Universidad Nacional de Misiones

Facultad de Ciencias Exactas Químicas y Naturales

Tesis de grado Licenciatura en Sistemas de Información

Análisis de Riesgo en Proyectos Software

Un nuevo método integrando la metodología SEI y Magerit2

Autor: **ASC. Sergio Daniel Caballero**

Tutor: **Mgter. Ing. Soft. Lic. Horacio Daniel Kuna**

Año: **2010**

Dedicatoria

Al amor de mi vida Alicia, que sin su apoyo no sería lo que soy.

A Horacio Kuna, por alentarme a seguir, ayudándome siempre.

A mi mismo por el esfuerzo de no bajar los brazos.

No importa cuán estrecho sea el camino,
cuán cargada de castigo la sentencia.
Soy el amo de mi destino;
soy el capitán de mi alma
(Nelson Mandela)

Resumen

Un riesgo es la probabilidad de que un activo genere pérdidas o no permita generar las ganancias esperadas. Para proteger los activos hay que identificarlos, analizarlos y gestionarlos.

La gestión de riesgos como metodología, utiliza métodos, técnicas, procesos y herramientas para gestionar los riegos encontrados en un proceso software. Para lograr hallar los mismos, existen métodos específicos como las taxonomías.

Debido a que las metodologías de análisis de riesgos más importantes están orientadas a grandes emprendimientos software y generalmente utilizadas en grandes organizaciones, son escasamente incorporadas en la mayoría de las pequeñas y medianas empresas.

Tomando esto, como un problema a solucionar, y utilizando las mejores prácticas de las metodologías investigadas, se presenta un método adaptado denominado Sei-Mag, que fue desarrollado con el objetivo de brindar simpleza y agilidad, sin perder la formalidad en las tareas de análisis y gestión de riesgo, creando un marco intuitivo, que agiliza el reconocimiento de los riesgos, incorporando elementos definidos y clasificados por otras metodologías, agregando tareas innovadoras y necesarias, como ser, la gestión de incidencias. Para lograr agilizar el reconocimiento, tratamiento y seguimiento de los riesgos, además de facilitar el uso del método, se desarrolló una herramienta asistente denominada MySeiMag.

Palabras Claves: *riesgo, análisis y gestión de riesgos, taxonomía.*

Abstract

A risk is the probability that an asset generates losses, or does not allow to generate the expected earnings. To protect the assets, they must be identified, analysed and managed.

Risk management as a methodology, utilizes methods, techniques, processes and tools to manage the risks found in software processes. To find them, there are specific methods, such as taxonomy. Because the most important risk analysis methodologies are orientated to large software enterprises and are commonly used in large organizations, they are rarely incorporated in most small and medium enterprises.

Taking this as a problem to be solved, and utilizing the best practices of investigated methodology, it is presented a new method, called Sei-Mag, which was developed in order to provide simplicity and flexibility, without losing the formality in analysis and risk management tasks, creating an intuitive framework, that streamlines the recognition of the risks, incorporating elements defined and classified by other methods, adding innovative and necessary tasks, such as incidence management. To achieve speed up recognition, treatment and monitoring of risks, and to facilitate the use of methods, it has been developed an assistance tool, called MySeiMag.

Keywords: risk, analysis and risk management, taxonomy.

Índice

Capitulo 1 - Introducción *……..*

……..13

1.1. Sobre la Tesis del Licenciado……..14

1.2. Audiencia……..14

1.3. Organización de la Tesis del Licenciado……

……..14

Capitulo 2 - Metodologías de Análisis de Riesgos *……..17*

2.1 Introducción ……

…..18

2.2 Los Riesgos ……23

2.3 La Gestión ……25

2.4 Riesgos ……33

2.4.1 Estrategias para Tratar con Riesgos ……

33

2.4.2 Identificación de Riesgos ……35

2.4.3 Técnicas de Identificación de Riesgos ……

…….37

2.5 SEI CRM ……41

2.5.1 Características ……41

2.5.2 Taxonomías ……43

2.5.3 Etapas ……49

2.6 MageritV2 ……

…….52

2.6.1 Características y objetivos ……

…..52

2.6.2 El Método ……

…..52

2.6.3 El catálogo de elementos ……59

2.6.4 Guía de Técnicas ……59

2.6.5 Conclusión ……60

2.7 Evaluación de Software ……61

2.7.1 Pilar ……61

Capitulo 3 – Problema encontrado y Solución sugerida *…… 67*

3.1 El problema Encontrado ……68

3.1.1 Análisis y Gestión de riesgos en las organizaciones ……68

3.1.2 Métodos informales del análisis de riesgos …… ……70

3.1.3 Dificultades de gestionar los riegos en las pequeñas y medianas organizaciones ……70

3.1.4 Metodologías poco adaptativas ……71

3.1.4.1 Desventaja SEI – CRM ……71

3.1.4.2 Desventaja MageritV2 ……73

3.2 Solución Sugerida……75

Capitulo 4 - La Metodología SeiMag*……77*

4.1 Característica …… ……78

4.2 Fase I – Análisis y Gestión de Riesgos ……80

4.2.1 Inventario de activos ……80

4.2.2 Propósitos y Objetivos del análisis de riesgos ……84

4.2.3 Equipo de Trabajo ……84

4.2.4 Taxonomía de Riesgos …… ……84

4.2.5 Declaración de los Riesgos …… ……92

4.2.6 Estimación de la probabilidad e impacto ……92

4.2.7 Exposición al riesgo ……94

4.2.8 Gestión de los Riesgos ……..

……..95

4.3 Fase II – Seguimiento y Control ……

99

4.4 Fase III – Registros de incidencias ……100

4.5 Fase IV – Comunicación ……..102

Capitulo 5 – La Herramienta –MySeiMag V1*……105*

5.1 Introducción ……..

106

5.2 Objetivos Generales del nuevo Sistema ……..

…..106

5.3 Metodología elegida y justificación de la misma ……

……..106

5.4 AgEnD- Metodología Ágil y evolutiva. ……..

…..107

5. 5 Aspectos particulares del sistema MySeiMag ……117

Capitulo 6 – Conclusión y Futuras líneas de investigación*……..125*

6.1 Conclusión de la Investigación ……

126

6.2 Futuras líneas de investigación ……127

Capitulo 7– Bibliografía *……..129*

- *Referencias bibliográficas ……*

130

Anexo I – Estudio de Caso*……..*

……..135

- *Estudio de Caso ……..*

……136

Anexo II- Artefactos*……181*

- *Proyecto ……..*
  ……..183
- *Casos de requisitos ……..187*
- *Casos de uso …….*
  ……..227
- *Diagrama de secuencia …….*
  ……..321
- *Modelo de datos ……..329*
- *Casos de prueba ……..331*

Anexo III – Encuesta *……..337*

- *Encuesta realizada ……..*
  338

Índices de Figuras

Figura 1 – Modelo de gestión de Riesgos.....20
Figura 3- Preocupaciones, Riesgos y Problemas.....23
Figura 4 – Descripción de Riesgos.....24
Figura 5 - Los Riesgos y las Fases de Desarrollo.....26
Figura 6 - Perfiles de los Riesgos en Proyectos de Software.....32
Figura 7 - La Incertidumbre Descriptiva.....35
Figura 8 - Taxonomía de Riesgos.....44
Figura 9 - TBQ – Proceso.....48
Figura 10 – Etapas de gestión de riesgos SEI.....51
Figura 11 - UPilar.....63
Figura 12 – Pilar Básico.....64
Figura 13– Pilar versión full.....65
Figura 14 – Rmat.....66
Figura 15- [SEI ,2004].....72
Figura 16 – Fases del método Sei-Mag.....79
Figura 17 - Estimación de probabilidad.....93
Figura 18 – Estimación de Impacto.....93
Figura 19- Login de acceso al sistema.....137
Figura 20- Menú Parámetros.....138
Figura 21 – Gestión de Grupos de usuarios.....139
Figura 22 – Gestión de Usuarios.....140
Figura 23 – Gestión de Tipo de Activos.....141
Figura 24 – Gestión de Elementos.....142
Figura 25 – Gestión de Dimensión.....143
Figura 26 – Gestión de Valoración.....144
Figura 27 – Tipo de Amenazas.....145
Figura 28 – Gestión de Amenazas.....145
Figura 29– Amenazas por tipo de Activo.....146
Figura 30 – Amenazas por Dimensión.....147
Figura 31 – Gestión de Salvaguardas.....147
Figura 32 – Asignación de Dimensiones a la Salvaguarda.....148
Figura 33 – Gestión de la Organización.....149
Figura 34 – Gestión de fuentes de información.....150
Figura 35 – Gestión de medidas de tiempo.....150
Figura 36 – Menú Etapa 1.....151
Figura 37 – Gestión de Activos.....152
Figura 38 – Asignación de elementos a un activo.....152
Figura 39 – Dependencia de activos.....153
Figura 40 – Asignación de fuente de información.....153
Figura 41 – Gestión de proyectos.....154
Figura 42 – Asignación de propósitos y objetivos al proyecto.....155
Figura 43 – Asignación de personal al proyecto.....156
Figura 44 – Gestión de equipos.....157
Figura 45 – Selección de proyecto para generar la taxonomía.....158
Figura 46- Gestión de elementos y fuentes de información.....158

Figura 47 – Gestión de declaración.....159
Figura 48 – Tabla de probabilidad de ocurrencia por riesgo.....160
Figura 49 – Impacto de ocurrencia por proyecto.....161
Figura 50 – Asignación de probabilidad e impacto.....162
Figura 51 – Exposición al riesgo.....163
Figura 52 – Información de riesgos.....164
Figura 53 – Recursos.....164
Figura 54 – Asignación de plan de acción.....166
Figura 55 – Plan de contingencia.....166
Figura 56 - Información necesaria.....167
Figura 57 - Responsable.....167
Figura 58 – Recursos.....168
Figura 59 – Menú Seguimiento.....168
Figura 60 – Plan de seguimiento.....169
Figura 61 – Agenda de actividades.....169
Figura 62 – Gestión de control de Seguimiento.....170
Figura 63 – Menú de seguimiento.....170
Figura 64 – Carga de incidente.....171
Figura 65 – Control de tipo de riesgo.....172
Figura 66– Detalle de riesgos encontrado.....172
Figura 67 – Reporte Plan de contingencias.....174
Figura 68- Finalización de un incidente.....175
Figura 69 – Menú de Informes.....176
Figura 70 – Informe por incidente.....177
Figura 71 – Parámetros de estadística.....177
Figura 72 – Estadística de incidentes por activo evaluado.....178
Figura 73 – Seguimientos realizados.....179

Objetivo General

El objetivo de esta investigación es generar un método de análisis y gestión de riesgos adaptando los requerimientos y necesidades informáticas y tecnológicas de las organizaciones, utilizando como base de estudio dos de las metodologías mas importantes de análisis y gestión de riesgos en IT, utilizando la metodología SEI CRM y adaptando técnicas y elementos de la metodología Magerit V2; para facilitar y automatizar la alta carga de trabajo, gestión, control y mantenimiento de proyectos basados en el método creado, en el marco de estas tesis se realizará una herramienta software. El método y la herramienta servirán para analizar y gestionar los posibles riesgos que pueden tener los activos; generar un procedimiento de seguimiento de los planes de acción de los riesgos gestionados, comunicar y registrar los incidentes ocurridos para evaluar posteriormente el nivel de los ajustes a realizar en el AGR[1], esto ayudará a eliminar o minimizar los incidentes ocurridos, además, resguardar los activos de las organizaciones para que estos no corran riesgos desconocidos o que su impacto sea mínimo y controlado.

[1] Análisis y gestión de riesgos.

Capitulo 1

Introducción

1. Introducción

En este capítulo se presenta brevemente el trabajo a desarrollar y la estructura de la organización del mismo.

1.1. Sobre la Tesis del Licenciado

Esta tesis de licenciatura trata sobre el desarrollo de un método para el análisis y la gestión de riesgos en proyectos software a ser desarrollados y/o implementados en pequeñas y medianas empresas.

El trabajo persigue como objetivo fundamental el de brindar un simple, intuitivo y formal método, para lograr agilizar el reconocimiento, tratamiento y seguimiento de los riesgos, para agilizar y facilitar el uso del método se desarrollará una herramienta asistente.

1.2. Audiencia

El presente trabajo de Tesis de Licenciatura se encuentra dirigido principalmente a ingenieros de software, profesionales de la industria del software y cátedras universitarias vinculadas al software y enfocados a la administración de proyectos de desarrollo y dirección de centro de cómputos.

La documentación contenida en este trabajo puede tomarse como referencia para la adopción de prácticas básicas y avanzadas de gestión de riesgos en un entorno de desarrollo o en un centro de cómputos.

1.3. Organización de la Tesis del Licenciado

El documento se divide en siete capítulos y en tres anexos que abarcan la totalidad del trabajo de Tesis del Licenciado.

- El Capítulo 2. Metodologías de análisis de riesgos. Muestra una introducción a los Riesgos, que son, como se gestionan, identifican los riesgos, la

taxonomía y la administración de los mismos. Describe las características principales de la metodología SEI –CMR y de la metodología Magerit V2.0.

- El Capítulo 3. Analiza los problemas detectados en la gestión de riesgos en las organizaciones actuales, los métodos informales de la gestión de riesgos, las dificultades de gestionar los riesgos, analiza y describe las desventajas de las metodologías estudiadas. Fundamenta una solución con un método adaptativo propio.

- El Capítulo 4. Se expone las características principales, las fases y etapas del método desarrollado "Sei-Mag".

- El Capítulo 5. Se presenta una herramienta Software para la aplicación del método creado. Características generales de la herramienta y la metodología utilizada para el desarrollo de la misma y los aspectos particulares del sistema.

- El Capítulo 6. Se expone la conclusión del trabajo realizado y las futuras líneas de investigación.

- El Capítulo 7. Muestra la Bibliografía que se utilizó para la realización de este trabajo.

- Anexo I. Muestra un estudio de caso real, en donde fueron probados el método y la herramienta.

- Anexo II. Muestra los artefactos utilizados en el análisis, diseño y desarrollo del sistema MySeiMag.

- Anexo III. Muestra la encuesta realizada a las organizaciones.

Capitulo 2

Análisis de Riesgos basado en Taxonomías

Análisis de Riesgos en el Proceso Software

2.1. Introducción al Análisis y Gestión de Riesgo

El Análisis de Riego comienza en la etapa inicial de un proyecto de software, es decir, en el momento del examen de conceptos básico, y se prolonga a lo largo de su ciclo de vida, finaliza con la aceptación del resultado del proyecto.

Al llevar a cabo una Gestión de Riesgos, es esencial enunciar y describir de manera clara y precisa el riesgo, inferir los síntomas y sus derivaciones, con el objetivo de que este pueda ser interpretado y tratado convenientemente.

La incorrecta Gestión de Riesgos impide alcanzar el control seguro de un proyecto, y la apropiada dirección del mismo.

Se puede pensar en un Riesgo, como la probabilidad que ocurra una perdida [SEI, 2004] y en la Gestión de Riesgos, como la metodología que utiliza procesos, métodos y herramientas para gestionar los riesgos hallados en un proyecto software; además, esta posee métodos específicos que identifican riesgos importantes y estrategias de gestión; provee de un entorno disciplinado para la toma de decisiones de una manera pre activa basándose constantemente en identificar que puede salir mal. [SEI, 2004]; Según [Rosenberg, *et al.*, 1999], la Gestión de Riesgos es importante debido a que ayuda a evitar desastres, re-trabajo y sobre-trabajo, pero aún mas importante, porque estimula la generación de situaciones del tipo ganar-ganar.

Una correcta Gestión de Riesgos otorga la posibilidad de optimizar los recursos, que derivan en el incremento de ganancias y la depreciación de pérdidas. Fundamentado las consideraciones expuestas anteriormente, se debe hacer hincapié en el grado de importancia que posee la Gestión de Riesgos, en todo tipo de proyectos y esencialmente en proyectos de desarrollo de software incluyendo las

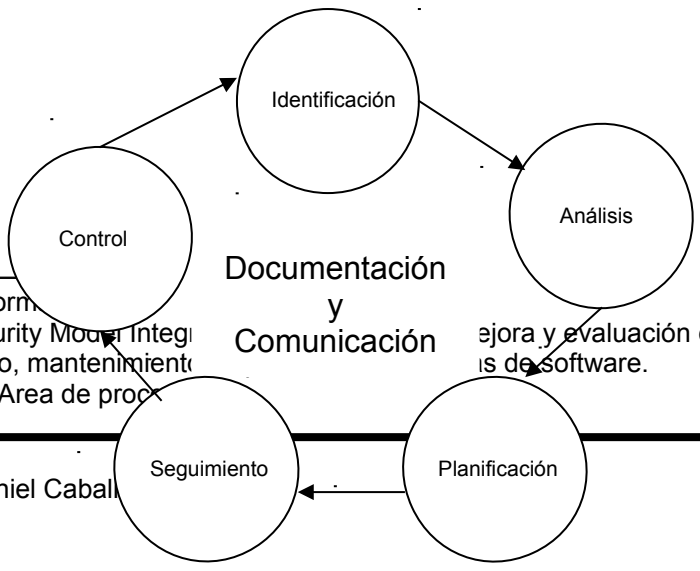
actividades y utilización de IT[2].

En proyectos de software la Identificación de Riesgos reside en establecer los componentes de riesgos potenciales utilizando algún procedimiento fehaciente, estructurado y metodológico; por lo cual, es considerado el paso más significativo entre los que constituyen las acciones de Gestión de Riesgos. Si no se logran determinar de manera correcta, es poco probable desarrollar y brindar indicaciones apropiadas ante los inconvenientes que surjan en el proyecto [Futrell, *et al.*, 2002]. El resultado de la individualización de riesgos identificados, es una enumeración de estos y sus correspondientes categorías.

CMMI[3] [CMMI, 2002] Se ha transformado en el nuevo estándar a nivel mundial para el control de la calidad de los procesos de desarrollo de software, y es un modelo para la determinación de la madurez de la capacidad de un proceso de software, presenta como una de sus PA[4] primordiales de Nivel 3 la Gestión de Riesgos.

Es preciso destacar, que existen diversos modelos de Gestión de Riesgos, el más usual consta de cinco pasos (Identificación, Análisis, Planificación, Seguimiento y Control) secuenciales e interactivos. Paralelamente coexisten dos actividades comunes a ellos: la documentación y comunicación (véase Figura 1 -Modelo de Gestión de Riesgos).

Gráfico que constituye el modelo referido:



[2] Tecnología Inform
[3] Capability Maturity Model Integ ejora y evaluación de procesos para el desarrollo, mantenimient s de software.
[4] Process Area, Area de proc

Figura 1 – Modelo de gestión de Riesgos

La Gestión de Riesgos en función a Taxonomías implica el valerse de una estructura, en la que los riegos son agrupados teniendo en cuenta sus diversidades, sirviendo como base de consulta al momento de llevar a cabo la tarea de Identificación de los Riesgos (la lista estructurada puede lograrse de la propia organización o también de otras fuentes, como por ej. : [Marvin J. Carr *et al.*, 1993] o [Microsoft, 2002]).

Definimos taxonomía como:

La clasificación ordenada de elementos conforme a su relación evidente; este razonamiento, presenta a las taxonomías como un instrumento de relevante utilidad en diferentes ramas de la ciencia y la industria, que posee la finalidad, de organizar y proporcionar el acceso a numerosos componentes que se hallan relacionados unos a otros de manera trascendental.

Por lo cual, las Taxonomías de fuentes de riesgos y la Identificación de Riesgos, adquieren un rol fundamental entre los objetivos trazados para el área de proceso de sistemas, relacionada al manejo de riesgos. Dado que las tareas enunciadas son inferidas como *Actividades* en el PA (véase Figura 2 -PA de Gestión de Riesgos en CMMI).

Adicionalmente, CMMI 2002, que es un modelo para la determinación de la madurez de un proceso de software y se ha convertido en el nuevo estándar a nivel

mundial para la medición de la calidad de los procesos de desarrollo de software, presenta como una de sus PA fundamentales de Nivel 3 la Gestión de Riesgos.

La figura Nº 2 muestra los distintos objetivos que deben realizar para la gestión de riesgos en CMMI, agrupados por los procesos de trabajos a elaborar.

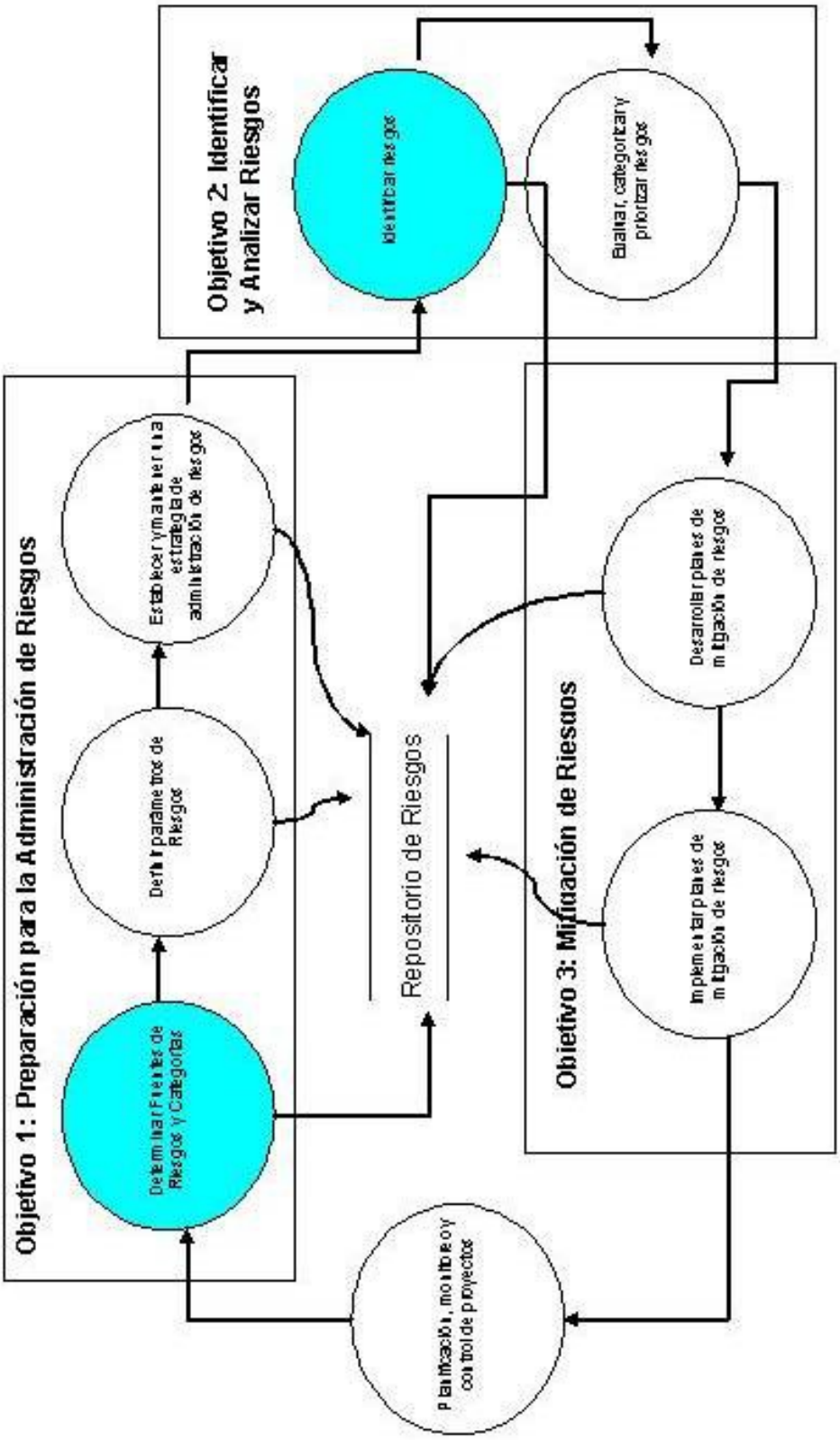


Figura 2 - PA Gestión de Riesgos en CMMI

2.2 Los Riesgos

En el ambiente de la Ingeniería de Software, un riesgo hace referencia a la "exposición a una pérdida" considerando la posibilidad de ocurrencia de un riesgo, como así también el impacto asociado. Mientras que para [SEI, 2004], un riego es "la posibilidad de sufrir una pérdida"

En muchas ocasiones se confunde preocupación, riesgos y problemas: se debe entender que una preocupación puede ser cualquier situación sobre la cual existen dudas en un delimitado contexto, se valora como un probable riesgo. Un problema es un riesgo, que ciertamente se ha producido (véase Figura 3 -Preocupaciones, Riesgos y Problemas).

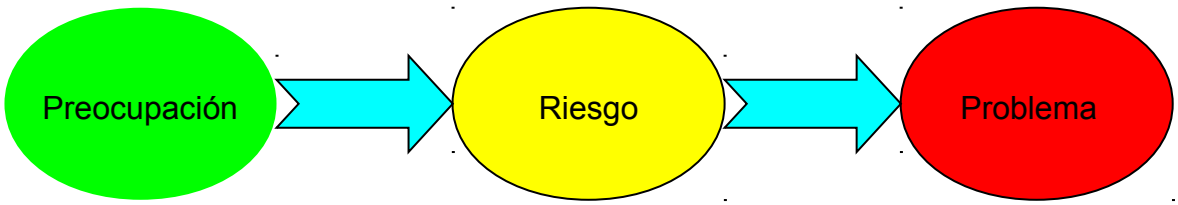


Figura 3- Preocupaciones, Riesgos y Problemas

En lenguaje natural se describe un riesgo, como la relación entre una situación real de proyecto y otra situación no deseada. Al primer segmento se lo designa condición y constituye una situación existente en el proyecto, que el equipo prevé, que podría implicar una pérdida o una disminución de beneficios. El segundo segmento se denomina consecuencia y refiere a la situación no anhelada para el proyecto, que podría ser la resultante de la ocurrencia de la condición. Las dos oraciones deben articularse por medio de un indicador de relación que simbolice incertidumbre y al mismo tiempo involucre una relación de tipo causal, por ej.: "como consecuencia de" (ver Figura 4 -Descripción de Riesgos).

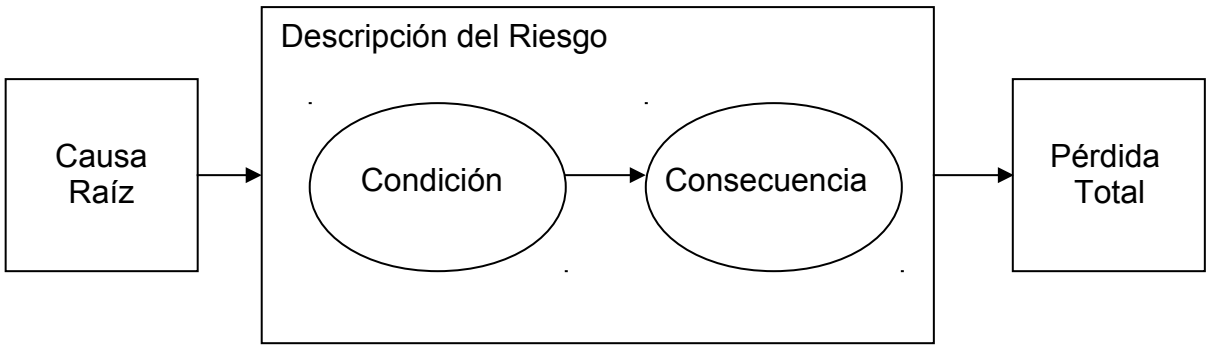


Figura 4 – Descripción de Riesgos

Podemos decir:

1. El riesgo que nos concierne, es el que podría producir en el futuro un problema, los riesgos pasados no nos atañen, son problemas que no se han solucionado. Lo primordial, es darnos cuenta hoy de los riesgos futuros y modificar nuestras acciones en el momento justo.

2. Todo riesgo implica un cambio de acciones, opiniones y modalidad de trabajo.

3. El riesgo implica una elección, la falta de certeza de que la elección sea correcta, es lo que nos debería preocupar. El Riesgo NO se puede evitar. [Charette, 1989]

4. El riesgo implica un daño probable [Magerit, 2002], el riesgos residual es el riesgo que permanece después de que se hayan tomado las medidas de seguridad correspondientes.

Al describir un riesgo la expresión debe ser estricta, específica y completa, posibilitando el análisis de la procedencia, el impacto y el despliegue de acciones o respuestas que prevengan y reduzcan los efectos. Resulta de utilidad adicionar información de contenido a un riesgo, siendo premisa contribuir con las personas, que no se encuentren al tanto de los detalles del proyecto, en la comprensión del tema.

En la descripción se deberá desechar el uso de abreviaciones o acrónimos que impliquen dificultad en la comprensión, generalizaciones y detalles irrelevante. La definición no deberá contener motivos ni características que generen duda alguna en la compresión y entendimiento.

Con el propósito de llevar a cabo una administración eficiente, describir un riesgo no es la única información que deberá disponerse y cotejarse, si bien posee un grado de importancia significativo, se hace necesario además, considerar un sin número de variables componentes. Por ello, usualmente el documento de descripción de riesgos o Base de Datos de Riesgos, se elabora separadamente del Plan de Riesgos.

2.3. La Gestión de Riesgos

Un proceso de gestión de riesgos eficaz, es un componente significativo para el progreso exitoso de cualquier proyecto de desarrollo software, teniendo en cuenta, que una gestión apropiada brinda posibilidades de éxito al proyecto y logro de los objetivos y propósitos a las organizaciones.

La gestión de riesgos de los proyectos permite además, definir en forma estructurada, operativa y organizativa una serie de actividades, a lo largo del desarrollo de software. En la mayoría de los casos, estas prácticas están destinadas a impedir que los riesgos se transformen en problemas.

El grado de importancia que posee la ejecución de una gestión de riesgos durante el ciclo de vida es destacadas por [Wideman, 1998] mediante el siguiente gráfico que muestra la correspondencia existente entre los riesgos y las distintas etapas del desarrollo (véase Figura 5 -Los Riesgos y las Fases de Desarrollo):

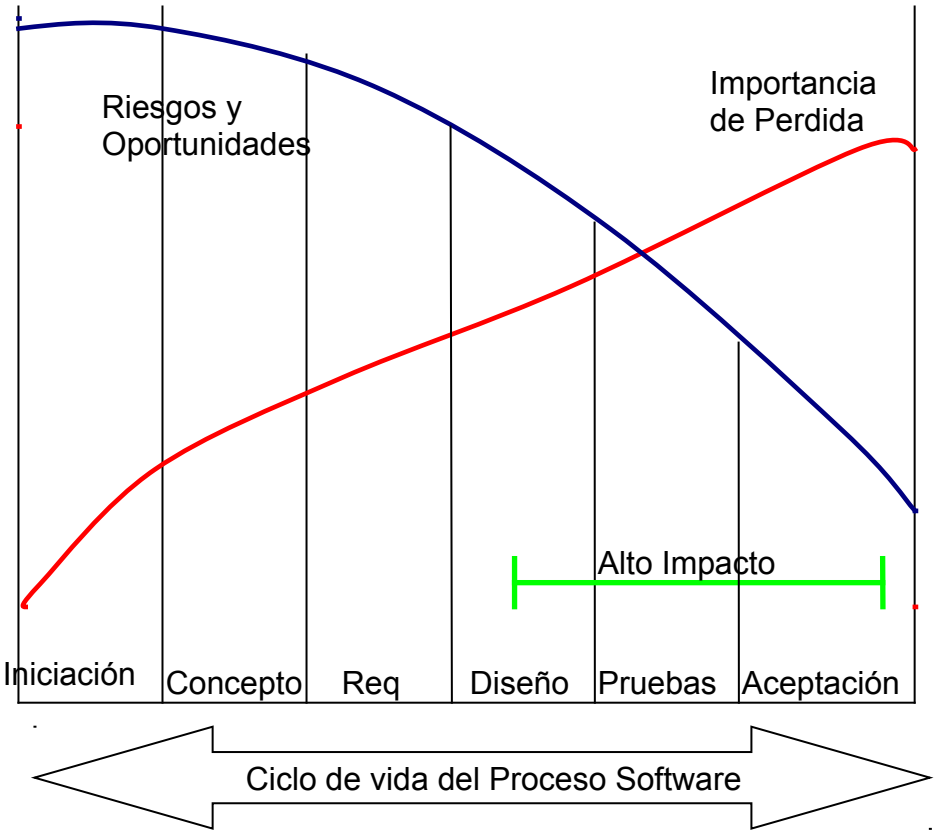


Figura 5 - Los Riesgos y las Fases de Desarrollo

Es básico para proyectos de cualquier tipo la gestión de riesgos pero, para los proyectos de desarrollo de software, esto es primordial; dado que, los emprendimientos están caracterizados por una serie de aspectos, que incrementan la presión sobre el proyecto, al obstaculizar la toma de decisiones a los responsables de administrar y gestionar los proyectos. Algunos aspectos pueden ser:

- Firmes presiones internas y externas.
- Cambios de las normativa técnicas, que podrían resultar en una variación de de las estrategias del proyecto.
- Habituales e incesantes modificaciones en los requerimientos de los beneficiarios.
- Modernización de las herramientas y tecnologías existentes.

- Persistentes riesgos en el campo de la seguridad.
- Inestabilidad de los recursos humanos.

Convendría tener en cuenta los siguientes aspectos [Motorola LMPS, 1999] para una política de gestión de riesgos de la organización exitosa:

.

- Los riesgos relacionados con los proyectos de desarrollo de software deben ser reconocidos, examinados, anticipados y estableciendo en un Plan de Gestión de Riesgos.

- El Plan de Gestión de Riesgos debe ser correctamente documentado. Esta documentación podría ser parte del Plan de Proyecto.

- Conservar en una Base de Datos de Riesgos de Proyecto separada, la lista de los riesgos y la información relacionada con su estado actual e historia reciente.

- A la Base de Datos de Riesgos se debe recurrir para ampliar la información incluida en la Base de Datos de Riesgos de la Organización.

Existen un conjunto de reglas concernientes con la Gestión de Riesgos, American Systems Corporation [ASC, 2003], las expone como reglas que se describen a continuación:

- ✓ Regla #1:
  "Los proyectos que no hacen gestión de riesgos se encuentran progresando a riesgo".

- ✓ Regla #2:
  "La gestión de riesgos no es gratuita, es necesario comprometer recursos, establecer planes y procesos y disponer de reservas".

- ✓ Regla #3:

  "Centralice las responsabilidades de gestión de riesgos porque la responsabilidad de administración distribuida debe ser coordinada".

- ✓ Regla #4:

  "Priorice los riesgos y concéntrese en aquellos que sean más críticos; a pesar de esto, todos los demás riesgos deberían contar con una estrategia de mitigación".

- ✓ Regla #5:

  "Los administradores de un proyecto son responsables por las acciones mientras que los administradores de los riesgos del proyecto son responsables por la identificación y seguimiento de los riesgos".

- ✓ Regla #6:

  "El proceso de gestión de riesgos debe definirse y seguirse de forma consistente en toda la organización. Todas las actividades deben ser tendientes a cumplimentar los requisitos de una política organizacional de gestión de riesgos".

Por último,[Microsoft, 2002] define una serie de principios básicos en los cuales asentar los procesos de gestión de riesgos:

- Agilidad:

  La agilidad requiere que los equipos de proyectos consideren y gestionen continuamente y de forma proactiva los riesgos en todas las etapas del ciclo de vida del proyecto software, debido a que los incesantes cambios en las facetas del proyecto involucran, paralelamente cambio de los riesgos. Una visión proactiva logra que un equipo asuma los cambios y los transforme en una oportunidad.

- Potenciar la comunicación:

  Los riesgos deberían discutirse de forma abierta y directa, tanto dentro como fuera del equipo de proyecto. Todos los integrantes del equipo deben participar, en mayor o menor medida, de las diferentes tareas relacionadas con la gestión de riesgos. Los miembros del equipo deben comunicar sus opiniones con libertad, a fin de evaluar con mayor precisión el estado del proyecto y tomar decisiones consensuadas.

- Aprender de todas las experiencias:

  El aprendizaje sólo puede ayudar a mejorar los resultados, el conocimiento obtenido en un proyecto puede reducir la incertidumbre de la toma de decisiones en otros proyectos cuando la información es poco fiable. El análisis directo de los resultados de proyectos anteriores fomenta el aprendizaje dentro del equipo mediante el intercambio de opiniones entre sus miembros.

- Participación necesaria:

  Si bien, la administración de los riesgos se encuentra centralizada. Es necesaria la responsabilidad de cada uno de los integrantes del equipo, en el proceso de Gestión de riesgos; además, de la responsabilidad por la tarea específica que le fuera asignada y una intervención activa en el proyecto.

- El riesgo es inherente en cualquier proyecto o proceso:

  Todos los proyectos sin excepción son amenazados por algún riesgo en mayor o menor grado de importancia.

- Pro actividad:

  La manera más efectiva de realizar una gestión de riesgos es la gestión de riesgos proactiva, ya que posibilita:

  - Pronosticar los problemas en vez de reaccionar ante ellos.
  - Analizar núcleo de un conflicto y no sus síntomas.

- Disminuir los períodos de respuestas y menguar el daño producido por una dificultad en etapas de crisis.

- La identificación de un riesgo es algo positivo:

  Se debe brindar precisión sobre los riesgos a enfrentar por el equipo del proyecto al realizar una gestión de riesgos de forma efectiva, dado que la moral de los miembros del equipo pueden verse negativamente influenciada cuando la complejidad de los desafíos y la dimensión de las pérdidas son indudables,

  Los riegos deben ser considerados como el único modo de crear la ocasión apropiada para conquistar los objetivos del proyecto. Siendo el proceso de tipificación de los mismos, lo que posibilita al equipo situar y tratar los riesgos de forma más eficaz.

- Valoración continua:

  Con el objetivo de detectar la aparición de nuevos riesgos, los equipos deben efectuar evaluaciones habituales del estado de los riesgos existentes, estimar o modificar los planes, a fin de prevenir o accionar frente a ellos. Esta consideración se debe, a los continuos cambios en los proyectos y los contextos operativos. Corresponde integrar en el ciclo de vida general del proyecto las actividades de gestión de riesgos.

- Primero especificar y luego administrar:

  El vínculo entre la gestión de riesgos y la toma de decisiones, lo establece la incertidumbre. Formular genéricamente un riesgo no logra dispersar la incertidumbre dando lugar a diferentes definiciones, que al ser axiomas permiten:

  - Afirmar que todos los participantes comprenden el riesgo de la misma forma.
  - Entender el origen de los riesgos y la correlación con los problemas en los que puedan resultar.

- Contar con una base para ejecutar un examen veraz y cuantitativo, proyectando los esfuerzos vinculados al proceso de administración del riesgo.
- Acrecentar la convicción de la capacidad del equipo por parte de los patrocinadores del proyecto.

- Las situaciones no deben juzgarse sólo por el número de riesgos:

  Los proyectos de ningún modo convienen calificarlo por la cantidad de riesgos encontrados; si bien los integrantes del equipo y los patrocinadores perciben la cantidad de riesgos encontrados como una contrariedad. Recordar que, un riesgo es únicamente una probabilidad, no la seguridad de una pérdida ni un resultado por debajo de lo esperado.

La relación que existe entre un punto de vista proactivo y un enfoque tradicional para las actividades de gestión de riesgos a través del ciclo de vida de un proyecto software, la ilustra claramente la siguiente figura [Walker, 1998] (véase Figura 6 -Perfil de los Riesgos en Proyectos de Software):

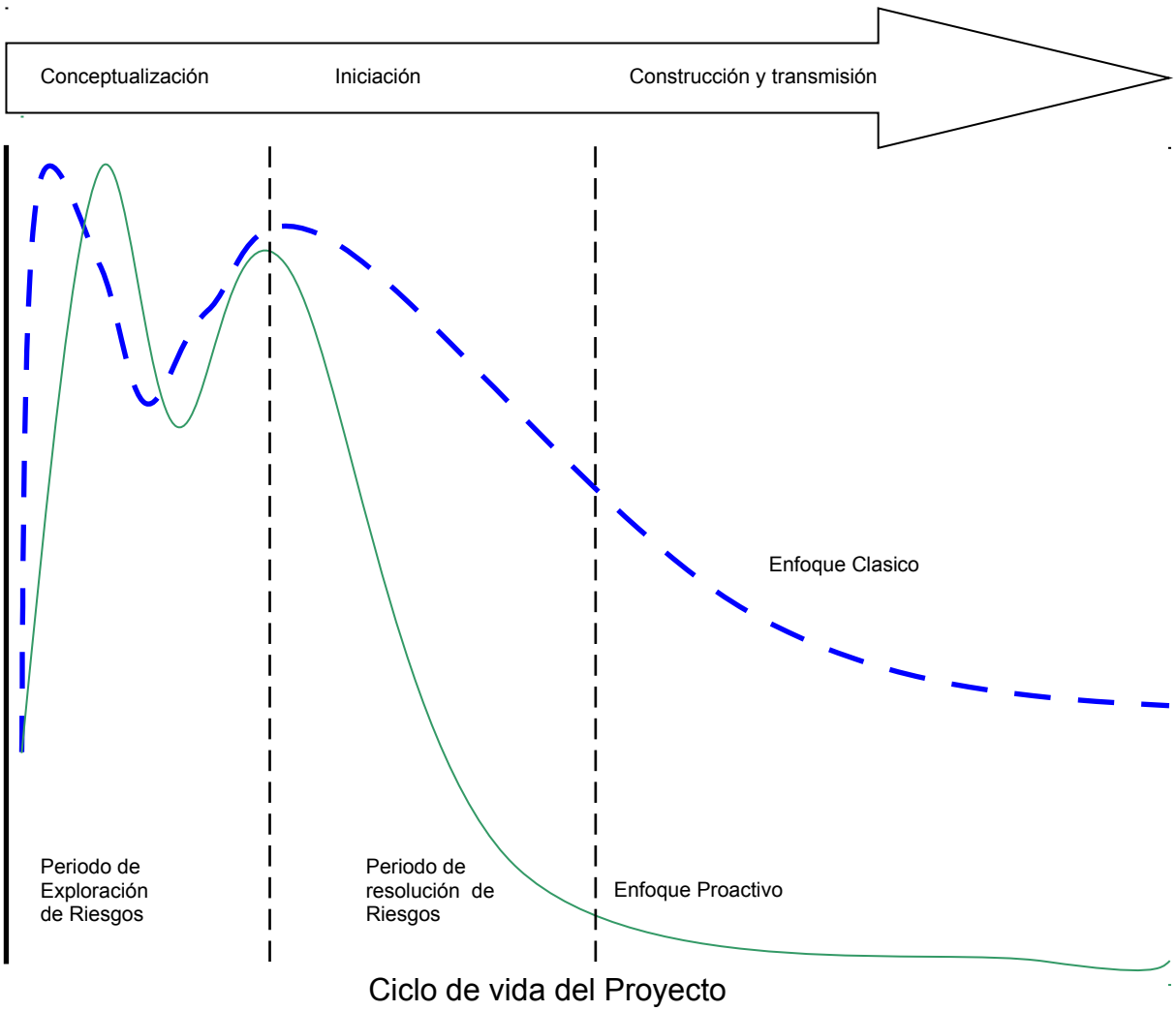


Figura 6 - Perfiles de los Riesgos en Proyectos de Software

En resumen podemos decir que la gestión de riesgos se basa, en el tratamiento proactivo de los riegos y en considerar la administración, como una iniciativa positiva inserta en un proceso criterioso y metódico.

2.4 Riesgos

2. 4.1 Estrategias para Tratar con Riesgos

Una adecuada definición de estrategia de respuesta es, calificarla como la actividad, que debe ser realizada para operar un riesgo previamente a que este se concrete.

Se podría decir además, que es una de las medidas más significativas a adoptarse, en cada uno de los riesgos individualizados en el proyecto. Asimismo se destaca, que para cada uno de los riesgos identificados se puede optar por una estrategia diferente y que esta, a su vez, puede ser sustituida por otra distinta, al momento en que se ejecutan, revisiones continuas de los riesgos.

Existen diferentes estrategias de respuesta, entre las más reconocidas y utilizadas pueden destacarse:

- Aceptar:

  Utilizar esta práctica revela una declaración manifiesta hacia el riesgo. Es una técnica pasiva que se encamina hacia la admisión de cualquier derivación de un riesgo sin intentar prevenirlo. Usualmente es utilizada para riesgos estimados de baja o muy baja escala, cuando no se hace posible divisar ganancias relevantes al intentar disminuir el riesgo.

- Evitar:

  Esta técnica se enfoca en impedir la posibilidad de ocurrencia de un riesgo, su empleo involucra modificaciones referentes a las condiciones establecidas originalmente para el proyecto, por ejemplo:
  - Disminución del alcance del trabajo.

- Modificación de requerimientos y/o especificaciones.
- Cambios en el SOW (*Statement of Work*).
- Modificaciones en las líneas base del proyecto.

- Controlar:

  En esta práctica se identifica la adopción de acciones concretas y puntuales tendientes a restringir la posibilidad de ocurrencia o el impacto para un riesgo. Generalmente se realizan durante todo el ciclo de vida del proyecto y los elementos de IT que estos utilizan, se convierten en prototipos de respuesta más usuales para los riesgos. En muchos casos, las acciones asociadas a este tipo de estrategia se consideran como un "producto" del proyecto, controladas y monitoreadas como parte de las acciones habituales de seguimiento.

- Investigar:

  En esta técnica se diferencian todas las acciones, hasta que se haya realizado una mayor cantidad de trabajo y/o hasta que se conozcan una mayor cantidad de hechos. Es importante destacar que no se define ningún tipo de respuesta para la reducción de un riesgo, simplemente porque la estrategia se emplea cuando no es posible identificar una solución clara y se requiere llevar a cabo una investigación. Puede incluirse como parte del desarrollo de la técnica el realizar análisis de causa raíz - problema.

- Reducir:

  Esta práctica se ocupa activamente con la finalidad de alcanzar una reducción de los riesgos en base a la ejecución de una sucesión de "acciones planificadas y constantes", como por ejemplo: uso de prototipos, exámenes con especialistas, conformación precoz de un equipo multidisciplinario,

simulacros, reuniones del equipo de trabajo, reducción de dependencias, intervención del cliente, etc.

- Transferir:

  Es el proceso de trasladar algo de un lugar a otro o de una persona a otra. Esta práctica referencia ajustadamente a este pensamiento o concepto, por ejemplo: transferir un riesgo del equipo de proyecto a un proveedor o un cliente. Particularmente la transferencia involucra, utilizar proveedores especializados en áreas establecidas y competentes, para disminuir la manifestación final del riesgo. Ej. Seguridad de Redes, Hardware etc.

2.4.2. Identificación de Riesgos

La identificación de riesgos es la primera de las fases en cualquier metodología de análisis y gestión de riesgos. Determina completamente los componentes potenciales de riesgos, valiéndose de algún procedimiento estructurado y seguro con el objeto de alcanzar la disminución de la "incertidumbre descriptiva", es decir, tiene el objetivo de conseguir una adecuada identificación de los "problemas" factibles en el proyecto, y la administración adecuada de los mismos (véase Figura 7 -La Incertidumbre Descriptiva).

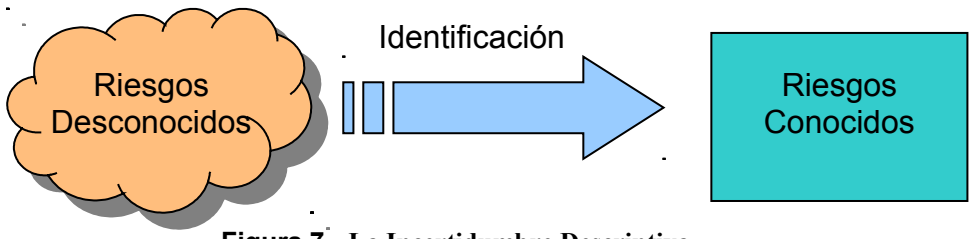


Figura 7 - La Incertidumbre Descriptiva

Es el paso más significativo de cualquier modelo, dado que, no identificar los riesgos apropiadamente conlleva a que las acciones para atenuarlos sean inadecuadas, con el agravante de que esta fase, es el inicio efectivo del proceso de gestión de riesgos.

Son dos, los aspectos primordiales en los que estriba la identificación de riesgos:

1. La comunicación abierta y la capacidad de pronosticar inconvenientes a posteriori

2. La contribución de ideas, fundadas en opiniones y experiencias que logren como resultado la excelencia en el producto final. Por lo cual, es trascendente la colaboración personal de los integrantes del equipo de trabajo.

Tal vez el aspecto más relevante en este ciclo, esta dado en detectar la mayor cantidad de riesgos posibles, garantizando un proceso de evaluación claro, sobre problemas futuros. En una primera instancia no se abarcará todos los riesgos. Un examen posterior, permite distinguir en cuales centrarse.

No es factible identificar todos los riesgos vinculados a un proyecto en un tiempo establecido, por lo que resulta primordial reiniciar esta fase del proceso de manera constante a lo largo de todo del ciclo de vida del proyecto, con el objetivo de conseguir la identificación de riesgos que podrían permanecer ocultos en las primeras revisiones.

Las entradas en la identificación de riesgos se componen, de toda la información disponible acerca de riesgos genéricos y específicos del proyecto en las áreas de negocios, técnicas, organizacionales y de entorno, que resulten destacables.

Si bien, los riesgos genéricos son una amenaza potencial para todos los proyectos, los riesgos específicos, solo pueden ser identificados, por personas con experiencia y visión clara sobre la tecnología a utilizar. Examinar el plan de proyectos y la declaración del ámbito del software - hardware para luego responder la pregunta ¿Qué características especiales de este proyecto pueden estar amenazadas? contribuirá a identificar los riesgos específicos.

Los aspectos adicionales a considera son: el enfoque organizativo a manera de estrategias, procesos, registros e investigaciones acerca del proyecto, conteniendo su período presente, pasado y la experiencia del equipo ante los riesgos. Todo lo que sea considerado por el equipo de proyecto, como aporte en la identificación de los riesgos, deberá ser tenido en cuenta. En las primeras etapas, es muy válido generar una metodología del proceso de conocimiento, ejecutando reuniones orientadas o talleres, tendientes a lograr un análisis sobre las apreciaciones que cada uno de los partícipes del proyecto poseen sobre de los riesgos y las oportunidades.

Los riesgos considerables del proyecto pueden ser identificados recurriendo a esquemas de clasificación de la industria (metodologías existentes), listas de control e informes de resumen de proyectos preliminares o cualquier otro origen de investigación divulgada.

En el transcurso de esta etapa es preciso utilizar la estructura del proyecto como plataforma para la tarea a llevar a cabo, las actividades de identificación serán asignadas a los miembros que se consideren mas adecuados del equipo. Es necesario ser meticuloso pero no irracional en el proceso, debe aspirarse a obtener una lista de riesgos tan perfeccionada como sea viable y no deben examinarse los riesgos reconocidos.

El resultado deseable de las acciones preliminarmente indicadas, es una declaración clara, consensuada y sin tergiversaciones que se registra a manera de listado, conteniendo una enumeración de los riesgos con los que el equipo de proyecto deberá analizarla. Esa lista se transforma en una tabla que será la entrada principal para la siguiente etapa de estudio del proceso de gestión de riesgos.

La tarea de identificación de los riesgos genera una importante cantidad de información válida, que incluye la individualización de las causas raíz y los consecuencias que provocan, las partes afectadas, el propietario, etc.

2.4.3. Técnicas de Identificación de Riesgos

Durante la fase de identificación de riesgos, los métodos y herramientas que se emplean son variados; en ocasiones, la elección del método considerado más conveniente a utilizar, esta basado en las particularidades del equipo de proyecto. Se debe remarcar además que, frecuentemente, estas prácticas suelen utilizarse combinadas. Las más utilizadas son:

- Tormenta de ideas:

  En este método, los miembros identifican los posibles riesgos sin utilizar ningún formalismo o estructura como base, y de forma oral, en donde existe un moderador y no se permiten "críticas" a ninguna de las ideas expresadas por los participantes, para permitir construir nuevas ideas en base a los pensamientos de otros. Para lograr los resultados esperados, es importante elegir como miembros del grupo a personas que estén familiarizadas con los temas a discutir y, en muchos de los casos, suele ser común el entregar documentación pertinente, antes de las sesiones de identificación de riesgos con el fin de lograr una mayor efectividad. El uso de esta técnica suele trasladarse además a otras etapas (por ejemplo, al momento de generar estrategias de mitigación).

