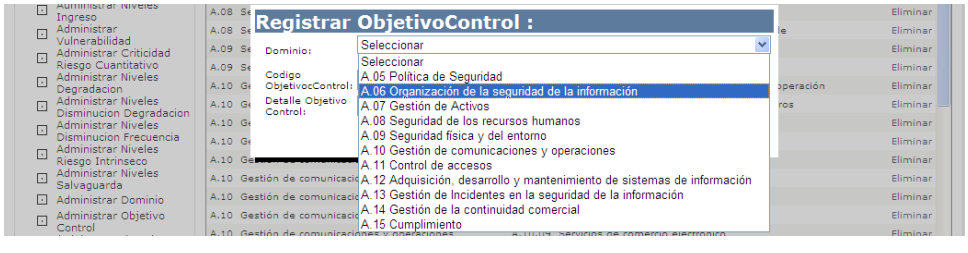


En la siguiente pantalla el administrador realizara el registro de los dominios de control a los cuales se adecua cada objetivo control.

Pantalla Objetivos de Control

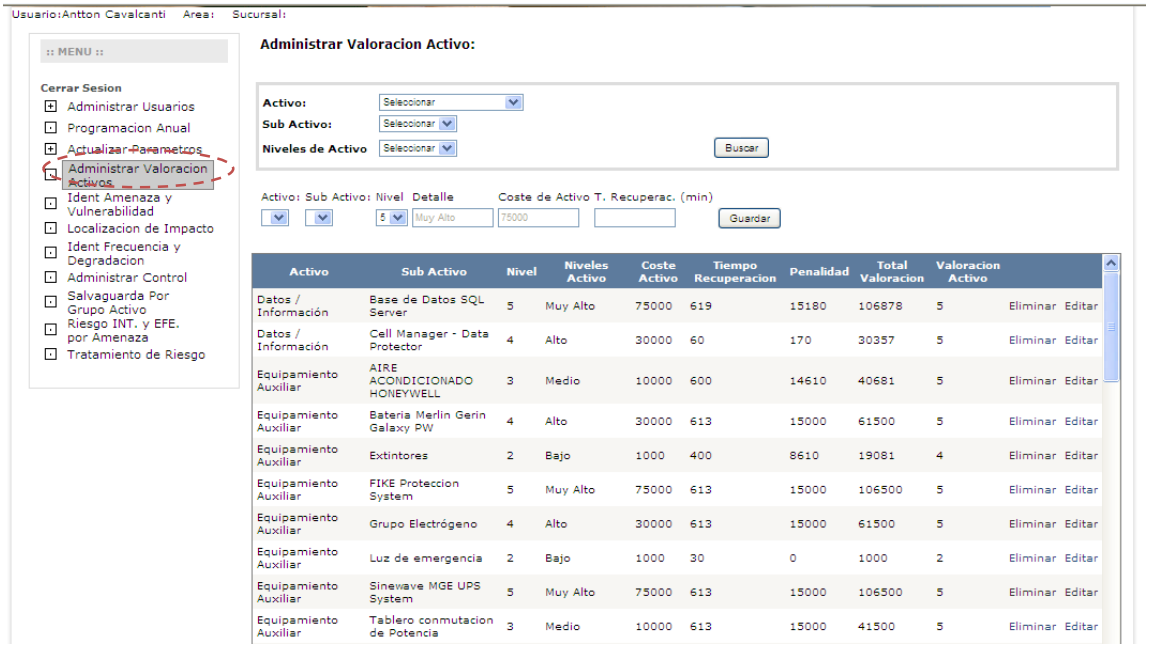




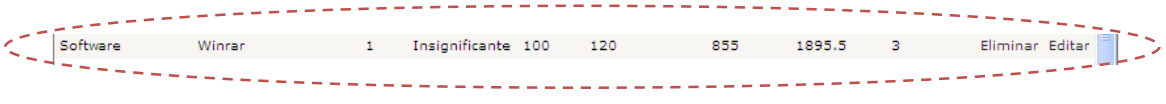


En la siguiente pantalla el administrador realizara el registro de los objetivos de control, dependiendo al dominio que se le deba asignar. Por ejemplo: Política de seguridad de la información, se encontraría dentro de dominio: Política de Seguridad.