- Encuestas:

  Se denomina así a la sucesión de preguntas destinadas a lograr la identificación de riesgos en un plano específico de interés. Este procedimiento algunas veces plantea la problemática de que las personas sienten cierto rechazo a las mismas, y por consiguiente no otorgar información apropiada; Es también, una tarea complicada el apreciar de manera correcta las respuestas, por el grado de subjetividad relacionada a estas. Una ventaja importante es la posibilidad de alcanzar una gran variedad de respuestas e información, evitando reunir a los participantes para lograr el objetivo.

- Entrevistas:

  Básicamente se fundamenta en la idea de la utilizar una serie de consultas, para establecer la línea base de riesgos, es una práctica relevante pero, debe pensarse que el proceso de entrevistas es solo un mecanismo de preguntas y respuestas, en donde el resultado final dependerá exclusivamente por la capacidad del entrevistador y de la formulación apropiada de las preguntas. Usualmente se entrelazan la utilización de las entrevistas con el de la tormenta de ideas, de manera anterior o posterior a la reunión, como manera de acceder a la concepción de ideas o dispositivo de validación.

- Grupos de trabajo:

  Son un mecanismo muy significativo para el análisis de un área o tema específico, al efectuar un planteo de discernimientos, que brinde la posibilidad de develar de riesgos, que podrían no ser elementales para el grupo que se encarga, concretamente de la individualización. Habitualmente los grupos de trabajo se encuentran integrados por individuos especializados en las distintas áreas temáticas referidas al proyecto.

- Conocimiento por experiencia o documentado:

  El conocimiento por experiencia es una recopilación de investigación que un sujeto ha conseguido a través su experiencia. El conocimiento documentado es la compilación de información que se ha documentado, referenciado a un tema específico. Es importante validar mediante referencias anteriores (empresas serias del ramo, entidades educativas prestigiosas etc), los conocimientos del experto y de la documentación, al momento de utilizar estas técnicas.

- Taxonomías de riesgos – Lecciones aprendidas:

  Las taxonomías son registros de riesgos que han sido hallados en programas, proyectos o situaciones análogas, a las que se pretende analizar. Es significativo considerar la importancia y la aplicación que tiene la información al hacer uso de esta practica. Las taxonomías se basan en la utilización de preguntas referidas a situaciones o eventos de un área específica de un proyecto o programa, pudiendo

derivar estos en una cadena de riesgos para el mismo; habitualmente estas preguntas están agrupadas por áreas temáticas (utilidades, costos, agenda, por ejemplo). Las lecciones aprendidas son conocimiento en función o la experiencia recogidas a través del tiempo, como investigación que puede ser apreciable en el momento de la identificación de riesgos para los distintos proyectos que se están elaborando en una organización.

- Salidas del Análisis Orientado a Riesgos:
  Existen diversos prototipos de análisis encaminado a riesgos, uno de ellos se funda en la utilización de árboles de análisis de fallas y el otro en el uso de árboles de análisis de eventos; ambos establecen un concepto de arriba hacia abajo, que pretenden estipular que eventos, condiciones o fallas pueden traer aparejada una circunstancias adversa. Esta situación con su derivación asociada puede componer un riesgo para el proyecto o programa.

- Información histórica:
  Es esencialmente lo equivalente a la información documentada y suele utilizarse de la misma forma, la diferencia entre ambas radica en que la información histórica suele ser, considerablemente aceptada como un hecho efectivo.

- Plantillas de ingeniería:
  Compuesto por un conjunto de diagramas de flujo referidos a diversos aspectos del proceso de desarrollo, y se emplean como guía de validación de las actividades a efectuar, durante un proyecto utilizando una visión de arriba hacia abajo. Dado que tienen información de entradas, salidas y acciones esperadas para cada segmento del proceso, y también de los factores implicados, brindando normalmente un significativo marco de referencia. El hecho de que estas plantillas estén incompletas, podría considerarse como un inconveniente substancial, En caso de escogerse su utilización, se exhorta llevar a cabo una meticulosa revisión de las mismas.

- Plantillas de camino crítico:

Estas plantillas adoptan también el nombre de plantillas Willoughby y se caracterizan por mostrar áreas de riesgos y suministrar un mecanismo de disminución de los mismos, para cada una de las fases de un ciclo de vida de desarrollo de software, dado que hacen posible su identificación fácilmente. Debido a las constantes actualizaciones de estas plantillas, es primordial tener en cuenta que, se debe contar con información lo más actualizada posible a la hora de recurrir a esta técnica.

2.5 Modelo de Gestión de Riesgos SEI – CRM

2.5.1 Características

El método Continuous Risk Management (SEI-CRM), desarrollado por el Software Engineering Institute (SEI), es una metodología en el ámbito de la ingeniería del software cuyos conceptos, procesos y herramientas permiten gestionar de manera continua los riesgos de un proyecto, proporcionando un entorno disciplinado para la toma proactiva de decisiones a lo largo de todas las fases del proyecto: análisis de los problemas en potencia (riesgos), determinación de los riesgos importantes, para elaborar estrategias y planes de gestión. Además, esta metodología también incluye el concepto de gestionar estas actividades como un ciclo básico, es decir, identificar, analizar, planificar, seguir, controlar y comunicar los riesgos a lo largo de todo el ciclo de vida del proyecto. (Véase Figura 1 -Modelo de Gestión de Riesgos).

El modelo gráfico tiene forma circular, a fin de indicar que la gestión de riesgos establece un proceso continuo, y el sentido de las flechas, pretende mostrar el orden lógico del intercambio de información entre cada una de las etapas que constituyen el modelo.

En el centro se ubican la comunicación y la documentación, con el fin de hacer resaltar el hecho de que, constituyen los elementos conectores del modelo y el de evidenciar, que en numerosos casos crean las mayores dificultades del proceso de gestión de riesgos. [Marvin J. Carr *et al.*, 1993]

Etapas del Modelo de Gestión de Riesgos SEI - CRM

1º Identificación: Permite anticipar los riesgos antes de que estos ocurran y se transformen en problemas serios afectando adversamente el desarrollo del proyecto. Cabe destacar, que la identificación de riesgos (al igual que cada una de las etapas del modelo) convendría sea realizado de manera disciplinada y consistente, estimulando a los miembros del equipo de proyecto a formular sus inquietudes y facilitando el análisis posterior.

2º Análisis: Pretende transformar una serie de datos que han sido obtenidos en la etapa de identificación, en información que permita llevar adelante una toma de decisiones enfocada en los riesgos más importantes para el proyecto. "El análisis de riesgos es un proceso sistemático de estimación de la probabilidad de ocurrencia y la magnitud de la pérdida o impacto de cada uno de los riesgos identificados mediante el cual se logra reducir la incertidumbre de la medida y del resultado del acontecimiento asociado a un riesgo." [Maniasi, 2005]

3º Planificación: Convierte a la información relacionada a cada riesgo, en medidas y acciones efectivas en un tiempo inmediato y futuro. Esta fase incluye el proceso de acciones para cada uno de los riesgos en particular, como así también, otorgar un rango de prioridad a las acciones y a la implementación de un procedimiento de administración integral de riesgos.

4º Seguimiento: Radica en monitorear continuamente el estado de los riesgos y las acciones que fueron adoptadas, con el objetivo de evitar o reducir las pérdidas. Realizar un seguimiento de los riesgos, conlleva inevitablemente a tener que tomar una serie de medidas vinculadas con la gestión, haciendo posible a los referentes de la administración del proyecto realizar una permanente y precisa revisión de los planes.

5º Control: Proporciona la factibilidad de corregir las desviaciones que puedan causarse a los planes de gestión efectuados.

La comunicación y documentación del proceso son significativas en el modelo, ya que la carencia de garantías en ellas imposibilita la aplicación de cualquier estrategia de administración. La comunicación está y se hace notoria en el modelo en distintos niveles: el primero de ellos, establece la comunicación que corresponde cumplir entre cada uno de las fases del proceso, un segundo nivel esta determinado por la comunicación dentro del equipo de proyecto y el tercer nivel por la que surge entre el proyecto y los diferentes participantes del mismo.

2.5.2 Metodología basada en Taxonomías

El método de identificación de riesgos basado en taxonomías fue desarrollado originariamente por el SEI [Marvin J. Carr et al., 1993], y en su versión original, trabaja agrupando las distintas fuentes de riesgos en varias categorías, y proveyendo de un cuestionario llamado TBQ[5] para realizar un proceso sistemático de identificación.

La taxonomía de riesgos presentada sigue el tradicional ciclo de vida de desarrollo de software en cascada y provee un marco para organizar los datos y la información. Adicionalmente, la estructura fundamental del método consta de un Cuestionario Basado en Taxonomías y un proceso para su aplicación.

La taxonomía organiza los riesgos de desarrollo de software en tres niveles (véase Figura 8 - Taxonomía de Riesgos):

- Clases.
- Elementos.
- Atributos.

[5] Taxonomy-Based Questionnaire, Cuestionario basado en taxonomías.

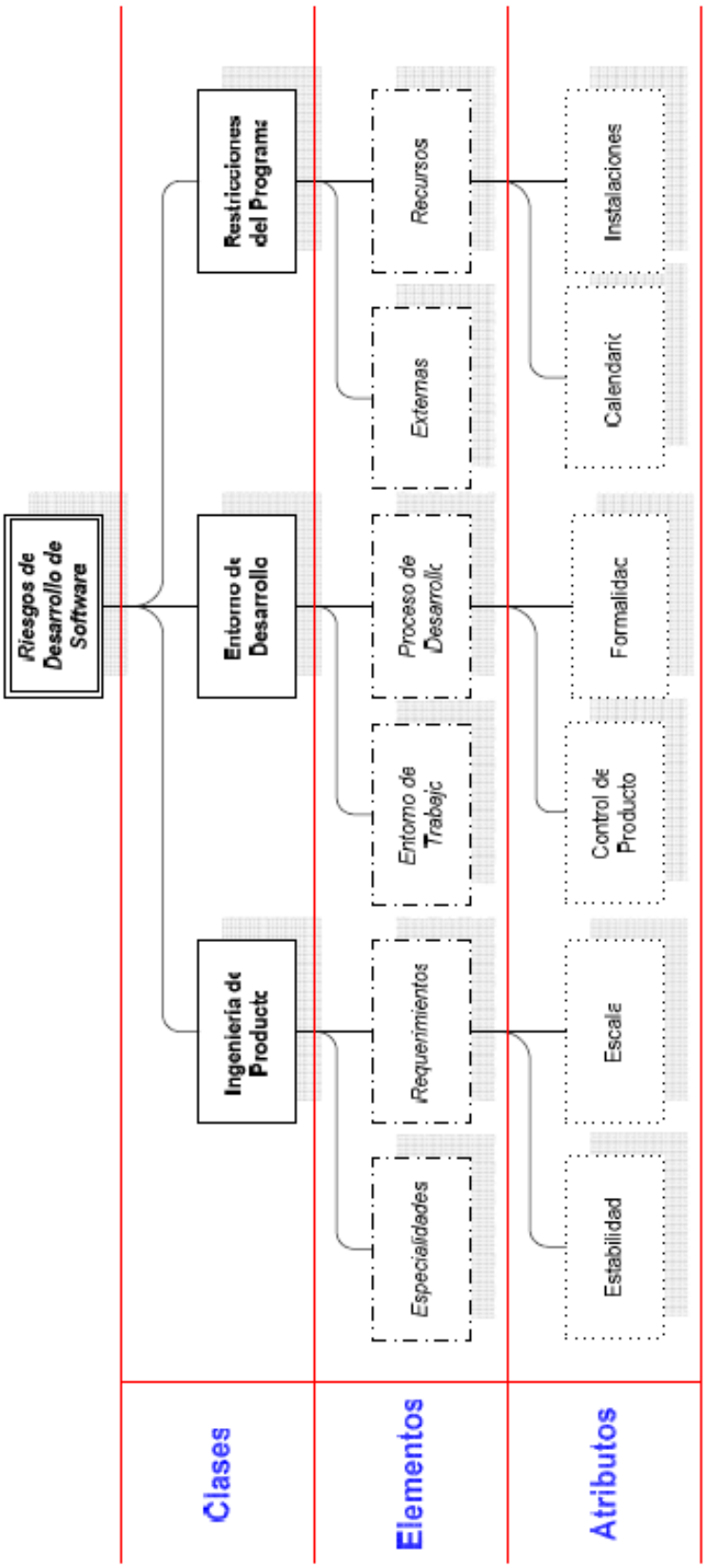


Figura 8 - Taxonomía de Riesgos

Tal como puede observarse, la taxonomía esta organizada en tres grandes clases, que a su vez, se dividen elementos caracterizados por una serie de atributos.

Las tres clases y elementos mencionados son:

Clases

- Ingeniería de Producto:
  Incluye los aspectos técnicos del trabajo a realizar.

- Entorno de Desarrollo:
  Involucra métodos, procedimientos y herramientas a emplear en la elaboración del producto.

- Restricciones del Programa:
  Abarca los factores contractuales, organizacionales y operacionales dentro del cual se enmarcar el software. Generalmente, se encuentran de manera externa a la operatoria de la administración del proyecto.

Elementos

- Ingeniería del Producto
  - Requerimientos: Los atributos de este elemento contempla la calidad de la especificación de los requisitos y la dificultad de implementar un sistema que satisfaga los mismos.
  - Diseño: Los atributos del diseño cubre, el diseño y la viabilidad de los algoritmos, funciones o requerimientos de performance, y las interfaces interna y externa del producto. Las dificultades en el testeo pueden comenzar, con el fallo de los elementos a ser testeados, e inclusive con el fallo del modelo de testeo.

- Código y unidad de Testeo: Los atributos de estos elementos, se asocian a la calidad y estabilidad de las especificaciones del software o sus interfaces, además de, los problemas que se podrían presentar en la implementación o dificultad en el testeo.-
- Integración y Testeo: Estos elementos cubren la integración y la planificación del testeo, ejecución e instalación del producto y la integración de este, dentro del sistema o el mismo entorno.
- Ingeniería Específica: Los requisitos específicos se tratan separadamente de los requisitos generales, frecuentemente son evaluados por especialistas que , no están dedicados "full time" al proyecto, pues son los responsables de evaluar elementos puntales.

  Esta separación taxonómica es un dispositivo, que asegura que sean convocados para el el análisis de los riegos asociados a los campos de su especialización.

- Entorno de desarrollo
  - Proceso de Desarrollo: Definición, planificación, documentación, adecuación, aplicación y comunicación de los métodos y procedimientos utilizados para el desarrollo del producto.
  - Proceso de Sistema: Herramientas y equipos de apoyo a utilizar en el desarrollo del producto, tales como la ingeniería de software asistida por ordenador (CASE), herramientas, simuladores, compiladores, y alojamiento del sistema.
  - Administración de Procesos: Planificación, seguimiento y control de presupuestos y tiempos; factores de control involucrados en la definición, implementación y pruebas del producto; experiencia del jefe de proyecto en desarrollo de software, gestión, el dominio del producto; y la experiencia del administrador, en relacionarse con organizaciones externas.
  - Administración de Métodos: Métodos, herramientas y equipo de apoyo a utilizar en la gestión y control del desarrollo de productos, tales

como, herramientas de monitoreo, gestión de personal, control de calidad y gestión de configuración.

- Entorno de trabajo: Ambiente general en que se realizara el trabajo incluye actitudes personales, niveles de cooperación, comunicación, y moral.

- Restricciones de Programas
  - Recursos: Limitaciones externas impuestas por horarios, personal, presupuesto, o instalaciones.
  - Contratos: Términos y condiciones del contrato del proyecto.
  - Interfaces de programas: Interfaces externas a clientes, demás contratistas, gestión empresarial y vendedores.

El cuestionario TBQ, consta de una serie de preguntas objetivas relacionadas con cada uno de los atributos de la taxonomía, diseñadas para deducir un conjunto de riesgos y preocupaciones, que potencialmente puedan afectar al producto o al proyecto en el cual se trabaja. El proceso se desarrolla considerando, la posibilidad de realizar una aplicación práctica, eficiente y consistente del cuestionario en los diferentes proyectos de una organización. La aplicación es semiestructurada y, tanto las preguntas como las consecuencias, se emplean como instrumento de definición de riesgos, que no limita el empleo de otras metodologías; mas aún, este cuestionario suele ser definido como una tormenta de ideas estructuradas. El TBQ produce mejores resultados, cuando es aplicado a través de un equipo independiente.

El proceso de aplicación de TBQ consta de cuatro etapas secuenciales (véase Figura 9 – TBQ - Proceso):

1. Compromiso de la Gerencia:

   Antes de comenzar la elaboración del cuestionario, es necesario contar con la aceptación y el compromiso de los ejecutivos de la organización, además seleccionar el proyecto sobre el cual se ejecutará la técnica, elegir los participantes de diferentes áreas, por ejemplo, personal de calidad o del equipo encargado de las pruebas.

2. Selección del Equipo y Entrenamiento:

   La conformación del equipo incluye la selección del personal del proyecto como también, la incorporación de personal perteneciente a la organización cliente. Una vez conformado el equipo, es preciso entrenar al grupo de trabajo en la técnica a utilizar, la responsabilidad de cada rol, y el protocolo de entrevistas a emplear, entre otros.

3. Identificación de Riesgos:

   La etapa de identificación comienza con la sesión de introducción, el equipo y de la metodología a emplear, luego, continúa con una serie de entrevistas al personal seleccionado, como miembro del grupo de participantes. Cada una de las entrevistas, se divide en dos etapas:

   - Preguntas y respuestas: Implica el uso explícito de TBQ.
   - Clarificación: Implica la aclaración de cualquier situación, comentario expresión recogida en la etapa anterior y que expusiera algún tipo de duda.

4. Conclusión de la Identificación: Finalizada la identificación se presenta a los participantes los resultados obtenidos.

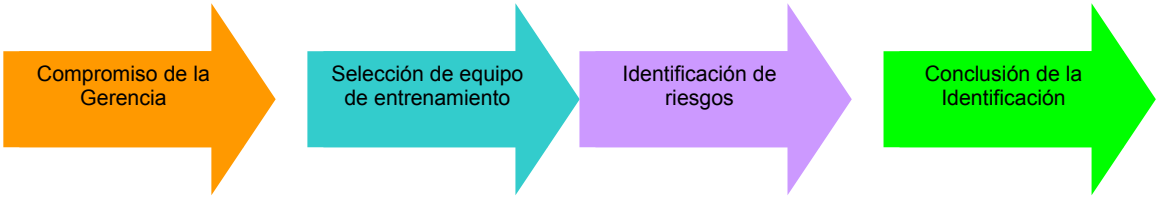


Figura 9 - TBQ – Proceso

Esta metodología, es un instrumento que posibilita obtener una amplia gama de riesgos a nivel del sistema y permite adicionalmente, destacar aquellas áreas que requieren mayor atención por parte del equipo de proyecto.

[Hantos, 2000] Afirma, que una serie de experiencias en el uso de taxonomías para las actividades de identificación de riesgos, han demostrado que la adaptación

previa a la realidad organizacional de las taxonomías estándares, posibilita obtener, mejores resultados con la mayor eficiencia.

2.5.3 Etapa de la Metodología

1º Etapa - Inventario de activos:

Se deberá analizar los activos que podrían ser amenazados por algún tipo de riesgo, como ser. Hardware y telecomunicaciones, software y personal.

2º Etapa - Propósitos y Objetivos del análisis de riesgos

En este punto se debe establecer los objetivos generales del análisis de riesgos y establecer claramente los límites que tendrá el proyecto.

3º Etapa - Equipo de Trabajo

Establecidos los límites y objetivos del análisis de riesgo se debe formalizar el equipo de trabajo que realizará la tarea.

4º Etapa - Taxonomía de Riesgos

En esta etapa se ordena de manera taxonómica los riesgos basados en el cuestionario TBQ descripto anteriormente en este capitulo.

5º Etapa - Declaración de los Riesgos

En las declaraciones de riesgos se definen en forma mas precisa los riesgos identificados, siguiendo un proceso de declaración en dos partes (condición – consecuencia). La condición describe una situación o atributo del proyecto existente que el equipo prevé que puede resultar en una pérdida en el proyecto o en una reducción de beneficios. La consecuencia describe el atributo o situación no deseable del proyecto. Además se incluyen los efectos que tendrían estos riesgos de no controlarse debidamente.

6º Etapa - Estimación de la probabilidad

La probabilidad del riesgo es una medida que calcula la probabilidad de que la situación descripta en el apartado de consecuencias de los riesgos de la declaración de riesgos llegue a producirse de verdad.

Para cuantificar la incertidumbre acerca de la ocurrencia de los riesgos se emplearán las categorizaciones expresadas en lenguaje natural, en base a un rango de probabilidades establecido en un cuadro de referencia.

7º Etapa - Estimación del impacto

El impacto del riesgo calcula la gravedad de los efectos adversos, la magnitud de una pérdida o el costo potencial de la oportunidad si el riesgo llega a producirse dentro del proyecto.

8º Etapa - Exposición al riesgo

La exposición al riesgo calcula la amenaza general que supone el riesgo combinando la información que expresa la probabilidad de una pérdida real con información que indica la magnitud de la pérdida potencial en un único valor numérico.

La exposición al riesgo se calcula multiplicando la probabilidad de riesgo por el impacto. Luego se utilizará la magnitud de la exposición al riesgo para clasificar los riesgos.

9º Etapa - Gestión de los Riesgos

Líneas de Acción

Para ejercer una adecuada gestión y supervisión de los riesgos mencionados anteriormente, se elaborará un Plan de Acción y un Plan de Contingencias para cada unos de ellos.

El Plan de Acción será utilizado para minimizar los riesgos mediante acciones preventivas. La probabilidad de que un riesgo ocurra así como el impacto que el mismo podría ocasionar en el proyecto pueden ser mitigados encarando los problemas en forma proactiva.

El Plan de Contingencia, por el contrario intenta implementar respuestas

rápidas para mitigar los efectos en caso de que los riesgos se concreten, es decir reducir el impacto de los mismos mediante una reacción planeada. Este plan, además definirá ciertos indicadores que permitirán poner en marcha las acciones previstas, es decir, en caso que se verifiquen ciertos disparadores se adoptarán las medidas indicadas.

En el siguiente gráfico se muestra de forma gráficas las etapas de la metodología SEI

Figura 10 – Etapas de gestión de riesgos SEI

Para concluir con las características y ventajas de esta metodología, puede afirmarse, que las taxonomías podrían usarse con diferentes propósitos a lo largo de todo el proceso de gestión de riesgos. Durante la etapa de identificación, a fin de estimular el pensamiento sobre los inconvenientes que podrían producirse en las distintas áreas del proyecto; en el momento de la puesta en común de ideas, aligera la complejidad de trabajar con incontables tipos de riesgos, porque los riesgos similares pueden agruparse; además, de emplearse para proporcionar una

terminología unificada, que el equipo podría utilizar para supervisar y notificar el estado de los riesgos a lo largo del proyecto y, finalmente, es sumamente útil, para establecer las bases de conocimientos de riesgos en las organizaciones [Microsoft, 2002].

2.6 Magerit V2.0

2.6.1 Características y objetivos

La metodología Magerit (Metodología de Análisis y gestión de riesgos de los sistemas de información), es una metodología propuesta por el Ministerio de administraciones Públicas del Gobierno Español para los organismos públicos de este país, realizado por el Ministerio de Administraciones públicas, Centro Criptográfico Nacional y la Universidad Politécnica de Madrid y liberado para su ser utilizado en cualquier ámbito.

Se podría definir a los objetivos principales de Magerit V2 como:

- Concientizar a los responsables de sistemas de información (dueños del proceso) de la existencia de riesgos y procesos, y la necesidad de detenerlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar, las medidas eficaces para conservar los riesgos bajo control.
- Apoyar la preparación de la Organización en procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.
- Fundamentar sólidamente los argumentos que defenderán la toma de decisiones por parte de los directivos de la organización..

Esta metodología en su versión 2 se compone de tres partes, que se describen a continuación.

2.6.2 El Método

Es el documento que describe los pasos y tareas básicas a realizar en un proyecto de análisis y gestión de riesgos, proporciona una serie de aspectos prácticos y además describe la metodología desde un punto de vista de tres ángulos.

Primero, destaca los pasos a realizar en un análisis del estado de riesgo y gestiona la atenuación de los mismos, define de forma conceptual, en qué consiste el análisis de

riesgo, qué se busca a cada momento, y las conclusiones a las que se arriba. Se divide en 2 etapas.

- Análisis de Riesgos: Permite determinar que tiene la organización y estima que podría pasar. Los elementos son:
    - Activos: Elementos del sistema de información, o elementos que utiliza éste y aportan valor a la Organización
    - Amenazas: Acciones no esperadas, que pueden suceder a un activo, causando un perjuicio a la organización.
    - Salvaguardas: Elementos de defensa, desplegados a fin de que las amenazas no originen daños a los activos.

  Esta etapa posee pasos a seguir y analizar.

    1. Determinar los activos relevantes para la organización, la interrelación y valor.
    2. Determinar a qué amenazas están expuestos cada uno de los activos analizados.
    3. Determinar que salvaguardas existen, para disminuir la posibilidad de que el activo se convierta en un problema.

- Gestión de Riesgos: Permiten organizar la defensa de los activos de manera metodológica y prudente, evitando que los riesgos, no se transformen en problemas o minimizado el impacto .

  Las etapas que posee la gestión del riesgo son las siguientes:

    1. Estimar el impacto, definido como es el daño sobre el activo, derivado de la materialización de la amenaza.
    2. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia.

3. Seleccionar la salvaguarda adecuada para cada riesgo, y establecer políticas de organización del trabajo para el equipo de riesgos.
4. Establecer normas, con el objeto de afirmar con propiedad que la amenaza ha sido ejecutada.
5. Establecer procedimientos paso a paso, con directivas tendientes a solucionar el problema generado por la ejecución de la amenaza.
6. Desplegar controles que permitan medir y corroborar que las salvaguardas se están realizando correctamente.

Se podría decir que la gestión de la seguridad de un sistema según Magerit V2 es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

Como segunda etapa, la metodología presenta las tareas fundamentales y prioritarias para poder abordar un proyecto de análisis y gestión de riesgos, para realizar correctamente esto, no solo se debe poseer los conceptos claros de las tareas, si no que además de ello se sugiere pautar: roles, actividades, hitos y documentación. Se realizan estas actividades con el objetivo de que el proyecto permanezca en todo momento controlado.

Las tareas básicas se dividen en dos partes, la primera es la gestión de los participantes del proyecto de AGR y seguidamente los procesos, actividades y tareas a realizar.

- Participantes

    - Comité de Dirección: Personas con un perfil de alto rango en la organización con las tareas de, asignar los recursos necesarios para la ejecución del proyecto y aprobar resultados finales de cada proceso.

    - Comité de seguimiento: Está constituido por los responsables de las unidades afectadas en el proyecto. Con la tarea de resolver incidencias,

asegurar la disponibilidad de recursos, aprobar los informes intermedios, elaborar informes finales.

- Equipo de proyecto: Formado por personal experto en tecnología y sistemas. Las responsabilidades de este comité es, llevar a cabo las tareas del proyecto, recopilar, procesar ,consolidar datos y elaborar informes.

- Grupo de interlocutores: Está formado por usuarios representativos de las áreas en donde se ejecuta el proyecto.

- Desarrollo del Proyecto

  - Proceso P1: Planificación: Establece las consideraciones necesarias para arrancar el proyecto de AGR, investiga la oportunidad, define los objetivos y límites del proyecto, planifica los medios materiales y humanos, y procede al lanzamiento del proyecto.
    - Actividad A1.1: Estudio de oportunidad: fundamenta la oportunidad de la realización del proyecto.
      - Tarea T1.1.1: Determinar la oportunidad
    - Actividad A1.2: Determinar el alcance del proyecto: definir los objetivos principales del proyecto, dominio y límites. Realiza la primera identificación del entorno y las restricciones generales a considerar.
      - Tarea T1.2.1: Objetivos y restricciones generales.
      - Tarea T1.2.2: Determinación del dominio y límites.
      - Tarea T1.2.3: Identificación del entorno.
      - Tarea T1.2.4: Estimación de dimensiones y coste.
    - Actividad A1.3: Planificación del proyecto: determinar la carga de trabajo, planificar las entrevistas, elaborar el plan de trabajo, determinar los participantes y estructuras de los diferentes grupos y comités que llevarán a cabo el proyecto.

  - Tarea T1.3.1: Evaluar cargas y planificar entrevistas.
  - Tarea T1.3.2: Organizar a los participantes.
  - Tarea T1.3.3: Planificar el trabajo.
- Actividad A1.4: Lanzamiento del proyecto: Se adaptan los cuestionarios, se eligen técnicas de evaluación de riesgos, se asignan recursos necesarios, se informa a los usuarios del alcance del proyecto.
  - Tarea T1.4.1: Adaptar los cuestionarios
  - Tarea T1.4.2: Criterios de evaluación
  - Tarea T1.4.3: Recursos necesarios
  - Tarea T1.4.4: Sensibilización

- Proceso P2: Análisis de riesgos: Identifican los activos a tratar, las relaciones entre ellos y la valoración por cada uno, identifican amenazas significativas, salvaguardas existentes, estima el impacto y el riesgo al que es expuesto el activo, e interpreta el significado del impacto del riesgo.

  - Actividad A2.1: Caracterización de los activos: Identificar los activos relevantes, caracterizar por tipo de activo, evalauar la relación y dependencia entre activos, generar un valor a cada activo.
    - Tarea T2.1.1: Identificar de los activos.
    - Tarea T2.1.2: Dependencias entre activos.
    - Tarea T2.1.3: Valorar los activos.

  - Actividad A2.2: Caracterización de las amenazas: Identificar las amenazas, caracterizar la frecuencia estimada de ocurrencia y el daño si esta ocurriese. Como resultado final se obtiene el informe denominado “mapa de riesgos”.
    - Tarea T2.2.1: Identificar de las amenazas

- Tarea T2.2.2: Valorar las amenazas

- Actividad A2.3: Caracterización de las salvaguardas: identificar las salvaguardas, calificar por la eficacia. Como resultado se obtiene el informe "Evaluación de salvaguardas".
  - Tarea T2.3.1: Identificar las salvaguardas existentes.
  - Tarea T2.3.2: Valor las salvaguardas existentes.

- Actividad A2.4: Estimación del estado de riesgo: Procesar todos los datos recopilados para realizar los informes de "Estimación e impacto del riesgo" e "Insuficiencias o debilidades del sistema de salvaguardas".
  - Tarea T2.4.1: Estimación del impacto.
  - Tarea T2.4.2: Estimación del riesgo.
  - Tarea T2.4.3: Interpretación de los resultados.

- Proceso P3: Gestión de riesgos: Elegir una estrategia para mitigar el impacto y riesgo, identificar las mejores salvaguardas para el objetivo anterior, determinar la calidad necesaria para las salvaguardas, diseñar un plan de seguridad (plan de acción) para controlar el impacto y el riesgo a niveles aceptables y llevar a cabo el plan de seguridad.

  - Actividad A3.1: Tomar decisiones: Emitir las conclusiones técnicas del proceso P2.
    - Tarea T3.1.1: Calificar los riesgos

  - Actividad A3.2: Plan de seguridad: Emitir informes sobre decisiones de actuación en acciones concretas: proyectos de mejoras de seguridad planificados en el tiempo.
    - Tarea T3.2.1: Programas de seguridad
    - Tarea T3.2.2: Plan de ejecución

- Actividad A3.3: Ejecución del plan: Esta actividad recoge la serie de proyectos que materializan el plan de seguridad y que van realizando según dicho plan.
    - Tarea T3.3: Ejecución de cada programa de seguridad

Cabe aclarar que los pasos de las actividades no son necesariamente secuenciales, pero sí, se espera secuencia en los procesos.

Además, la metodología posee capítulos donde muestra con casos prácticos como aplicar la metodología en un desarrollo de sistemas de información, entendiendo que los riesgos debe ser considerados desde el primer momento, en un proyecto software, además de los riesgos al que se expone le proyecto se debe evaluar los riesgos propios que inducen la utilización de los sistemas informáticos productos de estos proyectos.

Como complemento, posee un capítulo final, donde desgrana una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo, para la realización de un análisis y gestión realmente efectivos.

Los apéndices recogen material de consulta:

- Glosario.
- Referencias bibliográficas consideradas para el desarrollo de esta metodología.
- Referencias al marco legal que encuadra las tareas de análisis y gestión
- Marco normativo de evaluación y certificación.
- Las características que requieren las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos.
- Una guía comparativa de cómo MAGERIT versión 1 ha evolucionado en esta versión 2.

- Presenta una herramienta denominada "PILAR" desarrollada para ser utilizada con esta metodología.

2.6.3 El Catálogo de los elementos

Es un manual que específica claramente los elementos utilizados por la metodología, define y clasifica cada uno de estos, incorporando ejemplos sencillos y aclaratorios con respecto a:

- Tipos de activos
- Dimensiones de valoración.
- Criterios de valoración.
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información.

Persigue dos objetivos:

1. Facilitar la labor de las personas que acometen el proyecto, ofreciéndoles elementos estándares, a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
2. Unificar los resultados de los análisis realizados, generando una uniformidad de criterios y terminología, que permitan integrar el trabajo realizados por diferentes equipos.

Cada sección incluye una notación XML a emplear en la publicación regular de los elementos, capaz de ser procesado automáticamente por herramientas de análisis y gestión.

Si el lector usa la herramienta de análisis y gestión de riesgos, este catálogo será parte de la misma; sí el análisis se realiza manualmente, este catálogo proporciona una amplia base de partida, para avanzar rápidamente sin distracciones ni olvidos.

2.6.4 Guía de técnicas

Describe las técnicas utilizadas en la guía metodológica.

Técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi[6]

Por cada una de las técnicas y prácticas referenciadas se:

- Explica los objetivos que se pretende obtener.
- Describen los elementos básicos asociados.
- Expone los principios fundamentales de elaboración.
- Presenta notación textual y/o gráfica.

2.6.5 Conclusión sobre Magerit V2.

La metodología investigada es muy clara, didáctica e intuitiva y por sobre todo es una metodología de análisis y gestión de riesgos específica. Tanto, en la metodología como en el catálogo de los elementos, y su guía de técnicas.

Se destaca, el método que utiliza para clasificar los activos, pues además de clasificarlos por tipo, incluye un criterio de valoración específico de los atributos, que hacen valioso a un activo.-

Agrupar y ordenar las amenazas, es otro de los pilares que hacen a esta metodología muy entendible y práctica.-

[6] Delphi Wideband el método de la valoración es una técnica consenso-basada de la valoración para estimar esfuerzo. Fue desarrollado en los años 40 en RAND Corporation como herramienta del pronóstico. Se ha adaptado desde entonces a través de muchas industrias para estimar muchas clases de tareas, el extenderse de la colección de datos estadística resulta a las ventas y a los pronósticos de la comercialización.

Definir las salvaguardas, para alcanzar los objetivos propuestos por el análisis de riesgos que permitan hacer frente a las amenazas.-

Con referencia a las técnicas utilizadas en la estimación del impacto del riesgo es muy intuitiva, fácilmente comprensible y semejante a la propuesta por la metodología SEI.

La metodología propone dos maneras de medir los activos, una cualitativa donde no mide en valores, sino que busca saber "que es lo que hay". Y un modelo cuantitativo, donde mide en escala de valores naturales positivos.-

Esta medición cuantitativa del valor del activo, el valor acumulado, la degradación, el impacto, la frecuencia de una amenaza y el riesgo están expresados en la formula:

Riesgo = Impacto X Frecuencia → Semejante a la metodología SEI

Se puede apreciar, en estas mediciones que la primera otorga importancia al valor del activo, y la segunda propone una valoración en moneda.-

La clasificación podría obtenerse respondiendo la siguiente pregunta ¿ Por que interesa el activo? O ¿Se deberá evaluar en este proyecto o caso?

El análisis no surge, de lo que "cuesta" el activo en dinero, sino del "valor" que posee para la organización.-

Si un activo No posee valor, es prescindible y hay que eliminarlo. Si no se puede prescindir, es porque algo vale, y hay que analizarlo cuantitativa y cualitativamente. Y si vale, hay que protegerlo.-

2.7 Descripción de Software

2.7.1 Pilar

La metodología Magerit propone la utilización de un software realizado en el lenguaje JAVA. Para el presente trabajo se obtuvo una versión only-view del software en su revisión 4.3

El software completo, es de utilización libre únicamente para las organizaciones públicas pertenecientes al gobierno Español. Las demás organizaciones privadas, que trabajan o poseen realización con el gobierno español puede obtener el software, a un costo mejorado, del que obtiene cualquier empresa del mundo, previa presentación de formularios específicos en la secretaria de informática de la administración pública.

Se intentó obtener el software en su versión completa para estudiarlo en profundidad, pero no se logró respuesta favorable por parte del Consejo Superior de Administración Electrónica del Gobierno Español, encargado de entregar el software, sin costo. Esta secretaría entrega el software únicamente, a las organizaciones antes mencionadas con previa autorización de los formularios correspondientes.

Características del PILAR

Una de las características esenciales del PILAR, es la de permitir asociar niveles cualitativos a valores cuantitativos.

El hecho de haberse realizado en el lenguaje JAVA, admite la instalación en diferentes plataformas de sistemas operativos, Windows, Unix, MAC OS

Posee 3 versiones

Verisión 1 - µPILAR - Análisis y Gestión de Riesgos

PILAR reducida a la mínima expresión, realizar análisis de riesgos muy expeditivos. El resultado del análisis puede cargarse en PILAR para estudios más detallados. Esta versión fue estudiada para el presente trabajo.

µPILAR es distribuido con perfiles específicos. Sólo se pueden analizar los perfiles de la distribución.

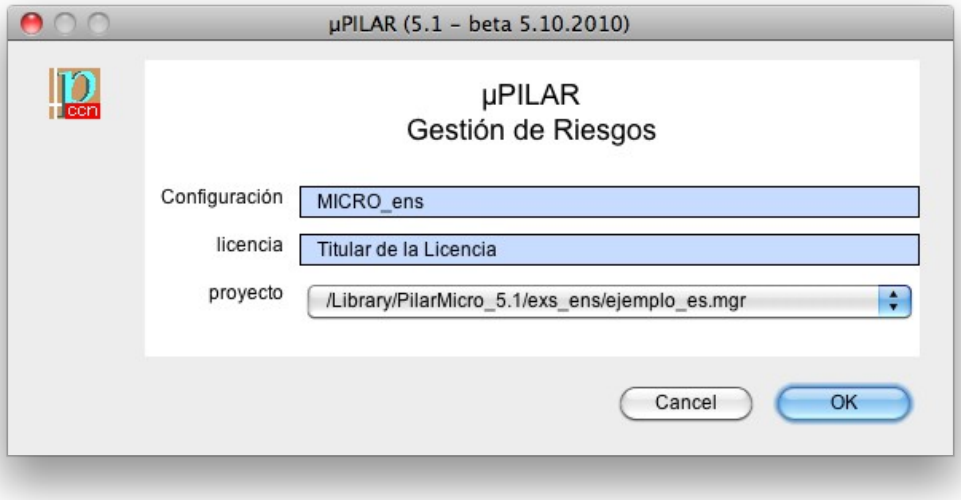


Figura 11 - UPilar

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (*accountability*).

En tratamiento del riesgo propone: salvaguardas (o contra medidas), analiza el riesgo residual.

Costo: No posee

Versión 2 - PILAR Basic - Análisis y Gestión de Riesgos

Versión sencilla para

- PYME - Empresa pequeña y mediada
- Administración local

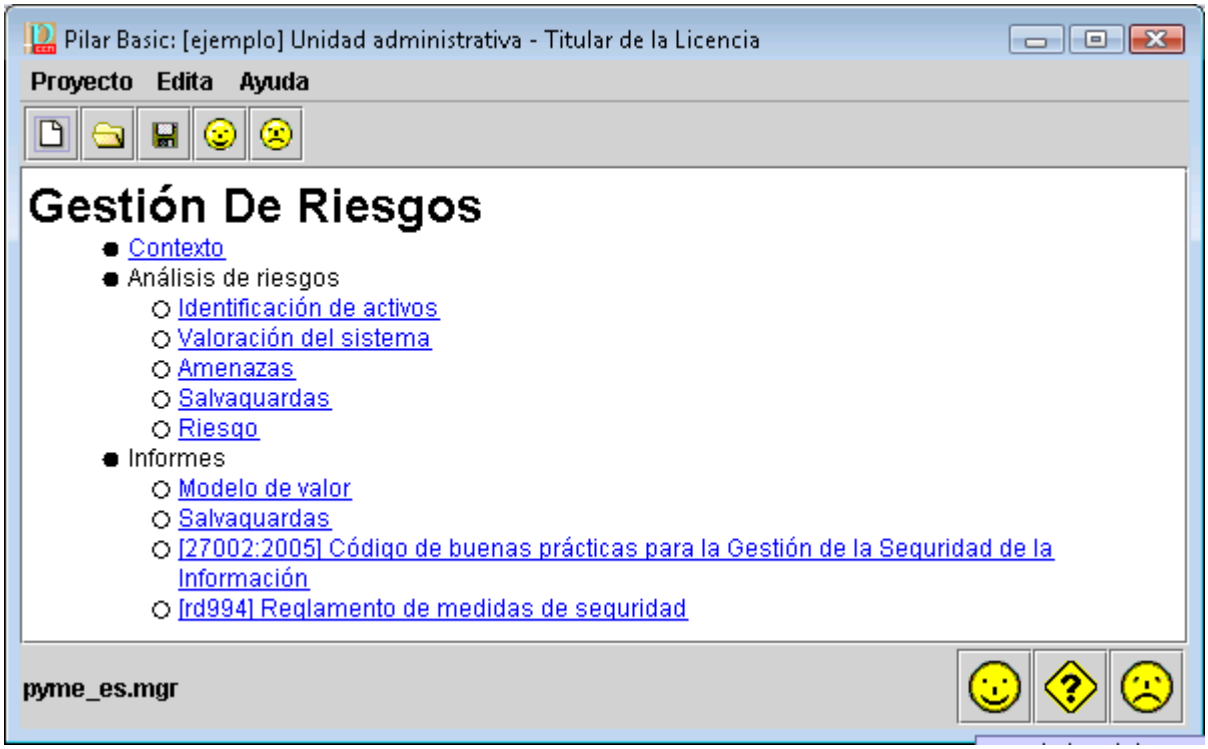


Figura 12 – Pilar Básico

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (*accountability*).

En el tratamiento del riesgo propone: salvaguardas (o contra medidas), analiza el riesgo residual en diversas etapas del tratamiento.

Costo : 500 Euros.

Versión 3 - PILAR - Análisis y Gestión de Riesgos

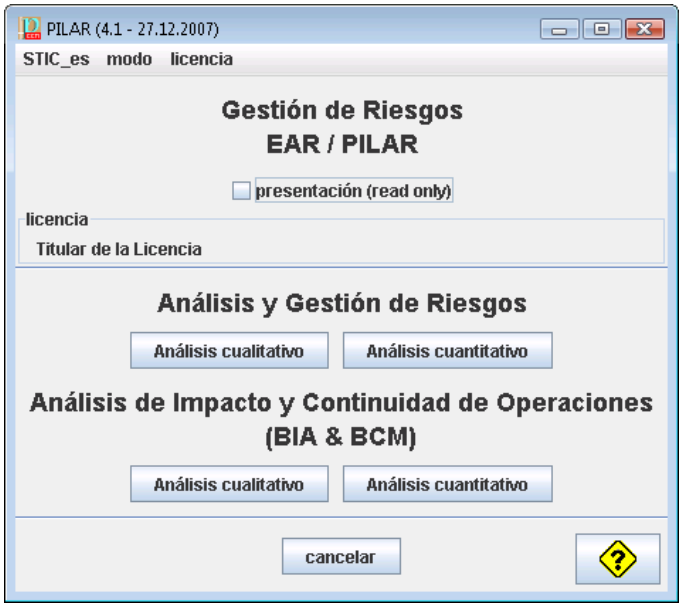


Figura 13– Pilar versión full

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (*accountability*).

En el tratamiento del riesgo propone :

- salvaguardas (o contra medidas)
- normas de seguridad
- procedimientos de seguridad

Analiza el riesgo residual en diversas etapas de tratamiento.

Análisis de Impacto y Continuidad de Operaciones

Analiza el efecto de las interrupciones de servicio, teniendo en cuenta la duración de la interrupción.

En el tratamiento del riesgo propone:

- salvaguardas (o contra medidas)
- elementos de respaldo (*back up*)
- planes de recuperación de desastres

Analiza el impacto residual en diversas etapas del tratamiento.

Costo: 2.000 Euros.

Se puede adquirir un complemento que personaliza el PILAR, denominado RMAT (Risk Management Additional Tools) - Personalización de las herramientas

Figura 14 – Rmat

Las herramientas se pueden personalizar en varios aspectos:

EVL - Perfiles de protección

Criterios de evaluación/acreditación, específicos de ciertos sectores o de puntos de vista específicos.

Por ejemplo: leyes nacionales de protección de datos personales.

TSV - Perfiles de amenazas

Establece la vulnerabilidad típica de los activos frente a las amenazas en diferentes entornos de operación.

KB - Protecciones adicionales

Detalla protecciones adicionales sobre ciertos tipos de activos. Se puede brindar instrucciones al administrador del activo.

Estas herramientas permiten preparar y mantener personalizaciones, de incorporación dinámica a la biblioteca, y extensión para adaptarse a un determinado contexto. Están previstas para consultores y grandes organizaciones.

Costo del componente 3.000 Euros.

Información obtenida de http://www.ar-tools.com/index.html?tools/pilar/index.html, consultado el 09/10/2010.

Capitulo 3

Problema encontrado y Solución sugerida

3.1 Problema Encontrado

El uso de la tecnología ha crecido considerablemente en los últimos años y las organizaciones cada vez dependen más de ella, para garantizar el éxito en el entorno de negocios actual; la habilidad que tenga la organización para implantar las tecnologías modernas que soporten de manera eficiente y controlada a los procesos de negocio críticos, tiene un gran impacto en su grado de competitividad.

Los planes estratégicos de negocio actualmente incluyen iniciativas que involucran la optimización de los recursos informáticos para asegurar la consecución de los objetivos de la organización; como consecuencia de lo anterior, los altos ejecutivos están cada vez más alertas sobre la forma en que la tecnología soporta al negocio y dependen cada día más en los Directores de Tecnología de Información para optimizar la organización.

Este incremento ha añadido complejidad a las arquitecturas tecnológicas y a los procesos para su implantación y administración; por consiguiente, se presentan nuevos riesgos que deben ser mitigados de forma efectiva y eficiente para mantener el cumplimiento de los objetivos de control. Dichos riesgos se encuentran en su mayoría inmersos en los cada vez más complejos sistemas de cómputos, recursos humanos en la etapa de su desarrollo, implementación y mantenimiento, y de TI (tecnología informática) en general.

3.1.1 Análisis y Gestión de riegos en las organizaciones

En el año 2001 KLCI [KLCI, 2001], realizó un estudio a nivel mundial en el cual 268 organizaciones fueron encuestadas, solo el 3% No utilizaba ningún marco de gestión de riesgos, el 18% utilizaba algunos métodos de forma caótica y rudimentaria, el 37% habían utilizado algún marco informal y solo el 14% utilizaban un enfoque formal de AGR. Según este estudio las razones más comunes que expresaban los encuestados era:

- La falta de procedimientos
- Necesidades del proyecto no adecuados.
- Organizaciones inmaduras y poco compromiso del equipo.

Según Kontio [Kontio, J. , 1997], creen que hay tres motivos principales para la escasa tasa de divulgación de tecnologías de gestión de riesgos:

1. Falta de conocimiento sobre posibles herramientas y métodos.
2. Limitaciones prácticas y teóricas de los marcos de gestión de riesgos que entorpecen la facilidad del uso de estos métodos.
3. Todavía hasta hoy existen pocos informes con evaluaciones sistemáticas o científicas que proporcionan feedback empírico sobre la viabilidad y beneficios.

Para este trabajo de tesis se realizó una encuesta sobre el estado de situación del análisis y gestión de riesgos y se invitó a participar de la misma a varias empresas del ramo local de la provincia de misiones y del ramo nacional a empresas de origen y base en todo el país Argentina.

El resultado de la misma fue muy clarificador, debido a que solo una empresa OSPRERA (Obra social de trabajadores rurales y estibadores de la república Argentina) contestó la encuesta formalmente (Ver Anexo 3). Las demás se rehusaron a contestar aduciendo que la información solicitada NO era autorizada a exponerla por parte de los directivos de la organización y la mayoría "informalmente" no contestaron por los siguientes motivos:

- No poseían un método formal para el AGR.
- La empresa no sabía que era el AGR, ni el análisis de riesgo.
- Estaban en los planes pero debido al poco personal informático y el alto costo de las consultoras no podían afrontar el costo.

3.1.2 Métodos informales del análisis de riesgos

En la mayoría de las organizaciones, inclusive en nuestros propios hogares siempre utilizamos algún método de análisis de riesgos. Por ejemplo, realizar copias de seguridad de los archivos importantes, conectando a los equipos UPS[7] etc.

La mayoría de las personas y las organizaciones toman como práctica resguardar estos activos, que inconcientemente creen que es una buena manera de estar seguros, pero es totalmente informal y se recomienda poseer un método adecuado para esto.

Esta acción se podría definir (algunos lo definen erróneamente) como una práctica de análisis de riesgo, el problema es que no se tiene noción de gestión, y sin gestión no sirve de mucho el análisis, debido a que, si ocurre un problema, no existe la manera de poder afrontarlo. Por ejemplo si el archivo original se destruye pueden pasar algunas de los siguientes escenarios:

- Tenemos varias copias, cual es la última?
- El dispositivo en donde se encuentra la copia de seguridad NO funciona.
- El software que realizaba la copia de seguridad automática, no genera la misma ya que se cambio el dispositivo destino de la copia.
- La copia no se puede recuperar.

Esto sucede debido a que no tenemos un plan de gestión del riesgo formal, en donde se expresar el plan de acción, que es el que abarca el seguimiento y control del resigo, o el plan de contingencia, para poder generar acciones controladas cuando el riesgo se transforme en un problema.

3.1.3 Dificultades de gestionar los riegos en las pequeñas y medianas organizaciones

Según el estudio realizado se puede decir que en las organizaciones pequeñas y medianas, no se realiza correctamente el análisis y gestión de riesgos por varios motivos como ser:

[7] Servicio de energía ininterrumpida

- *Costos*: Debido a la falta de conocimiento de los directivos de las organizaciones en cuando a ARG, que por lo general piensan, que el valor de un activo se limita a su valor económico y no al "Valor" real, que es el resultante del análisis de la importancia del activo para la organización.
  Contratar una consultora externa de auditoría informática para que realice un análisis y gestión de riesgos, o contratar personal que se dedique a la gestión de los riesgos y su seguimiento en el tiempo, cuesta mucho dinero, y si bien se considera necesario analizar y gestionar los riesgos, no cuentan con una planificación de costos para ello, por lo cual deciden no hacerlo.

- *Ignorancia metodológica:* Por lo general, una de las creencias más frecuentes entre los informáticos no profesionales, es que realizando copias de seguridad y/o teniendo agendado el número de telefónico del técnico reparador de pc, es la solución a los posibles problemas de análisis y gestión de riesgos, en estas acciones se aprecian la falta de conocimientos de las metodologías de AGR.

- *Falta de Compromiso*: Es un caso muy común la falta de compromiso por parte de los directivo de las organizaciones en base al AGR, en la mayoría de los casos, al principio del proyecto están de acuerdo el desarrollo del análisis y gestión de los riesgos, pero con el paso del tiempo y debido a otros aspectos más importantes de la organización, no cumplen con el compromiso asumido.

3.1.4 Metodologías poco adaptativas

3.1.4.1 Desventaja SEI - CRM

Gestión de Riesgo: El SEI – CRM no incluye específicamente una fase o actividad para el desarrollo del plan de gestión de riesgos.

Clasificación del activo y cuestionario TBQ muy abstracto y amplio: como se definió en el capitulo 2, el SEI generó el cuestionario TBQ para realizar la taxonomía de los riesgos, el mismo se utiliza para identificar riesgos técnicos, que consiste en 194 preguntas muy abstractas que son clasificadas en tres grandes clases, las cuales a su vez se subdividen en subclases, como podemos apreciar en la tabla 1 [SEI, 2004].

1) Product Engineering a) Requirements i) Stability ii) Completeness iii) Clarity iv) Validity v) Feasibility vi) Precedent vii) Scale b) Design i) Functionality ii) Difficulty iii) Interfaces iv) Performance v) Testability vi) Hardware c) Constraints i) Non-Developmental d) Software i) Code and Unit Test ii) Feasibility iii) Testing iv) Coding/Implementation e) Integration and Test i) Environment ii) Product iii) System f) Engineering Specialties i) Maintainability ii) Reliability iii) Safety iv) Security v) Human Factors vi) Specifications	2) Development Environment a) Development Process i) Formality ii) Suitability iii) Process Control iv) Familiarity v) Product Control b) Development System i) Capacity ii) Suitability iii) Usability c) Familiarity i) Reliability ii) System Support iii) Deliverability d) Management Process i) Planning ii) Project Organization iii) Management Experience iv) Program Interfaces e) Management Methods i) Monitoring ii) Personnel Management iii) Quality Assurance iv) Configuration Management f) Work Environment i) Quality Attitude ii) Cooperation iii) Communication iv) Morale	3) Program Constraints a) Resources i) Schedule ii) Staff iii) Budget iv) Facilities b) Contract i) Type of Contract ii) Restrictions iii) Dependencies c) Program Interfaces i) Customer ii) Associate Contractors iii) Subcontractors iv) Prime Contractor v) Corporate Management vi) Vendors vii)Politics

Figura 15- [SEI ,2004]

Según Teylor Moynihan [Moynihan T., 1997], como otros autores, han mencionado que la taxonomía del SEI está diseñada para la identificación de riesgos en proyectos grandes, formales y muy técnicos, que por lo general se aplican en grandes organizaciones. La realidad del cuestionario TBQ es que demuestra sus orígenes, es decir, que los tipos de riesgos aquí expuestos son aquellos riesgos típicos que existen en organizaciones grandes, generalmente militares u organizaciones con planes muy claros de manejo de la información y con desarrollos de software muy amplios.

Necesidad de experticia por parte de los miembros del equipo de AGR: Al contemplar el punto anterior, se divisa la necesidad de que los miembros del equipo de AGR que trabajen con la metodología SEI – CRM, posean amplia experiencia en el campo del análisis de riesgos y amplia experticia en ingeniería del software, debido a que las preguntas expresadas en el cuestionario TBQ, son abstractas y requieren un amplio espectro de análisis.

Enfoque basado en la creación y mantenimiento de software: La metodología SEI – CRM como se definió en este capitulo, posee una orientación hacia el proyecto software y como complemento la tecnología informática añadida a ese proyecto. No es específica de todo el IT, para las organizaciones pequeñas y medianas que no poseen desarrollo propio esta metodología no es aplicable.

3.1.4.2 Desventaja MageritV2

Metodología Amplia y rígida: como hemos definido en el capitulo 2 la principal desventaja de Magetit V2 es que cuenta con tres procesos, once actividades y veintiséis tareas, las cuales son imprescindibles de realizar en su totalidad. Al estar orientado a organizaciones estatales, está diseñado para ser utilizado en grandes organizaciones, y el hecho de tener que traducir de forma directa todas las

valoraciones en valores económicos, hace que la aplicación de esta metodología sea realmente costosa.

Herramientas con alto costo económico: Como se presentó al final del capítulo 2, el software existente para gestionar esta metodología es muy costosa, y aquellas versiones que se pueden conseguir gratuitamente, son solo formatos de visión de ejemplos.

3.2 Solución Sugerida

Luego de haber realizado el estudio de ambas metodologías Magerit V2 - SEI- CRM, y analizando el contexto del ambiente informático de las pequeñas y medianas empresas, se tomó la decisión de generar un método adaptado, se que llamará "Método SeiMag" cuya característica principal será la utilización las etapas de la metodología SEI, que son pocas etapas, simples, bien definidas, muy utilizadas y recomendadas por una enorme cantidad de organizaciones gubernamentales y educativas, y como innovación, este método contará dentro de algunas de sus etapas, los elementos ofrecidos por la metodología Magerit.

De la metodología SEI se utilizarán las nueve etapas propuestas, y de la metodología Magerit V2 las técnicas de clasificación y elementos, como por ejemplo: clasificación de activos por tipo, salvaguardas, amenazas y valoración de activos.

Con la ayuda de Magerit se podrá realizar una clasificación simple, válida y formalmente correcta introduciendo técnicas y elementos de la metodología Magerit V2 a las etapas SEI, esta práctica le proporcionará al método adaptado que brinda adaptabilidad al nivel de evaluación de riesgos que se busca en esta investigación.

Además se incluirán dos etapas externas como el seguimiento de los planes de acción y la gestión de incidencias, poniendo énfasis en esta última, la cual no existe dentro de ninguna de las metodologías antes mencionadas, y por lo tanto generará un alto valor agregado al método desarrollado.

Debido a que es importante y necesaria la realización del análisis y gestión de riesgos en una organización, y ya que es uno de los puntos neurálgicos de la Auditoría de Sistemas, junto a la metodología SeiMag V1, se va a desarrollar un software herramienta denominado "MySeiMag V1", cuyo objetivo es impulsar el análisis y gestión de riesgos en los sistemas de información dentro de las organizaciones, facilitando la utilización de un método formal basado en la metodología propuesta y conformando un ámbito intuitivo, rápido y fácil de mantener.-

Capitulo 4

La Metodología Sei-Mag

4.1 Características

La metodología Sei-Mag fue desarrollada con el objetivo de brindar un método simple, intuitivo y que agiliza el reconocimiento de los riesgos, incorporando elementos ya definidos y clasificados. La metodología se distribuye en cuatro fases:

1. Análisis y gestión de riesgos: Esta fase implementa 8 etapas o actividades secuenciales. En donde se evalúan los riesgos de un activo, la relación entre ellos, la taxonomía, analiza los posibles riesgos y los gestiona.

2. Seguimiento y Control: Las salvaguardas, también llamadas en este método plan de acción, posee actividades de seguimiento y control para cada riesgo que se gestione, designa a una persona que realice las tareas de seguimiento y control, con el fin de que los elementos del plan de acción estén en perfecto orden y control.

3. Registro de Incidencias: Cuando ocurre un problema hay que buscar una solución rápida y práctica, para reducirlo o controlarlo. La característica de este registro es el control y gestión de las incidencias ocurridas. Dicha gestión posee la particularidad de registrar los activos afectados, el tiempo transcurrido ante la declaración del incidente y su culminación, la probable solución existente, y la designación de un responsable a cargo de la solución del problema.

4. Comunicación: Según Esteves y Pastor [Esteves Pastor, 2000], la comunicación debe ser de dos tipos: "hacia dentro" en el seno del equipo del proyecto y "hacia fuera" con el resto de la organización que acoge al proyecto. La comunicación desde la fase de incidencias, "hacia adentro" se realiza con los reportes de incidencias y específicamente informes, y "hacia fuera", con los reportes de gestión de riesgos e información estadística sobre los resultados de los proyecto evaluados.

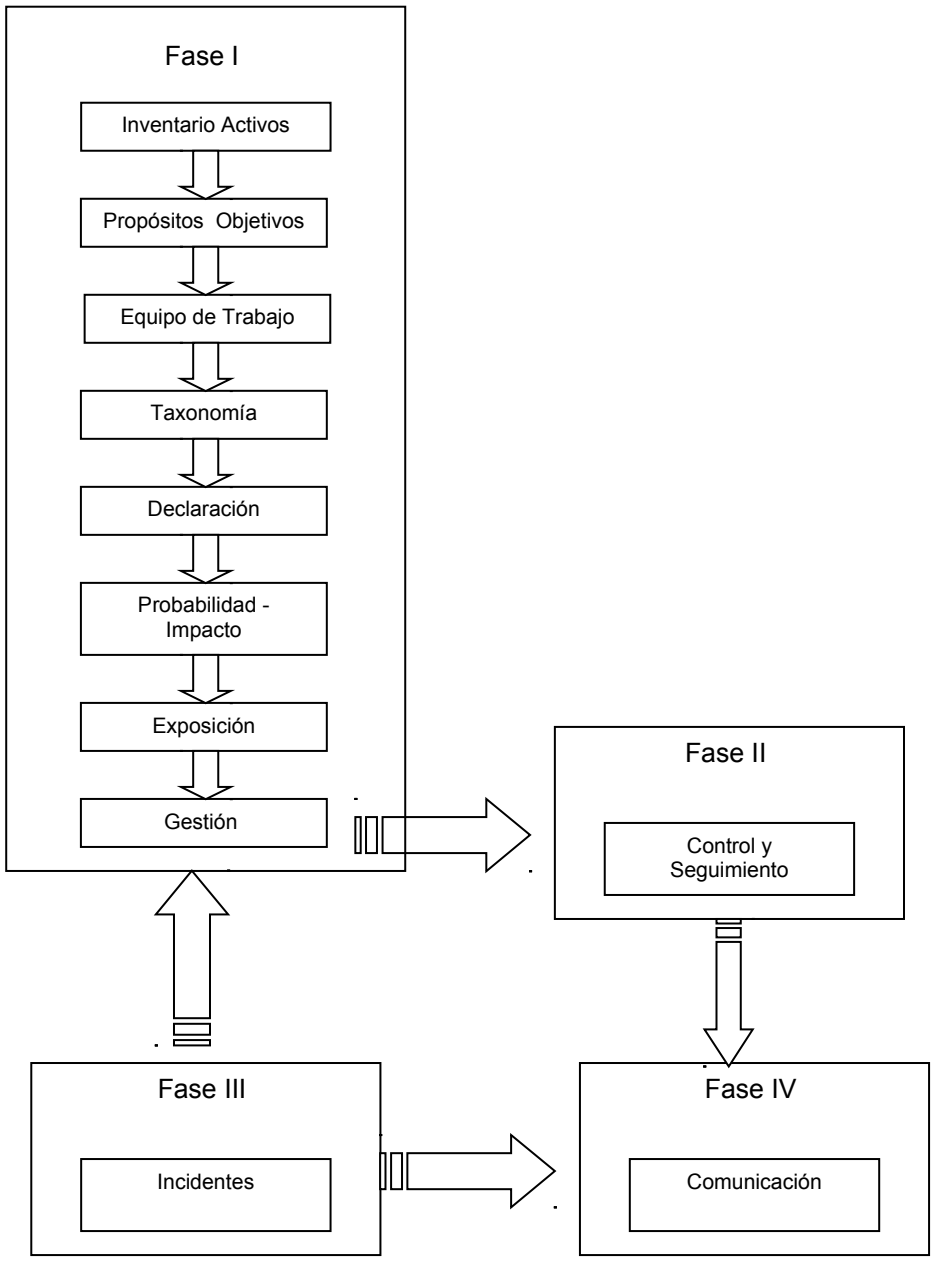


Figura 16 – Fases del método Sei-Mag

4.2 Fase I – Análisis y Gestión de Riesgos

4.2.1 Etapa I - Inventario de activos

Identificación de Activos

Se puede decir que los activos principales que manejan las organizaciones, estarían relacionado con la información o procesamiento de los datos.

El dato, es el activo más importante, y para poder procesarlo, son necesarios otros activos apreciables y necesarios como:

- Servicios: se proporcionan a partir de los datos, y son necesario para gestionar los mismos.
- Programas (Software) operan los datos.
- Equipos (Hardware) lugar donde se almacenan los datos, los programas y los servicios.
- Soporte de información: dispositivos para salvaguardar los datos.
- Equipamiento Auxiliar: complementan material informático.-
- Redes de comunicaciones: intercambian los datos entre programas y servicios.
- Instalaciones: alojan los equipos informáticos y de comunicaciones.
- Personas: que operan o explotan todo los demás activos nombrados.

Existen activos que deben tener ciertos resguardos según la ley. Se hace necesario contemplarlos en el análisis de riesgo, aunque no sean de importancia para la organización.-

Dependencias entre Activos

En un sistema de información los activos, para su correcto funcionamiento, dependen de otros activos. En otras palabras un activo superior depende de un activo inferior.

Los activos mas observados son, datos y servicios (activos superiores), pero estos activos, dependen de otros, como equipos, comunicaciones o personas. (Activos inferiores).-

Se puede decir que un "activo superior" es dependiente de un "activo inferior", cuando las necesidades de seguridad de un activo superior se enmarcan en las necesidades de seguridad del inferior.

Las dependencias se podrían organizar en capas.

- Capa 1: Entorno: activos necesarios para garantizar las siguientes capas:
  - Equipamiento y suministros: energía, climatización, comunicaciones.
  - Personal: de dirección, de operación, de desarrollo, etc.
  - Otros: edificios, mobiliario, etc.
- Capa 2: Sistema de información propiamente dicho
  - Equipos informáticos *(hardware)*
  - Aplicaciones *(software)*
  - Comunicaciones
  - Soportes de información: discos, cintas, etc.
- Capa 3: Información
  - Datos
  - Meta-datos: estructuras, índices, claves, etc.
- Capa 4: Funciones de la Organización, justifican la existencia del sistema de información y finalidad
  - Objetivos y misión
  - Bienes y servicios producidos
- Capa 5: Otros activos

- Credibilidad o buena imagen.
- Conocimiento acumulado.
- Independencia de criterio o actuación.
- Intimidad de las personas.
- Integridad física de las personas.

Para aclarar la dependencia entre activos se muestra el siguiente ejemplo:
Se roban una notebook de un ejecutivo de la empresa, por este hecho no solo se pierde el equipo, sino que también otros activos dependientes por ejemplo:

- Notebook
- Confidencialidad de los Datos
- Futuros negocios.
- Imagen.

Valoración de los activos

Un activo es más importante por su valor, que por su costo económico. Si algo "no" vale nada es prescindible y hay que sacarlo, pero si no se puede presindir de un activo es por que algo vale.

Esto es lo que hay que investigar (su valor) y protegerlo.-

Dimensiones

Un activo puede poseer muchas dimensiones. Las dimensiones se utilizan para caracterizar los activos y luego poder tratarlos según los riesgos que corran.

Las dimensiones de un activo pueden ser:

- Autenticidad: Quién, cuándo y dónde se realizó la carga de datos específicos?, Quién hace o ha hecho cada cosa?, es la valoración típica de un servicio (autenticidad del usuario).
- Confidencialidad: Que problemas originaría el conocimiento de los datos por parte de quien no debe?. Valoración típica de los datos.
- Integridad: Si el activo está dañado o corrupto ¿qué problemas ocasionaría?. Valoración de datos y de soporte informático (Discos).-

- Disponibilidad: Que problemas traería aparejado "no" poder contar o "no" poder utilizar un activo. Valorización típica de servicio (telecomunicaciones etc.)

Ha estas dimensiones básicas se le agregan otras auxiliares, por ejemplo a las organizaciones que proveen administración electrónica (e-learnig) comercio electrónico (e-commerce) o de gobierno (e-goberment). ISO/IEC 13335[8].

- Trazabilidad de uso del servicio. ¿Qué problemas acarrearía "no" saber a quien se le presta el servicio?
- Trazabilidad de acceso a los datos. ¿Quién accede a los datos es, quien tiene que ser?

En esta investigación se ha referido a la autenticidad para distinguir entre el uso de un servicio y el acceso a los datos.-

Elementos

Una vez identificados los activos, dependencias, valoración y dimensiones, se debe asignar el elemento en el que el activo es importante.

Los activos poseen elementos, el conjunto de ellos, es la característica de la información con la que trabaja o procesa el activo, y se define en grupos, según cada tipo de activo.

Fuentes de información

Es primordial, para poder llevar a cabo un buen análisis de riesgos, que la información obtenida de los activos sea registrada, para en caso de que el riesgo se transforme en un problema, se pueda acudir e informar al área o personas de las

[8] ISO / IEC 13335-1:2004 presenta los conceptos y modelos fundamentales para una comprensión básica de la seguridad de las TIC, y aborda las cuestiones generales de gestión que son esenciales para la planificación, implementación y operación de seguridad de las TIC. Proporciona orientación operativa en materia de TIC. En conjunto, estas piezas se pueden utilizar para ayudar a identificar y gestionar todos los aspectos de seguridad de las TIC.

cuales obtuvimos la información del activo. Ya que en teoría son los que más saben del funcionamiento del activo y en general ocupan estos para su trabajo.

4.2.2 Etapa II - Propósitos y Objetivos del análisis de riesgos

En esta etapa se debe gestionar los proyectos, estableciendo claramente los propósitos, objetivos y límites que tendrá el proyecto de análisis de riesgos. Además en esta etapa se asignan al proyecto los activos evaluados en la etapa anterior.

4.2.3 Etapa III - Equipo de Trabajo

Establecidos los límites y objetivos del análisis de riesgo se debe formalizar el equipo de trabajo que realizará la tarea. La actividad de esta etapa es: designar al proyecto las personas que serán parte del equipo de AGR, además los roles que se utilizarán en el proyecto y los equipos que se formarán para trabajar.

4.2.4 Etapa IV - Taxonomía de Riesgos

La clasificación de los riesgos -también denominadas taxonomías de riesgos- puede servir de ayuda para elaborar un enfoque coherente, reproducible y medible de los riesgos a los cuales se puede enfrentar un activo. Las listas de clasificación permiten al equipo pensar con mayor amplitud sobre los riesgos que pueden afectar al proyecto, dado que se dispone de una lista de áreas del proyecto susceptibles de esconder riesgos.

Existen muchas taxonomías o clasificaciones generales, para los riesgos de proyectos software.

Para el presente trabajo se ha escogido la clasificación propuesta por el por la metodología Magerit V2. , denominado “Amenazas”, la cual ordena taxonomicamente que amenazas o riesgos que corren los activos.

Para ello se creo una taxonomía propia, en la cual se obtiene, procesando las amenazas por el tipo y la dimensión del activo.

Las amenazas se agrupan por tipos y pueden ser:

- Desastres Naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
    - Fuego: incendios: posibilidad de que el fuego acabe con recursos del sistema.
    - Agua: inundaciones: posibilidad de que el agua acabe con recursos del sistema.
    - Desastres Varios: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras. Se excluyen desastres específicos tales como incendios e inundaciones. Se excluye al personal por cuanto se ha previsto una amenaza específica para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.
- De Origen Industrial

: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

- Fuego - incendio: posibilidad de que el fuego acabe con los recursos del sistema.
- Agua: escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
- Desastres Industriales: otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, Se excluyen amenazas específicas como incendio e inundación .Se excluye al personal por cuanto se ha previsto una amenaza específica, para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.
- Contaminación Mecánica: vibraciones, polvo, suciedad.
- Contaminación Electromagnética: interferencias de radio, campos magnéticos, luz ultravioleta
- Avería de origen físico o lógico: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida

durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.

- Corte de suministro eléctrico: cese de la alimentación de potencia
- Condiciones inadecuadas de temperatura y humedad: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad
- Fallo del Servicio de Comunicaciones: cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
- Interrupción de otros servicios y suministros esenciales: otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante.
- Degradación de los soportes de almacenamiento de la información: como consecuencia del paso del tiempo
- Emanaciones electromagnéticas: Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.

- Errores y Fallos No Intencionados.
  - Errores de los usuarios: equivocaciones de las personas cuando usan los servicios, datos, etc.
  - Errores del administrador: equivocaciones de personas con responsabilidades de instalación y operación

- Errores de monitorización *(log):* inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.
- Errores de configuración: introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
- Deficiencias en la organización: cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
- Difusión de software dañino: propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.
- Errores de [re-]encaminamiento: envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.
- Errores de secuencia: alteración accidental del orden de los mensajes transmitidos.
- Escapes de información: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
- Alteración de la información: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

- Introducción de información incorrecta: inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
- Degradación de la información: degradación accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
- Destrucción de información: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
- Divulgación de información: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.
- Vulnerabilidades de los programas (software): defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
- Errores de mantenimiento / actualización de programas (software): defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
- Errores de mantenimiento / actualización de equipos (hardware): defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
- Caída del sistema por agotamiento de recursos: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

- Indisponibilidad del personal: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.

- Ataques Intencionados: Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.
    - Manipulación de la configuración: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
    - Suplantación de la identidad del usuario: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
    - Abuso de privilegios de acceso: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
    - Uso no previsto: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
    - Difusión de software dañino: propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.
    - [Re-]encaminamiento de mensajes: envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la

red donde puede ser interceptado. Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.

- Alteración de secuencia: alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.
- Acceso no autorizado: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
- Análisis de tráfico: también denominado "monitorización de tráfico" el atacante, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios, sin necesidad de entrar a analizar el contenido de las comunicaciones.
- Repudio: es la negación de actuaciones o compromisos adquiridos con anterioridad. Se definen en tres:
  - De origen: es la negación de ser el remitente u origen de un mensaje o comunicación.
  - De recepción: negación de haber recibido un mensaje o comunicación.
  - De entrega: negación de haber recibido un mensaje para su entrega a otro.
- Interceptación de información (escucha): el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
- Modificación de la información: es la alteración o modificación intencional de la información, con ánimo de obtener un beneficio o causar un daño. Esta amenaza sólo se genera sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

- Introducción de falsa información: inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
- Alteración de la información: modificación intencional de la información, con ánimo de obtener un beneficio o causar un daño. Esta amenaza únicamente se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
- Destrucción la información: eliminación intencional de información, con ánimo de obtener un beneficio o generar un daño.
- Divulgación de información: revelación de información.
- Manipulación de programas: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
- Denegación de servicio: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
- Robo: El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.
- Ataque destructivo: vandalismo, terrorismo, acción militar. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.
- Ocupación enemiga: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

- Indisponibilidad del personal: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.
- Extorsión: presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
- Ingeniería social: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

4.2.5 Etapa V - Declaración de los Riesgos

Las definiciones genéricas de un riesgo no hacen desaparecer la incertidumbre y dan lugar a distintas interpretaciones del riesgo. Las definiciones que no dejan lugar a dudas permiten a los equipos:

- Asegurarse de que todos los miembros del equipo comprenden el riesgo de la misma forma.
- Comprender la causa o causas del riesgo y la relación con los problemas que puedan surgir.
- Disponer de una base, para realizar un análisis formal y cuantitativo, planear los esfuerzos.

En las declaraciones de riesgos se definen en forma mas precisa los riesgos identificados, siguiendo un proceso de declaración que se compone de dos partes (condición – consecuencia). La primera parte de la declaración del riesgo se denomina condición, y describe una situación o atributo del proyecto existente que el equipo prevé que puede resultar en una pérdida en el proyecto o en una reducción de beneficios. La segunda parte se denomina consecuencia, y describe el atributo o situación no deseable del proyecto. Además se incluyen los efectos que tendrían estos riesgos de no controlarse debidamente.

Análisis y prioridad de los riesgos

La meta principal del análisis de riesgos consiste en establecer las prioridades de los elementos de la lista de riesgos y determinar cuál de ellos justifica la reserva de recursos para el planeamiento. Por otro lado la asignación de prioridades a los riesgos permitirá tratar en primer lugar los riesgos más importantes del proyecto.

4.2.6 Etapa VI - Estimación de la probabilidad e Impacto

La probabilidad del riesgo es el porcentaje de que la situación descripta en el apartado de consecuencias, llegue a producirse de verdad.

Para cuantificar la incertidumbre acerca de la ocurrencia de los riesgos se emplearán las categorizaciones expresadas en lenguaje natural, en base a un rango de probabilidades establecido en un cuadro de referencia. A modo de ejemplo se propone la valoración con el siguiente cuadro:

Rango de probabilidad	Promedio para el calculo	Expresión de lenguaje natural	Valor numérico
de 1% a 10%	5 %	Baja	1
de 11 % a 25%	18 %	Poco probable	2
de 26% a 55%	40 %	Media	3
de 56% a 80%	68 %	Altamente probable	4
de 81% a 99%	90 %	Casi seguro	5

Figura 17 - Estimación de probabilidad

El impacto del riesgo calcula la gravedad de los efectos adversos, la magnitud de una pérdida o el costo potencial de la oportunidad si el riesgo llega a producirse dentro del proyecto, por lo cual, a cada uno de los riesgos debemos asignarle un valor de impacto que va tener en la organización si el riesgo se transformase en un problema. Debido a que no todos los proyectos de AGR dentro de una organización pueden poseer el mismo valor de impacto para el mismo activo, debemos generar y utilizar una tabla de valoración de impacto por proyecto.

A modo de ejemplo se muestra la tabla de impacto.

Criterio	Retraso en la planificación	Valor numérico
Insignificante	1 semana	1
Marginal	2 semanas	2
Medio	1 mes	3
Crítico	2 meses	4
Catastrófico	Mas de 2 meses	5

Figura 18 – Estimación de Impacto

En la cual se pueden diferenciar:

- El criterio, que la clasificación del impacto en lenguaje natural.
- Retraso en la Planificación, es la medida de tiempo en que se podría atrasar el proyecto.
- Valor numérico, es el valor utilizado para clasificar la importancia del impacto.

4.2.7 Etapa VII - Exposición al riesgo

La exposición al riesgo calcula la amenaza general a la que se podría enfrentar un activo, combinando la información que expresa la probabilidad de una pérdida real con información que indica la magnitud de la pérdida potencial en un único valor numérico.

La exposición al riesgo se calcula multiplicando la probabilidad de riesgo por el impacto. Luego se utilizará la magnitud de la exposición al riesgo para clasificar los riesgos.

Riesgo = Impacto X Frecuencia

Magnitud de exposición al riesgo:

- Aprox. 1 = bajo riesgo.
- Aprox. 2 = riesgo medio.
- Aprox. 3 = alto riesgo[9]

[9] HIGUERA, Ronald P. y HAIMES, Yacov Y., "Software Risk Management", Technical Report. Pittsburgh, Pennsylvania : SEI (Software Engineering Institute) ; Carnegie Mellon University, 1996. Disponible en: www.sei.cmu.edu/pub/documents/96.reports/pdf/tr012.96.pdf. [Consultado el 8 de agosto 2008].

Únicamente serán gestionados los riesgos que posean un valor final mayor 1 (uno), a estos riesgos se los denomina riesgo AGR, mientras que si el valor de la exposición es menor a 1, denominará al riesgo como AG.

Por lo cual tendremos dos grupos de activos:

- AGR, activos analizados, con exposición positiva y que deberán ser gestionados.
- AR, activos analizados, con exposición negativa.

4.2.8 Etapa VIII - Gestión de los Riesgos

Se debe gestionar el riesgo cuya exposición es positiva utilizando, primeramente los denominados "Planes de acción o Salvaguardas".

Magerit define una salvaguarda como "un procedimiento o mecanismo tecnológico que reduce un riesgo al cual se expone un activo" [Magerit v2- Catalogo de Elementos].

La correcta planificación de un conjunto de salvaguardas conlleva a reducir el impacto, reducir el riesgo y reducir la degradación[10] del activo minimizando el daño y/o la frecuencia de ocurrencia del mismo.

Existen amenazas que simplemente mediante una correcta planificación de actividades desaparecen o pueden disminuir su aparición, otras por el contrario necesitan de elementos técnicos (programas o equipos), otras seguridad física y otras de política del personal, que al no ser específicamente un activo informático/tecnológico muchas metodologías no lo toman en cuenta y es de suma importancia poseer una política de salvaguardas del personal interno y externo de la organización.-

[10] Degradación: La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

En realidad no se puede preveer todos los riesgos, y tampoco todos los riesgos previstos son económicamente razonables de poder enfrentarlos en su totalidad, ya que para enfrentar lo desconocido y protegerse de las amenazas expuestas, deberíamos disponer de elementos que detecten el inicio de un incidente y que mediante políticas pro activas y correctamente definidas impidamos que el incidente se convierta en un desastre.-

Siempre es conveniente llegar a un equilibro entre:

- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones.-
- Salvaguardas físicas: protegiendo el elemento de trabajo de las personas y los equipos.
- Medidas de la Organización: de prevención y gestión de los incidentes.
- Políticas de Personal: Es el activo mas delicado e imprescindible, en donde deberían poseer claramente políticas de contratación, formación permanente, medicas disciplinarias al no cumplir con las políticas preestablecidas de las gestión de riesgos.

La salvaguarda deberá ser adecuada para cada activo y para cada dimensión del activo. Además se deberá ajustar a la tecnología vigente, debido a que todos los activos de la IT (con excepción del personal) están en constante cambio y actualización, por lo cual las salvaguardas deberán ser revisadas con periodicidad y actualizadas de ser necesario. Por lo cual es recomendable implementar una estrategia dinámica de revisión y actualización.

<u>Las salvaguardas deben aplicarse para la protección de:</u>

- Protección General: son aquellos que se refiere al buen gobierno de la seguridad sobre todo tipo de activo:

  - Organización de la seguridad.
  - Políticas corporativas de seguridad de la información
  - Gestión de privilegios: adjudicación y revisión.-
  - Protección escalonado y gestión de incidencias.-
  - Procedimientos de continuidad de operaciones: Emergencias y recuperación.-
  - Auditoría, registro (certificación) y acreditación del sistema.-
- Protección de los Servicios.
  - Control de Accesos: se aplica a múltiples tipos de activos (servicios, aplicaciones, equipos etc.).
  - Registro de actuaciones: registro de las actuaciones realizadas por las personas o sistemas.-
  - Registro de incidencias: Registro de errores y observaciones.-
- Protección de los datos / información
  - Control de accesos.
  - Firma electrónica: veracidad de los datos.-
  - Registro de actuaciones.
  - Registro de incidencias.
  - Detección y recuperación: Política de copias de seguridad y recuperación de copias.-
  - Cifrado (preventivo): encriptación de los datos en contraseñas, códigos específicas etc.-
- Protección de Aplicaciones
  - Protección frente a código dañino.-
  - Control de accesos.-
  - Registro de actuaciones.-
- Protección de los equipos.
  - Configuración
  - Mantenimiento
  - Protección frente código dañino.-

  - Registro de actuaciones
  - Gestión de privilegios.
  - Control de accesos.-
- Protección de las comunicaciones.-
  - Plan de continuidad
  - Garantías de integridad.
  - Cifrado
  - Control de accesos.-
  - Registro de actuaciones.-
- Seguridad física.-
  - Protección frente a accidente naturales.-
  - Protección frente a accidentes industriales.-
  - Protección frente a emanaciones electromagnéticas.-
  - Protección del recinto.-
  - Control de acceso al recinto.-
- Relativas al Personal
  - Especificación del puesto de trabajo
  - Selección de personal
  - Condiciones contractuales: responsabilidad en seguridad.-
  - Formación continua.-

Las salvaguardas, deben ser ejecutadas para los activos internos y los externos (Servicios tercerizados).-

En la declaración de la salvaguarda se deben incluir características tales como:

- Control: Es necesario reflejar si la salvaguarda necesita ser controlada y en que periodo de tiempo necesita que se realicen estos controles.
- Seguimiento: Es necesario reflejar si la salvaguarda necesita que se le generan un plan de seguimiento y en que periodo de tiempo necesita que se realicen estos controles.

- Aplicabilidad: Si la salvaguarda se puede aplicar a todas las dimensiones.

Como segunda instancia es necesario definir el "Plan de Contingencia", que por el contrario intenta implementar respuestas rápidas para mitigar los efectos en caso de que los riesgos se concreten, es decir reducir el impacto de los mismos mediante una reacción planeada, para lo cual se debe generar por cada riesgo un plan de contingencia que posea:

1. Disparador: Que acción es la que dispara el Riesgo transformándolo en un problema.
2. Responsable: Quien del equipo de AGR estará a cargo de ejecutar este plan.
3. Pasos a seguir: Que pasos debe seguir el miembro del equipo para poder solucionar el problema.

Además para como información complementaria para gestionar el riesgo de un activo es necesario definir:

- Información necesaria: trata sobre la información necesaria para poder controlar y gestionar los riegos, como por ejemplo, si el riesgo de incendio se ejecuta sobre un activo como la sala de servidores, es necesario contar con los manuales de incendios, plan de corte de energía etc.
- Responsable del Riesgo: una vez que el riesgo se ejecuta, se debe asignar un responsable o un grupo de personas o equipos responsables de solucionar el problema ocasionado por la ejecución del riesgo, por lo cual en esta etapa se deben asignar estos recursos humanos.
- Recursos necesarios: para hacer frente a un problema generado por un riesgo podría ser necesario que se necesiten recursos extras, tanto económicos (planificación presupuestaria) como no económicos (asesoramiento externo, asignación de personal interno etc.), la cual se debe incluir en este punto.

4.3 Fase II – Seguimiento y Control

Un riesgo posee métodos de salvaguardas o comúnmente llamado en su conjunto "Plan de Acción" como hemos visto en este capitulo, que son controles preventivos que poseen los riesgos.

El plan de seguimiento y control, posee características específicas tanto de control como de seguimiento sobre las actividades indicadas en el plan de acción.

Se puede planificar un control para un riesgo y además se debe generar un plan de seguimientos para verificar que las especificaciones expuestas en el plan de acción, sean los correctos y estén bien definidos, catalogados, sean de fácil ubicación y acceso, el cual se establece dentro de periodo de tiempo con acciones de control – mantenimiento bien definidos.

Para este método se propone el siguiente plan de seguimiento

- Gestión de Seguimiento: El seguimiento de una salvaguarda se asignará a un miembro del equipo de ARG, en un proyecto establecido (ver etapa VIII – Gestión de riesgo), el cual verificará las tareas asignadas y realizar los controles pertinentes informando por cada control :

  - Porcentaje de finalización de la tarea de control: Es importante llevar a cabo el porcentaje de finalización de la tarea, debido a que las mismas pueden llevar un tiempo prolongado o puede existir el caso de que el resultado esperado se obtenga de la finalización de otras tareas.

  - Observación de la Tarea: el encargado de la tarea deberá incorporar notas de observación sobre la tareas realizada.

  - Observación de tarea Finalizada: se deberá informar de manera escrita en lenguaje natural, el resultado de la finalización de la tarea.

- Forma de finalización: una vez terminada la tarea se deberá informar si la misma finalizó con los resultados esperados.

❖ Control: El director del proyecto controlará las tareas de seguimiento de las salvaguardas para lo cual se recomienda utilizar técnicas de "tablero de comandos", para informar al director, de una manera visual, cuales actividades no se han realizado o no se ha concluido o si su tiempo de realización ya está vencido.

4.4 Fase III – Registros de incidencias

Esta fase proporciona al AGR un elemento clave para el mejoramiento funcional y operacional de la evolución de riesgos.

De ella se desprende información vital para el proyecto, debido a que se podrá evaluar los incidentes ocurridos, motivos por los cuales ocurrió (amenazas), estado del activo en el AGR y los ajustes que se deberán realizar para optimizar y mejorar el mismo.

El registro de incidentes posee cuatro etapas.

Etapa 1- Denuncia de la incidencia

En esta etapa se asienta una incidencia, la cual puede ser registrada por cualquier miembro de la organización que posea conocimientos del AGR.

En el registro se debe contemplar, que activo sufrió el incidente, cual es la amenaza que disparó el incidente, la fecha - hora del mismo y las acciones primaras a tomar por parte del usuario denunciante. Por ejemplo: se apagó el equipo.

Etapa 2- Control del activo

Pueden suceder tres escenarios con respecto al análisis del activo:

a) Activo no registrado (N/A): el activo no fue registrado en el proyecto AGR, primeramente hay registrarlo para poder continuar con el control de la

incidencia. Para ello se deberá ejecutar lo establecido en el punto 4.2.1 de este capitulo.

b) Activo analizado pero no gestionado (AR): Esto ocurre cuando en el cálculo de la exposición del riesgo es negativo y no se tomo a este como un activo de alto riesgo. Por lo cual se emitirá un informe del estado de revista del mismo.
c) Activo analizado y gestionado (AGR): significa que el activo posee un riesgo que fue analizado y gestionado, por lo que se deberá reportar e informar el plan de contingencias del mismo.

Etapa 3- Información del Incidente

En esta etapa se informan los resultado obtenidos del control del incidente, y consta de dos partes.

I. Informe Plan de Contingencias: Si el riesgo que generó el incidente posee plan de contingencias, se deberá generar un informe en el cual se reflejen:
    a. El plan de contingencias.
    b. El responsable de ejecución del plan.
    c. Pasos a seguir establecidos en el plan.
II. Informe al Responsable: Generar un informe sobre el incidente ocurrido, al responsable designado, al responsable establecido en el plan de contingencias y al encargado o jefe del proyecto.

Etapa 4 – Finalización del Incidente

En esta etapa se formaliza la finalización del incidente en el cual se informa:

- Acciones realizadas para la finalización del mismo.
- Dictamen de finalización.
- Informar si el incidente se finalizó correctamente.
- Fecha de finalización.
- Informe en donde consta si el plan de contingencias fue ejecutado y si lo fue, si el mismo es adecuado para la resolución del problema o se debería mejorar.

En el caso de que el activo que sufriese el incidente fuera del escenario "b" del control del activo se establecerá si se actualizó el mismo.-

4.5 Fase IV – Comunicación

"Comunicar es el proceso mediante el cual se transmite información de un entidad a otra"[11], por que es muy importante comunicar la información procesada de los seguimiento realizados en el AGR y de los incidentes ocurridos en la organizaciones.

Por lo que esta fase contempla:

1) Informe de seguimiento: se debe generar informes periódico referidos al estado del seguimiento de acciones del plan de contingencias, estos reportes deben ser:
   a) Informe de actividad de seguimiento por fecha.
   b) Informe de seguimiento por salvaguarda
   c) Informe de seguimiento por amenaza
   d) Informe de seguimiento por dimensión
   e) Informe de seguimiento finalizado correctamente.
   f) Informe de seguimiento que tuvieron problemas para su finalización.
2) Informe de incidente: se debe generar informes de los incidentes ocurridos, los reportes a generar deben ser:
   a) Informe de total de incidentes ocurridos.
   b) Informe de incidentes finalizados correctamente.
   c) Informe de incidentes finalizados con problemas.
   d) Informe de incidentes con activos que no estuvieron analizados en el proyecto.
   e) Informe de incidentes con activos que estuvieron analizados en el proyecto pero no gestionados.
   f) Informe de incidentes con activos que tuvieron analizados y gestionados.

[11] http://es.wikipedia.org/wiki/Comunicaci%C3%B3n

Debido a que se generó una herramienta software, que genera la confección automática de los reportes y controles, solo remenciona los elementos que debería poseer los mismos.

A modo de conclusión del capitulo, queda establecido el modelo Sei-Mag cuya versión es la 1, en donde se establecen las fases y etapas para lograr generar un análisis y gestión de riesgos, simple, debido a que solo posee 4 etapas, rápido debido a que se incorporan los elementos de clasificación de activos, amenazas y salvaguardas que ya están establecidas en su generalidad para la mayoría de los casos de proyectos software y IT que pudieran existir en una pequeña o mediana empresa, y efectivo ya que está derivado de las dos metodologías más importantes y abarcativas que comprende el análisis y gestión de riesgos en la actualidad.

Capitulo 5

La Herramienta –MySeiMag

5.1 Introducción

En este capítulo se desarrolla los componentes utilizados para la elaboración de la herramienta construida para ser de soporte del método SeiMag, se expone los objetivos del sistema, metodología de análisis, diseño y características del sistema.-

5.2 Objetivos Generales del nuevo Sistema

Desarrollar un Sistema Software para realizar el análisis y gestión de riesgos basados en el método Sei-Mag, el cual permitirá el manejo y la gestión de activos, amenazas, salvaguardas, proyectos, personas, taxonomías, gestión de riesgos, plan de contingencias y generación automática de plan de acción por proyecto, seguimiento, incidencias e informes, el mismo constará de procedimientos de aprendizaje automático de componentes, para generar información estadística y proponer mejoramiento de los planes antes mencionados. Deberá exportar la información procesada en las distintas fases que propone el método en formatos txt, xml, HTML y pdf, deberá poseer seguridad de acceso y control del sistema, auditoría de sistema y de procesos.

5.3 Metodología elegida y justificación de la misma

Luego de analizar las características del sistema a desarrollar. Se divisó la necesidad que la metodología a utilizar para el análisis y diseño del mismo, deberá cumplir necesariamente con las siguientes características:

I. Construcción de prototipos evolutivos: El sistema software a desarrollar será una herramienta asistente, basado en un modelo nuevo en el que no se posee experiencia, por lo cual, una de las mejores prácticas recomendadas por la ingeniería del software, es generar prototipos y que

los mismos evolucionen y mejoren con la ayuda del usuario y los casos de práctica.

II. Método ágil de construcción: No se cuenta con usuarios con experiencia en el negocio, ni en el método además los tiempos de construcción son escasos, por lo cual el paradigma deberá posee la particularidad de generar software de una manera ágil sin perder la formalidad en el análisis y desarrollo, esto permitirá a los pequeños grupos de trabajo concentrarse en la tarea de construir software fomentando prácticas de fácil adopción y mediante un entorno ordenado que ayude a que las personas trabajen mejor y permita que los proyectos finalicen exitosamente y en mínimos lapsos de tiempo.

III. Análisis de riesgos: Basados en las dos características anteriores, será conveniente que la metodología elegida, contemple un mecanismo o técnica de evaluación de riesgos, para abordar tempranamente los aspectos más complejos, costosos y riesgosos del proyecto, dejando para el final los procesos más simples.

5.4 AgEnD- Metodología Ágil y evolutiva.

Para la elaboración del software "MySeiMag V1", se seleccionó la metodología AgEnD, desarrollada por el Ing. Marcelo Hernan Schenone [Schenone, 2004], ya que además de cumplir con las características sugeridas, avanza en el conocimiento teórico de procesos ágiles, analiza los principios de estos y reúne prácticas y patrones que contribuyen a la implementación y posterior adaptación del proceso a la realidad del sistema, esto genera la posibilidad de evolución del mismo. Otro aspecto importante que se tomó en cuenta para la selección de esta metodología es la adaptatibilidad de sus elementos, los cuales pueden ser utilizados adaptándose a la necesidad del proyecto software, ya que brinda flexibilidad en sus

etapas y artefactos a utilizar.

Especificaciones del desarrollo utilizando ADgnD

Background del Proyecto

Para el desarrollo de MySeiMag se ha decidido utilizar un equipo de desarrollo que inicialmente será de una persona. El proyecto será conducido, utilizando algunas prácticas de la metodología AgEnD como proceso, siendo las prácticas seleccionadas por un coordinador con conocimiento de la metodología, la cual se ha estudiado en su totalidad. Debido a que AgEnD es una metodología adaptativa se desarrollará todas sus fases pudiendo adaptarlo a medida se avanza en el desarrollo mediante la intervención del Coordinador (en este caso es el tesista y desarrollador).

Roles y Recursos

Los trabajos de AgEnD están llevados a cabo por una sola persona, que cumple distintos "roles" dentro del proyecto de análisis y desarrollo del software. A continuación mencionamos a los trabajadores:

- Rol Líder de Proyecto.
  Reseña: El Líder de Proyecto es la persona encargada de gestionar el proyecto.

- Rol Analista Funcional, encargado de llevar a cabo el relevamiento.

  Reseña: La Analista es una persona con mucha habilidad y experiencia en relevamientos en grandes proyectos. Está especializada en la confección de Casos de Uso y en el uso de herramientas CASE como el Enterprise Architect para el modelado.

- Rol Coordinador, ayudará al equipo en la implementación de la metodología.

  Reseña: El Coordinador ayudará al Equipo de Desarrollo en la implementación de las prácticas de AgEnD y en la creación de los artefactos propuestos. También actuará de mentor en relación a las tecnologías seleccionadas en el proyecto.

- Rol Desarrollador, posee distintos grados de experiencia en las tecnologías del proyecto.

  Reseña: El desarrollador es un experto en la herramienta seleccionada para el desarrollo del software.

- Rol Tester, se encargará de diseñar y ejecutar los casos de prueba de la aplicación

  Reseña: El Tester será el responsable de llevar a cabo el control de calidad de la aplicación. A medida se vayan liberando versiones realizará el testing funcional de las mismas en base a los casos de prueba que este construyó.

Tecnologías

Al momento de formular la propuesta económica se realizó la selección basada en herramientas RAD[12] 4GL[13] para el desarrollo de la aplicación, debido a que las mismas comprende el desarrollo iterativo, la construcción de prototipos y el uso de utilidades de herramientas de diseño y codificación, reduciendo considerablemente el tiempo de desarrollo (el desarrollador es un experto en esta

[12] Desarrollo rápido de aplicaciones.
[13] Lenguajes de cuarta generación, cuya característica principal es que basado en un modelo de datos posee generación automática de código fuente.

herramienta), programación y aumentando la calidad del trabajo, basándose principalmente en el diseño del sistema.

Como herramientas de análisis y diseño de priorizó por herramientas CASE[14].

Arquitectura de la Aplicación

La arquitectura elegida para el funcionamiento del sistema es la arquitectura cliente/Servidor que contiene tres capas.

La arquitectura de la aplicación estará compuesta por las siguientes capas:

Capa de Presentación: En formato de ventanas, se desacopla esta capa de las capas de lógica del negocio y manejo de datos.

Capa de Lógica del Negocio: inicialmente, se puede pensar en un esquema sencillo de lógica del negocio que simplemente reciba/envíe la información a la capa de presentación, mediante la interacción directa con la capa de manejo de datos.

Capa de Manejo de Datos: El diccionario de datos es un depósito de metadatos que almacena descripciones de tablas, atributos por default sobre como las columnas deben ser desplazadas en las ventanas y reportes, controla las reglas de negocios y opciones de uso.

Plataforma Base y Herramientas

- Microsoft Windows: SO de desarrollo

[14] Son diversas aplicaciones informáticas destinadas a aumentar la productividad en el desarrollo de software reduciendo el costos de las mismas en términos de tiempo. Estas herramientas nos pueden ayudar en todos los aspectos del ciclo de vida de desarrollo del software en tareas como el proceso de realizar un diseño del proyecto, calculo de costes, implementación de parte del código automáticamente con el diseño dado, compilación automática, documentación o detección de errores entre otras.

- CVS Clarion EE: Sistema de Administración de la Configuración.

- Clarion 7.2: IDE de Desarrollo

- Enterprise Architect: Herramienta de modelado para realizar el modelo de casos de uso, diagrama de requerimientos y de secuencia.

- Gantt Proyect: Herramienta para realizar proyectos.

Framework de Aplicación y Reportes

Clarion 7.2 es el Framework utilizado para la capa de presentación de la aplicación y para el diseño de los reportes.

Data Access Object (DAO) – Diccionario de Datos

DAO: patrón de diseño a ser implementado en la solución. El mismo especifica una framework que se utiliza para realizar la capa de persistencia de la aplicación, que en este caso es el denominado "diccionario de datos" con el que trabaja el lenguaje seleccionado.

Lanzamiento del Proyecto

El desarrollo del software MySeiMag V1 se inicia una vez que el método SeyMag fue culminado y evaluado satisfactoriamente.

Se genera un primer relevamiento en el que se obtienen los requisitos de la etapa de aplicación, generando además los límites del sistema y casos de uso de requisitos.

Una vez finalizada la etapa de requerimientos y con los límites ya establecidos, se genera el proyecto, estableciendo los tiempos estimados para las actividades y los recursos necesarios para su desarrollo. Se establece una planificación con las fases en que el proyecto MySeiMag será dividido tomando como referencia las fases AgEnD.

Disciplinas de Soporte

Administración del Proyecto

AgEnD recomienda ir customizando la metodología de acuerdo a las necesidades del proyecto y de las personas.

Primeramente se realizaron los requerimientos funcionales del sistema, utilizando el formalismo UML. Luego se definió los límites del sistema y se pudo distinguir claramente el alcance del mismo.

Se observó que al ser un sistema herramienta y al no contar en esta etapa con un usuario real, fue necesario tomar un rol de arquitecto de software para tener una clara idea de los requerimientos no funcionales del sistema abordando primeramente los mismos.

Tomando el concepto del Scrum Daily Meeting sugerido por Scrum [Schwaber,2001], se decidió agregar dentro de la disciplina de Administración de Proyecto de AgEnD esta reunión diaria de quince minutos a primera hora de la mañana. Al no contar con un equipo de personas como es lo común en las reuniones diarias, se simuló esta práctica generando igualmente las actividades diarias para los distintos roles. En un principio está practica fue muy dificultosa de entender debido a que una sola persona debe asumir distintos roles; pero con el paso de los días, no solo fue desapareciendo esa dificultad, si no que, fue incrementando la productividad en todos los roles definidos.

Como técnica de documentación, se anotaba en una planilla por cada uno de los roles las actividades que se realizó el día anterior y que se planificó realizar en el día, aclarando los obstáculos que se podrían presentar en las actividades. Está practica permitió ir obteniendo un control y monitoreo constante sobre el progreso y los riesgos que se iban presentando.

Administración de la Configuración

Se armó el repositorio en CVS utilizando el mismo lenguaje de programación, ya que el Clarion 7.2 posee herramientas de control de versiones, esto se utilizó únicamente para el desarrollo del sistema y del modelado de los datos.

Máxima Comunicación

La práctica de Máxima Comunicación no pudo ser implementada en su totalidad, debido a que no se cuenta con el cliente como especifica la metodología. Pero de todas maneras, se utilizó al tutor de la tesis en el rol de cliente, con el que se realizó esta práctica.

Enfoque en la Arquitectura

Una vez que se comenzó con la especificación de los primeros casos de uso, en paralelo se empezó a definir la arquitectura del sistema.

Uno de los requerimientos no funcionales más importante, era el construir un sistema flexible y de simple mantenimiento, el cual pudiera incorporar cambios con facilidad y ser parametrizable.

Tomando como input los casos de uso que se iban observando y las cualidades sistémicas requeridas, se fue armando el documento de Descripción de la Arquitectura.

Estimaciones Ágiles

Siguiendo a AgEnD, se tomaron el total de los casos de uso para la primera versión del sistema, de manera de efectuar una estimación global de la duración del proyecto. Se dejó en claro que dicha estimación arrojaría un resultado aproximado en tiempo y esfuerzo que se establece utilizando el artefacto “Plan de proyecto” (ver

Anexo II), y dada la naturaleza de los procesos ágiles, el mismo, serviría para planificar hitos importantes del proyecto.

Integración Continua

De acuerdo a la práctica de AgEnD, se configuró un entorno de desarrollo que fomentara la integración continua. Con el rol de desarrollador, se trabajo arduamente en la implementación de los casos de uso y diariamente se subía el trabajo realizado al repositorio, en este caso el CVS.

Una vez que estaba finalizado el release, era testeado unitariamente y funcionalmente para verificar que el sistema cumplía con los requisitos relevados. Al fin de cada etapa, en el rol de tester, se tomaba todo lo construido y guiándose con los casos de prueba, se llevaba a cabo el testing funcional. En el proyecto MySeiMag no existieron problemas relacionados con la integración.

Artefactos

De acuerdo a la definición de AgEnD, se recomienda especificar al principio del proyecto, aquellos artefactos que serán generados y mantenidos durante el ciclo de vida. Esta es una de las tareas que el rol de Coordinador de Proceso realiza durante las primeras iteraciones. El resultado de la misma es el siguiente:

Plan de Proyecto: representado mediante un diagrama de Gantt en el que se irá plasmando la planificación del proyecto durante el tiempo.

Modelo de requisitos: contiene los requerimientos funcionales de carácter más técnico y no funcional del sistema con apéndices de diseño.

Casos de Uso: contiene la especificación de los requerimientos funcionales del sistema.

Diagrama de Secuencia: es una forma de diagrama de interacción que muestra los objetos como líneas de vida en el tiempo, y se aplica a la construcción de los casos de uso.

Modelo de diseño o datos: Típicamente un modelo de datos permite describir, las estructuras de datos de la base, las restricciones de integridad y las operaciones de manipulación de los datos.

Código Fuente: incluye el código de las clases, las imágenes, los archivos de configuración, los scripts de despliegue y demás recursos que componen el proyecto de desarrollo.

Casos de Prueba: contienen los flujos de ejecución que serán utilizados por los testers para probar la aplicación desde un punto de vista funcional; son creados a partir de los casos de uso.

Se presenta cada uno de los artefactos utilizados en el Anexo II.

Resultados del Proyecto

Después de 3 meses de desarrollo, llega el hito de entrega del primer release V1.0, que concluye la puesta en práctica de las características AgEnD.

El producto final, al ser una herramienta asistente para un método adaptado, se decidió generar un "estudio de caso" del método y la herramienta en el Colegio de Médicos de la Pcia. de Misiones, en donde se realizaron dos proyectos de AGR:

Sala de Servidores y Recursos Humanos. Se testeó el sistema y se observó que el mismo cumple con la funcionalidad requerida y con la calidad esperada.