Pantalla Valoración de Activos



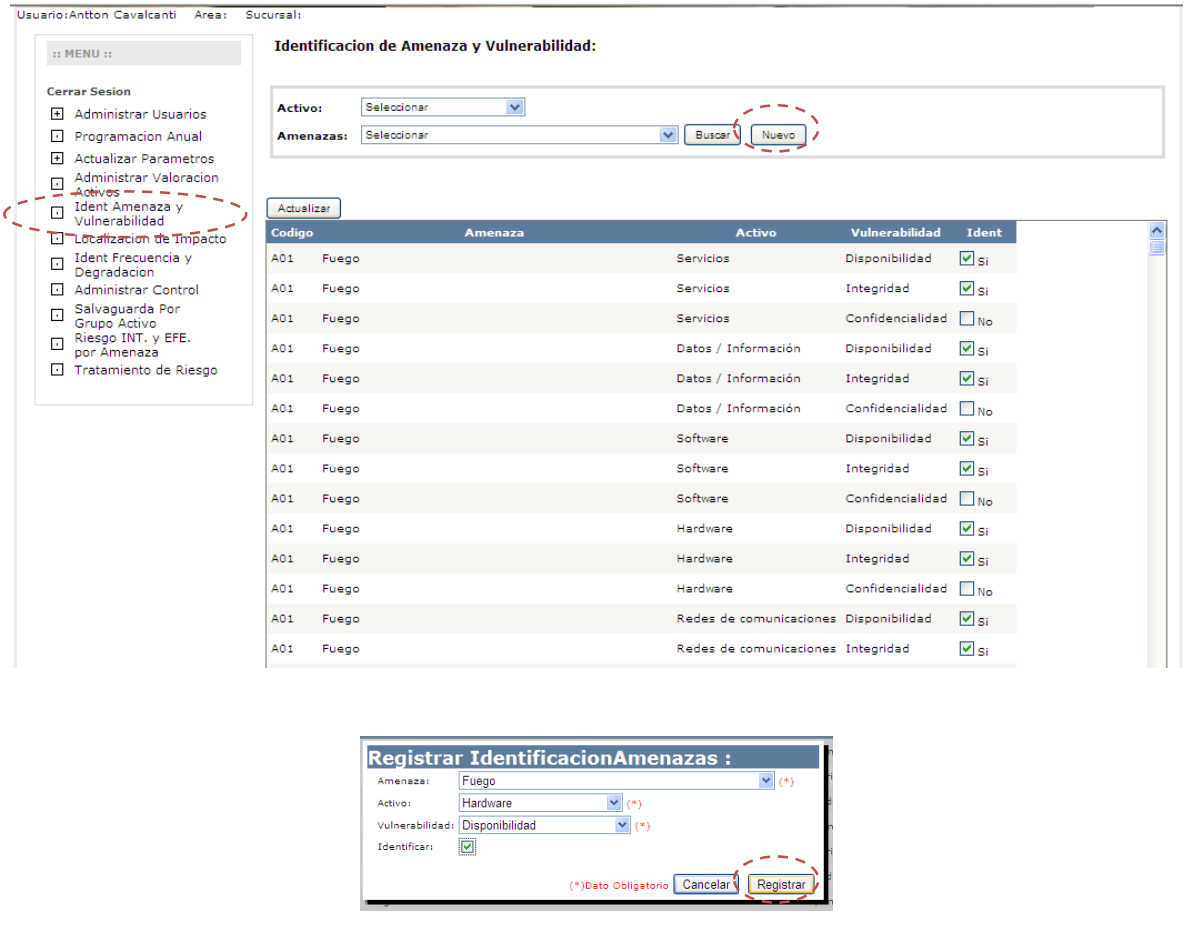
Una vez accedida la información, el sistema cuantifica la valoración del activo.