Se han implementado gran parte de las prácticas recomendadas por el AgEnD.

Debido a que este trabajo está orientado a la investigación y construcción de un método adaptado de AGR no se podrá hincapié en este capitulo en el formalismo de la metodología de análisis y diseño del sistema, únicamente se comentan aspectos de la metodología que contribuyen al éxito del proyecto.

5. 5 Aspectos particulares del sistema MySeiMag

A continuación se define puntualmente los aspectos particulares del sistema desarrollado.

I. Ingreso al sistema: El sistema contiene un panel de ingreso, en donde para acceder, se deberá ingresar el usuario y contraseña asignados. Únicamente ingresarán los usuarios autorizados, además el alcance de la utilización del sistema, lo da el nivel de acceso que el usuario posea.

II. Parámetros Iniciales: Trata sobre los parámetros generales. Estos deben está cargados para poder ejecutar las demás fases del método.

   a. Tipos de activos: Trata sobre el tipo de activo en los cuales se clasifican los activos.

   b. Elementos: Este módulo gestiona los elementos (características de los tipos de activos).

   c. Dimensión: Gestiona las diferentes dimisiones que posee un activo, y son las características principales en donde se ejecutan las salvaguardas.

   d. Valoración: Trata sobre el valor de importancia que se le asigna al activo. Dicho valor dimensiona al activo asignado una variable ha ser evaluada cuando el riesgo llegara trasformaste en una perdida para la empresa o que su funcionamiento del activo no sea el esperado.

   e. Tipo de Amenazas: Trata sobre los grupos en donde se enmarcan las amenazas.

f. Amenazas: Riesgos que corren los activos, a cada amenaza se agrupara dentro de un tipo de amenaza.

g. Salvaguardas: Trata sobre las acciones detectivas que deben poseer los activos para que los riesgos se no activen. Se asignará a las salvaguardas las etapas del ciclo de vida en donde es importante, si posee seguimiento y control agregado, cada cuanto tiempo hay que generar el seguimiento.

h. Datos de la Organización: Trata sobre la configuración de datos propios de la organización, este módulo le da flexibilidad al sistema, ya que el mismo software puede dar soporte a cualquier organización.

i. Fuentes de información: Trata sobre el área de la organización en las cuales se visita en búsqueda de información de los activos.

j. Medidas de tiempo: Módulo de configuración de los tiempos que son utilizados en el módulo de salvaguardas. En este módulo se configuran las medidas de tiempo de seguimiento, como así también el espacio entre días.

k. Gestión de usuarios: En este módulo se gestionan los usuarios del sistema, asignándolos una identificación al usuario, una contraseña de acceso y se especifica a que grupo de usuarios pertenece y que nivel de acceso posee en el sistema.

III. Análisis y gestión de Riesgos: Trata sobre las la fase I del método SeiMag. Está distribuido en etapas y algunas de ellas en sub-etapas.

a. Etapa - inventario de activo:

   i. Gestión de activos: Trata sobre la gestión de los activos, se detallan las características de los activos que posee la organización y se asigna una valoración, que resulta del análisis de importancia de pérdida del mismo.

   ii. Gestión de Elementos por activo: Gestiona los elementos de los activos, basándose en el tipo de activos.

   iii. Asignación de dependencia: módulo que gestiona la dependencia entre activos.

   iv. Fuente de información: El módulo gestiona la asignación de la fuente de información a los activos.

b. Etapa - Propósitos y Objetivos:
   i. Gestión de Proyecto: Módulo en donde se gestiona el proyecto, asignándole un código, una descripción, definiendo límites, propósitos y objetivos del proyecto, asignando activos al mismo.

c. Etapa - Equipo de Trabajo:
   i. Gestión de Equipo: El módulo trata sobre la asignación de equipos de trabajo a los proyectos, además proporciona la gestión de roles y personas.

d. Etapa - Taxonomía: Modulo que genera automáticamente la taxonomía de los riesgos que se encuentran en un proyecto

dado. A cada riesgo se debe asignar a que elemento pertenece y la fuente de información, la cual es la encargada de clarificar el riesgo tomado, filtra además, el listado de los riesgos que pueden ser evaluados en la próxima etapa.

e. Etapa - Declaración: Trata sobre la gestión de los riesgos por proyectos, asignándoles las variables de condición, consecuencia y efectos que posee cada uno, también muestra un filtro de los activos a ser evaluados.

f. Etapa – Probabilidad – Impacto:

   i. Probabilidad de ocurrencia por proyecto: Módulo que genera las tablas de probabilidades por proyectos, en la misma se asignan, el proyecto, el valor de los rangos mínimos y máximos de probabilidad de ocurrencia, el valor medio, la exposición al riesgo y el valor nominal de este.

   ii. Impacto de ocurrencia por proyecto: Trata sobre la gestión de la tabla de impacto por proyecto, en donde se establecen por cada uno los criterios de impacto, los retrasos producidos y el valor nominal.

   iii. Estimación de Probabilidad – Impacto: Este módulo trata sobre la asignación a cada riesgo del porcentaje de probabilidad de ocurrencia y el valor nominal del impacto acumulado, además posee una función de filtrado los activos que serán evaluados en la siguiente etapa.

g. Etapa – Exposición: Módulo que genera automáticamente la exposición de cada riesgo y muestra en un listado, los activos que son expuestos a los riesgos.

h. Etapa – Gestión de Riesgos: Trata sobre la gestión de los riesgos que son expuestos. Este módulo consta de las siguientes partes:

   i. Detalles del Riesgo: se establecen la información necesaria para el abordaje del riesgo, el responsable del control y seguimiento y los recursos necesarios para afrontar el control del mismo.
   ii. Plan de acción: módulo que genera automáticamente el plan de acción por cada proyecto, evaluando los riesgos, activos y dimensiones de estos. Y presenta el listado resultante de este proceso, en el cual se pueden añadir las salvaguardas que sean necesarias.
   iii. Plan de Contingencias: en este módulo se carga el plan de contingencia del riesgo, se asigna un disparador, un responsable de realizar el plan y los pasos a seguir para la solución del problema.

IV. Seguimiento y Control: Trata sobre la fase II del método.

a. Generar Plan de Seguimiento: Genera automáticamente el plan de seguimiento por proyecto, evaluando cada uno los elementos del plan de acción de la etapa de gestión de riesgos del la fase I.

b. Agenda de Actividades: Módulo que gestiona la agenda de actividades del seguimiento por persona asignada. El mismo filtra las actividades a realizar por persona, la gestión de esta, se lleva a cabo asignado el porcentaje de avance de la

actividad, y el control de finalización de la misma. Además muestra un orden de actividades por fecha planificada, por amenaza o salvaguarda.

V. Incidencias: Aborda la fase III del método SeiMag.
    a. Carga de la Incidencia: Módulo en donde se cargan las incidencias ocurridas, se asigna el activo y la amenaza que disparo la incidencia, la persona responsable de la misma, fecha , hora y una acción inmediata a tomar. El módulo automáticamente una vez aceptada la carga, procesa la información y genera las siguientes acciones :
        i. Evalúa y expone el tipo de riesgo que posee el activo.
        ii. Emite un reporte con el plan de acción designado para este riesgo si correspondiese.
        iii. Envía un email a los responsables de ejecutar el plan de acción, como también al encargado del proyecto.

    b. Finalización de la incidencia: Módulo que gestiona la baja de la incidencia cargada, muestra únicamente las incidencias sin resolución y solicita para poder dar de baja la incidencia los siguientes datos:
        i. Observación de finalización de la incidencia.
        ii. Fecha de la finalización de la incidencia.
        iii. Pregunta si la incidencia se solucionó correctamente.
        iv. Pregunta si el plan de contingencias es adecuado.
        v. Pregunta si es necesario mejorar el plan.

VI. Informes: Trata sobre la Fase IV del método, denominado comunicación.

    a. Incidentes

i. Riesgos por Incidente: Genera informes sobre los incidentes tratados. Muestra la manera de finalización del incidente, los finalizados, los pendientes de finalización, los riesgos por tipo de análisis (sin análisis, analizados y no gestionados, gestionados).

ii. Estadística: este módulo posee como finalidad procesar datos estadísticos sobre los incidentes, para lograr aumentar la línea de aprendizaje del método de gestión de riesgos. El mismo muestra en un lapso de tiempo los indecentes que se produjeron, los activos a los cuales pertenecen, y la evaluación de los riesgos. También se puede filtrar el proceso para evaluar únicamente los incidentes finalizados.

b. Seguimientos

i. Finalizados: Genera informes sobre seguimientos terminados, forma de finalización, muestra un orden por amenazas, salvaguardas y activos.

ii. Activos: Módulo que genera información sobre los seguimientos de activos, muestra las tareas activas por personal asignado y el porcentaje de finalización de las tareas.

VII. Ayuda: Módulos de ayuda y manuales de usuario del sistema.

Como conclusión de este capitulo se pudo obtener una visión general sobre los objetivos principales que deberá tener el software, las características específicas y metodología de análisis y desarrollo del mismo.

Con el objetivo de no extender la base de este trabajo se incluyeron tres anexos (Estudio de Cado para la prueba del método y la herramienta, artefactos para el análisis y desarrollo del mismo y encuesta realizada en la investigación).

Capitulo 6

Conclusión del trabajo
Futuras líneas de investigación

6.1 Conclusión

Se pudo observar en la bibliografía obtenida y en otros trabajos de investigación, que muchas organizaciones han modificado el método original del análisis y gestión de riesgos adaptándolo a sus necesidades, lo que no se observó, fue la adaptación de un método utilizando elementos de otro, en otras palabras, integrar lo mejor de dos metodologías, y sobre todo con la posibilidad de ser utilizada por cualquier organización.

Métodos de AGR hay muchos, pero ha diferencia de los demás, este método busca la agilidad y adaptabilidad de las actividades, por lo cual, se impulsa a tratar únicamente las tareas necesarias, pero, el manejo de la base de conocimiento como las amenazas, salvaguardas, fuentes de información etc., derivan en una alta carga de trabajo manual, que fueron abordadas con la herramienta creada para tal efecto.

A fin de cumplir con la totalidad de los objetivos propuestos y facilitar el trabajo a los auditores informáticos de las organizaciones, se desarrollo MySeiMag V1, herramienta que abre paso a la automatización de procesos y genera una base de conocimientos y un proceso de aprendizaje, que se podrá ampliar en futuras líneas de investigación.

Fue muy importante generar un estudio de caso real, ya que se puso a prueba SeiMag y MySeiMag, obteniendo como resultado, que el método y la herramienta creada cumplen con las características de:

- Formalidad
- Practicidad
- Facilidad
- Automatización
- Información para la optimización del modelo.

Por ello, se podría decir que el objetivo fue cumplido, debido que, es un método que se podrá utilizar independientemente de la tecnología actual y futura, en las organizaciones de cualquier tipo.-

6. 2 Futuras líneas de investigación

Inicialmente el método y la herramienta creados para esta tesis, se enmarcan en un trabajo de investigación, presentado y aprobado por la secretaría de investigación y postgrado de la Facultad de Ciencias Exactas Químicas y Naturales de la Universidad Nacional de Misiones.

Además, está pensado, utilizar la herramienta en el servicio médico asistencial de la universidad nacional de Misiones, lo cual brindará la valiosa realimentación del uso del método y del sistema en entornos y situaciones reales, lo cual, dará origen muy probablemente a nuevas propuestas de ampliación de la herramienta.

Aun antes de esto, expongo futuras líneas de investigación ya identificadas para el método y la herramienta que puede abarcar los siguientes trabajos:

- Mejorar el tratamiento de los riesgos críticos, generando un plan de seguridad para corregir estas situaciones.

- Realizar un estudio más minucioso de los incidentes que poseen los activos, para generar información sobre la degradación generada en un activo y sus dependientes.

- Proponer un análisis de la mitigación de los riesgos, generando un balance entre las salvaguardas existentes y su plan de mitigación.

- Basándose en la información de incidentes y seguimientos que procesa el sistema, esté deberá adquirir la capacidad de aprender de dicha información, es decir, tomando como base el sistema actual generar nuevas aplicaciones para trasformar este sistema en un sistema experto.

- Automatizar la simulación de riesgos mediante árboles de ataque.

- Profundizar y ver la posibilidad metodológica, para gestionar el impacto acumulado producido por un riesgo y su repercusión.

- Ampliar las facilidades del sistema con ayuda en línea.

- Adaptar de la herramienta para su ejecución de modo remoto o en un ambiente web, utilizando un lenguaje de programación y motor de base de datos con licencia GNU[15].

- Mejorar de la herramienta para soportar multi organizaciones y que el software, pueda asistir además de a una organización a un profesional en gestión de riesgos.

- Añadir informes estadísticos y gráficos.

- Mejorar los avisos de incidentes incluyendo además de la notificación vía email, avisos por sms.

[15] Licencia pública de distribución de software libre.

Capitulo 7

Referencia Bibliográfica

Bibliografía

En este capitulo se detallan la bibliografía y abreviaturas empleadas durante el desarrollo del presente trabajo.

Referencias Bibliográficas

[Active Risk Manager, SEI 2004]. *Active Risk Manager*. Disponible en http://www.strategicthought.com/QuickPlace/stlwebsite/PageLibrary80256D6D007EC8CB.nsf/h_Toc/d84e8c26d5c18c1888256deb006ef979/?OpenDocument. Página vigente al 24-Jul-2008.

[ANSI/IEEE 1042, 1987]. *IEEE Guide to Software Configuration Management (ANSI/IEEE STD 1042-1987).* Disponible en http://www.standards.ieee.org/. Página vigente al 24-Jul-2008.

[ASC, 2003]. *Risk Management Process & Implementation*. American Systems Corporation. Disponible en http://www.2asc.com. Página vigente al 24-Jul-2008.

[Caper Jones, 1994]. *Assessment and Control of Software Risks*. Editorial Prentice Hall. ISBN 0137414064.

[Carabajal Armando , 2008] *Análisis y Gestión de riesgos- Metodología Magerit.* http://www.acis.org.co/fileadmin/Conferencias/ConfArmandoCarvajMayo8.pdf - Visitado el 10-Oct-2010.

[Carr M., Konda S., Monarch I., Ulrich F., Walker C. , 1993]. *Taxonomy- Based Risk Identification, Technical Report CMU/SEI-93-TR-6*, Software Engineering Institute, Carnegie Mellon University.

[Charette, 1989]. *Software Engineering Risk Analysis and Management*. McGraw-Hill/Intertext.

[CMMI, 2002]. *Capability Maturity Model Integration*. Software Engineering Institute. Disponible en http://www.sei.cmu.edu/cmmi/cmmi.html. Página vigente al 24-Jul-2008.

[Futrell, Shafer & Shafer, 2002]. *Quality Software Project Management*. Editorial Prentice Hall. ISBN 0130912972.

[Gerorge Nattey, 2005]. A Short *Taxonomy*-Based Questionnairen Disponible en http://www.controllingchaos.com/Examples/Risk%20Identification%20-%20Classification%20%28SEI%29.pdf. Página vigente al 19-Feb-2010.

[Hantos, 2000]. *A Practical Approach to Quantifying Risk Evaluation Results*. Disponible en http://www.stsc.hill.af.mil/crosstalk/2000/02/hantos.html. Página vigente al 24-Jul-2008.

[IEEE 1058, 1987]. *IEEE Standard for Software Project Management Plans (IEEE Std 1058.1-1987).* Disponible en http://www.standards.ieee.org/. Página vigente al 24-Jul-2008.

[IEEE 1540, 2001]. *IEEE Standard for Software Life Cycle Processes-Risk Management (IEEE Std 1540-2001).* Disponible en http://www.standards.ieee.org/. Página vigente al 24-Jul-2008.

[IEEE 730, 2002]. *IEEE Standard for Software Quality Assurance Plans (IEEE Std 730-2002).* Disponible en http://www.standards.ieee.org/. Página vigente al 24-Jul-2008.

[IEEE 829,1983]. *IEEE Standard for Software Test Documentation (ANSI/IEEE*

Std 829-1983). Disponible en http://www.standards.ieee.org/. Página vigente al 24-Jul-2008.

[IEEE 830,1998]. *IEEE recommended practice for software requirements specifications (IEEE Std 830-1998).* Disponible en http://www.standards.ieee.org/. Página vigente al 24-Jul-2008.

[ISO/IEC 13335-1, 2004]. *Information technology, Security techniques, Management of information and communications technology security.* Disponible en http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066 . Página vigente al 07-Abr-2010.

[KLCI , 2001]. *Software Risk management Practices* , KLCI research group report, Disponible en http://www.klci.com. Página vigente al 09-Abr-2010.

[Kontio, J. , 1997]. *Empirical Evaluation of a risk management Method*, SEI conference on risk management, USA.

[Kuna H., 2004]. *Proyecto de desarrollo de un sistema, Análisis de riesgo*. Apuntes de cátedra. Disponible en http://www.aulavirtual-exactas.dyndns.org/claroline/document/document.php?cmd=exChDir&file=%2FClases. Página vigente al 18-Oct-2010.

[Marvin J. Carr, Suresh L. Konda, Ira Monarch, F. Carol Ulrich y Clay F. Walker, 1993]. *Taxonomy-Based Risk Identification*. 90 páginas. Disponible en www.sei.cmu.edu/pub/documents/93.reports/pdf/tr06.93.pdf. Página vigente al 24-Jul-2008.

[Mergerit V2, 2006]. *MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Disponible en http://www.csae.map.es/csi/pdf/magerit_v2/metodo_v11_final.pdf, Página vigente al 21-Jul-2009.

[Microsoft, 2002]. *MSF Risk Management Discipline v.1.1*. 54 Páginas. Disponible en http://www.microsoft.com/downloads/details.aspx?FamilyID=6c2f2c7eddbd-448c-a218-074d88240942&DisplayLang=en. Página vigente al 24- Jul-2008.

[Motorola LMPS, 1999].*Risk Management*, Motorola Land Mobile Products Sector. Publicado el 20-Abr-1999

[Moynihan T. , 1997]. *How Experienced Project Managers Assess Risk*, IEEE software, pp. 35-41.

[Rosenberg, L., Hammer, T., Gallo, A., 1999]. *Continuous Risk Management at NASA*. Disponible en http://satc.gsfc.nasa.gov/support/ASM_FEB99/crm_at_nasa.html. Página vigente al 24-Jul-2008.

[Schenone Marcelo H., 2004]. *Diseño de una metodología agil de desarrollo de software*. Disponible http://materias.fi.uba.ar/7500/schenone-tesisdegradoingenieriainformatica.pdf . Página vigente al 13-Sep-2010.

[Schwaber, 2001] Schwaber, Ken, Mike *Beedle, Agile Software Development with Scrum*, Prentice Hall, 2001.

[Walker, 1998]. *Software Project Management, A Unified Framework*. Addison Wesley.

[Wideman, 1998]. *Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities (PMBOK Handbooks)*. Editorial PMI. ISBN 1880410060.

[Williams Ray, 2003]. *New directions in Risk Management at SEI*. NASA RMC IV. Disponible en www.sei.cmu.edu/programs/acquisitionsupport/ presentations/williams/new-directions/new-directions.pdf. Página vigente al 24-Jul-2008.

Anexo I

Estudio de Caso

Software MySeiMag V1

Estudio de Caso

Para lograr evaluar el sistema, y al no poseer un usuario final que solicitó el desarrollo del mismo, se logró, gracias a la colaboración del presidente del colegio médico de Misiones, Dr. Luis Flores, generar un estudio de caso del método y sistema desarrollado en esa institución.

Se generaron tres proyectos, basando nuestro estudio de caso en el proyecto "Personal", en donde se generó un análisis y gestión de riesgos basados en el personal informático de dicho colegio, se simularon incidencias bajo la amenaza "Extorsión" del activo "Personal informático externo" e informes que se detallan a continuación.

Estado de Situación

El colegio de médicos de Misiones, cuenta con sistema de gestión propio desarrollado a medida, y además con software herramientas de uso de oficina (procesador de texto, planilla de cálculos), cuenta con una sala de servidores en el cual posee dos servidores, un servidor de datos y otro de comunicaciones y backup. El colegio no cuenta con personal informático de planta permanente, cuenta con un profesional informático que realiza el rol de encargado de IT que posee un contrato anual, y un profesional en diseño web con un contrato free.

Lanzamiento del Estudio de caso

Etapa 1 – Instalación y parametrización del sistema.

Utilizando el instalador del sistema MySeiMag V1, se instaló el mismo en una computadora tipo PC, con sistema operativo Windows XP SP2, que es utilizada como terminal unida a la red LAN del colegio, sin observarse problema alguno.

Una vez instalado el sistema de manera local se procedió a ingresar por primera vez al mismo, para lo cual, el sistema posee un usuario y contraseña de primer ingreso, que luego hay que modificarlo (ver Figura 19).

Figura 19- Login de acceso al sistema

La primera vez se ingresó al sistema con el usuario de acceso correspondiente, y luego se modificó por los usuarios habilitados para el uso del mismo, que se explicará en el módulo de gestión de usuarios.

Parámetros

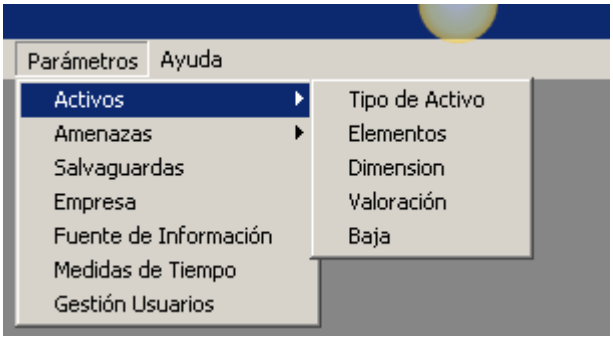


Figura 20- Menú Parámetros

Gestión de Usuarios

Como primer paso se ingresó al menú parámetros y luego a gestión de usuarios.

En la gestión de usuarios, existen dos módulos a parametrizar, por un lado está "Grupos" en donde se gestionan los grupos de usuarios, y por el otro lado esta "Usuarios" donde se gestionan los usuarios del sistema. Un usuario puede o no, pertenecer a uno o varios grupos.

En el sistema, el nivel de acceso al mismo se realiza por niveles, que son asignados a los usuarios, y cuya prioridad es:

- Nivel 4 – Administrador del sistema, posee acceso a todos los módulos del sistema.
- Nivel 3 – Usuario Avanzado, posee autorización a la totalidad de los módulos del sistema, excepto a la gestión de usuarios, esté nivel está pensado para ser asignado a los jefes de proyectos.
- Nivel 2 – Usuario de ARG, posee acceso únicamente a las áreas de fase I, II, III y IV, el cual puede gestionar un proyecto, controlar y generar seguimiento, cargar y terminar incidencia, generar e imprimir información del sistema.

- Nivel 1 – Usuario común, posee privilegio únicamente para cargar un incidente.

Para la gestión de usuarios, primeramente se cargaron los grupos de usuarios (ver figura 21) y luego se generó el alta de los mismos (ver figura 22).

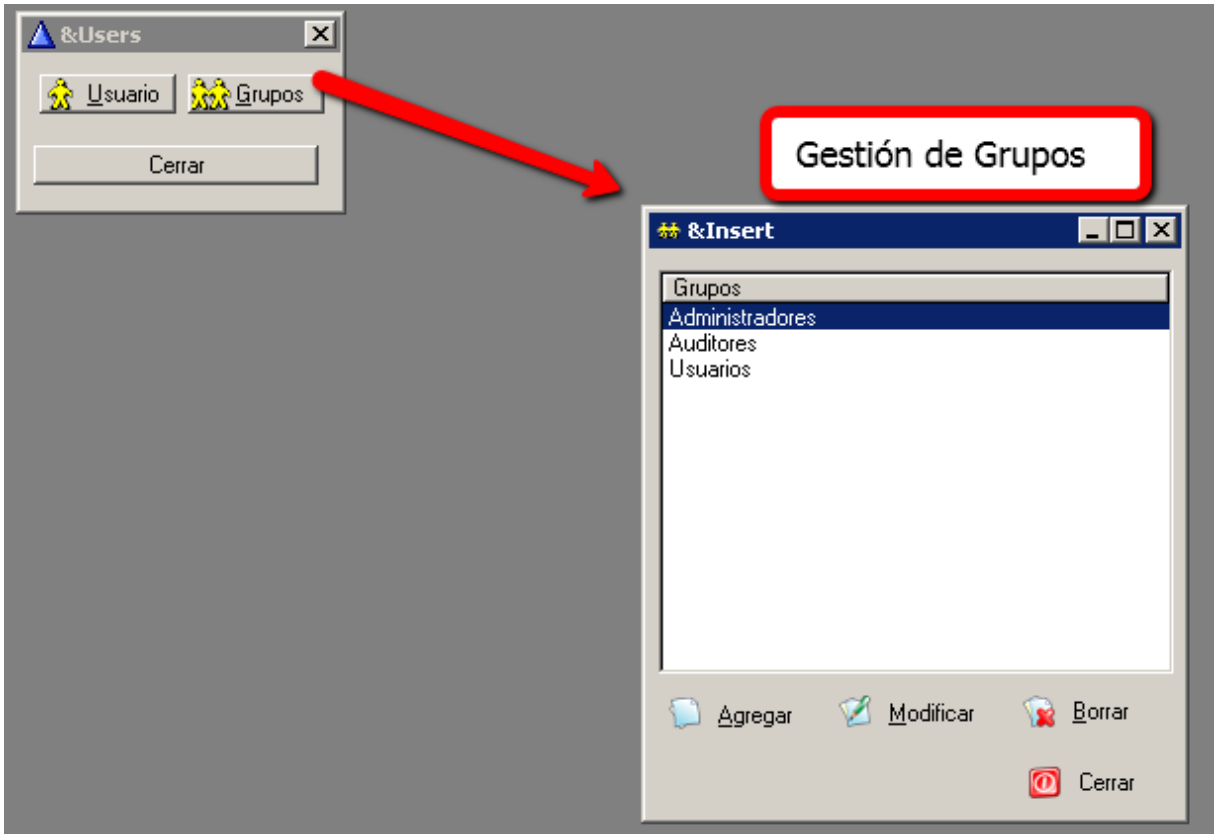


Figura 21 – Gestión de Grupos de usuarios

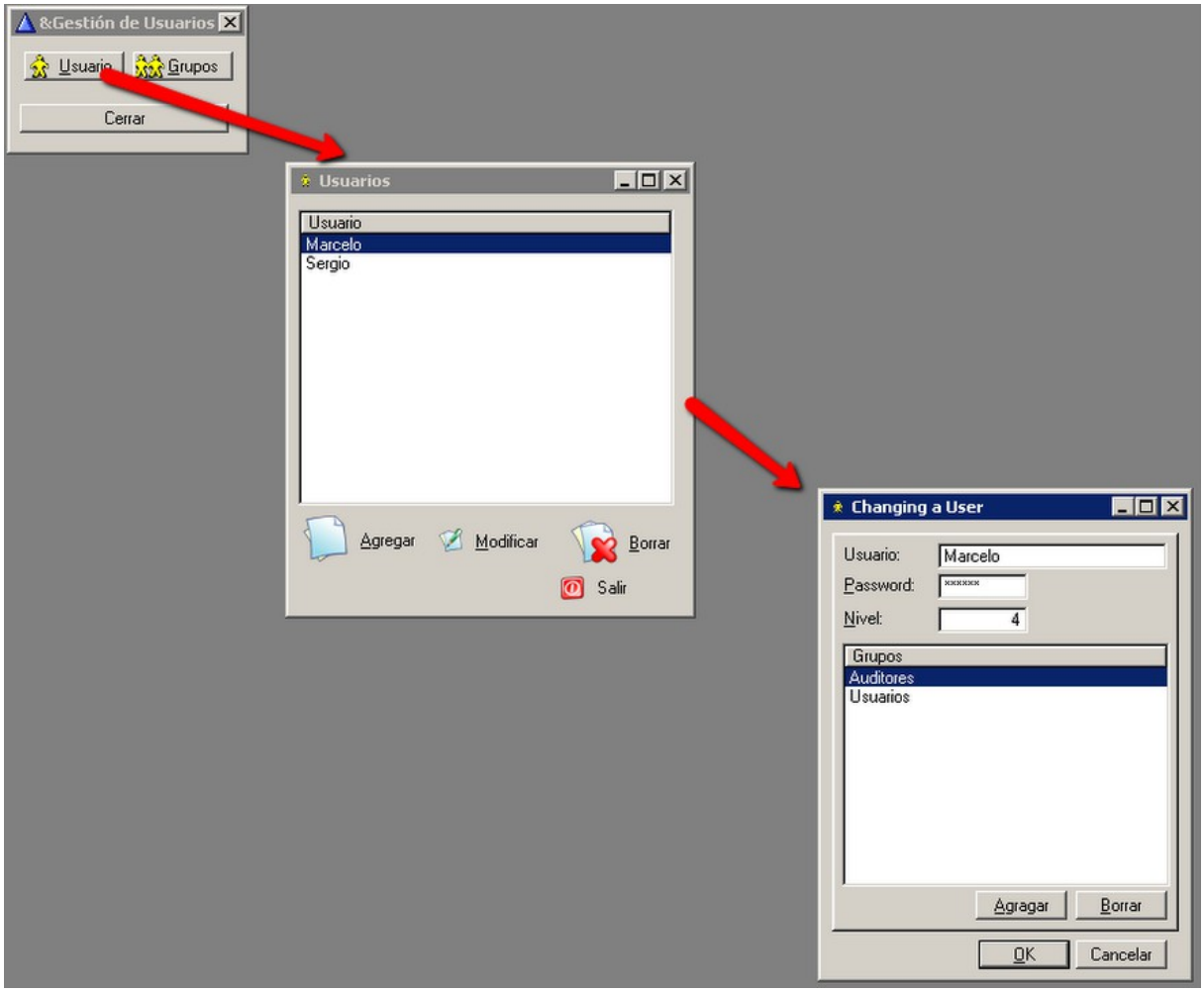


Figura 22 – Gestión de Usuarios

Tipos de Activos

Como parámetro inicial se cargaron los tipos de activos (sugeridos por MageritV2) con sus descripciones en el módulo de gestión de tipos de activos (ver figura 23).

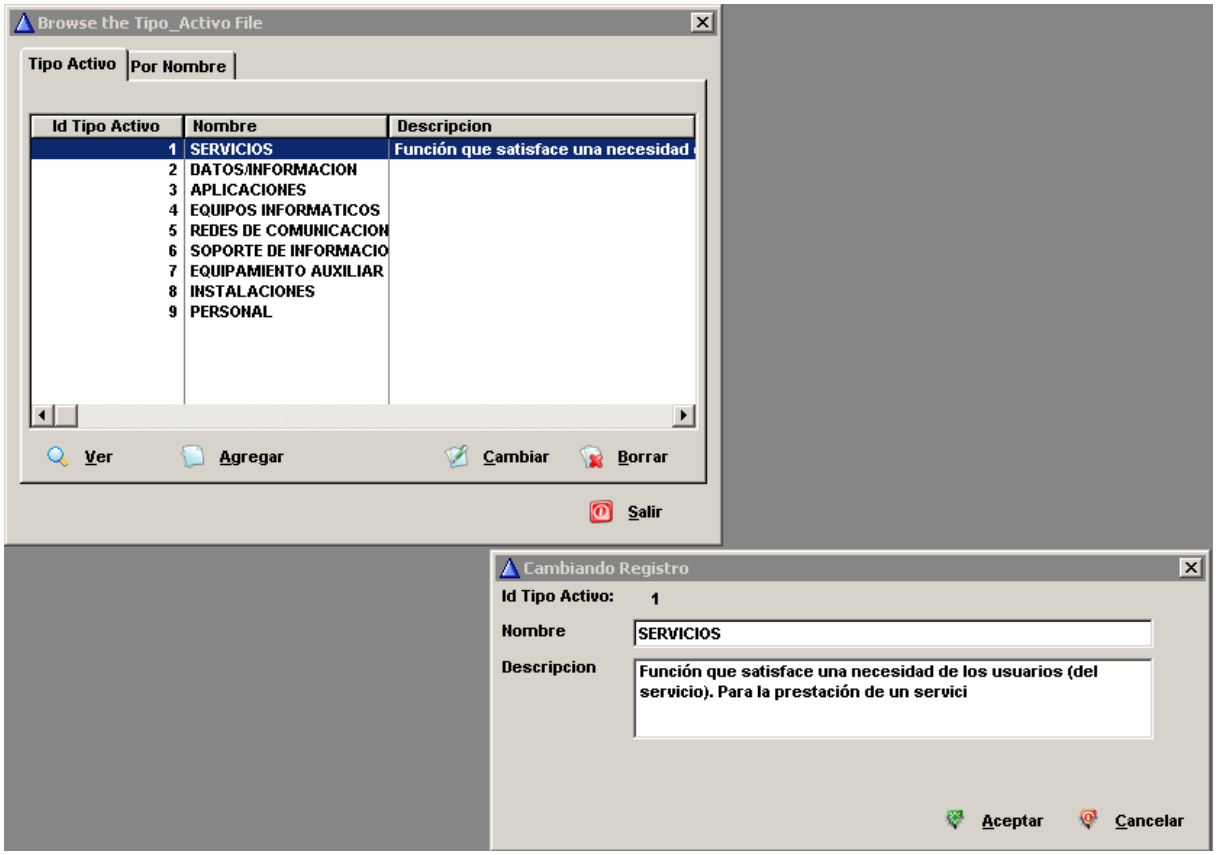


Figura 23 – Gestión de Tipo de Activos

Elementos

Se cargaron los elementos que posee cada tipo de activo, los mismos son sugeridos por Magetit V2, en donde se expresan el código propio del elemento, el nombre y el tipo de activo al cual pertenece (ver figura 24).

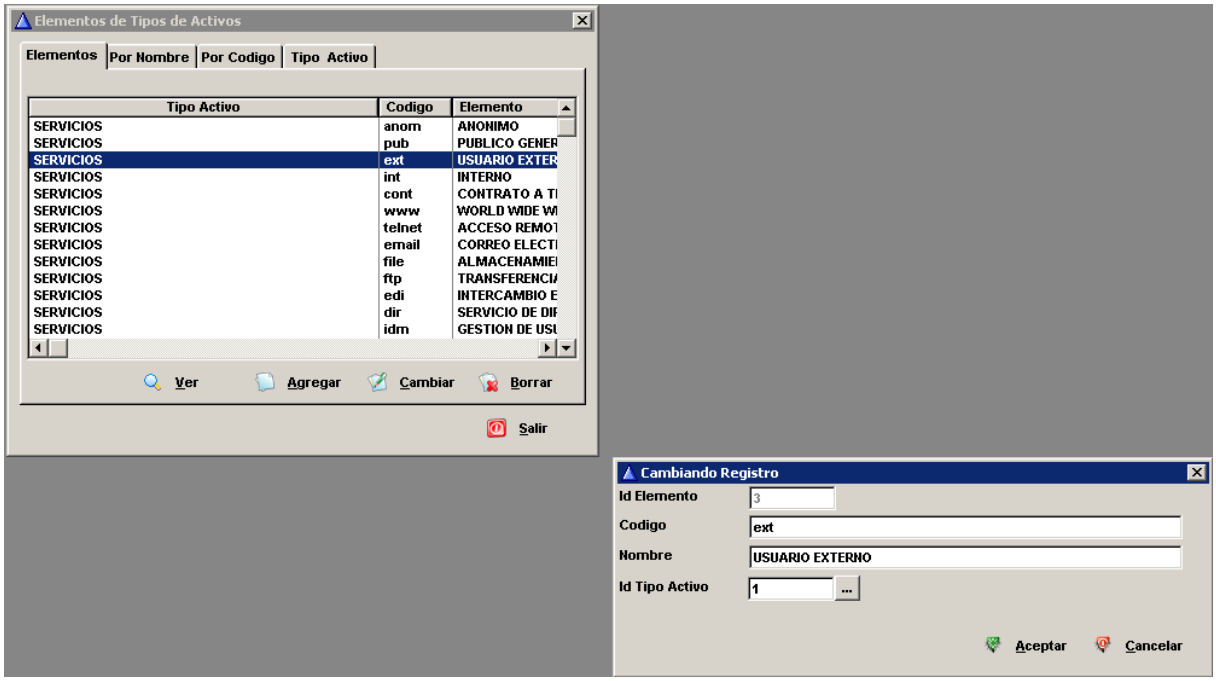


Figura 24 – Gestión de Elementos

Dimensión

Se cargaron las diferentes dimisiones que poseen los activos.

Para la carga inicial del sistema se tomo como base las dimensiones del Magerit V2, las cuales cuentan con el código propio de la dimensión, el nombre, una pregunta que se utiliza para aclarar la importancia del activo en la dimensión cargada y la descripción detalla de la dimensión (ver figura 25).

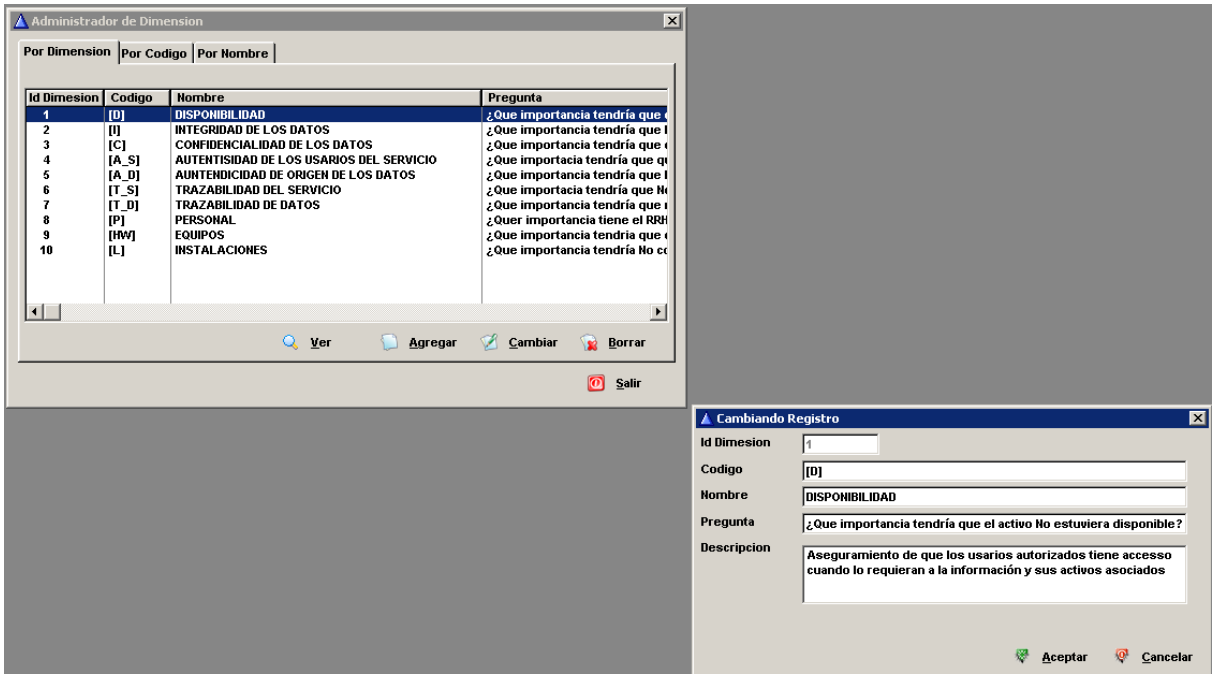


Figura 25 – Gestión de Dimensión

Valoración

Para la parametrización de la valoración del activo, se cargaron los valores representados en un cuadro de valoración, que se originó como resultante de una investigación con los usuarios de la organización.

En la figura 26 se puede apreciar la grilla de valoración y el formulario cargado por cada uno de los itmes.

En el campo valor, se cargó el número correspondiente, el cual está ubicado entre 0 y 10, se asignó además datos a los campos:

- Criterios: describe el tipo de daño que origina a la organización el mal funcionamiento del activo.
- Descripción: describe la valoración.

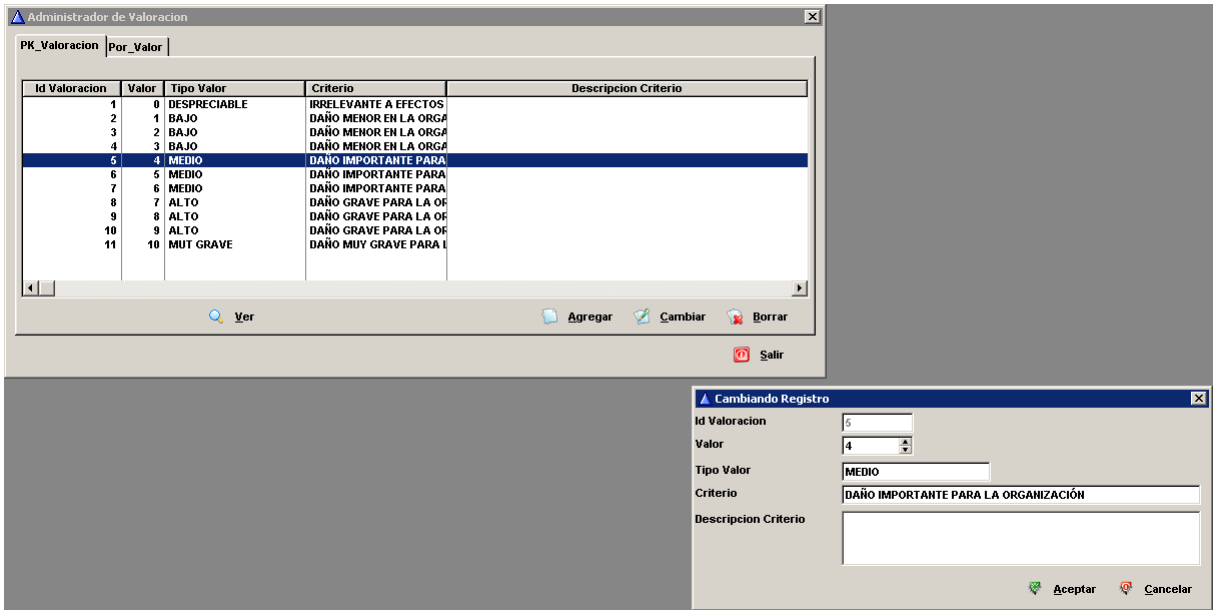


Figura 26 – Gestión de Valoración

Tipos de Amenazas

Se cargaron los tipos de amenazas en las cuales se agrupan.

Como muestra la figura 27, se incluyeron: el código interno, el cual se describe con una letra en mayúsculas, el nombre del tipo de amenaza y su descripción.

Para la carga inicial se introdujeron los tipos de amenazas sugeridos por Magerit V2.

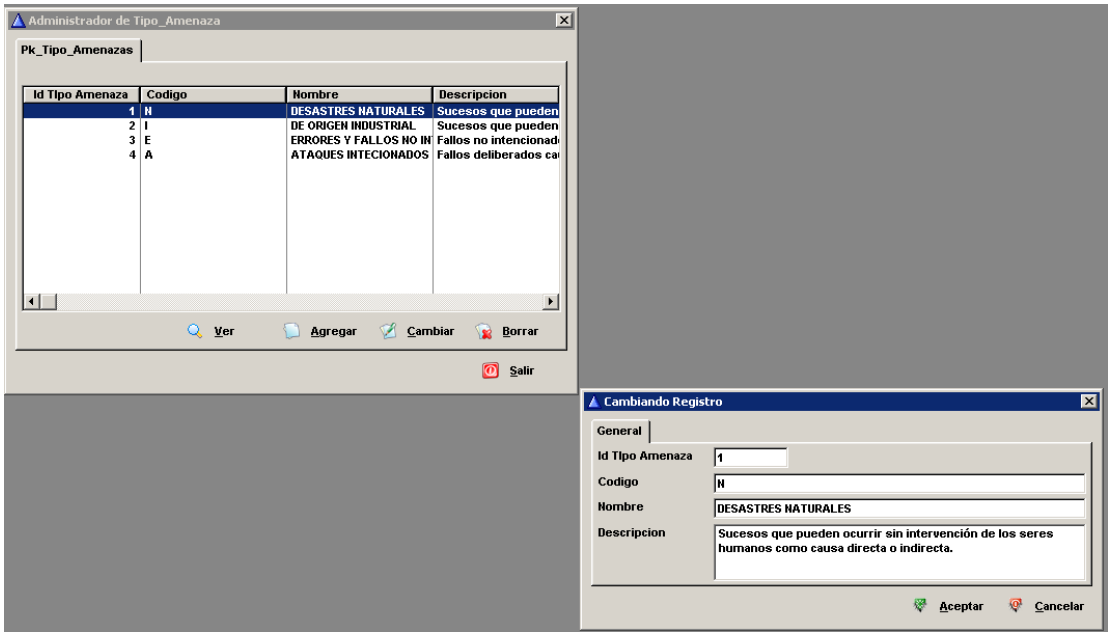


Figura 27 – Tipo de Amenazas

Amenazas

Se cargaron las 58 amenazas propuestas por Magerit V2, en las cuales se determinaron: el código interno, nombre de la amenaza, descripción detallada de la misma y el tipo de amenaza a la cual se agrupa (ver figura 28).

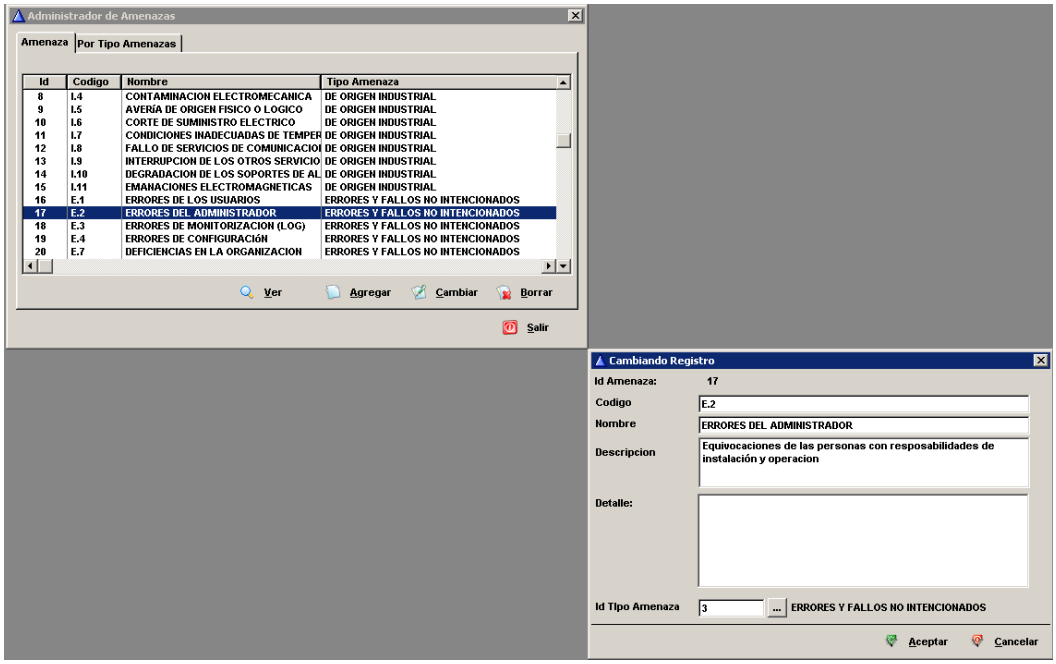


Figura 28 – Gestión de Amenazas

Amenazas por Tipo de Activo y dimensión

Una vez cargado el total de las amenazas y los tipos de activos, se parametrizó primeramente las amenazas que existían por tipos de activos como muestra la figura 29, y en segundo termino se asignaron dimensiones a las amenazas como muestra la figura 30.

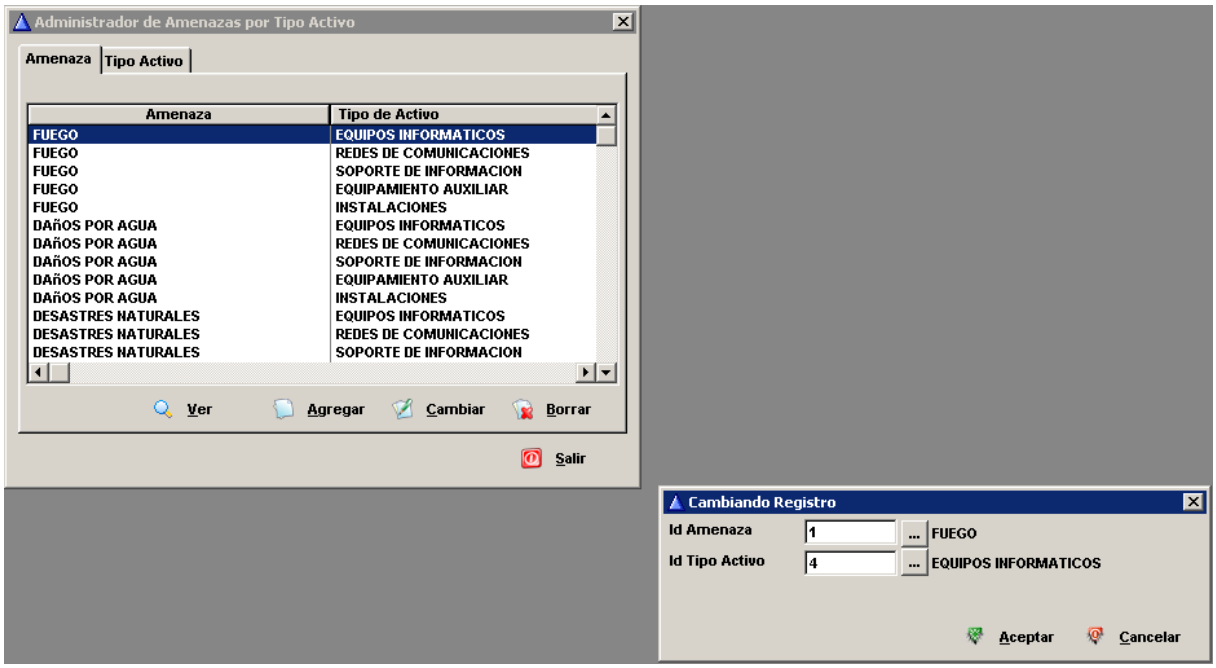


Figura 29– Amenazas por tipo de Activo

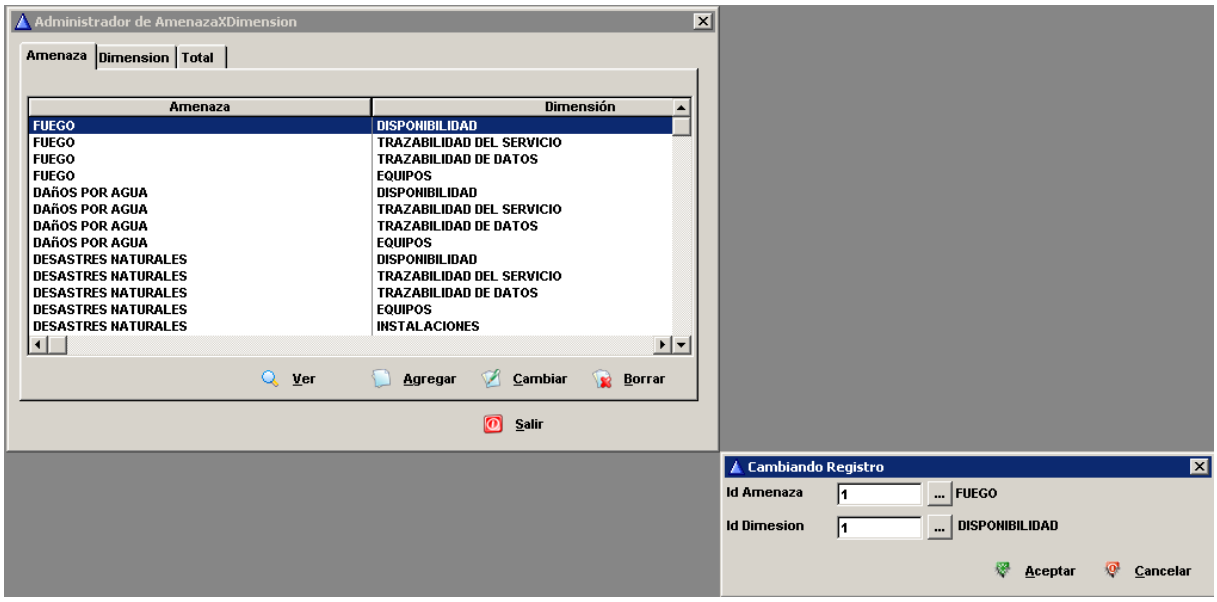


Figura 30 – Amenazas por Dimensión

Salvaguardas

Se cargaron las salvaguardas que serán utilizadas en el plan de acción en la fase I, como datos propios de la misma, se cargaron, la descripción, si posee control, si esto es afirmativo en que unidad de tiempo, si posee seguimiento y si es así, la unidad de tiempo del seguimiento, y una descripción detallada de la salvaguarda.