Una vez ingresados los parámetros por parte del Administrador. El usuario podrá realizar la valoración de activos. Esta valoración de activos nos podrá ayudar a verificar con un grado más fino los niveles con los que valora la empresa todos sus activos. Los parámetros a ingresar serian: nivele de activo y tiempo de recuperación. Una vez terminada accedido los datos el sistema realizara la valorización para tomarse en cuenta en la administración y tratamiento de riesgo. Ejemplo:

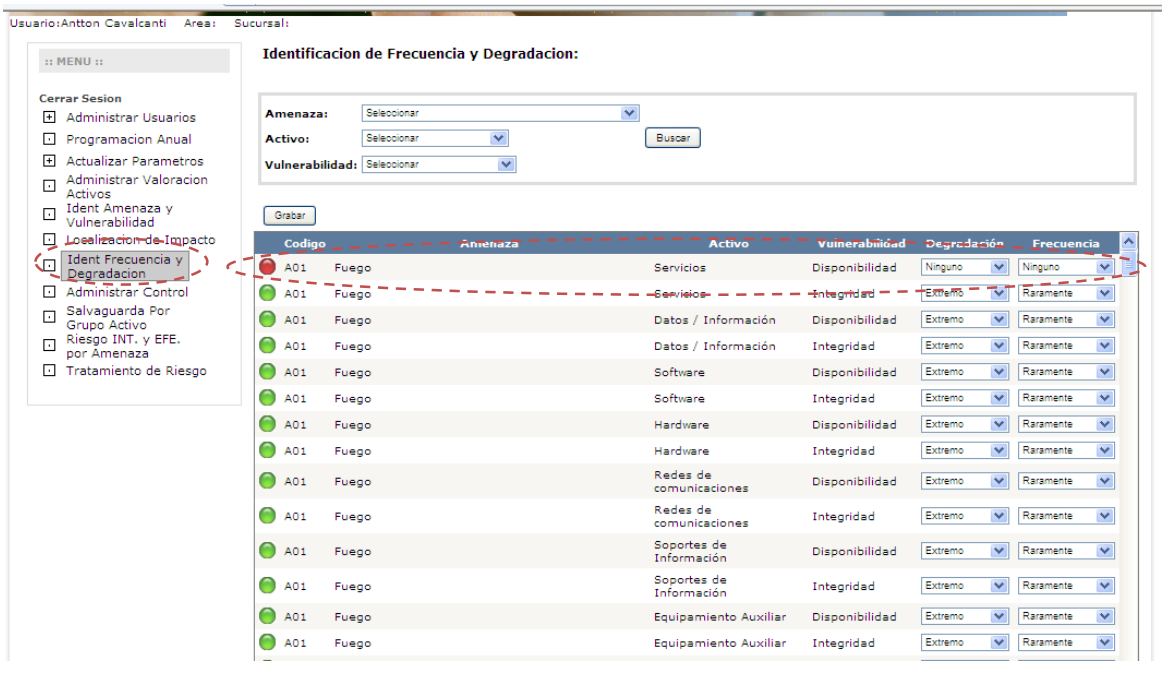
Activo: Software, SubActivo: Winzip, Tiempo de Recuperacion: 120.

Pantalla Identificación de Amenaza y Vulnerabilidad



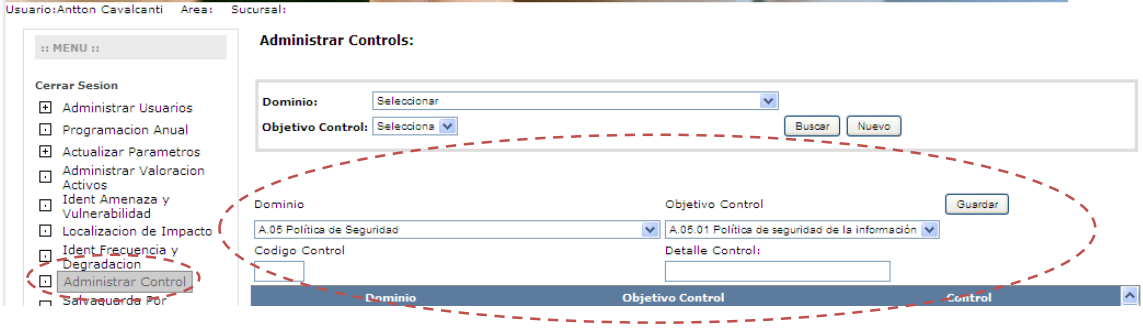
Una vez ingresado los parámetros de Amenaza, Activo y subActivo. El sistema podrá realizar la identificación de las Amenazas y Vulnerabilidades.