Las salvaguardas se tomaron de las sugeridas por Magerit V2 y se agregaron salvaguardas propias que surgieron como necesarias del estudio de caso (ver figura 31).

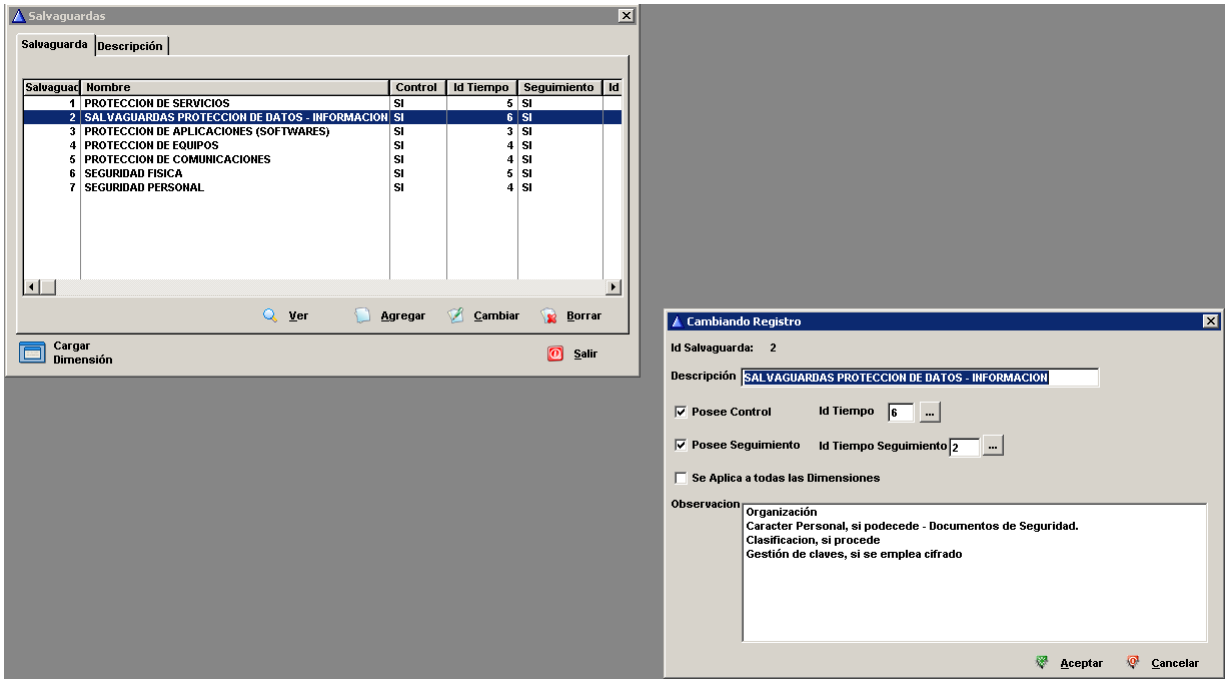


Figura 31 – Gestión de Salvaguardas

Una vez terminada la carga de las salvaguardas, se realizó la asignación de las dimensiones que posee cada una de las salvaguardas (ver figura 32).

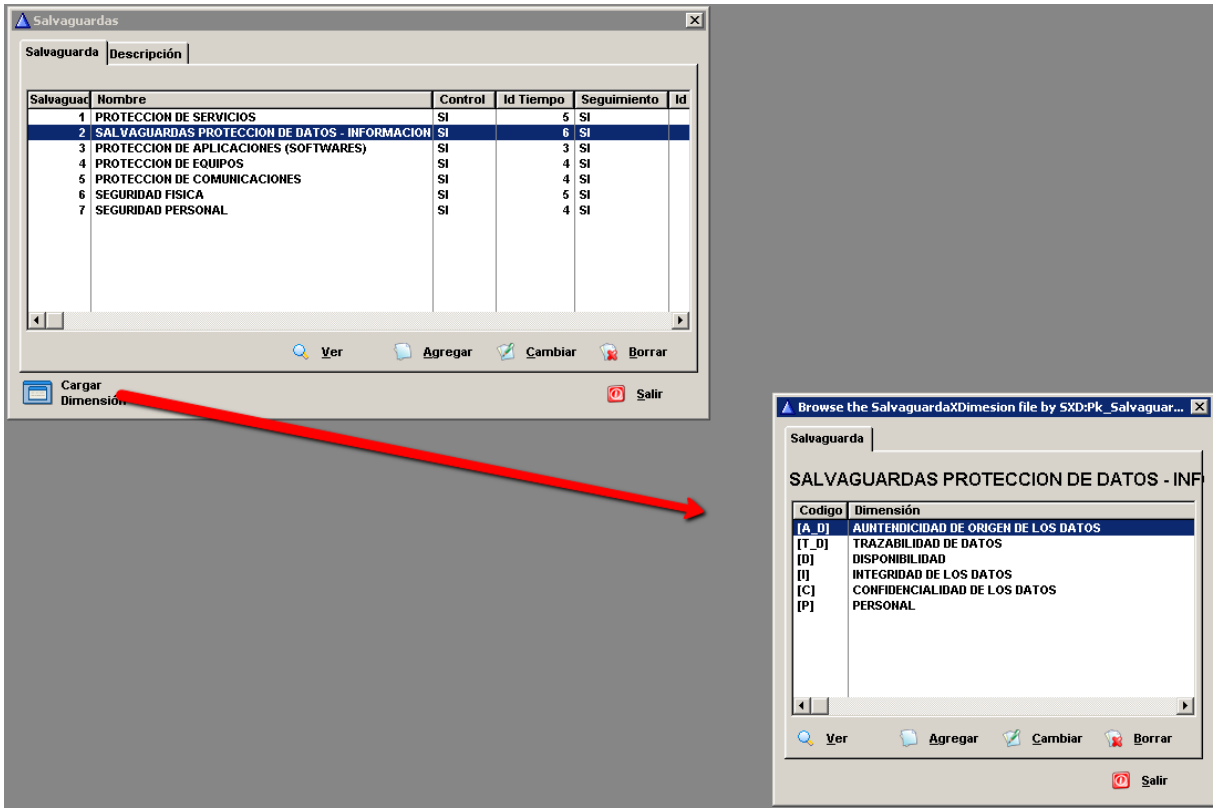


Figura 32 – Asignación de Dimensiones a la Salvaguarda

Catalogo de la Organización

Para logar adaptar el sistema a distintas organizaciones se generó el módulo de gestión de empresas, en la cual se cargaron los datos mínimos de la organización de prueba (ver figura 33).

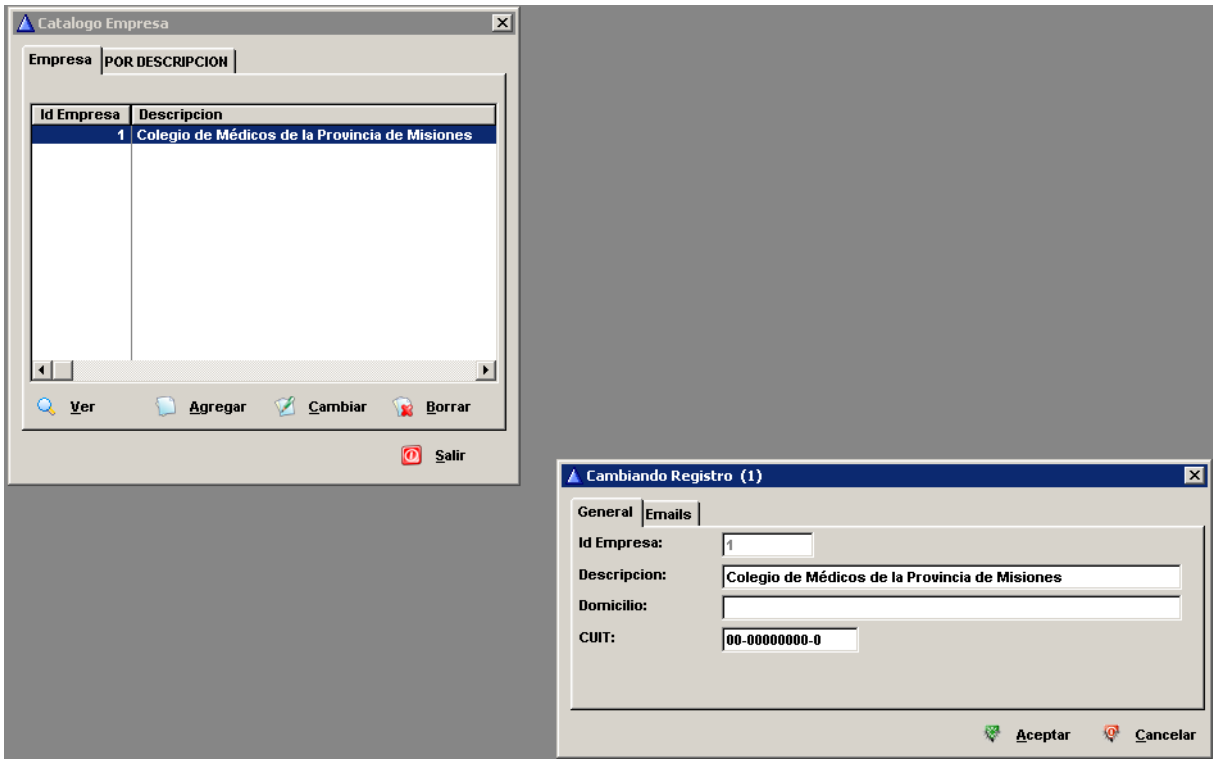


Figura 33 – Gestión de la Organización

Fuente de Información

Se relevaron las distintas áreas que utilizaban activos de IT, y los datos relevados fueron cargados al sistema en el módulo "Fuentes de información" (ver figura 34), en donde se le asignó un nombre al área o departamento investigado y una descripción de las tareas que realiza.

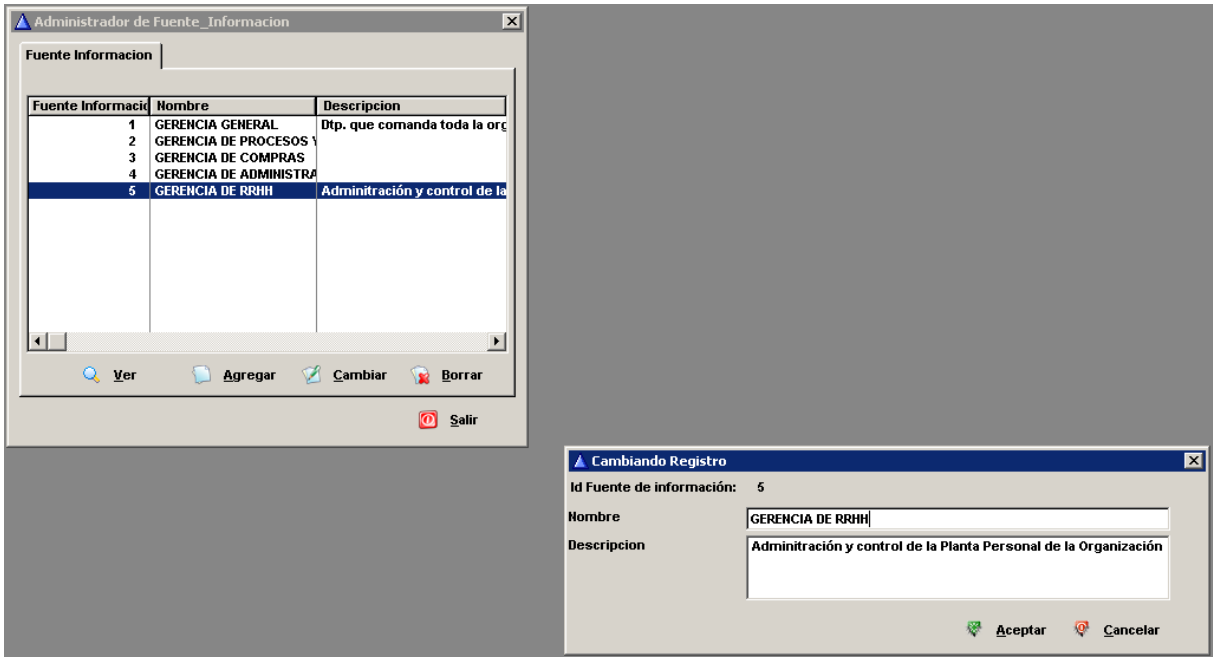


Figura 34 – **Gestión de fuentes de información**

Medidas de tiempo

Se parametrizaron las medidas de tiempo, las cuales van a ser utilizadas en el proceso de generación del seguimiento de los planes de acción. En estas se cargaron la descripción de la unidad de tiempo, la cantidad de ejecuciones por año y la distancia entre días de 24 Hs. (ver figura 35).

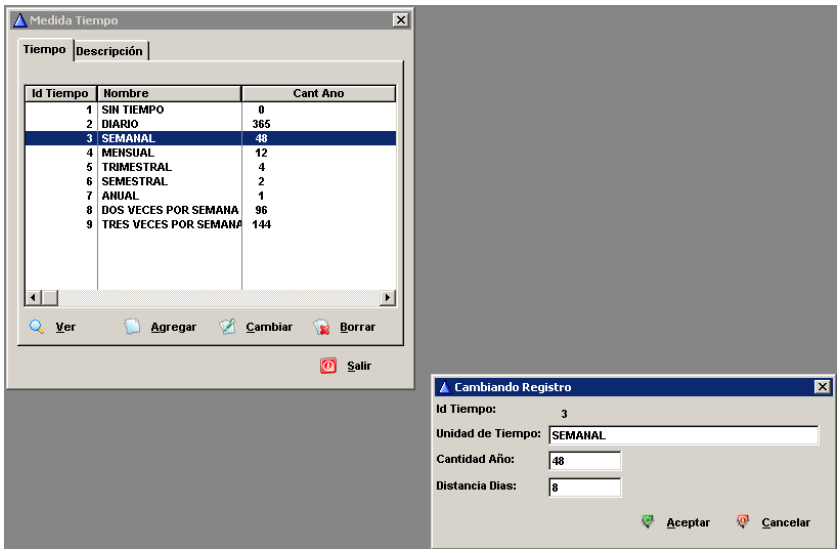


Figura 35 – **Gestión de medidas de tiempo**

Con todos los datos de parámetros principales cargados, se procedió a iniciar la fase I de AGR.

FASE I - Análisis y Gestión de Riesgos

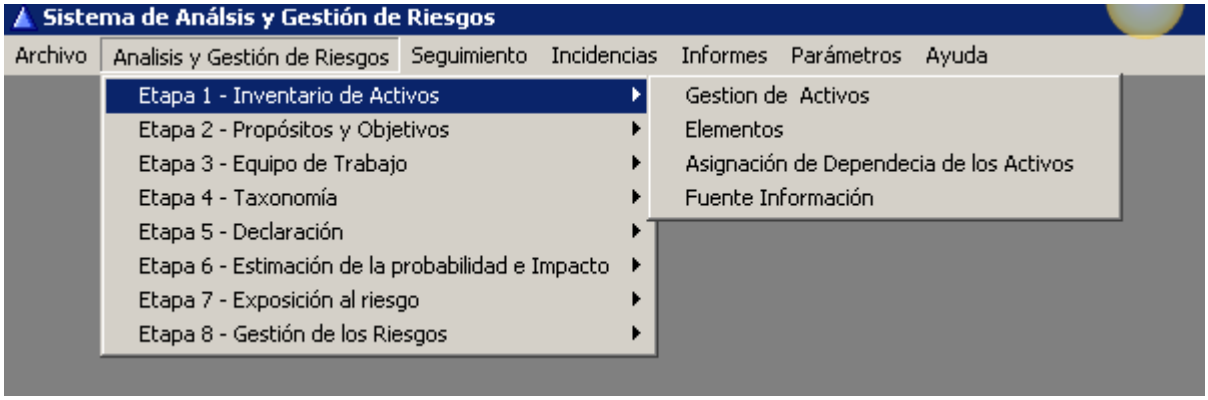


Figura 36 – Menú Etapa 1

Etapa I – Inventario de Activos

Gestión de Activos

Para comenzar con el análisis del riesgo, como primer paso, se relevó todos los activos correspondientes al IT que poseía la organización, y se cargaron al sistema como muestra la figura 37. El catálogo de activos esta compuesto por: el código del activo, proporcionado por el número de inventario que posee la organización, el nombre, la descripción, el contenido, el propietario (área la cual utiliza el activo), y la importancia que posee el activo para la organización.

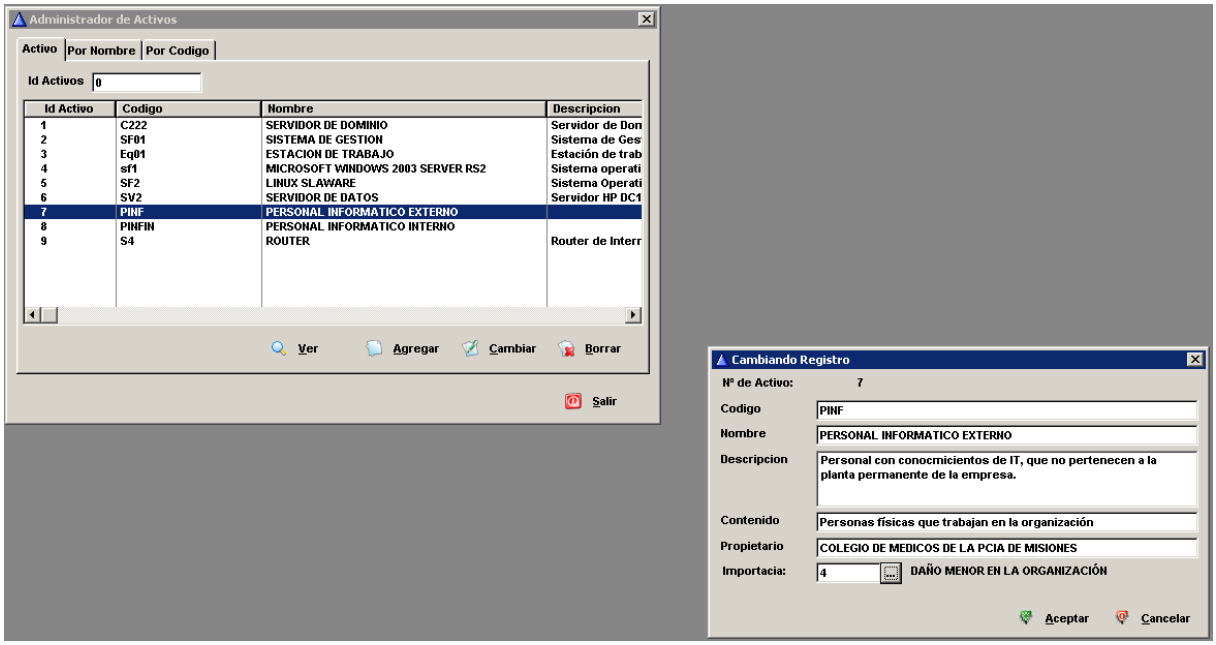


Figura 37 – Gestión de Activos

Elementos por Activo

Se asignó por cada activo, los elementos basados en el tipo de activo. El sistema, mediante el activo seleccionado, filtra de que tipo/s es, y una vez seleccionado el tipo, muestra únicamente los elementos asignado a ese tipo de activos para su elección (ver figura 38).

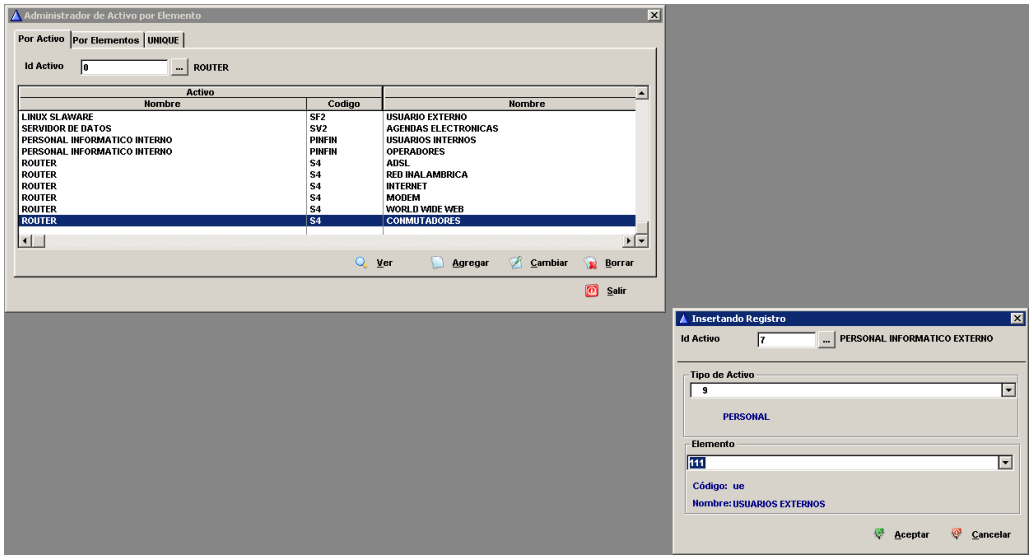


Figura 38 – Asignación de elementos a un activo

Asignación de dependencia

Se asignaron los activos de bajo nivel a los de alto nivel. Como la organización no posee muchos activos de alto nivel, está practica no tuvo mayores inconvenientes (ver figura 39).

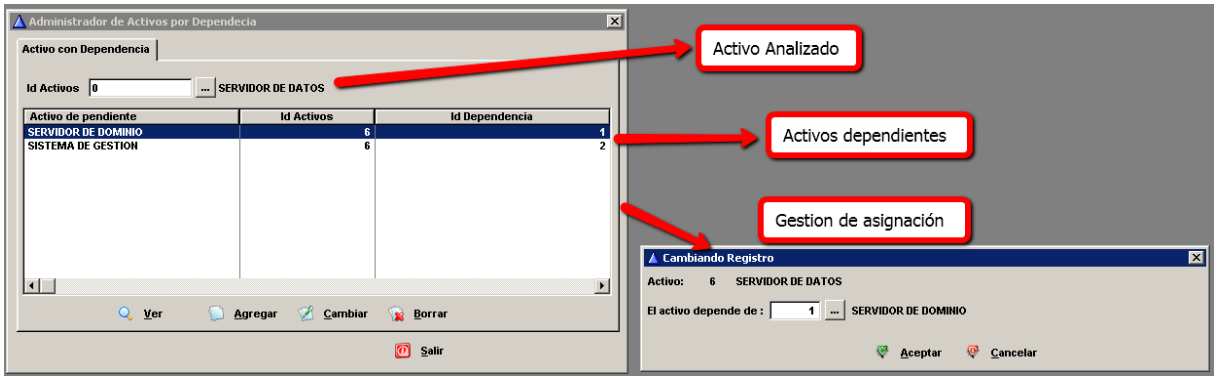


Figura 39 – Dependencia de activos

Fuentes de Información por Activo

A cada activo relevado se le asignó la fuente de información, como se definió anteriormente, es el departamento o área de donde se obtuvo información sobre el activo (ver figura 40).

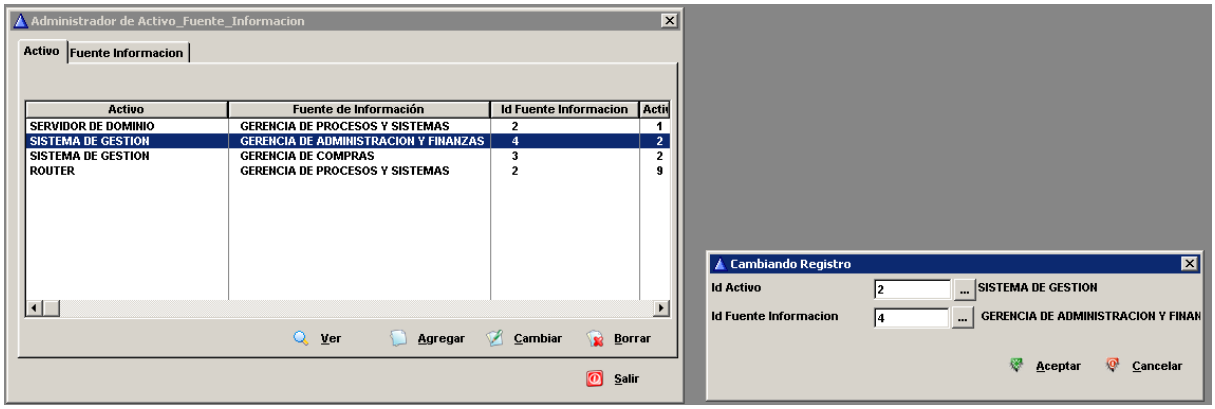


Figura 40 – Asignación de fuente de información

Etapa II - Gestión de propósitos y Objetivos

Gestión del proyecto

Se cargaron tres proyectos de análisis y gestión de riesgos: sala de servidores, departamento de informática y personal, los dos primeros fueron casos de prueba, en donde el sistema se realizaron ajustes en programación al sistema y el tercero es el estudio de caso de este trabajo con una revisión estable del software.

Como muestra la figura 41 los datos propios del proyecto son: el Propietario, en donde se describe le propietario de la organización o el propietario del proyecto, ya que el mismo puede ser realizado por empresas de terceros, el código del proyecto es una notación interna de la organización, el nombre y la descripción del proyecto.

Una vez terminado el proyecto se debe asignar la variable "SI" a la opción terminado. Asignando esta variable el proyecto finaliza y no se pueden asignar más riesgos.

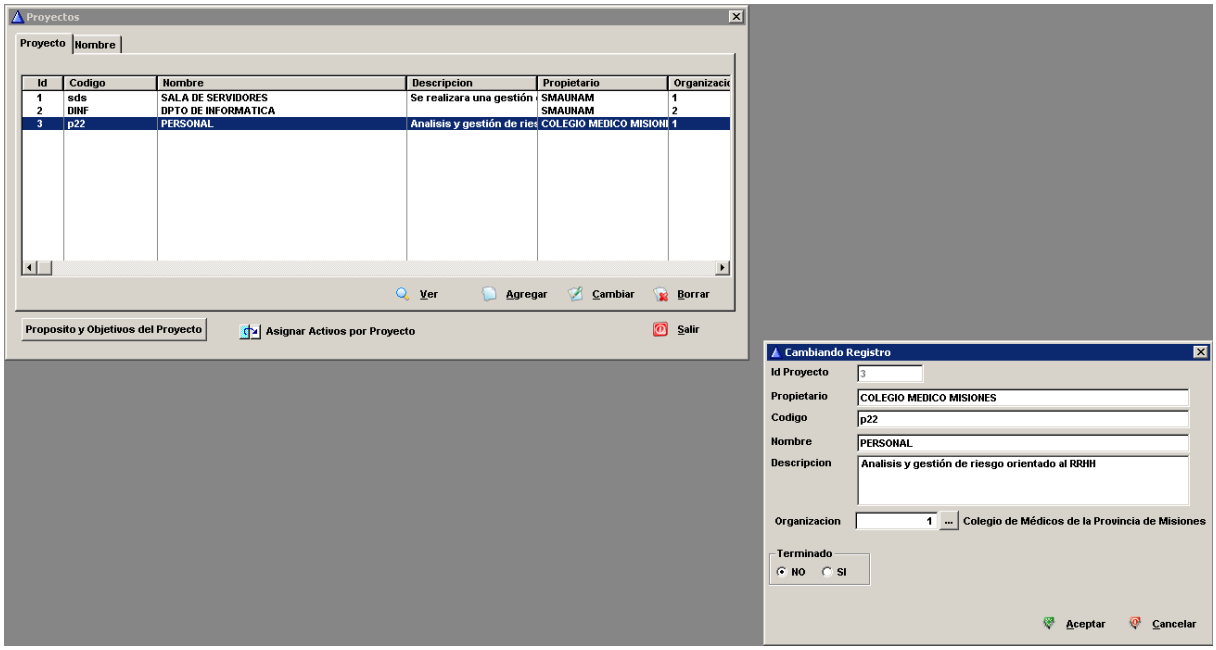


Figura 41 – Gestión de proyectos

Una vez cargado el proyecto se debe asignar los límites, propósitos y objetivos del proyecto. El sistema brinda la posibilidad de múltiples propósitos por cada proyecto como muestra la figura 42.

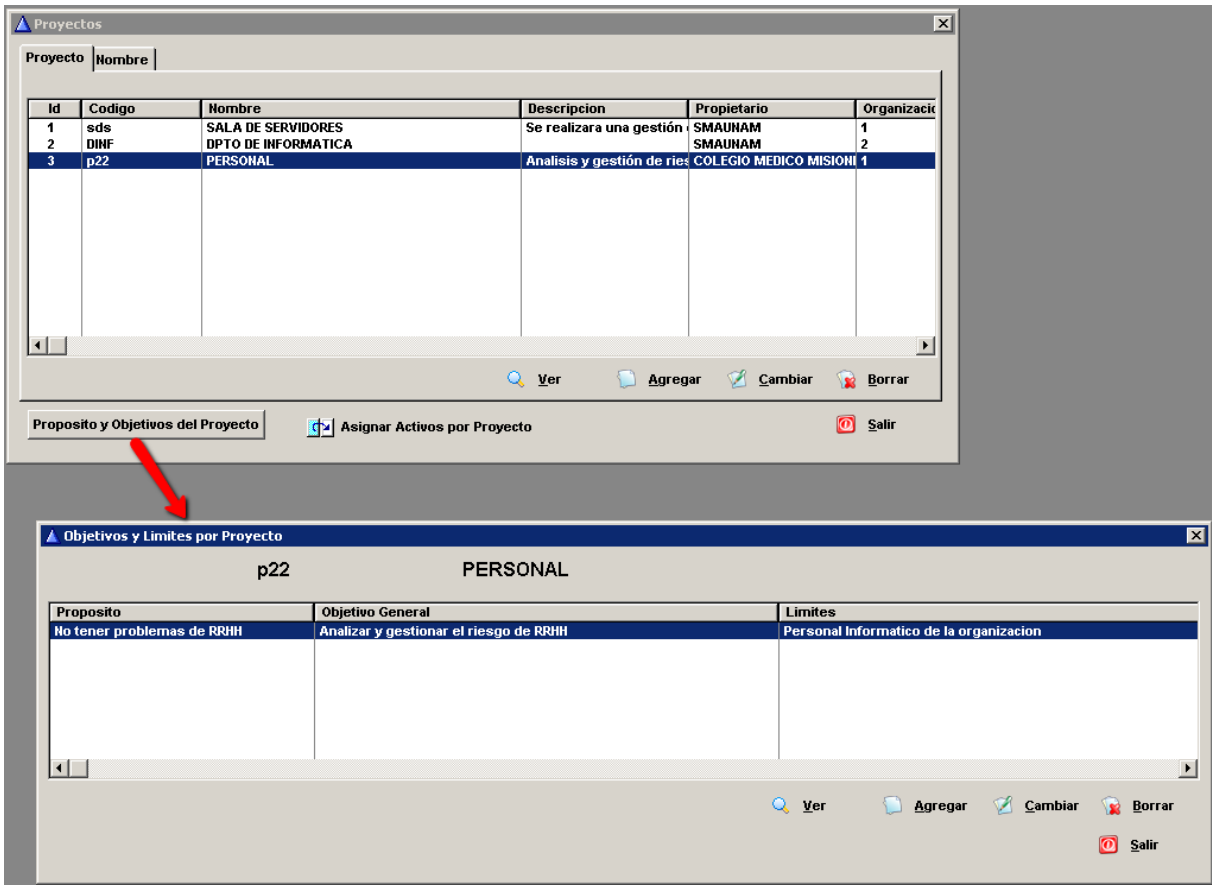


Figura 42 – Asignación de propósitos y objetivos al proyecto

También se asignó activos al proyecto como muestra la figura 43.

En el estudio de caso, al proyecto "personal" se le asignaron dos activos, personal informático externo y personal informático interno.

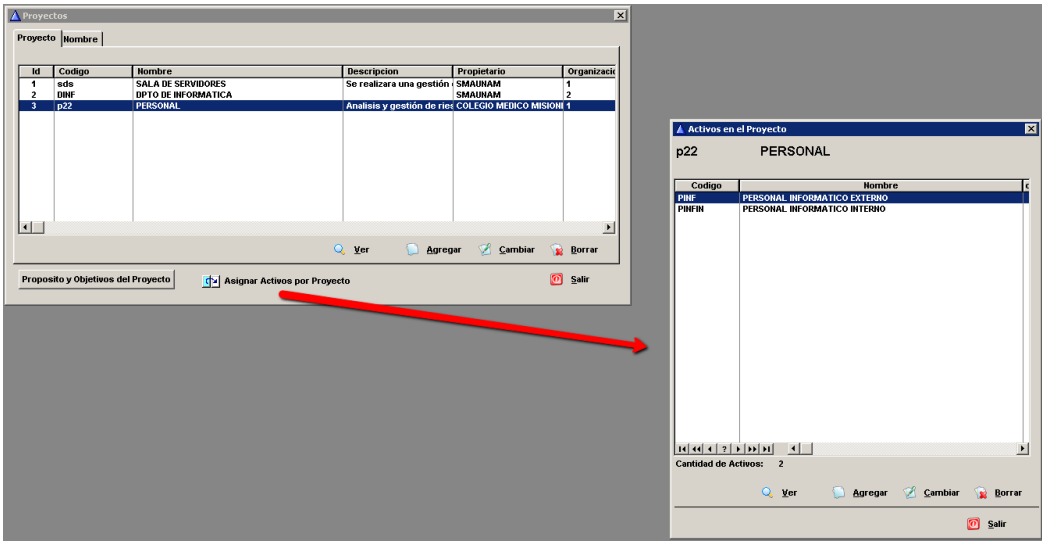


Figura 43 – Asignación de personal al proyecto

Etapa III – Equipo de Trabajo

Gestión de Equipos

En esta etapa se designó el equipo de trabajo para el proyecto "personal", para lo cual primeramente, se tuvo que gestionar los distintos roles a utilizar en el proyecto, los equipos y las personas. Una vez gestionados estos parámetros, se asignó las personas al proyecto, como muestra la figura 44. Por cada persona asignada se debió parametrizar de que equipo perteneces y que rol cumple en el proyecto.

La flexibilidad del sistema permite asignar la misma personas con distintos roles y equipos dentro del proyecto, como es la realidad de una organización pequeña.

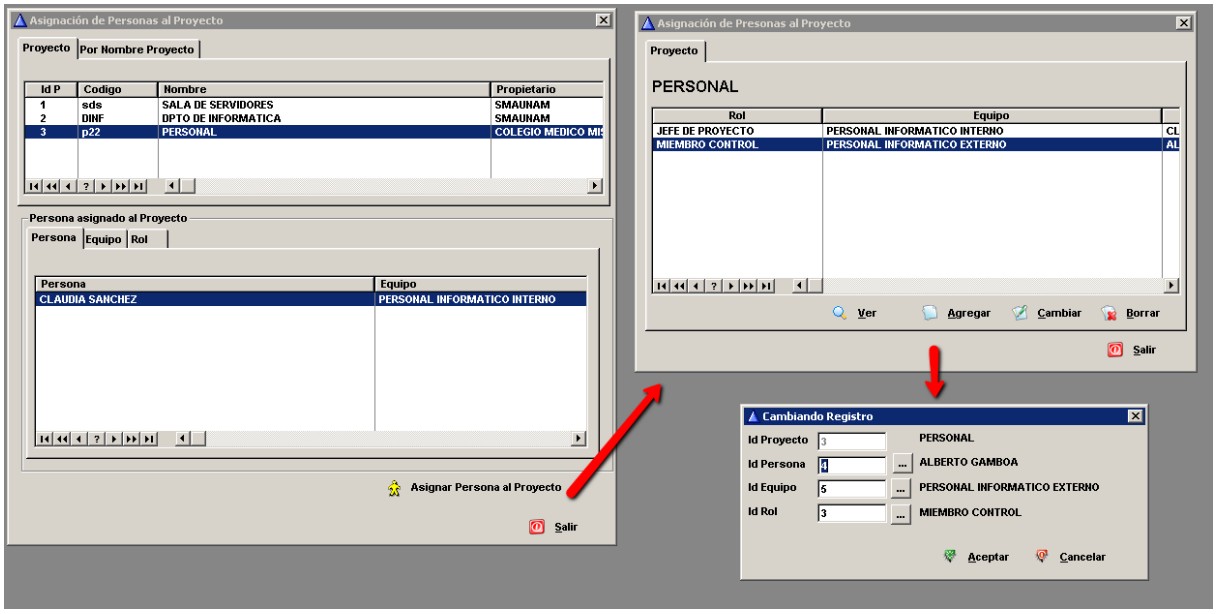


Figura 44 – Gestión de equipos

Etapa IV – Taxonomías

Amenazas por Tipo de Activo

En esta etapa, el sistema procesa todas las amenazas cargadas en el módulo de parámetros que poseen los activos asignados al proyecto. Por lo que, primeramente el sistema solicita la identificación del proyecto a procesar (ver figura 45) y luego procesa lo antes explicado.

Una vez terminado el proceso, el sistema muestra en pantalla, una grilla con el resultado del proceso, en donde por cada riesgo se debe asignar el elemento taxonómico y la fuente de información , como muestra la figura 46.

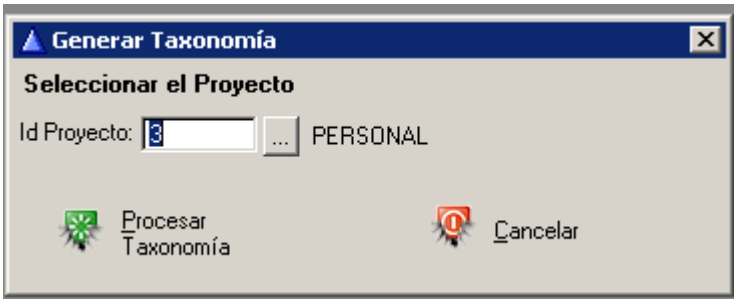


Figura 45 – Selección de proyecto para generar la taxonomía

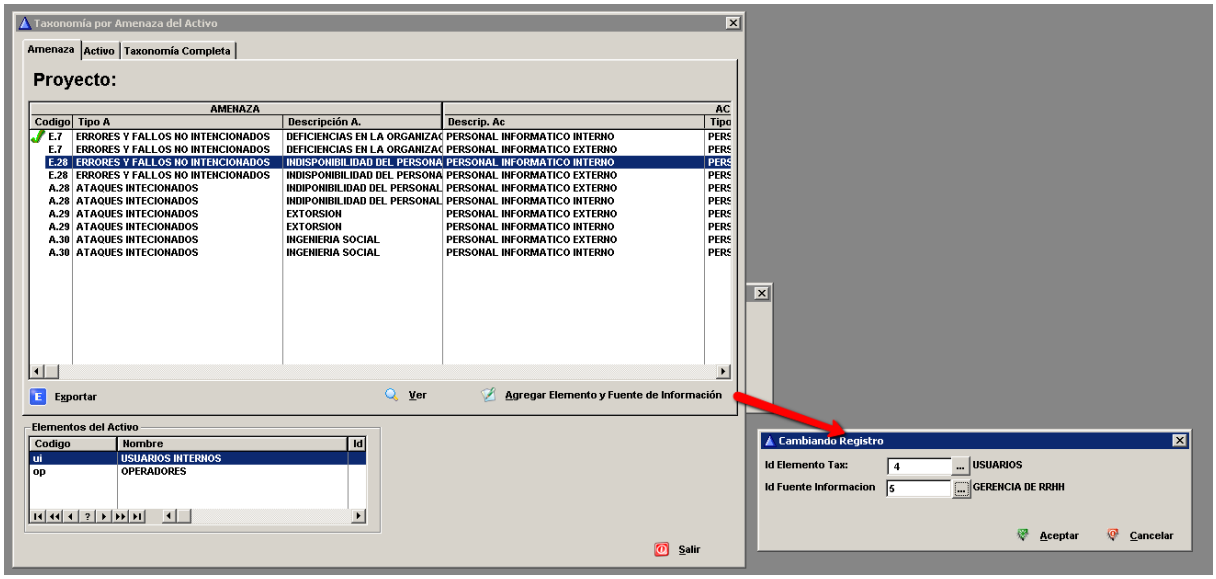


Figura 46- Gestión de elementos y fuentes de información

Una vez que se asignaron los datos necesarios, el sistema muestra el símbolo √, que identifica los riesgos a los que se les asignaron los datos anteriores, y que son los únicos que puede pasar e la etapa siguiente. Los riesgos que no estén finalizados, no son tomados en cuenta por la etapa V.

Etapa V – Declaración

Gestión Declaración

En esta etapa, se asigna la declaración del riesgo. El módulo muestra por proyecto seleccionado, únicamente los riesgos "completos" de la etapa anterior.

Por cada riesgo se asignó las variables de consecuencia y efecto.

La variable declaración, es automáticamente asignada por el sistema, ya que es una condición de la amenaza. Esta característica da agilidad a la carga del sistema, brindando la automatización de muchas de las variables y además, posibilitando al operador modificar los valores por defecto, como muestra la figura 47.

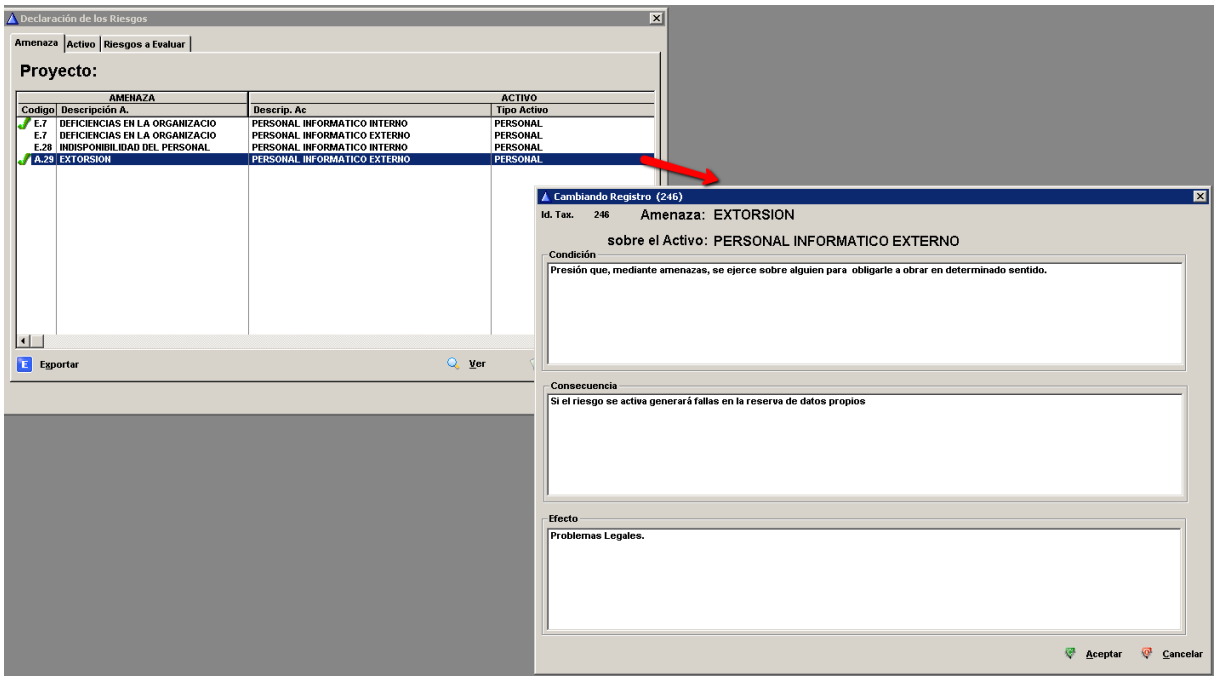


Figura 47 – Gestión de declaración

Igual que la etapa anterior, el sistema incluye el símbolo √ una vez completado los datos necesarios por riesgos, y que estos son los únicos que se tomarán en cuenta en la próxima etapa.

Etapa VI – Estimación de probabilidad – Impacto

Probabilidad de ocurrencia por proyecto

Se generó para este proyecto una tabla especial en donde se clasifican los niveles de probabilidad de ocurrencia de un problema. Los elementos para realizar la clasificación cargada son: el porcentaje mínimo y máximo de ocurrencia, el porcentaje medio de ambos, la descripción de la exposición y el valor nominal de estos, como muestra la figura 48.

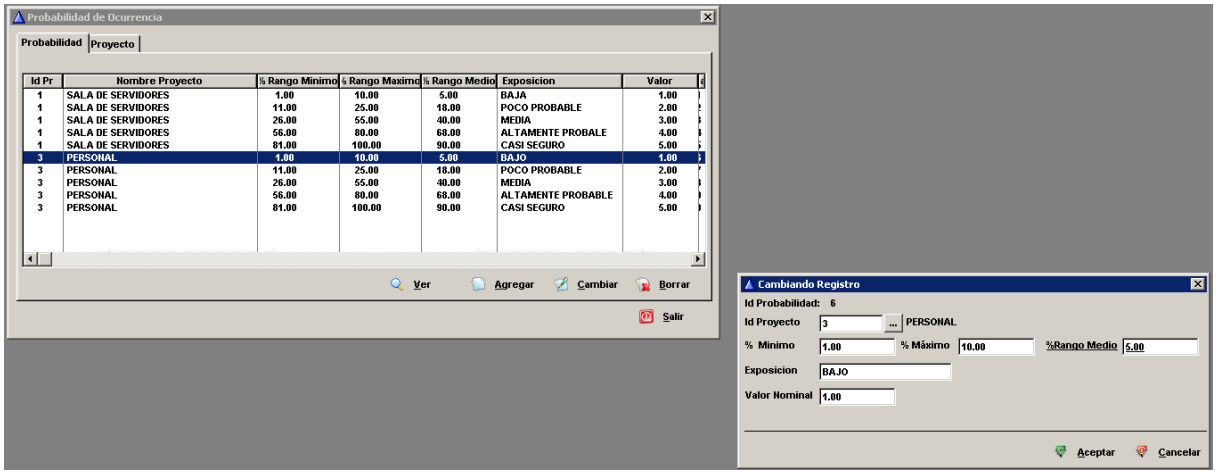


Figura 48 – Tabla de probabilidad de ocurrencia por riesgo

Impacto de ocurrencia por proyecto

Al igual que con la probabilidad, se generó una tabla con los valores de impacto que causará el activo cuando un riesgo asociado se transforme en un problema.

Como muestra la figura 49, el sistema maneja múltiples tablas (se debe asignar una tabla para cada proyecto), y por cada atributo se asigna: el criterio, que es

la descripción en lenguaje natural del impacto, el retraso, que es el tiempo en que retrasará el trabajo y el valor nominal del mismo.

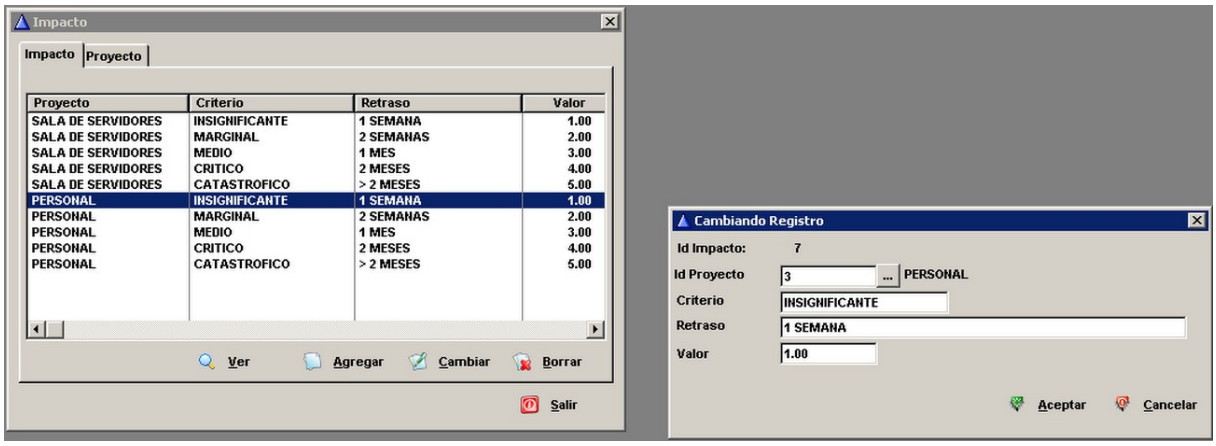


Figura 49 – Impacto de ocurrencia por proyecto

Estimación de probabilidad e impacto

Siguiendo con el estudio de caso, por cada riesgo finalizado en la etapa anterior, el sistema muestra una grilla, en donde se asignaron por cada uno de los riesgos, el porcentaje de probabilidad de ocurrencia y el impacto generado si el riesgo se transforma en un problema.

Automáticamente el sistema procesa esas dos variables y marca con un "*" los riesgos que posee exposición (ver figura 50).

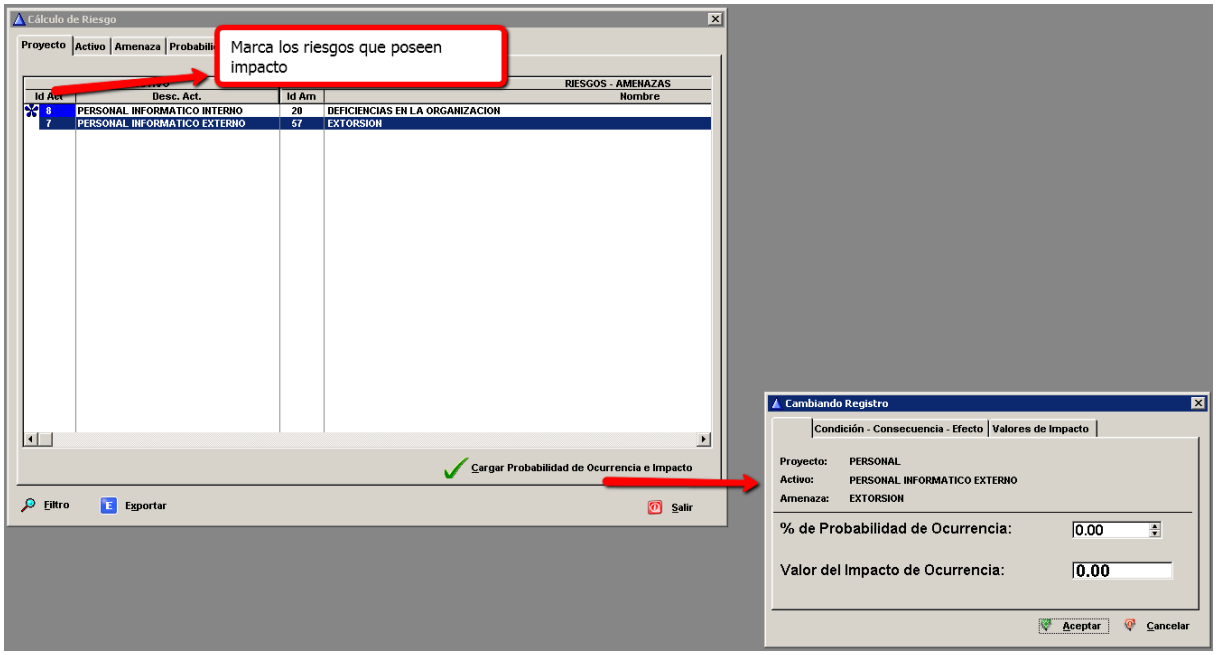


Figura 50 – **Asignación de probabilidad e impacto**

Etapa VII – Exposición al riesgo

Exposición

En esta etapa, el sistema muestra la exposición que poseen aquellos riesgos procesados en la etapa anterior. Se pueden exportar los datos identificados como se divisa en la figura 51.