Pantalla Frecuencia y degradación



Esta pantalla servirá al usuario para asignarle los valores a la Degradación y Frecuencia a la que se encuentra expuesto el Activo. También podemos notar que se provisionó de semáforos para poder realizar el llenado más fácilmente, ya que los colores nos muestran si es que se pudo hacer el análisis o se encuentra en estado pendiente.

Pantalla Administrar Controles

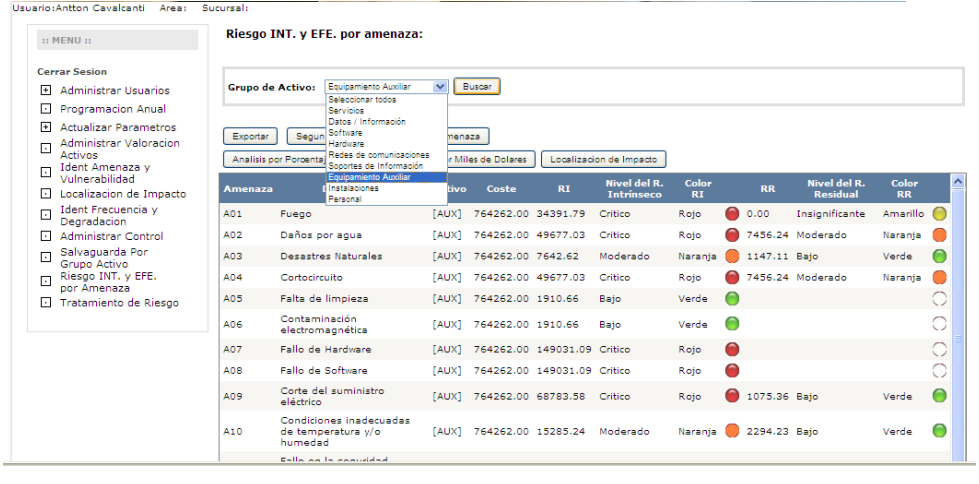


En esta pantalla el usuario podrá realizar la administración de controles para afrontar el riesgo, siguiendo los parámetros accedidos anteriormente. Posteriormente se asigna el Dominio, Objetivo Control, Codigo Control y se inserta el Detalle Control.

Pantalla Salvaguarda por Grupo de Activo

Una vez accedidos todos los controles, accederemos a la pantalla de salvaguarda por grupo de activos. Simplemente asignaremos el activo, la amenaza, el dominio en el que se encuentra, el control, la disminución de la degradación que se espera, disminución de la frecuencia y el coste. El sistema mostrara los datos accedidos en la grilla.

Pantalla Riesgo Intrinseco y Riesgo Residual



El usuario tendrá la posibilidad de ordenar la lista de Riesgos según el grupo de activo. Cabe subrayar que se logro darle semáforos a los niveles de los riesgos intrínsecos (RI) y riesgos residuales (RR). Que normalmente no teníamos una forma de ver rápidamente si se lograba minimizar el riesgo, una vez realizado el análisis. Ese requerimiento fue hecho por el cliente.

Pantalla Tratamiento de Riesgo

Primera pantalla de Tratamiento de riesgo:

El usuario tendrá una pantalla conteniendo: La amenaza, Criticidad del Riesgo Intrínseco y Criticidad del Riesgo Residual, además tendrá que realizar una toma de decisión acerca de Riesgo Objetivo y Tipo de Tratamiento a tomar.

Segunda Pantalla de Tratamiento de Riesgo:

Dándole click al nombre de la amenaza. Saltara una nueva pantalla, en donde veremos la amenaza contra las actividades propuestas y asignar a un responsable con su respectiva fecha de implementación del control. Una vez activados estos parámetros, automáticamente el sistema enviara a su correo un semáforo de alerta, indicándole el estado en que se encuentra el activo, la amenaza y la actividad propuesta.