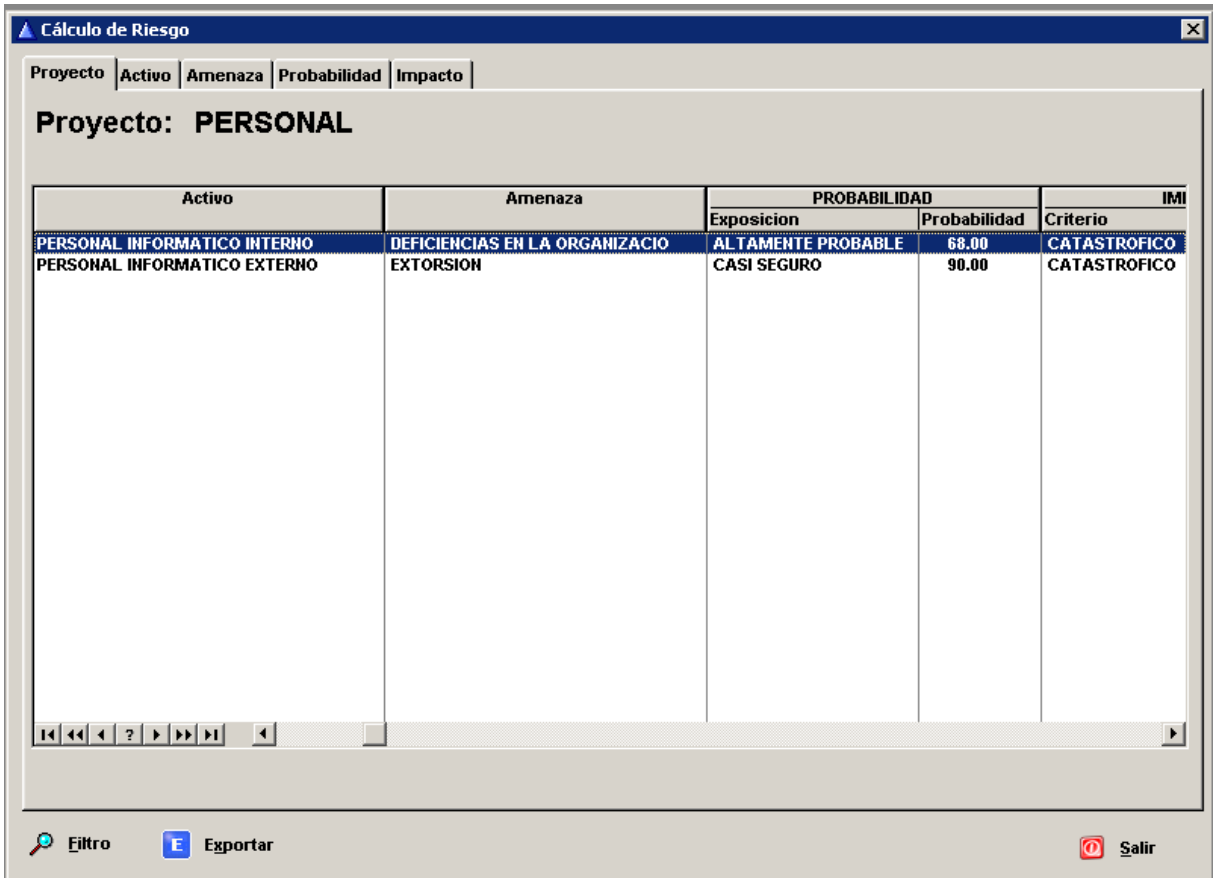


Figura 51 – **Exposición al riesgo**

Etapa VIII – Gestión de los riesgos

Información

En este módulo se cargaron las fuentes de información que se utilizaron en la gestión de riesgos (ver figura 52).

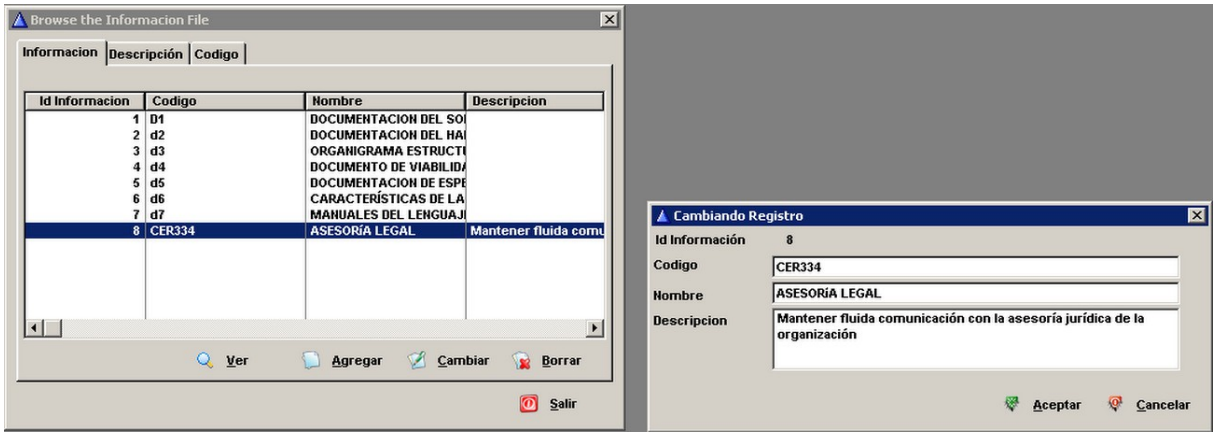


Figura 52 – Información de riesgos

Recursos

Gestiona los recursos necesarios para tratar los riesgos, estos recursos pueden ser asignados a distintos proyectos del sistema (ver figura 53).

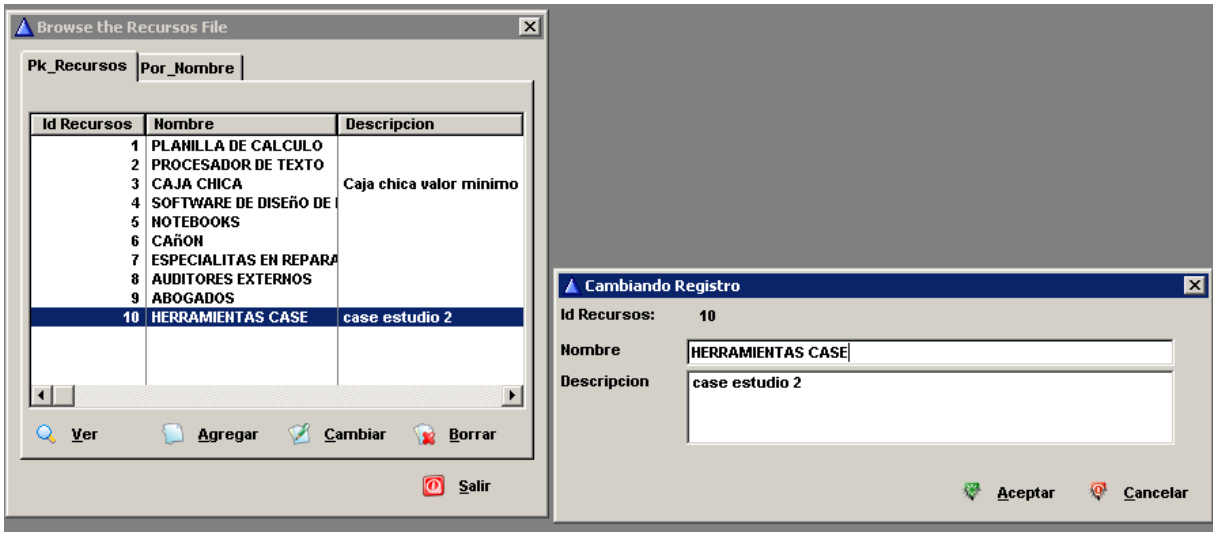


Figura 53 – Recursos

Gestión

Este es el módulo mas importante de las etapas de la fase I, debido que en el, se parametrizan los riesgos expuestos en el proyecto.

El sistema una vez seleccionado el proyecto, muestra una grilla en donde se exponen los riesgos expuestos. Y estos son los que se deben gestionar.
El trabajo realizado en este estudio de caso fue el siguiente:

1. Para ahorrar tiempo de trabajo se generaron automáticamente los planes de acción, como muestra la figura 54. Además de la generación automática, se le agregó al riesgo "problemas legales" una salvaguarda propia del proyecto.

2. Se parametrizaron manualmente el plan de contingencia por cada uno de los riesgos expuestos, asignando las siguiente variables (ver figura 55):
    a. Disparador: es la acción o reacción por la cual es riesgo se transforma en el problema.
    b. Responsable: es el miembro del proyecto que se responsabiliza por el riesgo.
    c. Pasos a seguir: es un manual secuencial de pasos, para lograr controlar el riesgo.
3. Se asignó la información necesaria para el control y seguimiento del riesgo (ver figura 56).

4. Se estableció el/los responsables del control y seguimiento del riesgo, y los encargados de solucionar el problema si este ocurriera (ver figura 57).

5. Se cargaron los recursos necesarios para la gestión del riesgo (ver figura 58).

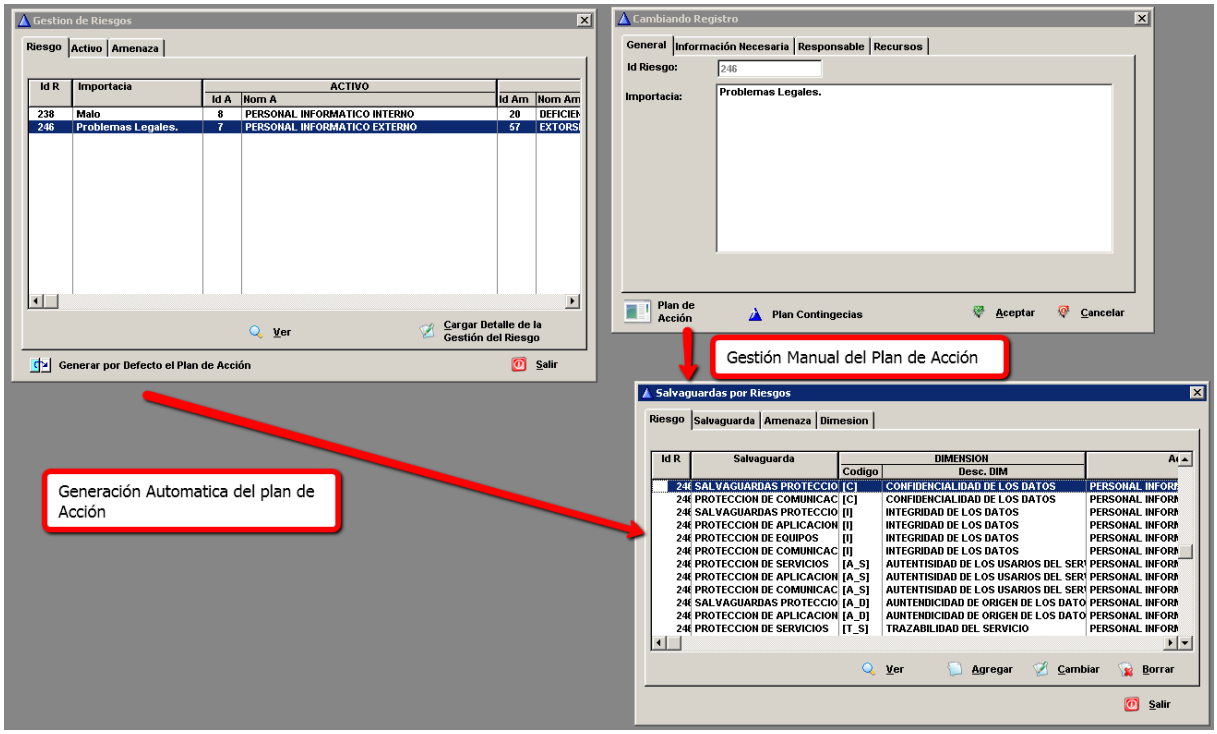


Figura 54 – Asignación de plan de acción

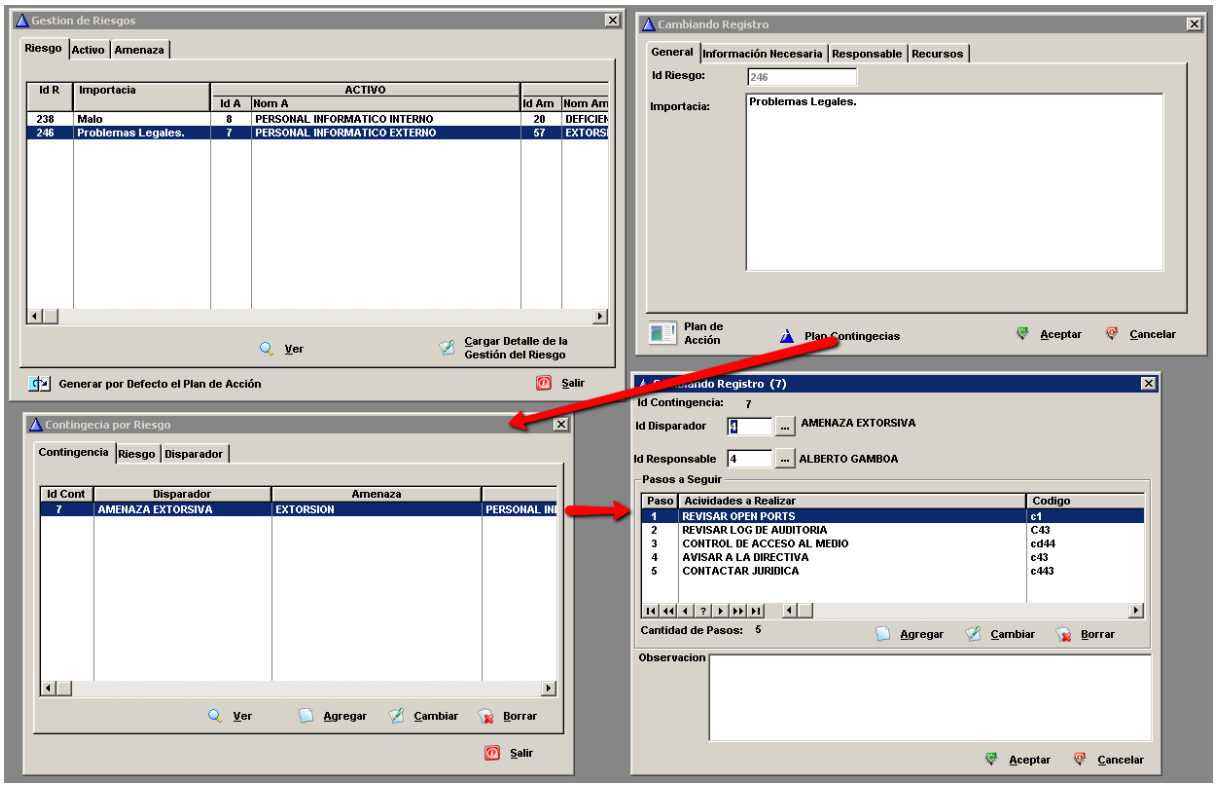


Figura 55 – Plan de contingencia

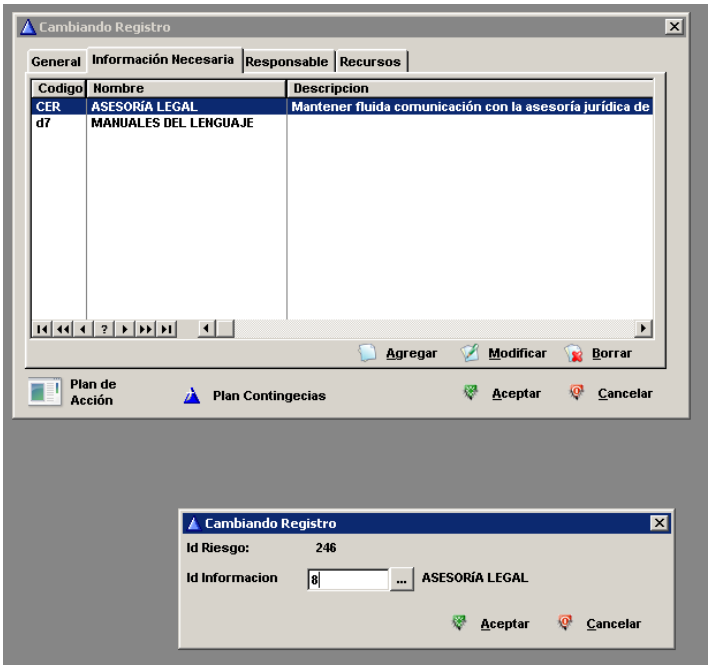


Figura 56 - Información necesaria

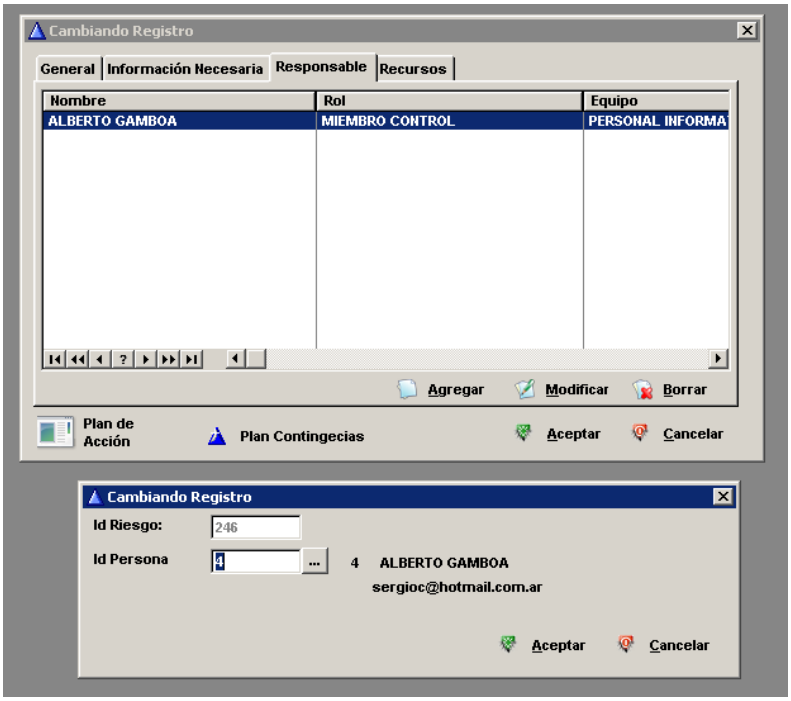


Figura 57 - Responsable

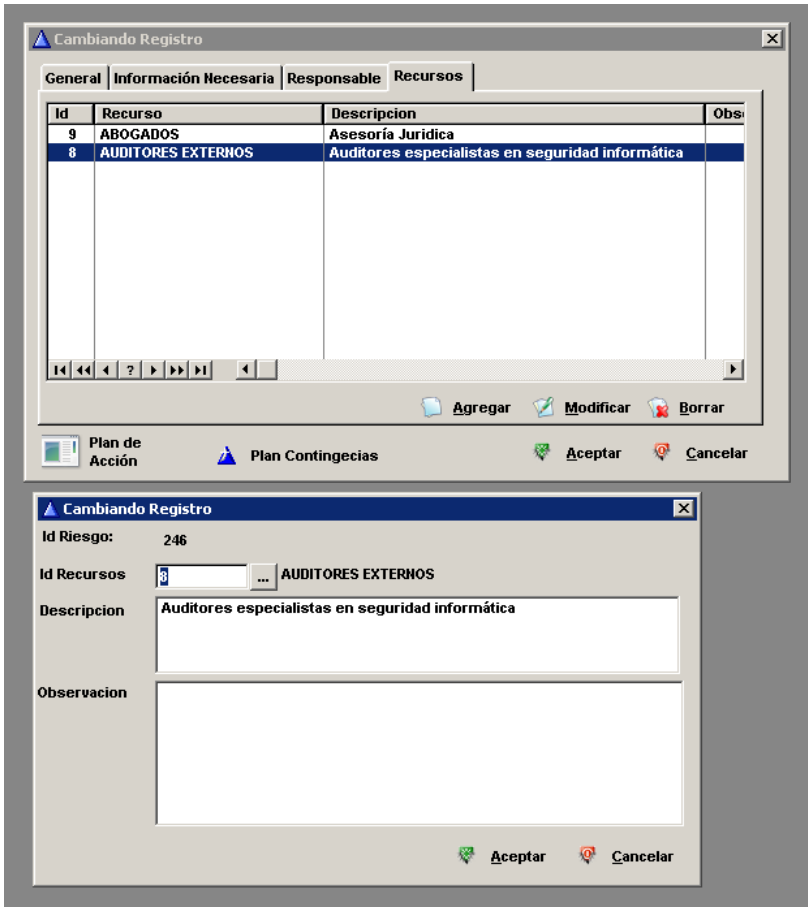


Figura 58 – **Recursos**

FASE II - Seguimiento

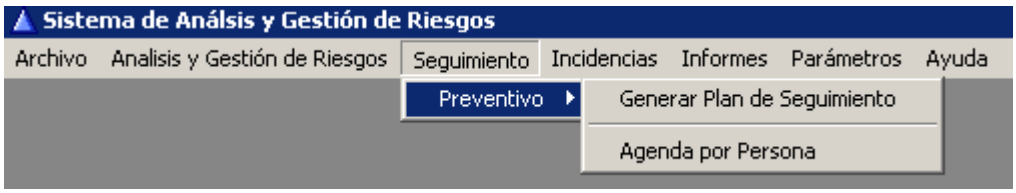


Figura 59 – **Menú Seguimiento**

Plan de Seguimiento

El sistema genera automáticamente el plan de seguimiento para proyecto. Este módulo puede actualizar el plan de seguimiento sin inconvenientes cuando en el proyecto se añaden nuevos riesgos. Figura 60

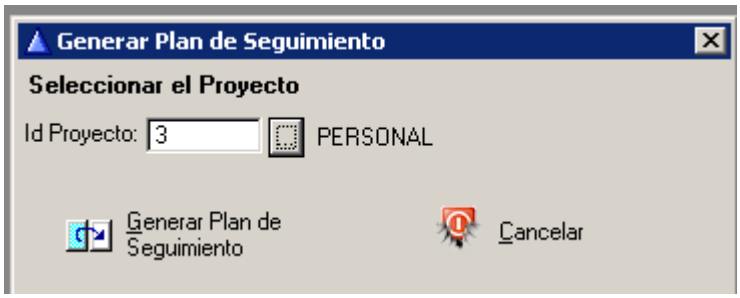


Figura 60 – **Plan de seguimiento**

Agenda por Persona

La agenda por persona es el módulo en donde se muestran las actividades de seguimiento y control por cada persona asignada al proyecto.

El primer paso es identificar a la persona, como muestra la figura 61.

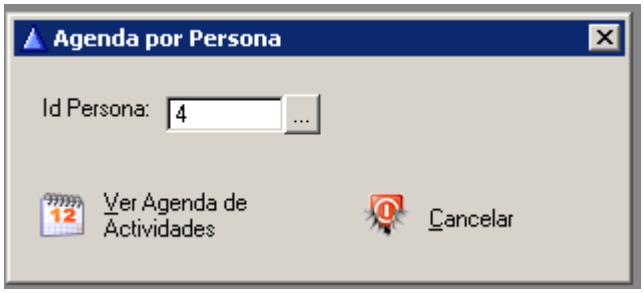


Figura 61 – **Agenda de actividades**

Una vez identificada la persona en el proyecto indicado, el sistema muestra el panel de control del seguimiento (ver figura 62).

Este panel expone las actividades que se encuentran en ejecución o por realizar, esta característica se puede apreciar en la columna % Realizado.

Si para la fecha actual no se han realizado actividades planificadas para días anteriores, el sistema muestra la actividad marcada con un icono de color rojo.

Una vez que se haya controlado la actividad, se debe cargar el porcentaje de finalización, una observación acerca de la actividad.

Si el porcentaje de finalización es del 100 % el sistema habilita la opción "termino bien", en el cual se marcará si la actividad de control no tuvo inconvenientes.

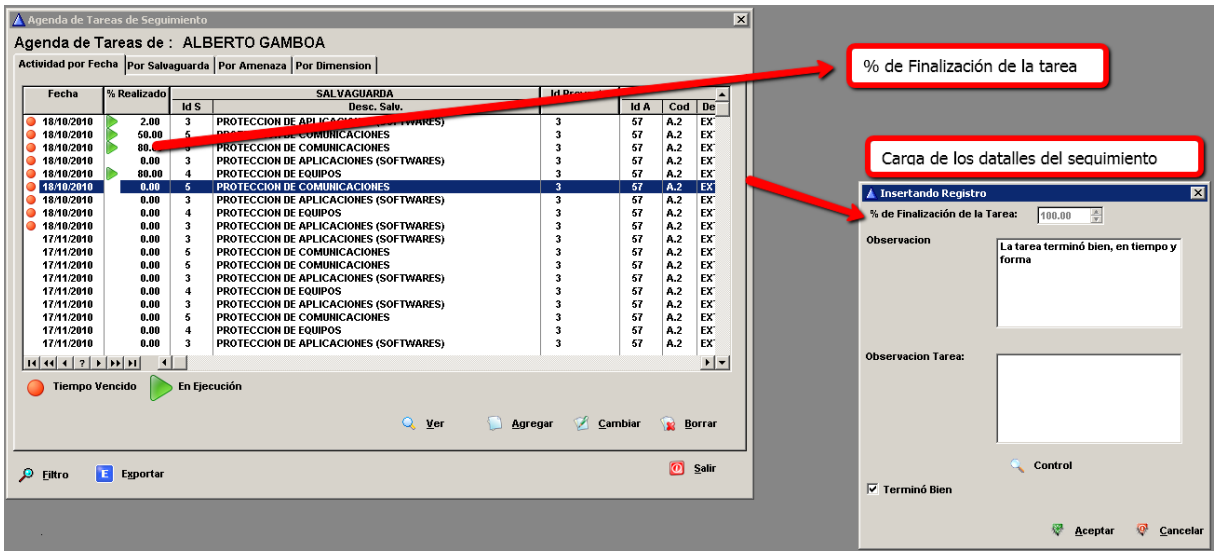


Figura 62 – Gestión de control de Seguimiento

En este estudio de caso se probó el seguimiento, modificando la fecha del sistema para corroborar los controles de atraso, y se cargaron varias actividades con distintos porcentajes de avances.

FASE III - Incidencias

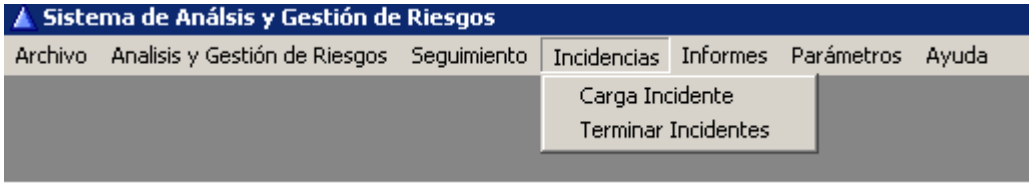


Figura 63 – Menú de seguimiento

Carga Incidente

Esté módulo se encarga de gestionar los incidentes ocurridos con un activo.

En este estudio de caso, simulamos el siguiente incidente:

- El profesional encargado del mantenimiento de la base de datos de la organización encuentra en su dispositivo móvil un mensaje de texto que le solicitaba cierto tipo de información de la base de datos.
- El profesional dio aviso a los gerentes de la empresa y se cargó al sistema el incidente para ver como se comportaba.

En la figura 64 se muestra la carga de este incidente. Primeramente se asigna el activo correspondiente, que en este caso es "personal informático externo", la amenaza "extorsión", el responsable de control del incidente, la fecha y hora de lo ocurrido y una acción inmediata.

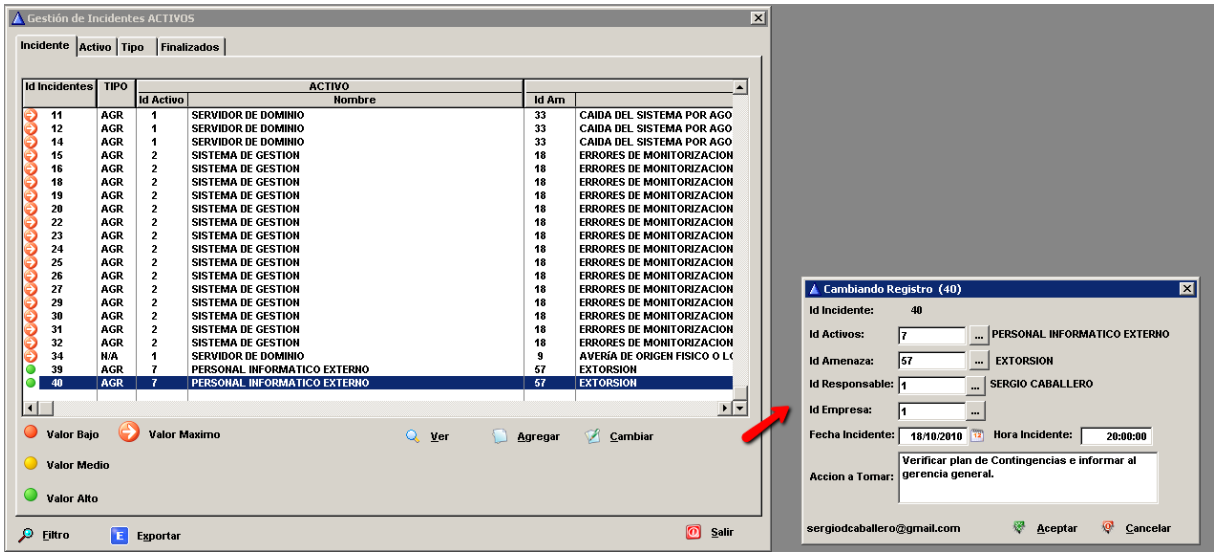


Figura 64 – Carga de incidente

Una vez aceptada la carga, el sistema procesa automáticamente los siguientes puntos.

Punto 1 – Verifica y expone en una pantalla de aviso, si el activo cargado posee análisis y gestión de riesgos (si el riesgo fue expuesto y gestionado), o solo el análisis (si el activo no fue expuesto) (ver figura 65).

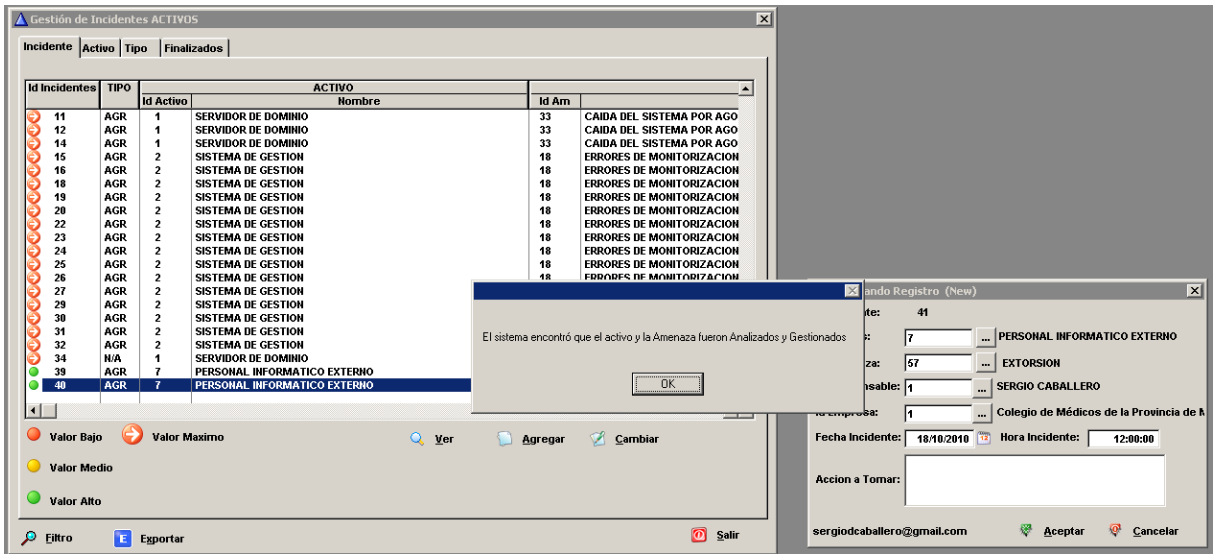


Figura 65 – Control de tipo de riesgo

Punto 2 – Si el activo seleccionado posee un riesgo asociado y este, está gestionado, el sistema muestra al operador, el/los riesgo que posee este activo, mostrando información detallada sobre la gestión del riesgo al usuario, como muestra la figura 66. El usuario deberá seleccionar el riesgo correspondiente.

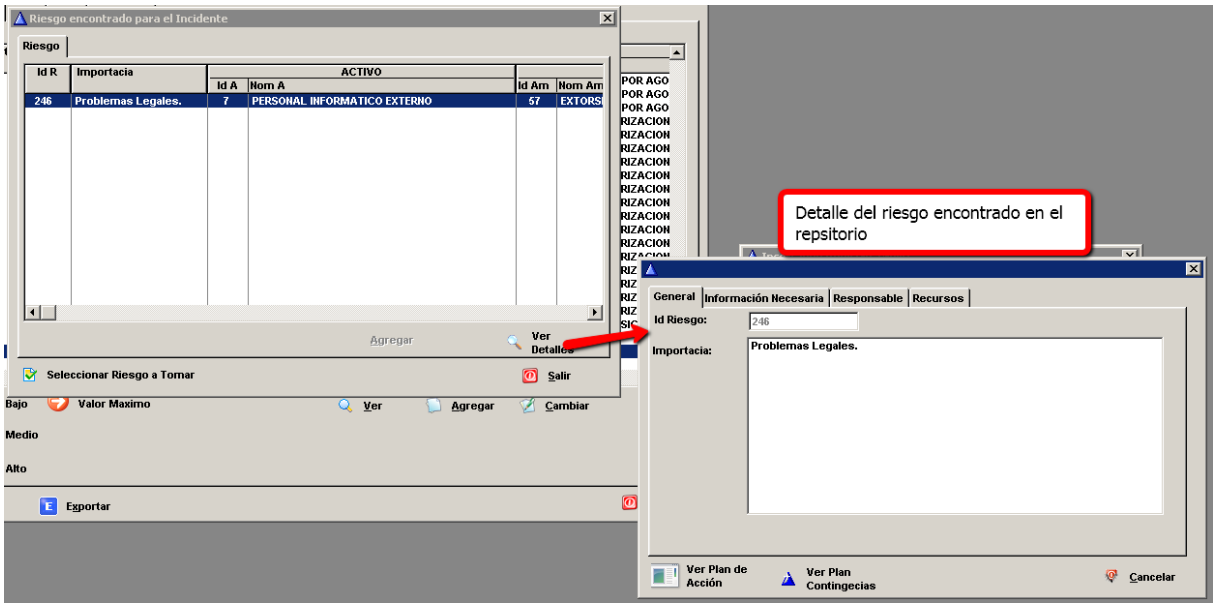


Figura 66– Detalle de riesgos encontrado

Paso 3 – Una vez seleccionado el riesgo, el sistema genera un reporte en el que se muestra el plan de contingencias correspondiente a la gestión del riesgo (ver figura 67), y envía por email una notificación de la carga del incidente, al encargado de la ejecución de dicho plan, como a jefe del proyecto.

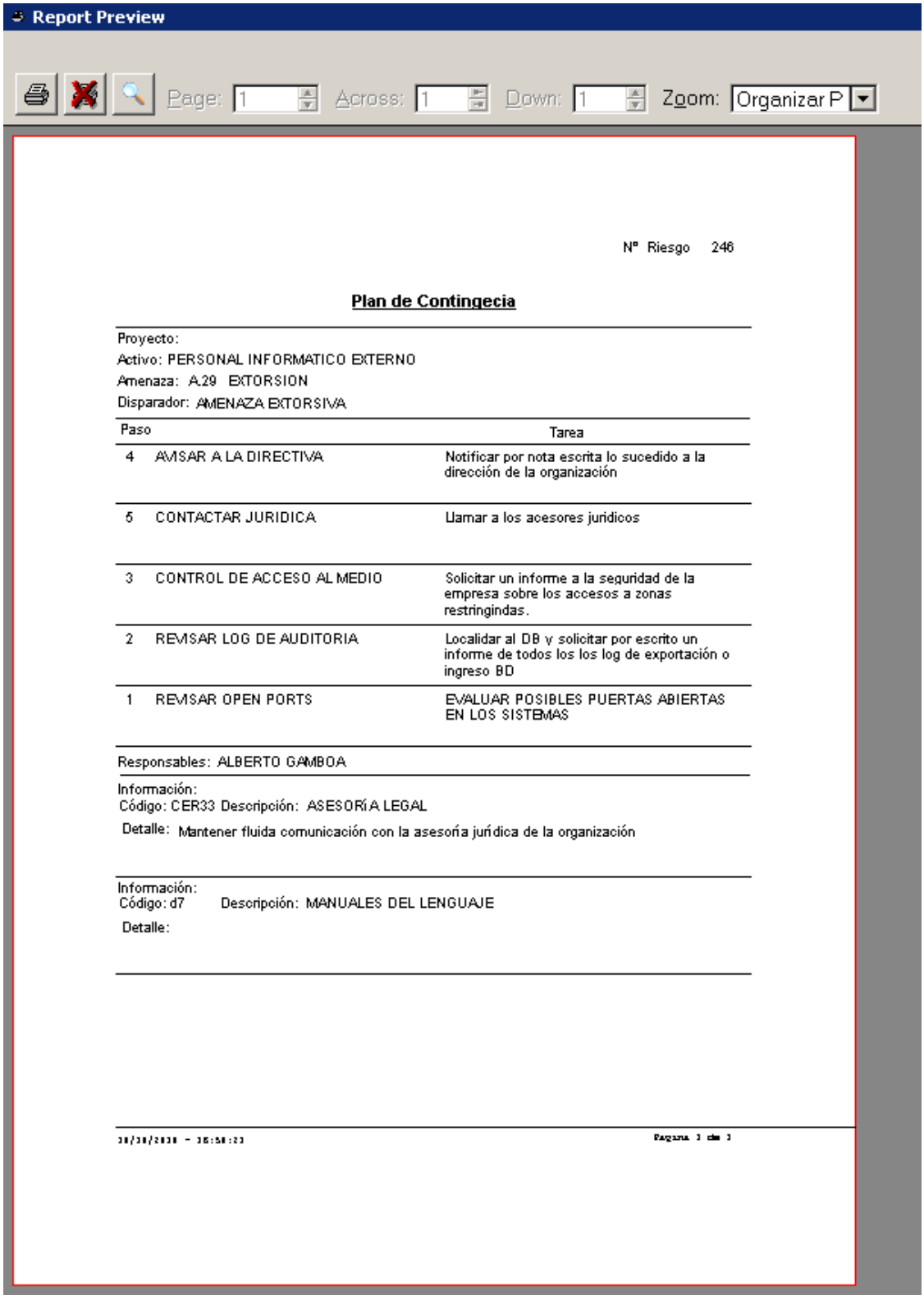


Figura 67 – Reporte Plan de contingencias.

Terminar Incidentes

Una vez terminado el incidente, se debe cargar al sistema los datos de finalización y evaluación del incidente.

El sistema muestra únicamente los incidentes activos que no fueron cerrados (ver figura 68).

Para poder cerrar un incidente se debe cargar: la observación sobre el incidente ocurrido, las acciones tomadas para solucionar el problema, la fecha de fin del incidente, y se debe marcar:

a. Si el incidente se solucionó correctamente
b. Si el plan de contingencias utilizado le resultó adecuado (esta opción se activa si el riesgo está gestionado y posee plan de contingencias).
c. Si se debería mejorar el plan de contingencias.

Estas preguntas son importantes para la evaluación y el mejoramiento cíclico de la gestión de los riesgos.

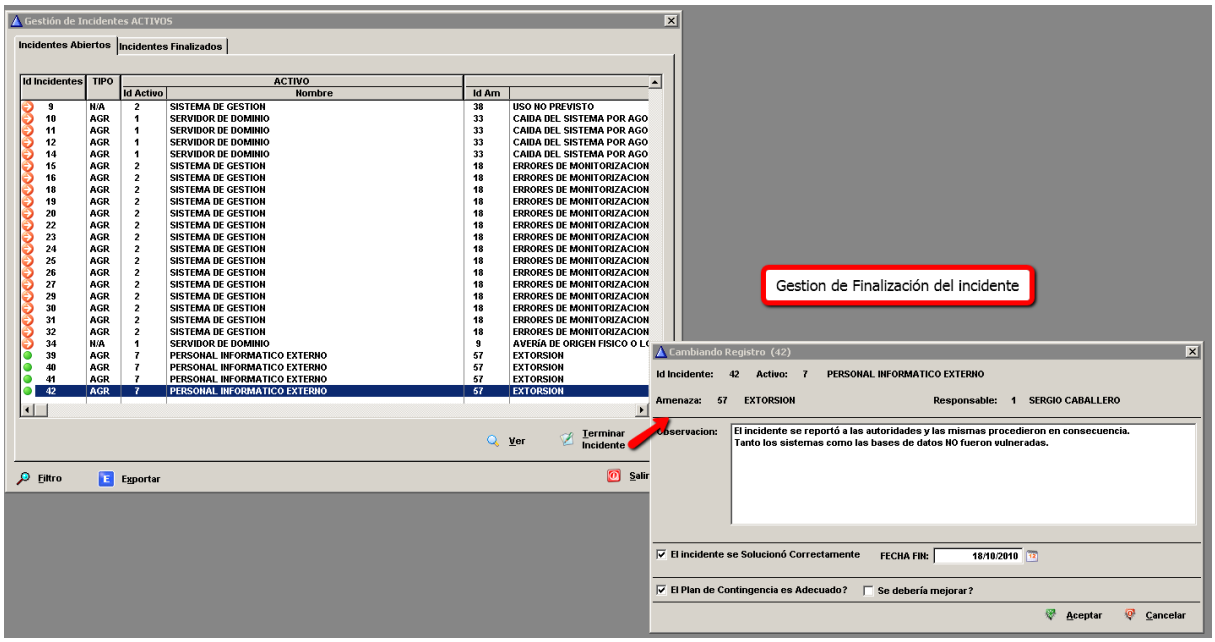


Figura 68- Finalización de un incidente

El módulo de incidentes es muy importante e innovador, ya que únicamente el método Sei-Mag propone incorporar la gestión de incidentes en el plan de AGR.

FASE IV - Informes

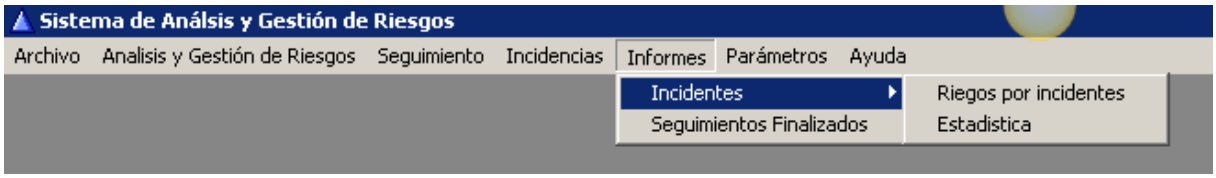


Figura 69 – Menú de Informes

Riesgos por Incidentes

El módulo de reporte de incidentes muestra una grilla en la que se expresa la información correspondiente a los incidentes, posee una serie de etiquetas que exponen únicamente la información que cumple con ciertas características como ser:

- Totales: Se muestran todos los incidentes.
- Terminados Bien: muestra los incidentes que terminaron correctamente.
- Terminados Mal: muestra los incidentes cuya finalización fue incorrecta.
- Pendientes: muestra los incidentes que no se han finalizado.
- Activos sin AGR: muestra los incidentes en los cuales se asignaron activos que no poseen análisis.
- Activos AR: muestra los incidentes en los cuales se asignaron activos que fueron analizados pero no expuestos.
- Activos AGR: muestra los incidentes en los cuales se asignaron activos que fueron analizados y gestionados.

En la figura 70 se muestra en el informe, solamente los incidentes que terminaron correctamente y utilizando el filtro avanzado que posee este módulo,

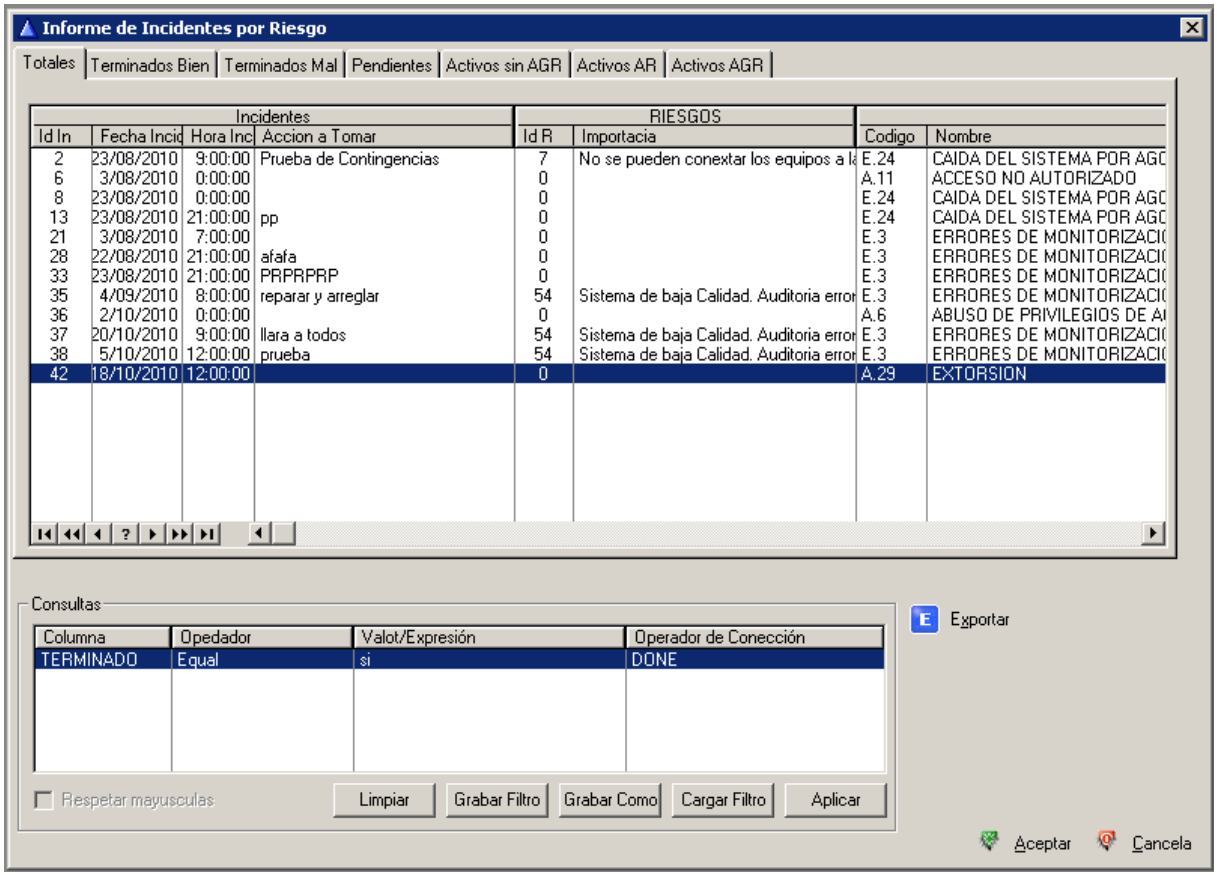


Figura 70 – Informe por incidente

Estadística

El sistema genera estadísticas de incidentes, evaluando el ranking de tipos de riesgos en los cuales se produjeron incidentes.

El primer paso para generar la estadística, es seleccionar el rango de fechas a tomar para el estudio, y si se toman todos los datos de los incidentes o únicamente los incidentes los que hayan finalizado (ver figura 71).

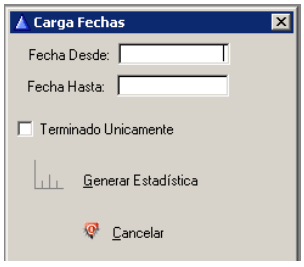


Figura 71 – Parámetros de estadística

Luego de generar los parámetros, se procesa la consulta estadística y como resultante se obtiene una tabla con los datos procesados y un gráfico de torta, en donde se muestra el porcentaje de cantidad de riesgos por cada tipo (ver figura 72).

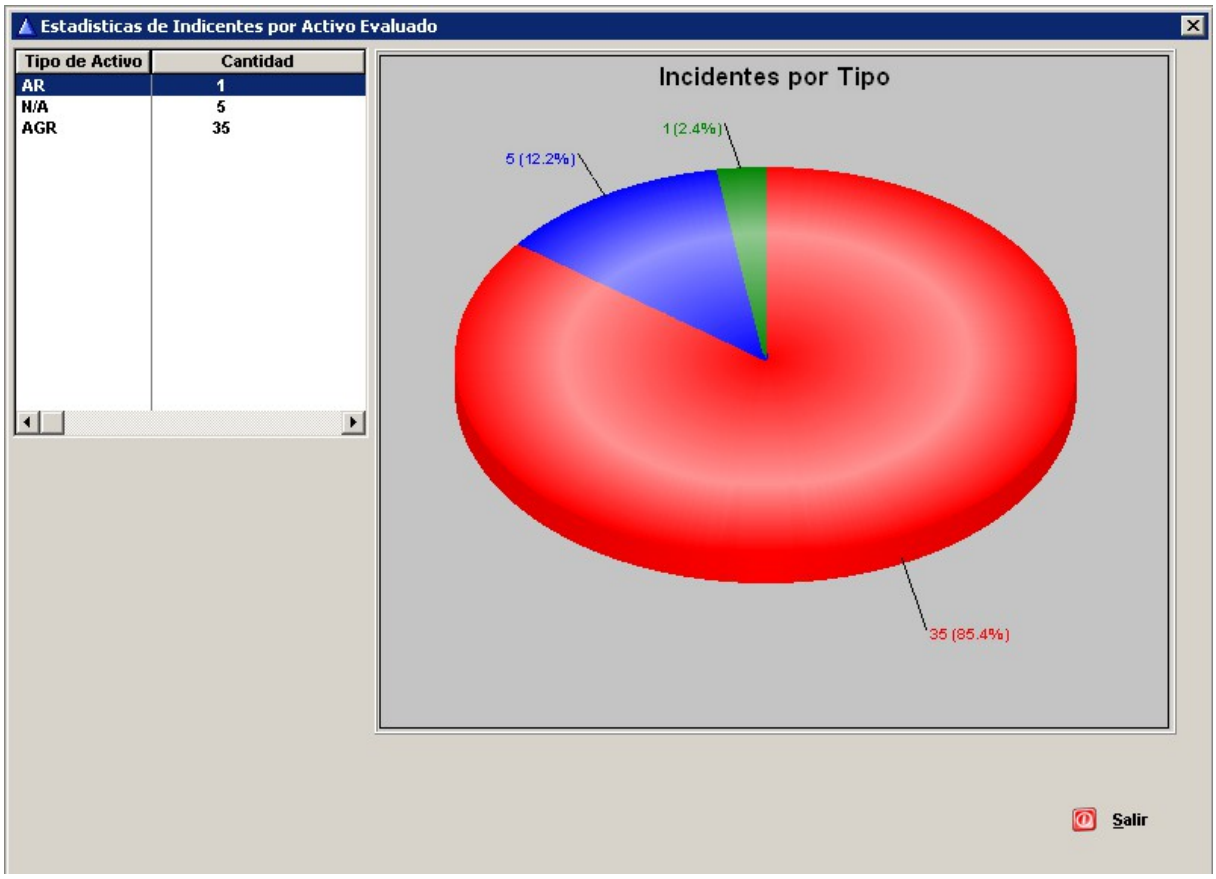


Figura 72 – Estadística de incidentes por activo evaluado

Seguimiento finalizado

El módulo de informes de seguimiento finalizado muestra los seguimientos terminados, y posee etiquetas para filtrar los datos por las siguientes características:

- Actividad por fecha: muestras las actividades finalizadas ordenada por fecha.
- Por Salvaguarda: muestra las actividades finalizadas ordenadas por la identificación de la salvaguarda.
- Por Amenaza: muestra las actividades finalizadas ordenadas por la identificación de la amenaza.

- Por Dimensión: muestra las actividades finalizadas ordenadas por la identificación de la dimensión.
- Terminado Bien: muestra las actividades que finalizaron correctamente.
- Terminados Mal: muestra las actividades que finalizaron mal o tuvieron problemas.

Además, como muestra la figura 73, el módulo cuenta con un componente de filtrado de datos.

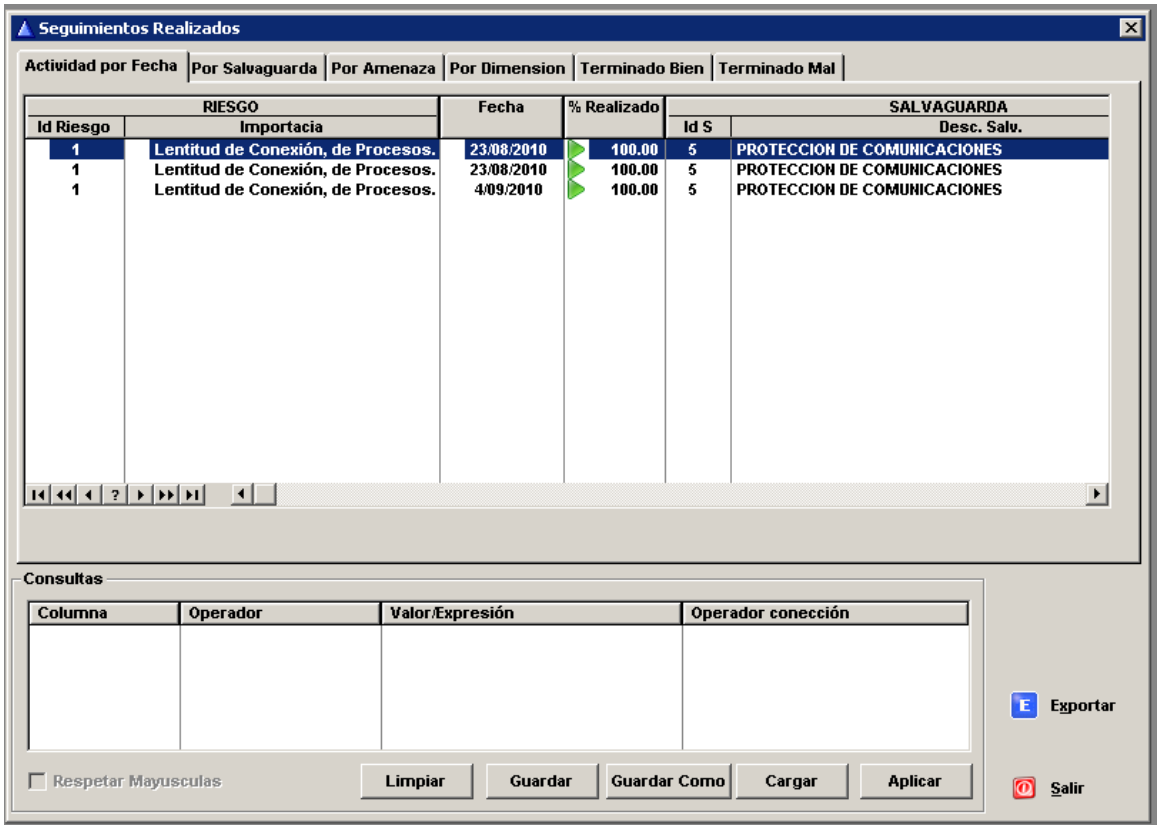


Figura 73 – **Seguimientos realizados**

Anexo II

Artefactos utilizados en el Análisis y Diseño

Planificación del Proyecto

MySeiMag
2/08/10-9/10/10

Informe GanttProject

Proyecto : MySeiMag

Inicio : 2/08/10

Fin : 9/10/10

Organización : Universidad Nacional de Misiones

Página web :

Descripción :

Desarrollar un Sistema Software para realizar el análisis y gestión de riesgos basados en el método Sei-Mag, el cual permitirá el manejo y la gestión de activos, amenazas, salvaguardas, proyectos, personas, taxonomías, gestión de riesgos, plan de contingencias y generación automática de plan de acción por proyecto, seguimiento, incidencias e informes, el mismo constará de procedimientos de aprendizaje automático de componentes, para generar información estadística y proponer mejoramiento de los planes antes mencionados. Deberá exportar la información procesada en las distintas fases que propone el método en formatos txt, xml, HTML y pdf, deberá poseer seguridad de acceso y control del sistema, auditoría de sistema y de procesos.

Date : 20-oct-2010 16:35:41

Lista de tareas

Nombre	Fecha de inicio	Fecha de fin	Recursos
Objetivos Generales	2/08/10	3/08/10	Horacio Daniel Kuna Sergio Daniel Caballero
Limites del Sistema	4/08/10	5/08/10	Sergio Daniel Caballero
Casos de Requisitos	6/08/10	13/08/10	Sergio Daniel Caballero
Caso de Uso	14/08/10	17/09/10	Sergio Daniel Caballero
Diagramas de Secuencia	14/08/10	17/09/10	Sergio Daniel Caballero
Diseño de Base de Datos	18/09/10	23/09/10	Sergio Daniel Caballero
Codificación	24/09/10	9/10/10	Sergio Daniel Caballero
Pruebas	24/09/10	9/10/10	Horacio Daniel Kuna Sergio Daniel Caballero

Lista de recursos

Nombre	Función
Sergio Daniel Caballero	Encargado del proyecto
Horacio Daniel Kuna	Encargado de pruebas

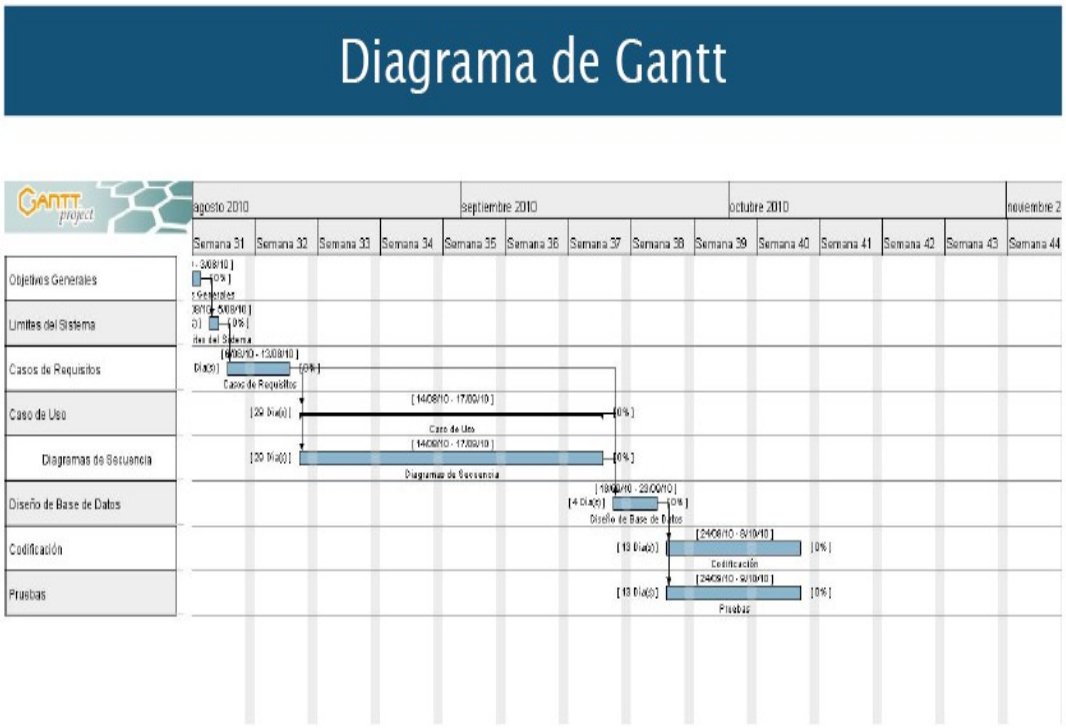


Diagrama de Gantt
agosto 2010
septiembre 2010
octubre 2010
Semana 31
Semana 32
Semana 33
Semana 34
Semana 35
Semana 36
Semana 37
Semana 38
Semana 39
Semana 40
Semana 41
Semana 42
Semana 43
Semana 44
Objetivos Generales
Límites del Sistema
Casos de Requisitos
Caso de Uso
Diagramas de Secuencia
Diseño de Base de Datos
Codificación
Pruebas

Modelo de Requisitos

Requisitos no funcionales

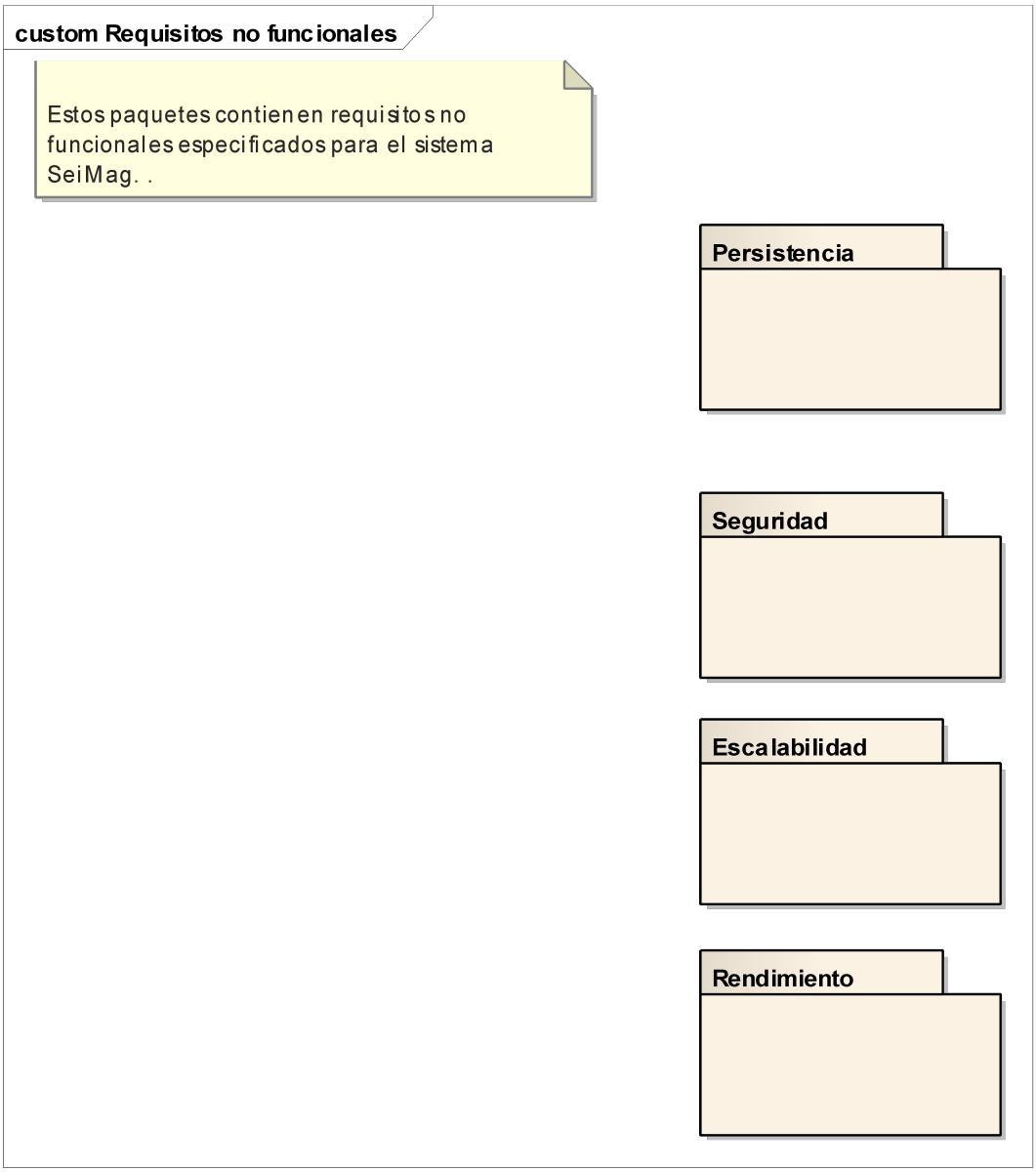


Imagen: Requisitos no funcionales

Nota

Estado: Proposed *Prioridad:* *Dificultad:*
Fase: 1.0 *Versión: 1.0*
Estos paquetes contienen requisitos no funcionales especificados para el sistema SeiMag. .

Escalabilidad

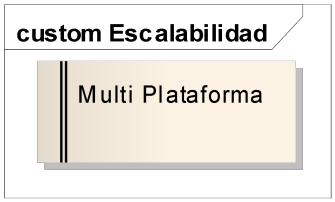


Imagen: Escalabilidad

Multi Plataforma

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
Operabilidad en cualquier Sistema Operativo.

Rendimiento

Imagen: Rendimiento

Tolerancia a Fallos

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
Las respuesta a las reserva como a las ventas de billetes no superaran mas de 5 segundos de procesamiento y controles.

Seguridad

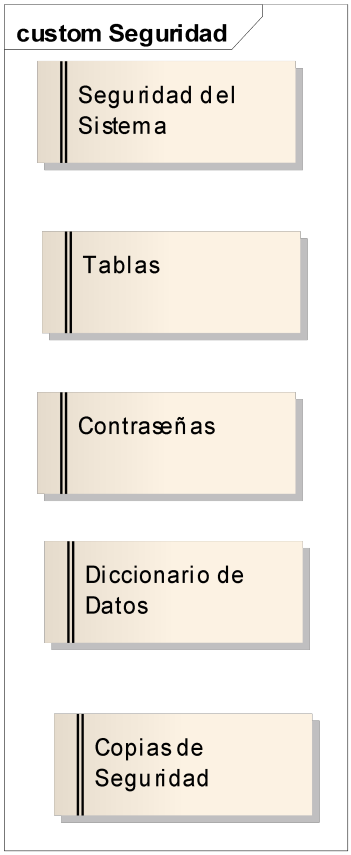


Imagen: Seguridad

Contraseñas

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
Serán encriptadas utilizando en los sistemas para su ingreso el caracter "*"

Copias de Seguridad

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
Se realizará copias de seguridad de los datos automáticamente dos veces por día.

Diccionario de Datos

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
El diccionario de datos deberá poseer contraseña para su acceso.

Seguridad del Sistema

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
La seguridad manejada por el sistema en donde se debe contemplar usuario y niveles de acceso al sistema.

Tablas

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
Las tablas poseerán seguridad de acceso a ellas, mediante una contraseña.

Persistencia

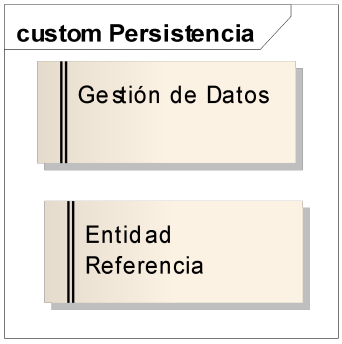


Imagen: Persistencia

Entidad Referencia

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
Las tablas del modelo de datos deben poseer identidad referencial.

Gestión de Datos

«Functional» *Estado:* *Prioridad:* Media *Dificultad:* Media
Fase: 1.0 *Versión: 1.0*
Capa de datos de conexión entre el sistema y los diferentes tipos de tablas y base de datos. Brinda independencia al sistema de los datos.

Transporte

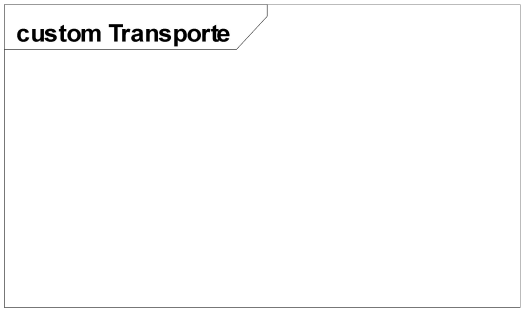


Imagen: Transporte

Requisitos Funcionales

Tabla de Contenidos

Requisitos funcionales
Nota
Fase I
<anónimo>
Etapa 1 - Inventario de activos
RF01 - Inventario de activos
RF02 - Elementos
RF03 - Dependencia entre Activos
RF04 - Fuente de Información del Activo
Etapa 2 - Propositos y Objetivos
RF05 - Gestión de Proyecto
RF06 - Asignar activos al proyeto
Etapa 3 - Equipo de Trabajo
RF07 - Gestion de Equipos
RF08 - Gestion de Rol
RF09 - Gestión de Equipo
RF10 -Gestion Persona
Etapa 4 - Taxonomía
RF11 - Generar Taxonomía
Etapa 5 - Declaración
RF 13 - Consecuencia
RF12 - Condición
RF14 - Efecto
Etapa 6 - Estimación de probabilidad - Impacto
RF15 - Probabilidad
RF16 - Impacto
Etapa 7 - Exposición
RF17 - Exposición
Etapa 8 - Gestión
RF 18 - Gestión del Riesgo
RF 19 - Plan de acción
RF20 - Plan de contingencias
Fase II
RF 21 - Generación de plan de Seguimiento
RF 22 - Gestión de seguimiento
Fase III
RF 26 - Informe de Plan de Contingecia
RF 27 - Notificación por email
RF23 Carga Incidente
RF24 - Final e Incidente
Fase IV
RF 28- Informe de Incidentes
RF 29 - Estadsiticas de Incidentes
RF 30 - Seguimiento
Parametros del Sistema
Fuente de Información
Gestión de Usuarios
Medidas de Tiempo
Salvaguarda por dimensión
Salvaguardas
Activos

Gestion de Elementos.....
Gestión de Dimensión.....
Gestión de Tipo de Activos.....
Gestión de Valoración.....
Amenazas.....
Amenzadas por Tipo de activo.....
Amenzas por Dimesión.....
Gestión de Amenazas.....
Gestión de Tipo de Amenazas.....
Reglas de negocio.....
Acceso al sistema.....
Conguración de Impresoras.....
Regla Principal.....
Características.....
Característica1.....
Interfaz de usuario.....
Pantalla.....
Grilla.....
Botón Agregar.....
Botón Cerrar.....
Botón Eliminar.....
Botón Modificar.....
Botón Ver.....
Grilla.....
Titulos de Ventanas.....

Requisitos funcionales

Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Modelo de requisitos
Detalle: *Creado el 19/11/2005. Última modificación el 19/11/2005*
GUID: {9F8E587E-2ECC-487b-B5DC-70D513EC5951}

Requisitos funcionales - *(diagrama Personalizado)*
Creado por: caballerosd el 19/11/2005
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {1AA2EE6C-6BD0-48f8-A179-688E208DF3A7}

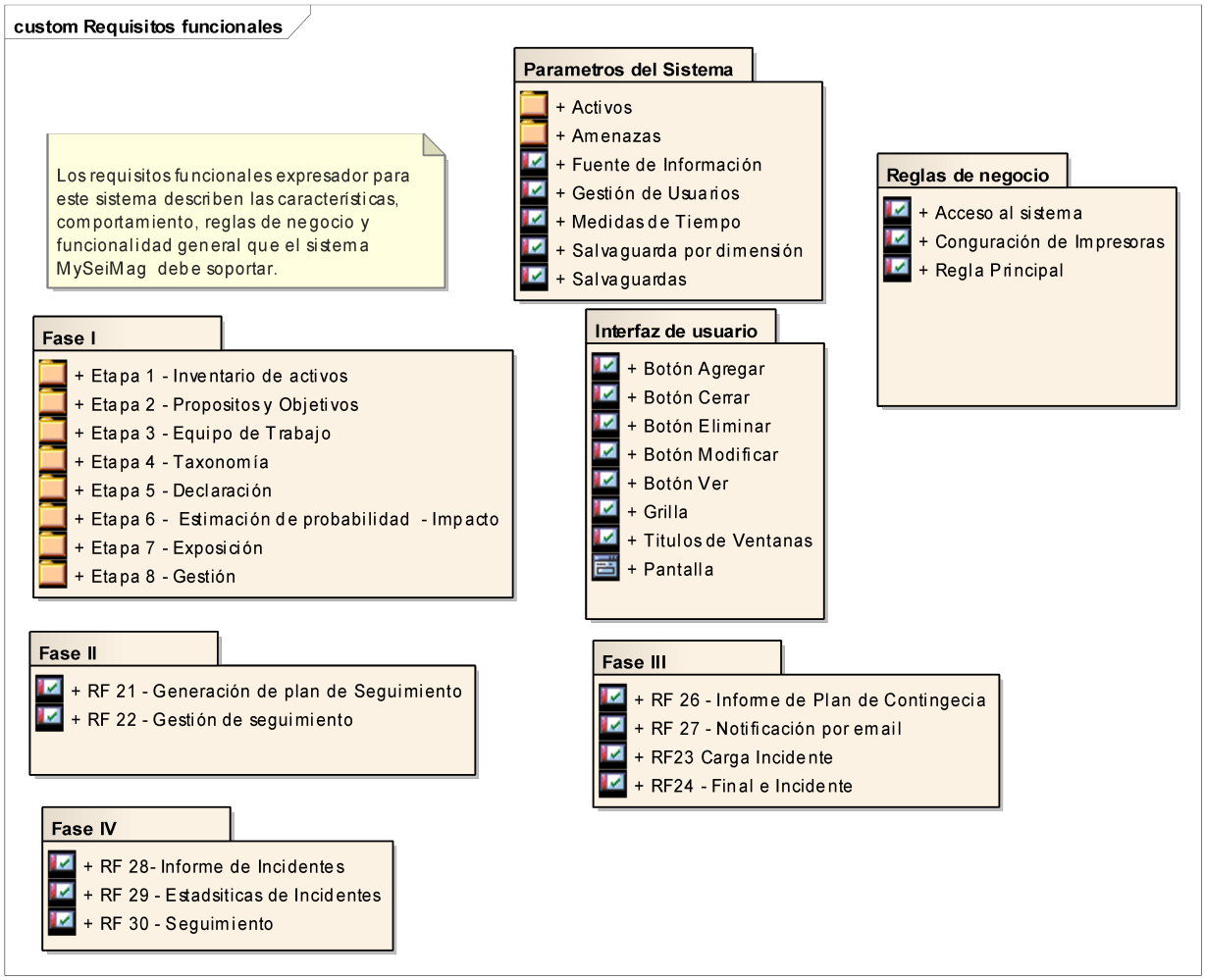


Imagen: 1

Nota
Tipo: Nota__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales *Palabras claves:*
Detalle: *Creado el* 19/11/2005. *Última modificación el 14/10/2010.*

GUID: {1B093CDE-B7F8-4283-994F-BCB36F52F64C}

Los requisitos funcionales expresados para este sistema describen las características, comportamiento, reglas de negocio y funcionalidad general que el sistema MySeiMag debe soportar.

Fase I
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {44CE00F4-0838-40f7-8469-D579509002B6}
Fase 1 del método Sei - Mag

Fase I - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 14/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {F1F38762-D31A-4171-9A10-13935C346FDE}

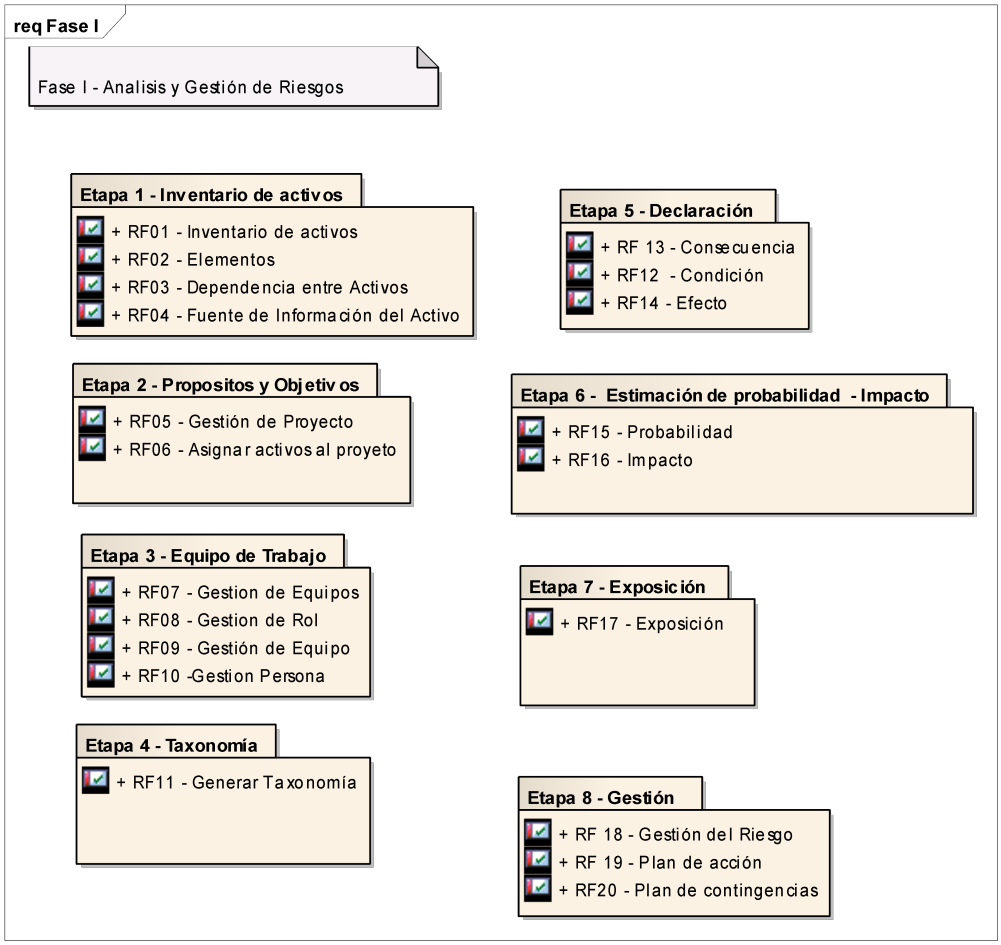


Imagen: 2

<Anónimo>

Tipo: Nota__
Estado: Propuesto. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010.*
GUID: {23DBA207-5B8E-4850-8FD1-B223D20B0701}

Fase I - Análisis y Gestión de Riesgos

Etapa 1 - Inventario de activos
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {40EB49F3-CF03-4871-B094-DFA8E45B12AD}

Etapa 1 - Inventario de activos - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {F1306217-1B7D-436f-8A0E-C1FC74888F1A}

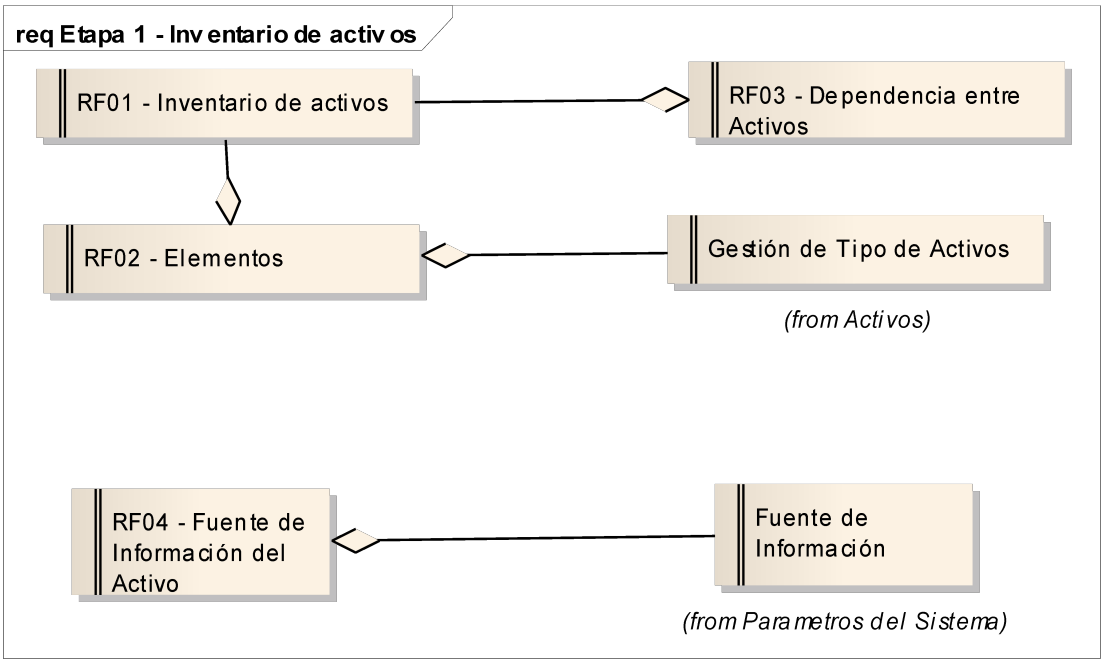


Imagen: 3

RF01 - Inventario de activos
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 1 - Inventario de activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {470C70ED-338E-4d63-B67B-77FA1E871181}

Es necesario gestionar los activos de la organización

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF01 - Inventario de activos	Public RF02 - Elementos	
Aggregation_ Origen -> Destino	Public RF01 - Inventario de activos	Public RF03 - Dependencia entre Activos	
Aggregation_ Origen -> Destino	Public RF01 - Inventario de activos	Public RF06 - Asignar activos al proyecto	
Aggregation_ Origen -> Destino	Public Gestión de Valoración	Public RF01 - Inventario de activos	

RF02 - Elementos

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 1 - Inventario de activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {9235C8AE-96DD-4900-8582-5A9926E2A1E4}

Define el elemento por activo según su tipo

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF01 - Inventario de activos	Public RF02 - Elementos	
Aggregation_ Origen -> Destino	Public Gestión de Tipo de Activos	Public RF02 - Elementos	

RF03 - Dependencia entre Activos

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 1 - Inventario de activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {E36AA0ED-CCAA-4620-9FBC-A9F911638AD3}

Un activo puede depender de otro.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF01 - Inventario de activos	Public RF03 - Dependencia entre Activos	

RF04 - Fuente de Información del Activo

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 1 - Inventario de activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {6CA9EFF0-3BED-4dff-BF67-88242FDF29B2}

Se asigna al activo la fuente/as de información

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Fuente de Información	Public RF04 - Fuente de Información del Activo	

Etapa 2 - Propósitos y Objetivos

Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {F7C57FC0-BFCD-44d1-805B-8DA1757A8D3F}

Etapa 2 - Propósitos y Objetivos - *(diagrama Requirements)*

Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {734C9DEE-F26F-49d0-8876-9D76BCEAE495}

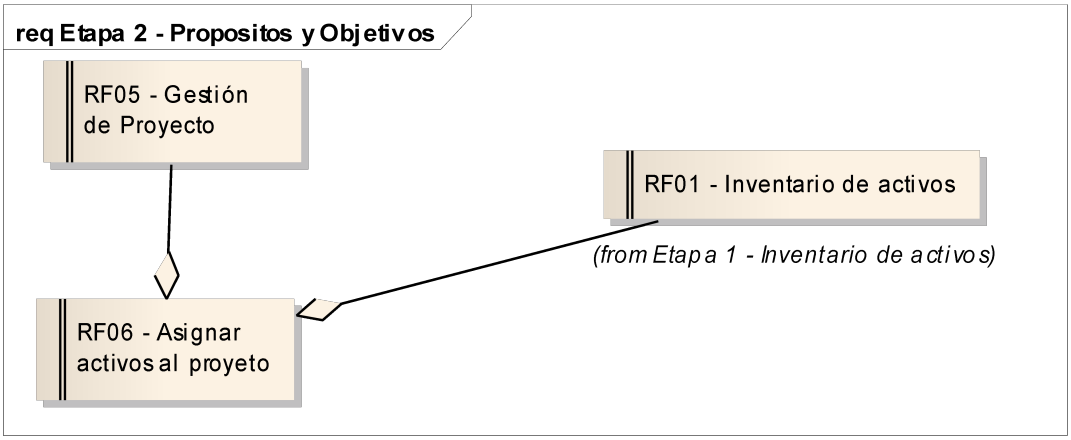


Imagen: 4

RF05 - Gestión de Proyecto

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 2 - Propósitos y Objetivos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {359BBAEC-93F7-4ccd-ACCB-4F4DA790DD75}

Gestionar los proyectos de AGR. Es necesario incluir Objetivos y limites.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF05 - Gestión de Proyecto	Public RF06 - Asignar activos al proyecto	

RF06 - Asignar activos al proyecto

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 2 - Propósitos y Objetivos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {D4A8DC29-D2A6-4f4f-AD3B-72CFE658C339}

Es necesario asigna activos a los proyectos.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF05 - Gestión de Proyecto	Public RF06 - Asignar activos al proyecto	

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF01 - Inventario de activos	Public RF06 - Asignar activos al proyecto	

Etapa 3 - Equipo de Trabajo
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {D0AC9C8D-2344-4b10-ACAB-71924AEC313E}

Etapa 3 - Equipo de Trabajo - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {03CCFFE1-1631-48cb-88A6-64C4A04F2402}

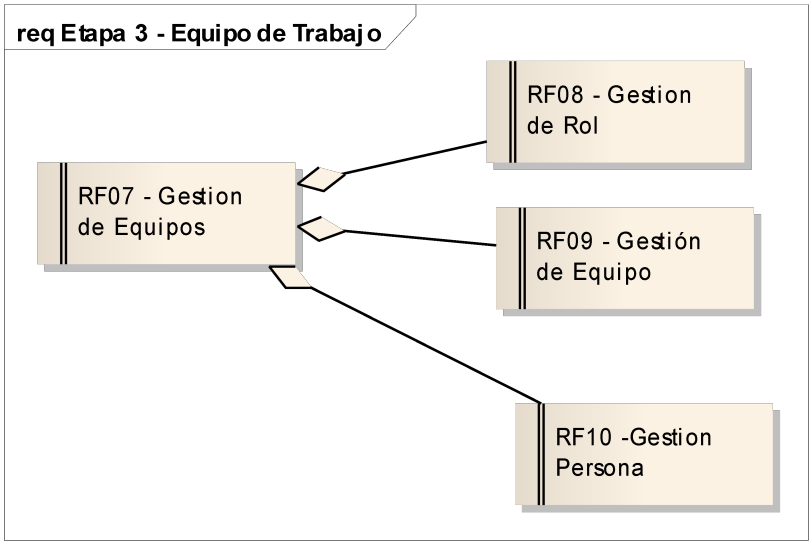


Imagen: 5

RF07 - Gestión de Equipos
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 3 - Equipo de Trabajo *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {B6CF113F-02F8-4310-87D6-6B0D13C6FF1B}

Es necesario asignar personas al proyecto. Para ellos se debe gestionar las personas y asignarle un rol y un equipo de trabajo

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF08 - Gestion de Rol	Public RF07 - Gestion de Equipos	
Aggregation_ Origen -> Destino	Public RF09 - Gestión de Equipo	Public RF07 - Gestion de Equipos	
Aggregation_ Origen -> Destino	Public RF10 -Gestion Persona	Public RF07 - Gestion de Equipos	

RF08 - Gestion de Rol

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 3 - Equipo de Trabajo *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {47966055-7223-4316-8CBA-0B4AC82420BC}

Se deberá gestionar el rol de las personas.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF08 - Gestion de Rol	Public RF07 - Gestion de Equipos	

RF09 - Gestión de Equipo

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 3 - Equipo de Trabajo *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {FD6E9F99-AB43-441f-A28F-222680C9EA10}

Se deberá gestionar los equipos que contendrán los distintos proyectos.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF09 - Gestión de Equipo	Public RF07 - Gestion de Equipos	

Connector	Origen	Destino	Notas

RF10 -Gestion Persona

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 3 - Equipo de Trabajo *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {E56E293E-6C4B-4e4f-9FFC-AD13F5A6851D}

Gestionar los datos de los miembros de equipo de AGR.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF10 -Gestion Persona	Public RF07 - Gestion de Equipos	

Etapa 4 - Taxonomía

Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {1855F438-B4D0-4b78-9B11-D6FC5EF84918}

Etapa 4 - Taxonomía - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {1C8A215D-2E7B-463d-AE4F-AC61CC36394B}

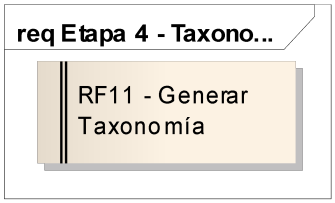


Imagen: 6

RF11 - Generar Taxonomía

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 4 - Taxonomía *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {1834A5E2-D23E-4222-ABE0-DC8F19A8E5A8}

Por cada proyecto es necesario generar automáticamente la taxonomía de los riesgos.

Etapa 5 - Declaración
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {F9140C3C-732B-45ea-86EC-F9DB6142CFE8}

Etapa 5 - Declaración - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {0CBCAC52-1B97-4b04-B851-D8F8880E86EE}

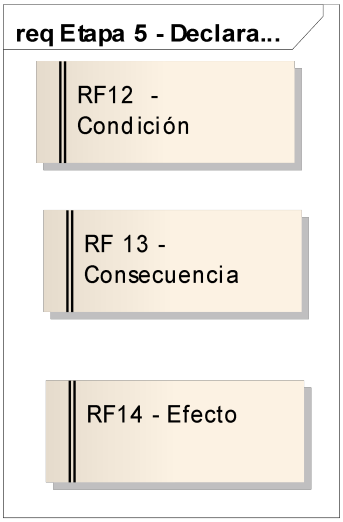


Imagen: 7

RF 13 - Consecuencia
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 5 - Declaración *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {E1B36BD7-2F91-4598-BC2C-5490D5D8F5FC}

Por cada riesgo se define la consecuencia que recibirá la organización si el riesgo se transforma en problema.

RF12 - Condición
Tipo: Requisito__

Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 5 - Declaración *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {2CA55FB8-0B8B-4d68-A40A-303625019BCD}

Por cada riesgo se define la condición que debe existir para que le riesgo se transforme en problema

RF14 - Efecto

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 5 - Declaración *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {DAC775F3-5968-4713-B074-77CE8B4921B5}

Por cada riesgo se definine el efecto que tendrá el problema en la organización.

Etapa 6 - Estimación de probabilidad - Impacto
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {5D7E1339-35C9-4a88-BD94-AF45FAF9F96C}

Etapa 6 - Estimación de probabilidad - Impacto - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {273E3A00-C966-438c-8BB6-ECD5A5C9C508}

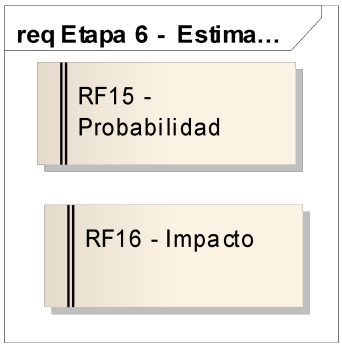


Imagen: 8

RF15 - Probabilidad

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 6 - Estimación de probabilidad - Impacto *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.

GUID: {87382A4C-82BC-425a-96F3-CC545E226A4C}

Por cada riesgo se define probabilidad de ocurrencia del riesgo.

RF16 - Impacto

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 6 - Estimación de probabilidad - Impacto *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {3159D5DB-5EE0-4058-95E9-5510894937E9}

Por cada riesgo se define el impacto que tendrá si el riesgo se ejecuta.

Etapa 7 - Exposición

Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {87F630B4-1CD2-47f5-8F0F-5BF6A4A9F774}

Etapa 7 - Exposición - *(diagrama Requirements)*

Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {69983725-4DC4-4ed6-BFCD-EB5F14BABCE8}

Imagen: 9

RF17 - Exposición

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 7 - Exposición *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {7223647B-5232-403c-A533-0496CED9C0E4}

Se calcula la exposición del riesgo.

Etapa 8 - Gestión
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Fase I
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {0282B77E-528E-4caf-A680-FBFBC49D7B25}

Etapa 8 - Gestión - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {A3496FD9-3D9C-45ee-90DC-88A6D44A8630}

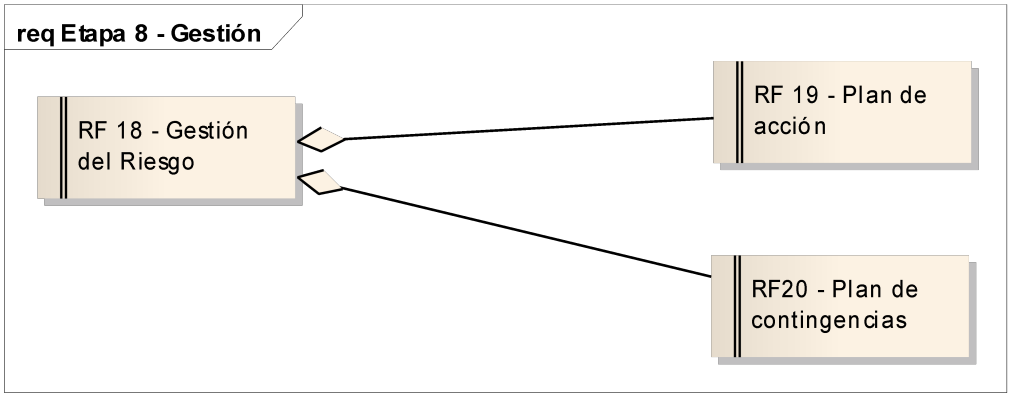


Imagen: 10

RF 18 - Gestión del Riesgo
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 8 - Gestión *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {E3BD0328-C7CA-4204-A5D5-26DD2B62447B}

Se gestionan los riesgos.
Es necesario describir la :

- información necesaria para manejar el riesgo
- Responsable del control de riesgo.
- Recursos necesarios.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF 19 - Plan de acción	Public RF 18 - Gestión del Riesgo	
Aggregation_ Origen -> Destino	Public RF20 - Plan de contingencias	Public RF 18 - Gestión del Riesgo	

Connector	Origen	Destino	Notas

RF 19 - Plan de acción

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 8 - Gestión *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {51454B8C-48A0-4f5a-8001-563EC4B72C98}

Por cada riesgo se asigna un plan de acción dependiente de las salvaguardas y los activos.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF 19 - Plan de acción	Public RF 18 - Gestión del Riesgo	

RF20 - Plan de contingencias

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Etapa 8 - Gestión *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {E5532571-C74F-4ecf-840C-547DC3BA0ACF}

Por cada riesgo se gestiona un plan de contingencias.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF20 - Plan de contingencias	Public RF 18 - Gestión del Riesgo	

Fase II

Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {0F175C0B-A4EA-4aa8-AC60-ECF9949689B4}

Fase II - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 14/10/2010

Versión: 1.0. *Bloqueado:* Falso
GUID: {874A891A-0BC7-4667-87DB-DEC3FF2E815F}

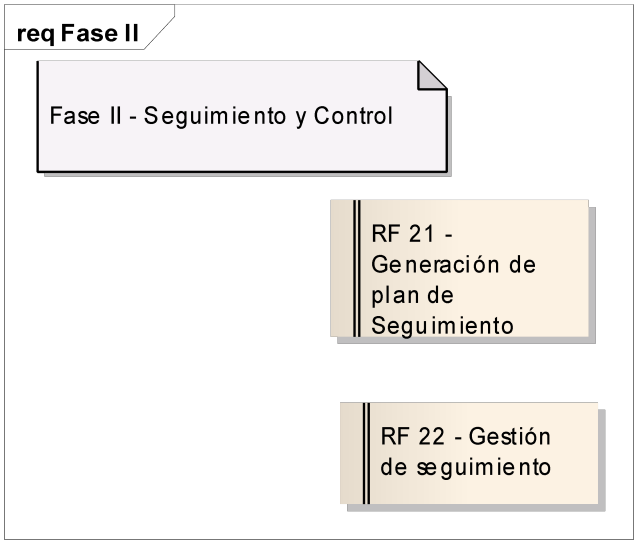


Imagen: 11

RF 21 - Generación de plan de Seguimiento
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase II *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {F5D04B76-9C2B-4095-B906-93917ADF114D}

Es necesario genera automáticamente por proyecto el plan de seguimiento de los planes de acción (salvaguardas), el mismo puede ser actualizado cuando se modifique el plan de acción.

RF 22 - Gestión de seguimiento
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase II *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {41D09DC8-D679-4abd-AF05-F732379D6331}

Es necesario que el sistema muestra una agenda con las actividades de seguimiento por persona, la cual deberá asentar en cada seguimiento el % de avance y observaciones por cada seguimiento. El sistema deberá mostrar gráficamente los estados de avances y distintas vistas de esta agenda. Tareas terminadas, tareas pendientes etc.

Fase III
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {C579F58C-F754-4a7b-BCDD-8C454D203C00}

Fase III - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 14/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {EA33E0E5-2CE3-4860-AA9C-19D29E643ECF}

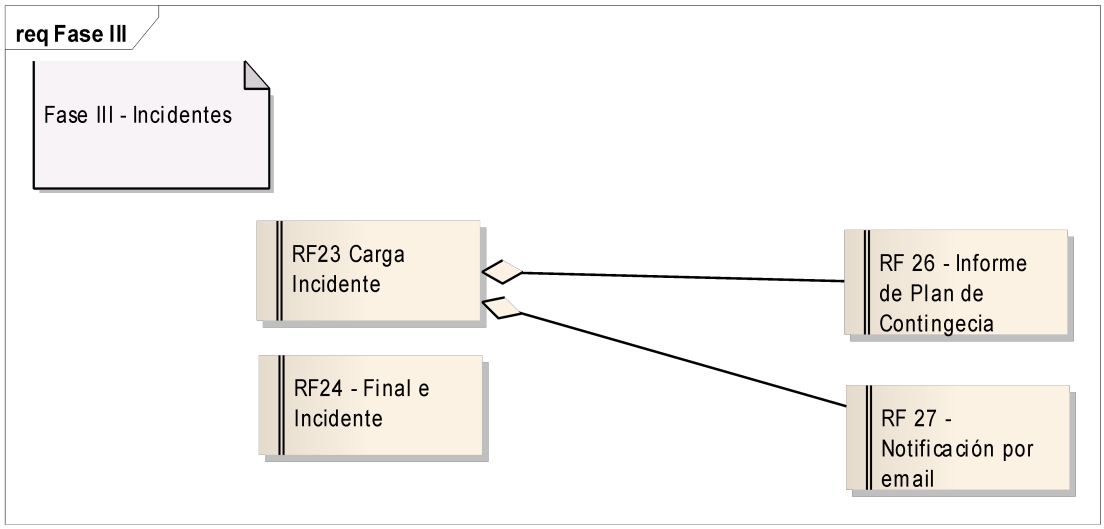


Imagen: 12

RF 26 - Informe de Plan de Contingencia
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase III *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010.*
GUID: {3E5F706B-AD6E-40e4-A60B-D9C3B8EEF337}

Una vez cargado el incidente, se deberá informar en formato de reporte el plan de contingencias, si el riesgo es un AGR.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF 26 - Informe de Plan de Contingencia	Public RF23 Carga Incidente	

RF 27 - Notificación por email
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase III *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010.*
GUID: {D2B3B4BF-4BDD-4dfa-9B41-7AD6D7B34331}

Una vez cargado el incidente, el sistema notificará al encargado de sistemas sobre le incidente. Y si el riesgo posee AGR además notificará al encargado de ejecutar el plan de contingencias.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF 27 - Notificación por email	Public RF23 Carga Incidente	

RF23 Carga Incidente
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase III *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010*.
GUID: {63CFDC0A-6B12-414c-B20E-9C89D1F28A3F}

El sistema deberá posee un módulo para cargar los incidentes ocurridos. El mismo permitir el ingreso de cualquier usuario del sistema.
Y en el cual se podrá cargar:

- El Activo que tuvo el incidente
- La Amenaza que se ejecuto.
- El responsable inmediato de tomar el caso.
- La fecha y hora del incidente
- Breve observación de acción a tomar

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public RF 27 - Notificación por email	Public RF23 Carga Incidente	
Aggregation_ Origen -> Destino	Public RF 26 - Informe de Plan de Contingencia	Public RF23 Carga Incidente	

RF24 - Final e Incidente
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase III *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010*.
GUID: {B0CAC978-2256-42eb-B3E7-61CCD94217DD}

Se deberá gestionar el final del incidente, el mismo estará en un formulario distinto al de carga y deberá contemplar la siguiente información:

- Observación del fin del incidente.
- Fecha del Fin

- Si termino correctamente.

Fase IV
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {844ADD6F-0606-45e1-BDCE-75A6216CD30F}

Fase IV - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 14/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {4DFDEBE8-81AB-441a-A60D-D51DF787AADF}

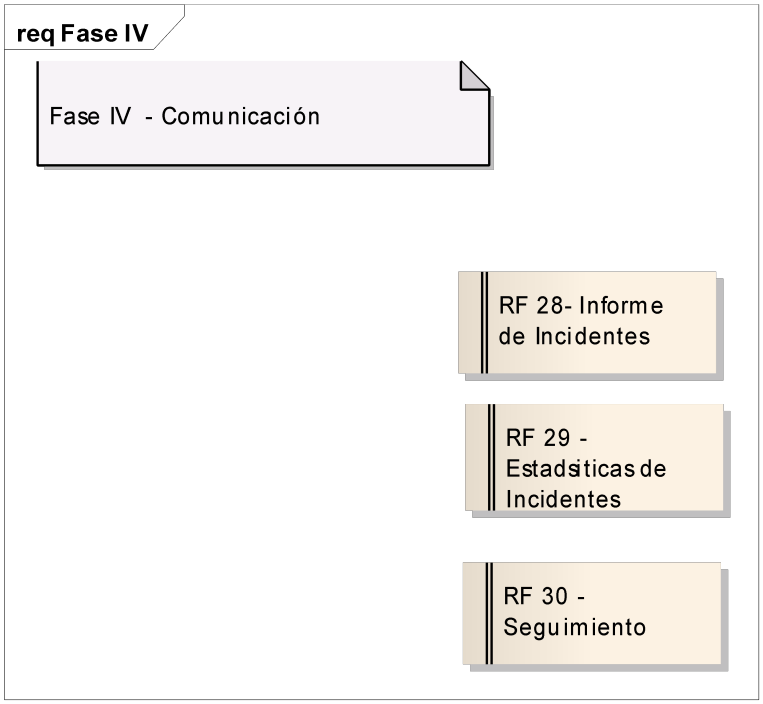


Imagen: 13

RF 28- Informe de Incidentes
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase IV *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010.*
GUID: {3F2A912F-5615-45c3-AF5C-3A8B00550B4D}

Se deberá generar un módulo de reportes de los activos por incidente en el deberá poseer:

- El total de los datos de los incidentes : Activo, riesgo, dimensión, fechas etc.

RF 29 - Estadísticas de Incidentes
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase IV *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010*.
GUID: {DD100952-7DFC-47b3-BDFE-37EA2EC6FE40}

El sistema deberá procesar y mostrar en forma gráfica el ranking de la cantidad de incidentes y evaluar el activo, obteniendo como resultado la cantidad incidentes que poseen activos:

- NA - No fueron analizados
- AG - Se analizaron pero no se gestionaron.
- AGR - SE analizaron y gestionaron

RF 30 - Seguimiento
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Fase IV *Palabras claves:*
Detalle: *Creado el* 14/10/2010. *Última modificación el 14/10/2010*.
GUID: {E3B2FE56-B1AC-49e8-B4A7-2A2DD8C05C60}

Se deberá preveer un informe sobre los seguimiento terminados y los activos en actualmente. También se deberá preveer la posibilidad de exportar el informe procesado.

Parametros del Sistema
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {97E850D0-CD92-49db-B5CD-B01237D5C940}
Se establecerán los parámetros del sistema antes de comenzar con la Fase I del mismo.

Parametros del Sistema - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {501A0003-444E-4a14-96A1-6B23302F90D1}

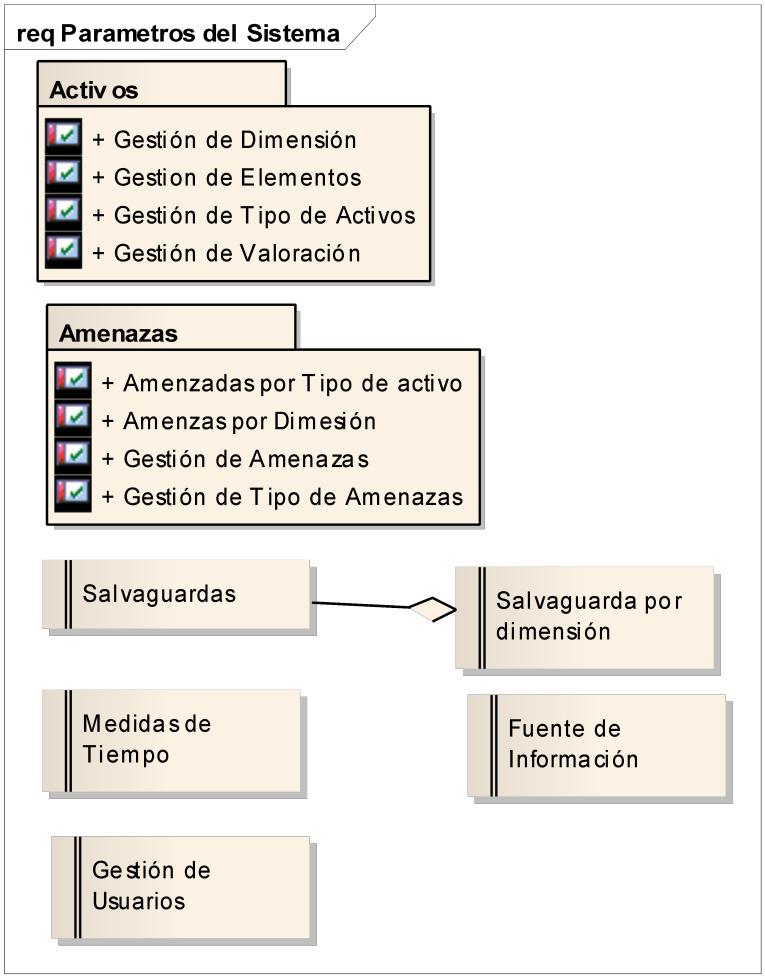


Imagen: 14

Fuente de Información
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Parametros del Sistema *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {BAC2996E-37D0-411d-913C-3B01D794DA83}

Es necesario gestionar las distintas dependencias de la organización en donde se tomara como fuente de información sobre los activos analizado.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Fuente de Información	Public RF04 - Fuente de Información del Activo	

Gestión de Usuarios
Tipo: Requisito__

Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Parametros del Sistema *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {845849A9-A6F5-4be8-9459-06327459A5A4}

Se necesita gestionar los usuarios del sistema, con descripción, acceso por niveles y contraseña encriptada.

Medidas de Tiempo
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Parametros del Sistema *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {5A040E84-D9A7-47e0-9A1B-B8E6A4BA0DE0}

Medida de tiempo ha ser utilizada por el plan de acción en la cuales es necesario poseer características de unidad de tiempo y distancia entre días.

Salvaguarda por dimensión
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Parametros del Sistema *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {881EC105-B052-4ba4-B0C7-F95089A797F8}

Es necesario asignar las dimensiones a la salvaguardas.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Salvaguardas	Public Salvaguarda por dimensión	

Salvaguardas
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Parametros del Sistema *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {5DD759F7-EF44-40a8-8B71-73320F385F1F}

Las salvaguardas se gestionarán utilizando como base las salvaguardas descriptas en la metodología Magerit V2

Conexiones

Connector	Origen	Destino	Notas
Aggregation_	Public	Public	

Connector	Origen	Destino	Notas
Origen -> Destino	Salvaguardas	Salvaguarda por dimensión	

Activos
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Parametros del Sistema
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {4606A1BB-D130-4448-B6FA-30B1D4F71D11}
Gestiona los parámetros del sistema en los cuales se agrupan los referentes a los activos.

Activos - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {32513E87-D65F-441b-8D55-BB9364663B81}

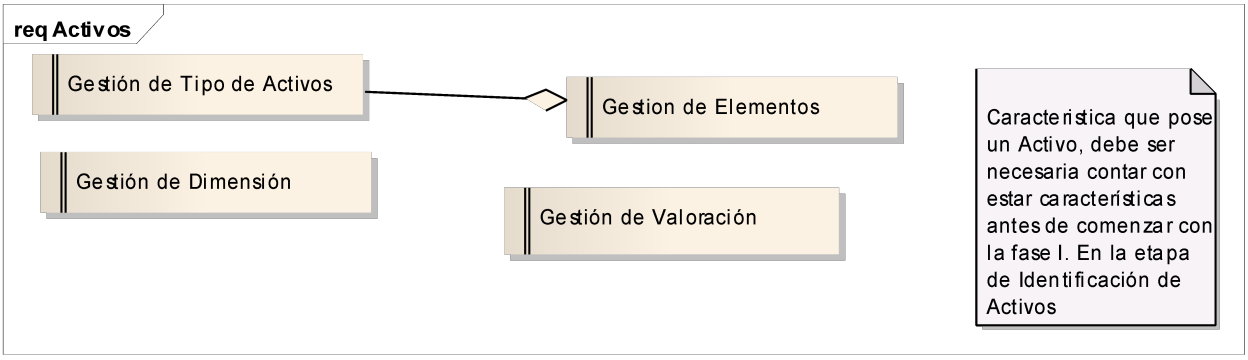


Imagen: 15

Gestión de Elementos
Tipo: Requisito
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {A63DFEB8-7B50-4325-A727-BB1E711EBD72}

Las gestión de elementos de un activo se cargarán utilizando como base los elementos determinados en la metodología Magerit V2. Deberá existir el tipo de activo

Conexiones

Connector	Origen	Destino	Notas
Aggregation Origen -> Destino	Public Gestión de Tipo de Activos	Public Gestion de Elementos	

Connector	Origen	Destino	Notas

Gestión de Dimensión

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {219E0831-D07E-4d15-B688-AF8F4B553480}

La gestión de dimensión de una activo se cargarán utilizando como base las dimensiones propuestas por la metodología Magerit V2

Gestión de Tipo de Activos

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {BF928D05-6929-4d82-B821-72750568180D}

Los tipos de activos se cargarán utilizando como base los tipos de activos de la metodología Magerit V2

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Gestión de Tipo de Activos	Public Gestion de Elementos	
Aggregation_ Origen -> Destino	Public Gestión de Tipo de Activos	Public RF02 - Elementos	

Gestión de Valoración

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Activos *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {6D2231EE-A4E2-40c0-A9D8-6D03C5FD0659}

La gestión de valoración de un activo se cargará utilizando como base la tabla de valores de los activos
de la metodología Magerit V2

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Gestión de Valoración	Public RF01 - Inventario de activos	

Amenazas
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Parametros del Sistema
Detalle: *Creado el 13/10/2010. Última modificación el 13/10/2010*
GUID: {1608C238-8F45-4d22-BA06-EB0EA344E7A6}

Amenazas - *(diagrama Requirements)*
Creado por: caballerosd el 13/10/2010
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {00AC87C1-271E-48b9-BB5A-76C9A794CDC7}

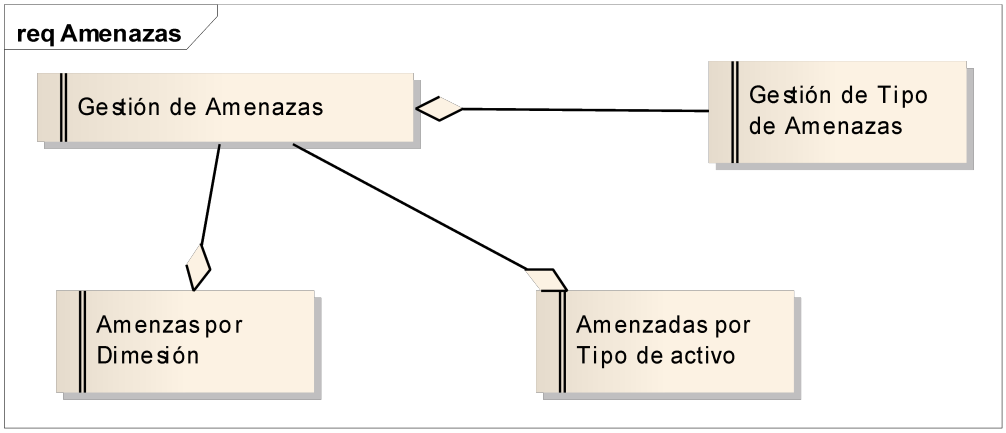


Imagen: 16

Amenazas por Tipo de activo
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Amenazas *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {749A24D0-0B11-4eef-8F76-B07824C3975B}

Se deberá clasificar las amenazas por lo tipos de activos.
Deberá estar cargados al sistemas tanto las amenazas y los tipos de activos.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Gestión de Amenazas	Public Amenazas por Tipo de activo	

Amenazas por Dimensión

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Amenazas *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {3570FED2-597B-42d6-A50E-6E26D0E28E9F}

Es necesario clasificar las amenazas por las dimensión de los activos.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Gestión de Amenazas	Public Amenazas por Dimesión	

Gestión de Amenazas

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Amenazas *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {7DC1B778-DDDF-4086-90D8-53DFD5B9D000}

Las amenazas se cargarán utilizando como base las amenazas descriptas en la metodología Magerit V2, deben estar cargados los tipos de amenazas

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Gestión de Tipo de Amenazas	Public Gestión de Amenazas	
Aggregation_ Origen -> Destino	Public Gestión de Amenazas	Public Amenazas por Dimesión	
Aggregation_ Origen -> Destino	Public Gestión de Amenazas	Public Amenazas por Tipo de activo	

Gestión de Tipo de Amenazas

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Amenazas *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {00CC4811-EDE4-4bc4-BD3B-796AC53DB4B2}

La gestión de los tipos de amenazas se cargará utilizando como base los tipos de activos de la metodología Magerit V2

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Gestión de Tipo de Amenazas	Public Gestión de Amenazas	

Reglas de negocio

Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 19/11/2005*. *Última modificación el 19/11/2005*
GUID: {9E4415C4-B2B2-42c5-8A5A-DAF2A57E5F15}

Lógica de negocios - *(diagrama Personalizado)*
Creado por: caballerosd el 19/11/2005
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {03E6B261-6C5F-4619-AFB0-A195CB298C50}

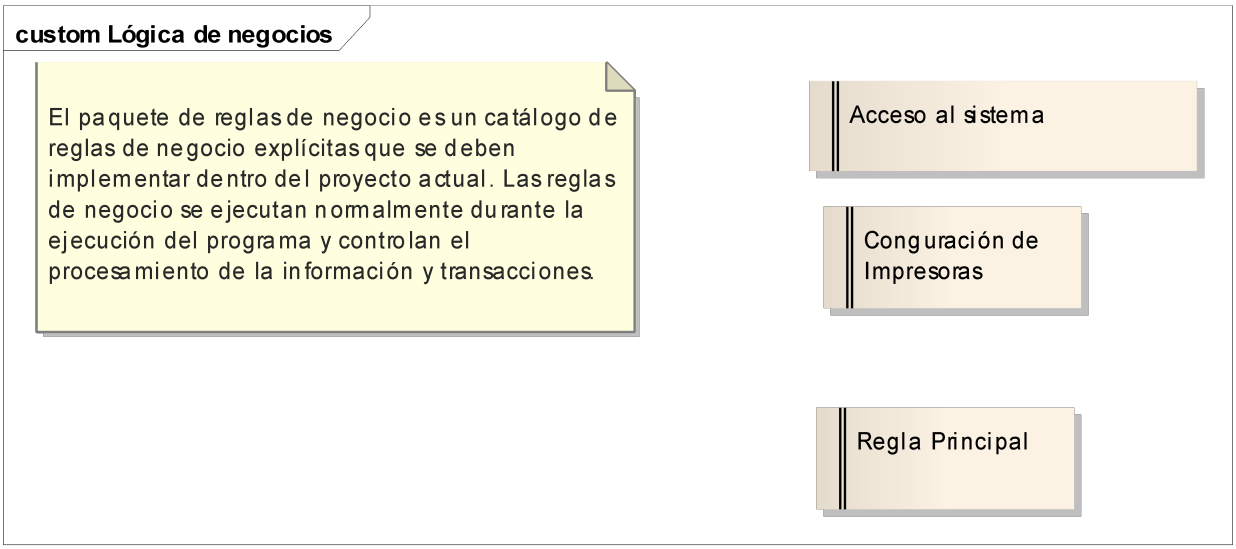


Imagen: 17

Acceso al sistema
Tipo: Requisito__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Reglas de negocio *Palabras claves:*
Detalle: *Creado el* 20/11/2005. *Última modificación el 13/10/2010*.
GUID: {E319B760-E66E-4788-9098-3CC0501D3F01}

Se realizará un control de acceso de usuario al sistema, en donde se evaluará el nivel de acceso que posee el usuario y mediante le mismo se le restringirá el acceso a los procedimiento cuyo nivel no sea el adecuado.

Configuración de Impresoras
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Reglas de negocio *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {3B38BCD9-8266-4ad4-AFCC-88DB2FD5B710}

Componente de impresión del sistema operativo

Regla Principal
Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Reglas de negocio *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {393F384C-A5F5-4232-94AC-F66DFEA3283E}

Deberá estar cargadas los parámetros del sistemas antes de comenzar la fase I del AGR.

Características
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 20/11/2005. Última modificación el 20/11/2005*
GUID: {98B74557-DBA9-44a6-BB02-1B78014BF42A}
El paquete de características contiene

Características - *(diagrama Personalized)*
Creado por: caballerosd el 20/11/2005
Última modificación: 11/01/2006
Versión: 1.0. *Bloqueado:* Falso
GUID: {3E23CB1B-193C-49bc-AE1E-6BCB16108726}

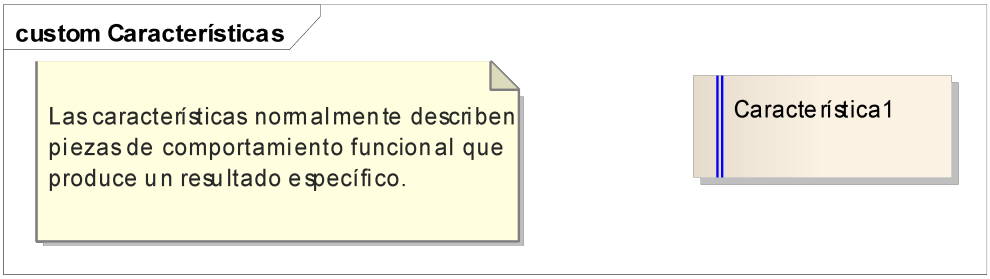


Imagen: 18

Característica1
Tipo: Característica__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Características *Palabras claves:*
Detalle: *Creado el* 20/11/2005. *Última modificación el 20/11/2005*.
GUID: {7811593A-4308-49bf-B4B2-88D7BE5C1FA9}

Propiedades Personalizadas

- isStatic = Falso

Interfaz de usuario
Tipo: **Paquete**
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Requisitos funcionales
Detalle: *Creado el 19/11/2005. Última modificación el 19/11/2005*
GUID: {9BC8FE71-404F-4c84-9CF6-BB22DA4D25A7}

Interfaz de usuario - *(diagrama Personalizado)*
Creado por: caballerosd el 11/01/2006
Última modificación: 13/10/2010
Versión: 1.0. *Bloqueado:* Falso
GUID: {76EC4CFE-1E43-4bfe-8855-BE866766A143}

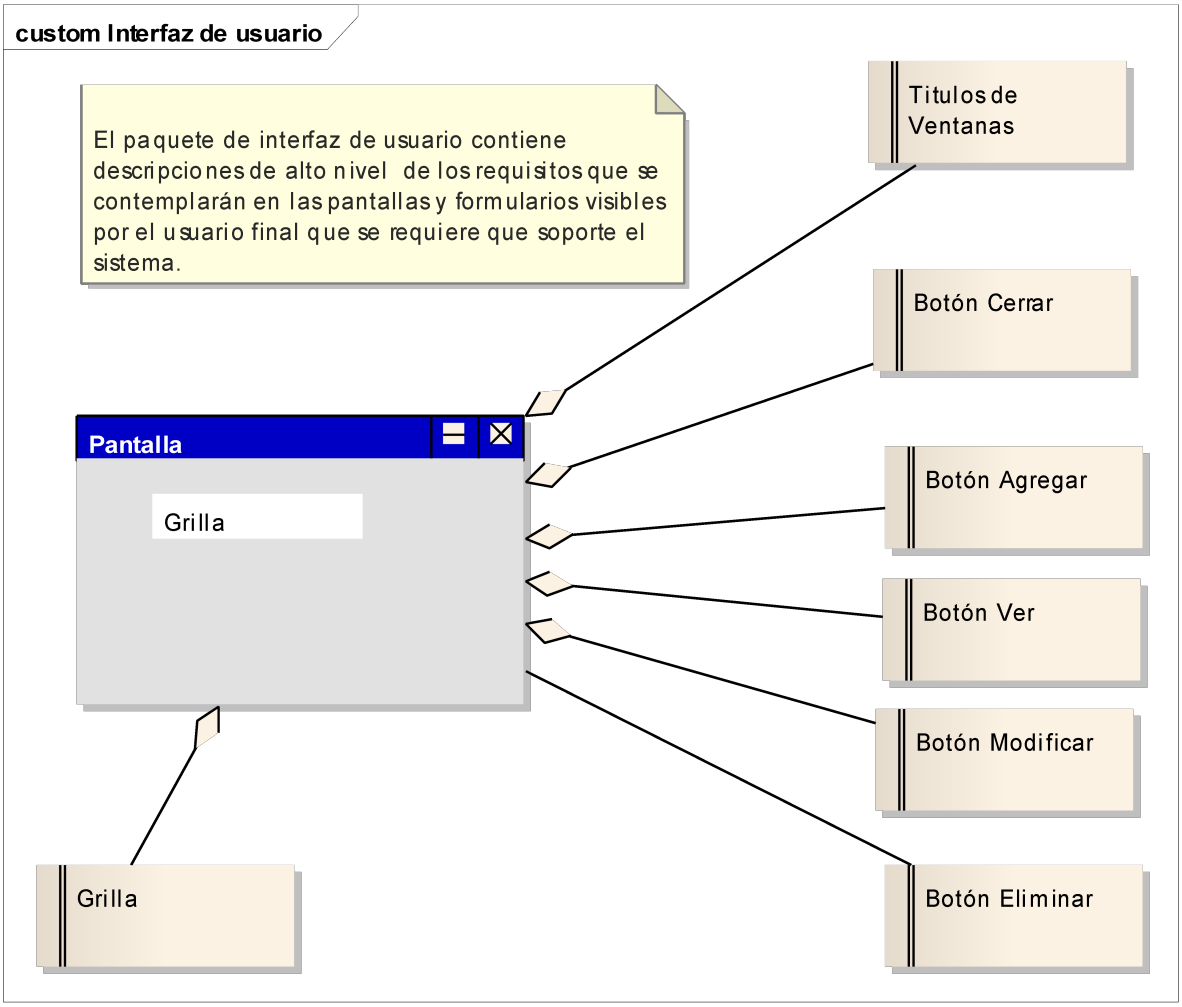


Imagen: 19

Pantalla

Tipo: Pantalla__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010.*
GUID: {379E9E94-B99D-4e97-8C4F-00796CBB6F7B}

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Títulos de Ventanas	Public Pantalla	
Aggregation_ Origen -> Destino	Public Botón Cerrar	Public Pantalla	
Aggregation_ Origen -> Destino	Public Botón Agregar	Public Pantalla	

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Botón Ver	Public Pantalla	
Aggregation_ Origen -> Destino	Public Botón Modificar	Public Pantalla	
Aggregation_ Origen -> Destino	Public Grilla	Public Pantalla	
Asociación_ Sin especificar	Public Botón Eliminar	Public Pantalla	

Grilla

Tipo: ElementoDeGUI__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {CB077F66-0EBA-4f0c-AECB-5DEA9CC956EB}

Botón Agregar

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {5DD9D148-E2E6-463a-A576-54909ED8CD14}

Para agregar registro el sistema tendrá un botón denominado "Agregar" con el mismo icono para todo el sistema

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Botón Agregar	Public Pantalla	

Botón Cerrar

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {6D253A14-1AFC-4bdc-889D-26A1A3ACE4F8}

Se utilizará el botón Cerrar con un icono de una "X" y cerrar las ventanas.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Botón Cerrar	Public Pantalla	

Botón Eliminar

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {07CD2E6F-4916-420c-8BF5-CE268C059D97}

Para borrar un registro el sistema tendrá un botón denominado "Eliminar" con el mismo icono para todo el sistema

Conexiones

Connector	Origen	Destino	Notas
Asociación_ Sin especificar	Public Botón Eliminar	Public Pantalla	

Botón Modificar

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {42B6DC87-75C6-4ff3-9661-27AC1D819640}

Para modificar un registro el sistema tendrá un botón denominado "Modificar" con el mismo icono para todo el sistema

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Botón Modificar	Public Pantalla	

Botón Ver

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {C00E1C8C-BBCD-41d1-90F2-1A0C0C7D8961}

Para ingresar a un formulario en modo de solo lectura, se deberá incluir en el sistema en un botón cuya descripción se "Ver" con el mismo icono para todo el sistema.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Botón Ver	Public Pantalla	

Grilla

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {44F9908B-CAD5-493c-B548-0F76A87DD9B7}

Los Browse poseerán por lo menos una etiqueta con el nombre de la clave o índice de ordenamiento.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Grilla	Public Pantalla	

Títulos de Ventanas

Tipo: Requisito__
Estado: . *Versión* 1.0. *Fase* 1.0.
Paquete: Interfaz de usuario *Palabras claves:*
Detalle: *Creado el* 13/10/2010. *Última modificación el 13/10/2010*.
GUID: {8F51672C-EB3B-4b64-BFAE-2C8E14E24E4A}

Los títulos de las ventas deberán describir acción - descripción de datos . Ej. Alta Personas.

Conexiones

Connector	Origen	Destino	Notas
Aggregation_ Origen -> Destino	Public Titulos de Ventanas	Public Pantalla	

Modelo de Casos de Uso

Tabla de Contenidos

1.1 Limites del Sistema.....
1.1.1 Administrador.....
1.1.2 Equipo.....
1.1.3 Usuario Centro Cómputos.....
1.1.4 ANG.....
1.1.5 Incidencias.....
1.1.6 Informes.....
1.1.7 parámetros.....
1.1.8 Seguimientos.....
1.2 Análisis y Gestión de Riesgos.....
1.2.1 Etapa 1 - Inventario de Activos.....
1.2.1.1 Dependencia.....
1.2.1.1.1 Alta Dependencia.....
1.2.1.1.2 Baja Dependencia.....
1.2.1.1.3 Modificación Dependencia.....
1.2.1.2 Elementos de los Activos.....
1.2.1.2.1 Alta Elemento.....
1.2.1.2.2 Baja de Elemento.....
1.2.1.2.3 Control de Activo.....
1.2.1.2.4 Modificación de Elemento.....
1.2.1.3 Fuente de Información.....
1.2.1.3.1 Alta Activo por Fuente de Información.....
1.2.1.3.2 Baja Activo por Fuente de Información.....
1.2.1.3.3 Modificación Activo por Fuente de Información.....
1.2.1.4 Gestión de activos.....
1.2.1.4.1 Alta Activos.....
1.2.1.4.2 Baja Activos.....
1.2.1.4.3 Modificación Activos.....
1.2.2 Etapa 2 - Propósitos y Objetivos.....
1.2.2.1 Gestión de Proyecto.....
1.2.2.1.1 Alta.....
1.2.2.1.2 Alta propósitos y Objetivos.....
1.2.2.1.3 Alta Proyecto.....
1.2.2.1.4 Alta seleccionar Activos.....
1.2.2.1.5 Asignar Activos.....
1.2.2.1.6 Baja.....
1.2.2.1.7 Baja Seleccionar Activos.....
1.2.2.1.8 Baja Proyecto.....
1.2.2.1.9 Modificación.....
1.2.2.1.10 Modificación Proyecto.....
1.2.2.1.11 Modificación seleccionar Activos.....
1.2.2.1.12 propósitos y Objetivos.....
1.2.3 Etapa 3 - Equipo de Trabajo.....
1.2.3.1 Gestión de Equipo.....
1.2.3.1.1 Alta Asignación de Persona al proyecto.....
1.2.3.1.2 Asignar Personas al Proyecto.....
1.2.3.1.3 Baja Asignación de Persona al proyecto.....
1.2.3.1.4 Modificación Asignación de Persona al proyecto.....
1.2.3.1.5 Seleccionar Proyecto.....
1.2.3.2 Personas.....
1.2.3.2.1 Equipo.....

1.2.3.2.1.1 Alta Equipo.....
1.2.3.2.1.2 Baja Equipo.....
1.2.3.2.1.3 Modificación Equipo.....
1.2.3.2.2 Personal.....
1.2.3.2.2.1 Alta Persona.....
1.2.3.2.2.2 Baja Persona.....
1.2.3.2.2.3 Modificación Persona.....
1.2.3.2.3 Rol.....
1.2.3.2.3.1 Alta Rol.....
1.2.3.2.3.2 Baja Rol.....
1.2.3.2.3.3 Modificación Rol.....
1.2.4 Etapa 4 - Taxonomía.....
1.2.4.1 Amenazas por Tipo de Activo.....
1.2.4.1.1 Agregar Elemento y Fuente de información.....
1.2.4.1.2 Mostrar Taxonomía.....
1.2.4.1.3 Procesar Taxonomía.....
1.2.4.2 Elementos de la Taxonomía.....
1.2.4.2.1 Alta Elemento de Taxonomía.....
1.2.4.2.2 Baja Elemento de Taxonomía.....
1.2.4.2.3 Modificación Elemento de Taxonomía.....
1.2.5 Etapa 5 - Declaración.....
1.2.5.1 Agregar Declaración.....
1.2.5.2 Mostrar Riesgos.....
1.2.5.3 Procesar Riesgo.....
1.2.6 Etapa 6 - Estimación de Probabilidad e impacto.....
1.2.6.1 Estimación de Probabilidad - Impacto.....
1.2.6.1.1 Agregar Probabilidad - Impacto.....
1.2.6.1.2 Mostrar Riesgos.....
1.2.6.2 Impacto.....
1.2.6.2.1 Alta Impacto.....
1.2.6.2.2 Baja Impacto.....
1.2.6.2.3 Modificación Impacto.....
1.2.6.3 Probabilidad de Ocurrencia.....
1.2.6.3.1 Alta Probabilidad de Ocurrencia.....
1.2.6.3.2 Baja Probabilidad de Ocurrencia.....
1.2.6.3.3 Modificación Probabilidad de Ocurrencia.....
1.2.7 Etapa 7 - Exposición.....
1.2.7.1 Exportar.....
1.2.8 Etapa 8 - Gestión de los Riesgos.....
1.2.8.1 Gestión.....
1.2.8.1.1 Alta Pasos a Seguir.....
1.2.8.1.2 Alta Plan de Acción.....
1.2.8.1.3 Alta Plan de Contingencias.....
1.2.8.1.4 Asignar Recurso.....
1.2.8.1.5 Asignar Responsable.....
1.2.8.1.6 Baja Disparador.....
1.2.8.1.7 Baja Pasos a seguir.....
1.2.8.1.8 Baja Plan de Acción.....
1.2.8.1.9 Baja Plan de Contingencias.....
1.2.8.1.10 Cargar Información.....
1.2.8.1.11 Detalle de la Gestión.....
1.2.8.1.12 Disparador.....
1.2.8.1.13 Disparador.....
1.2.8.1.14 Generar plan de acción total.....
1.2.8.1.15 importancia.....
1.2.8.1.16 Modificación Disparador.....

1.2.8.1.17 Modificación Pasos a seguir.....
1.2.8.1.18 Modificación Plan de Acción.....
1.2.8.1.19 Modificación Plan de Contingencias.....
1.2.8.1.20 Muestra Riesgos.....
1.2.8.1.21 Pasos a seguir.....
1.2.8.2 Información.....
1.2.8.2.1 Alta Información.....
1.2.8.2.2 Baja Información.....
1.2.8.2.3 Modificación Información.....
1.2.8.3 Recursos.....
1.2.8.3.1 Alta Recursos.....
1.2.8.3.2 Baja Recursos.....
1.2.8.3.3 Modificación Recursos.....
1.3 Incidencias.....
1.3.1 Carga el Incidente.....
1.3.2 Terminar incidentes.....
1.4 Informes.....
1.4.1 Estadística.....
1.4.2 Riesgos por Incidente.....
1.4.3 Seguimiento Terminados.....
1.5 parámetros.....
1.5.1 Activos.....
1.5.1.1 Dimensión.....
1.5.1.1.1 Alta Dimensión.....
1.5.1.1.2 Baja Dimensión.....
1.5.1.1.3 Modificación Dimensión.....
1.5.1.2 Elementos.....
1.5.1.2.1 Alta Elementos.....
1.5.1.2.2 Baja Elementos.....
1.5.1.2.3 Modificación Elementos.....
1.5.1.3 Tipos de Activos.....
1.5.1.3.1 Alta Tipos de Activo.....
1.5.1.3.2 Baja Tipos de Activo.....
1.5.1.3.3 Modificación Tipos de Activo.....
1.5.1.4 Valoración.....
1.5.1.4.1 Alta Valoración.....
1.5.1.4.2 Baja Valoración.....
1.5.1.4.3 Modificación Valoración.....
1.5.2 Amenazas.....
1.5.2.1 Dimensión.....
1.5.2.1.1 Alta Amenazas por dimensión.....
1.5.2.1.2 Baja Amenazas por dimensión.....
1.5.2.1.3 Modificación Amenaza por dimensión.....
1.5.2.2 Gestión de Amenazas.....
1.5.2.2.1 Alta Amenazas.....
1.5.2.2.2 Baja Amenazas.....
1.5.2.2.3 Modificación Amenazas.....
1.5.2.3 Tipos.....
1.5.2.3.1 Alta Tipos de Amenazas.....
1.5.2.3.2 Baja Tipos de Amenazas.....
1.5.2.3.3 Modificación Tipos de Amenazas.....
1.5.2.4 Tipos de Activos.....
1.5.2.4.1 Alta Amenazas x tipo Activo.....
1.5.2.4.2 Baja Amenazas por tipo de activo.....
1.5.2.4.3 Modificación Amenaza por tipo de activo.....
1.5.3 Empresa.....

1.5.3.1 Alta Empresa.....
1.5.3.2 Baja Empresa.....
1.5.3.3 Modificación Empresa.....
1.5.4 Fuente Información.....
1.5.4.1 Alta Fuente Información.....
1.5.4.2 Baja Fuentes de información.....
1.5.4.3 Modificación Fuente de información.....
1.5.5 Medidas de Tiempo.....
1.5.5.1 Alta Medidas de Tiempo.....
1.5.5.2 Baja Medidas de Tiempo.....
1.5.5.3 Modificación Medidas de Tiempo.....
1.5.6 Salvaguardas.....
1.5.6.1 Alta Salvaguarda.....
1.5.6.2 Alta Salvaguarda por Dimensión.....
1.5.6.3 Asignar Dimensión a la Salvaguarda.....
1.5.6.4 Baja Salvaguardas.....
1.5.6.5 Baja Salvaguardas por Dimensión.....
1.5.6.6 Modificación Salvaguardas.....
1.5.6.7 Modificación Salvaguardas por Dimensión.....
1.5.7 Usuarios.....
1.5.7.1 Alta Usuario.....
1.5.7.2 Baja Usuarios.....
1.5.7.3 Modificación Usuario.....
1.6 Seguimiento.....
1.6.1 Agenda Personal.....
1.6.2 Gestión Trabajos de Seguimiento.....
1.6.3 Plan de Seguimiento.....

Casos de Uso

1 Modelo de casos de uso

1.1 Limites del Sistema

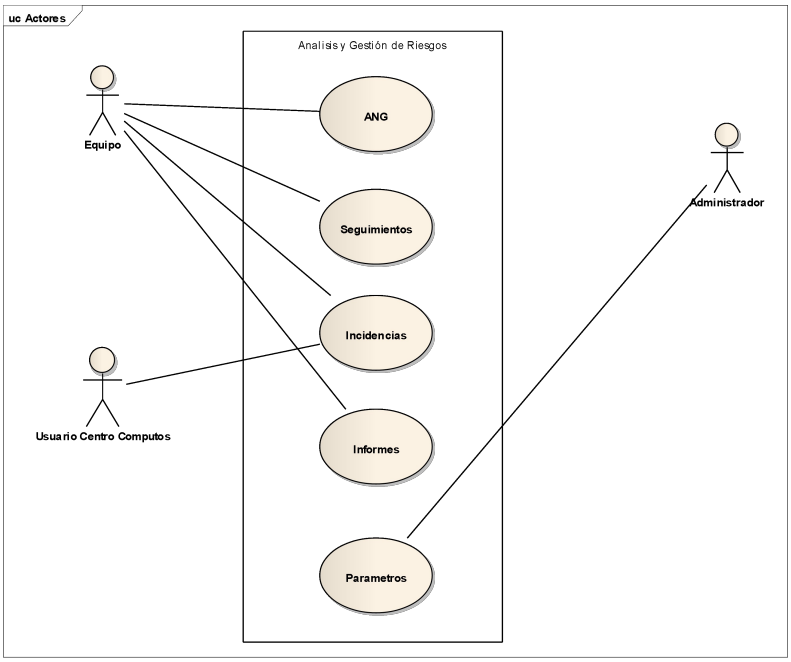


Imagen 1: Actores

1.1.1 Administrador

Administrador del Sistema. Nivel total de acceso al mismo.
Es el encargado de cargas y gestionar los parámetros del sistema.

Invariant *Estado:* Approved

Nivel Mayor de usuario. Acceso total al sistema

1.1.2 Equipo

Miembros del equipo de Análisis y gestión de Riesgos.

Invariant *Estado:* Approved

Deben Poseer nivel de usuario para poder gestionar los riesgos, seguimiento e informes.

1.1.3 Usuario Centro Cómputos

Usuarios de los activos tecnológicos de la organización con conocimientos del modelo de AGR.

Pueden cargar las incidencias.-

1.1.4 ANG

Análisis y Gestión de Riesgos

1. Inventarios de activos
2. Propósitos y Objetivos
3. Equipo de trabajo
4. Taxonomía
5. Declaración
6. Estimación de la Probabilidad
7. Estimación del Impacto
8. Exposición al Riesgo
9. Gestión de Riesgos.

PRE-condición *Estado:* Approved

Deben estar cargados todos los parámetros del sistema Previamente

1.1.5 Incidencias

Carga de Incidencias (problemas encontrados sobre un activo)
Gestión de la incidencia por parte del equipo.

1.1.6 Informes

- Seguimientos

1. Terminados
2. Activos

- Incidentes

1. Riesgos por incidente
2. Estadísticas.

1.1.7 parámetros

Parámetros del Sistema

1.1.8 Seguimientos

Seguimiento de los Planes de acción generados en la gestión de los riesgos.
Gestiona las actividades de los usuarios encargados de los seguimientos por amenazadas detectadas por activo.

PRE-condición *Estado:* Approved

Deben estar cargados la gestión de riesgos y parametrizados las salvaguardas.

1.2 Análisis y Gestión de Riesgos

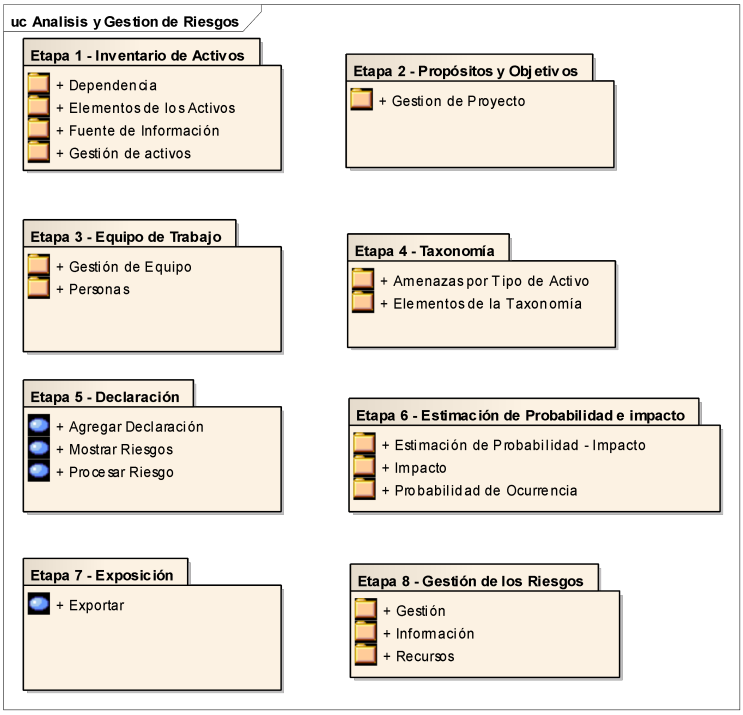


Imagen 2: Análisis y Gestión de Riesgos

1.2.1 Etapa 1 - Inventario de Activos

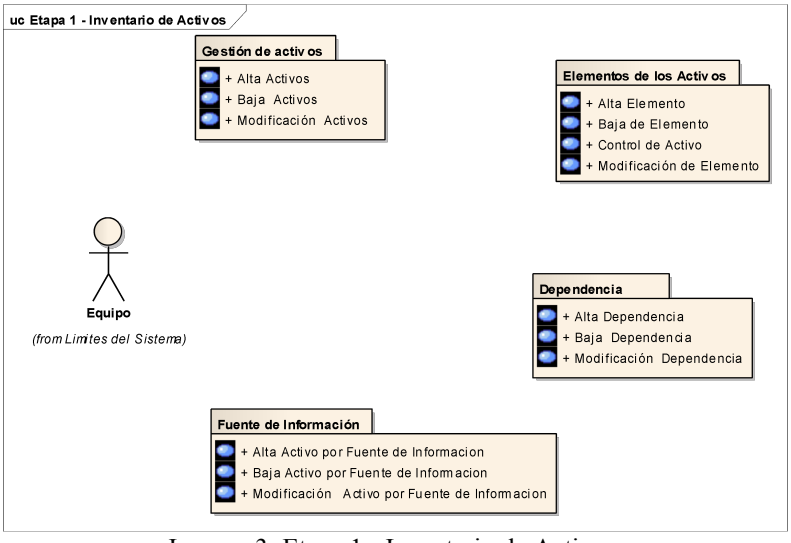


Imagen 3: Etapa 1 - Inventario de Activos

1.2.1.1 Dependencia

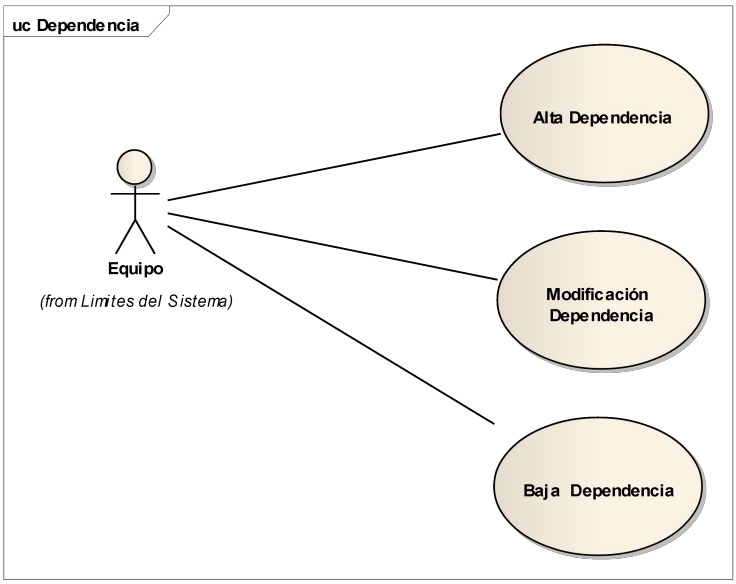


Imagen 4: Dependencia

1.2.1.1.1 Alta Dependencia

Gestión de Dependencia entre Activos

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona el activo padre y presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde se expresa el activo seleccionado y el usuario .puede cargar el ID del activo dependiente

Basic Path

Paso 3

El usuario cargar el dato y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved

.Debe Existir los activos

1.2.1.1.2 Baja Dependencia

Gestión de Dependencia entre Activos

Flujo de Eventos

Basic Path

Paso 1
El caso de uso comienza cuando el Usuario selecciona un activo, el sistema muestra en la grilla los activos dependientes y el usuario selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
.El usuario selecciona el botón Aceptar
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo .puede hacer informa al usuario

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.1.1.3 Modificación Dependencia

Gestión de Dependencia entre Activos

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un activo, el sistema muestra los registros de dependencia,, el usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
.El sistema muestra una ventana en donde el usuario puede modificar los datos
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.1.2 Elementos de los Activos

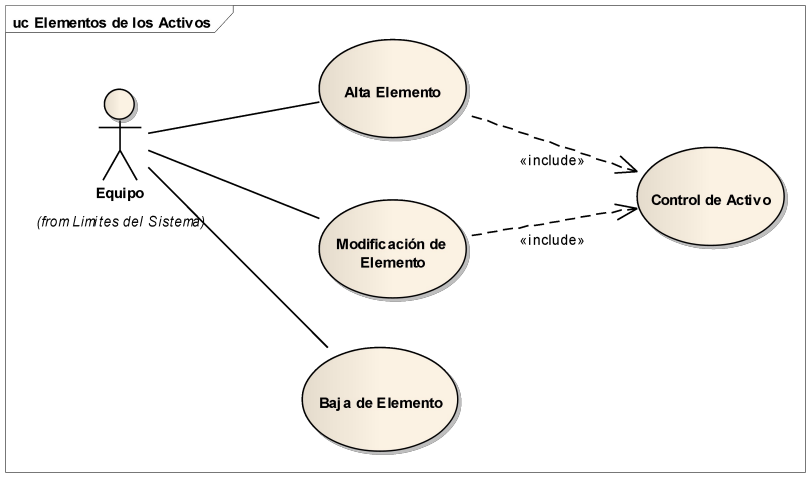


Imagen 5: Elementos de los Activos

1.2.1.2.1 Alta Elemento

Flujo de Eventos

Basic Path

Paso 1

.El caso de uso comienza cuando el usuario presiona el botón nuevo de la grilla

Basic Path

Paso 2

El sistema muestra la ventana en donde se cargarán el Nº del activo y se ejecutará el caso de uso Control Activo, luego se seleccionará un Tipo de activo y un elemento .del tipo de activo

Basic Path

Paso 3

.El usuario selecciona le Activo, el tipo de activo y el elemento y presiona aceptar

Basic Path

Paso 4

El sistema controla que los datos sean completos y correctos y guarda en la Base de .datos

Invariant *Estado:* Approved

.Deben existir la instancia elemento por tipo de activo. Paquete Elementos

1.2.1.2.2 Baja de Elemento

Gestiona los activos de la organización

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la

eliminación del registro
Basic Path
Paso 3
.El usuario selecciona el botón Aceptar
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos
Alternate
Si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.1.2.3Control de Activo

El caso de uso posee como funcionalidad el filtrar para el Activo seleccionado a que tipo de activo corresponde y por cada tipo de activo los elementos correspondientes a este.

1.2.1.2.4Modificación de Elemento

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el usuario selecciona un registro de la grilla y presiona
.el botón modificar
Basic Path
Paso 2
El sistema muestra los datos cargados para ese Activo, en los cuales el usuario puede
.modificar los datos de los mismos
Basic Path
Paso 3
.El usuario modifica los datos y presiona Aceptar
Basic Path
Paso 4
El sistema ejecuta el caso de uso "Control de Activo" y guarda los datos en la base de
.datos. Y devuelve el control a la grilla

Invariant *Estado:* Approved
.Se debe seleccionar un registro de la grilla

1.2.1.3 Fuente de Información

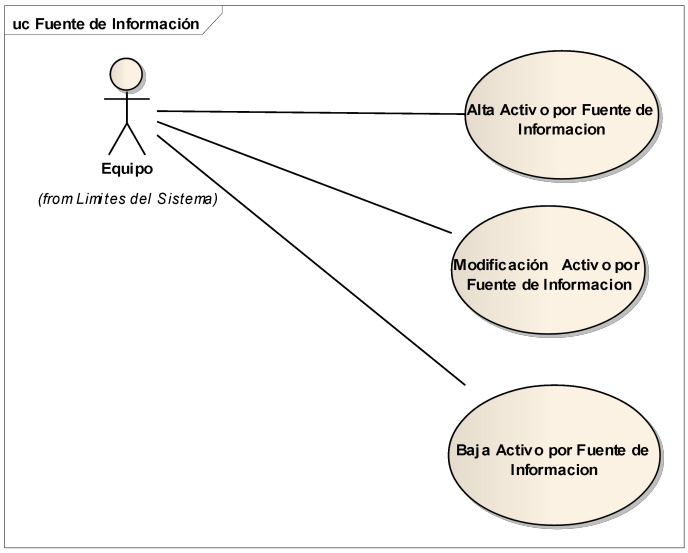


Imagen 6: Fuente de Información

1.2.1.3.1 Alta Activo por Fuente de Información

Gestiona los activos por la fuente de información de donde se recaba los mismos.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar el Id del Activo y el Id .de la fuente de información

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved

Debe Existir el Activo y la Fuente de Información

1.2.1.3.2 Baja Activo por Fuente de Información

Gestiona los activos por la fuente de información de donde se recaba los mismos.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
.El usuario selecciona el botón Aceptar
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo .puede hacer informa al usuario

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.1.3.3 Modificación Activo por Fuente de Información

Gestiona los activos por la fuente de información de donde se recaba los mismos.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
.El sistema muestra una ventana en donde el usuario puede modificar los datos
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.1.4 Gestión de activos

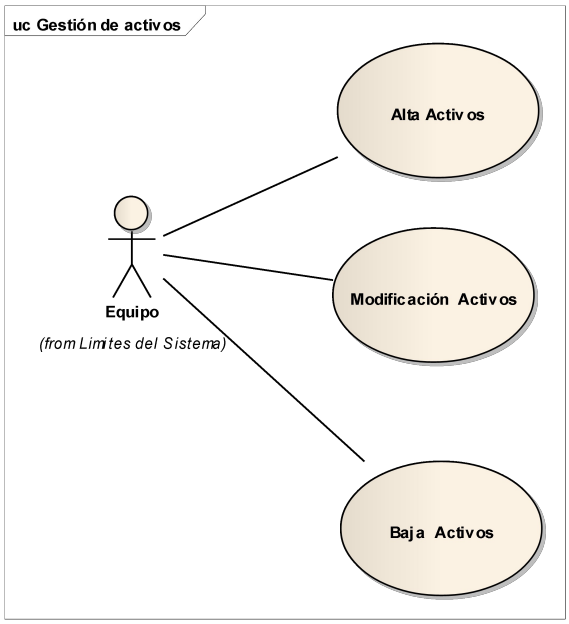


Imagen 7: Gestión de activos

1.2.1.4.1 Alta Activos

Gestiona los activos de la organización

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar el código, nombre, .descripción, contenido, propietario e importancia

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved

.Debe existir cargada la importancia en la base de datos

1.2.1.4.2 Baja Activos

Gestiona los activos de la organización

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a

Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
.El usuario selecciona el botón Aceptar
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo .puede hacer informa al usuario

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.1.4.3 Modificación Activos

Gestiona los activos de la organización

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
.El sistema muestra una ventana en donde el usuario puede modificar los datos
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.2 Etapa 2 - Propósitos y Objetivos

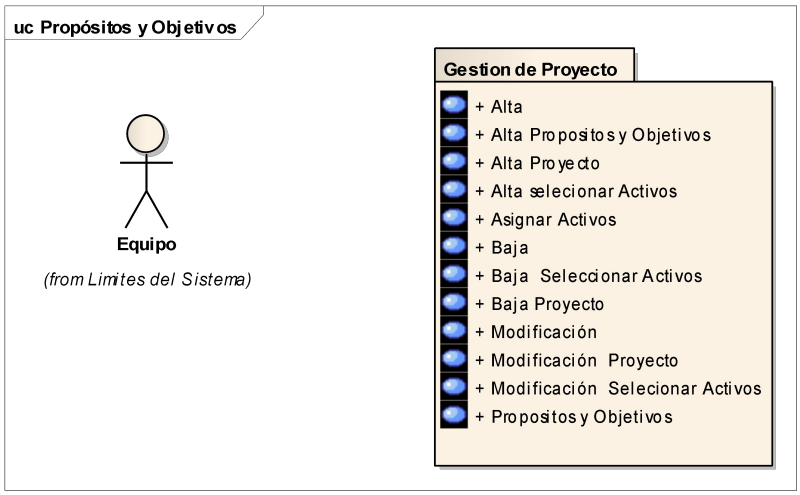


Imagen 8: Propósitos y Objetivos

1.2.2.1 Gestión de Proyecto

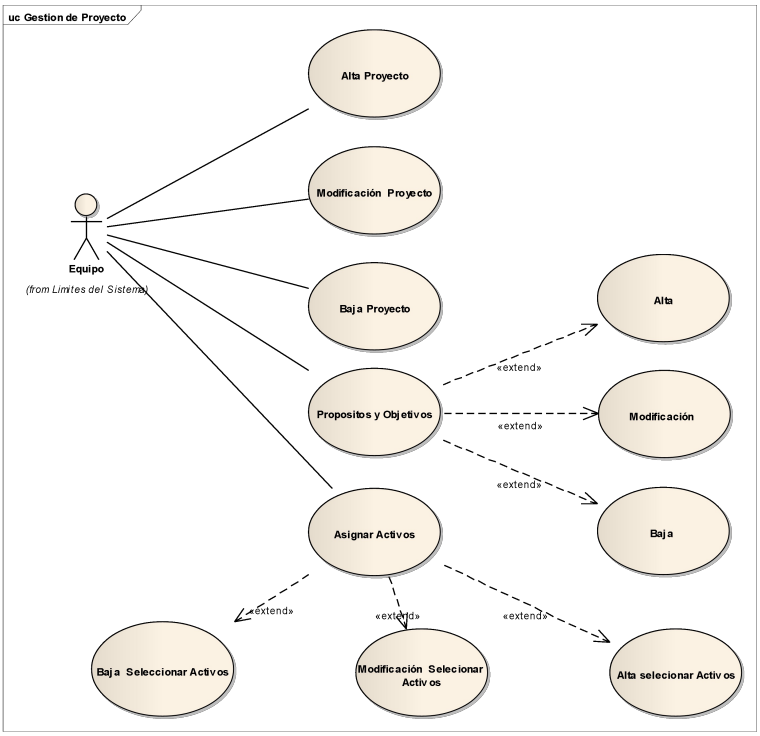


Imagen 9: Gestión de Proyecto

1.2.2.1.1 Alta

Gestiona los propósitos y Objetivos del proyecto seleccionado

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo en el caso de Uso
""propósitos y Objetivos
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el propósito, Objetivo
.general y limites
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego
.devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Debe existir el Dato de la Organización

1.2.2.1.2 Alta propósitos y Objetivos

1.2.2.1.3 Alta Proyecto

Gestiona los Proyectos

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el Propietario, código,
.nombre, descripción y seleccionar la empresa
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego
.devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Debe existir el Dato de la Organización

1.2.2.1.4 Alta seleccionar Activos

Gestiona los activos a asignar al proyecto seleccionado

Flujo de Eventos
Basic Path
Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo en el caso de Uso ""Asignar Activos
Basic Path
Paso 2
.El sistema muestra una ventana en donde el usuario puede cargar el Id del Activo
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar. El sistema corrobora que No .exista asignado ya el activo al proyecto
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

1.2.2.1.5Asignar Activos

Gestiona el Alta, Baja y Modificación de la selección de activos

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el usuario seleccionar un Proyecto y presiona el botón ""Asignar activos
Basic Path
Paso 2
El sistema abre una ventana en donde muestra los propósitos, objetivos y límites .cargados para ese Proyecto. Muestra los botones Nuevo, Modificar y Eliminar

1.2.2.1.6Baja

Gestiona los propósitos y Objetivos del proyecto seleccionado

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
.El usuario selecciona el botón Aceptar
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo .puede hacer informa al usuario

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.2.1.7Baja Seleccionar Activos

Gestiona los activos a asignar al proyecto seleccionado

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

.El usuario selecciona el botón Aceptar

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo .puede hacer informa al usuario

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.2.1.8Baja Proyecto

Gestiona los Proyectos

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

.El usuario selecciona el botón Aceptar

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo .puede hacer informa al usuario

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.2.1.9Modificación

Gestiona los propósitos y Objetivos del proyecto seleccionado

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
.El sistema muestra una ventana en donde el usuario puede modificar los datos
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.2.1.10 Modificación Proyecto

Gestiona los Proyectos

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
.El sistema muestra una ventana en donde el usuario puede modificar los datos
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.2.1.11 Modificación seleccionar Activos

Gestiona los activos a asignar al proyecto seleccionado

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path

Paso 2
.El sistema muestra una ventana en donde el usuario puede modificar los datos
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego
.devuelve el control a la pantalla grilla

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.2.1.12 propósitos y Objetivos

Gestiona el Alta, Baja y Modificación de los propósitos y objetivos para el Proyecto.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el usuario seleccionar un Proyecto y presiona el botón
""propósitos y Objetivos
Basic Path
Paso 2
El sistema abre una ventana en donde muestra los propósitos, objetivos y límites cargados para ese Proyecto. Muestra los botones Nuevo, Modificar y Eliminar.

Invariant *Estado:* Approved
.Debe existir el proyecto

1.2.3 Etapa 3 - Equipo de Trabajo

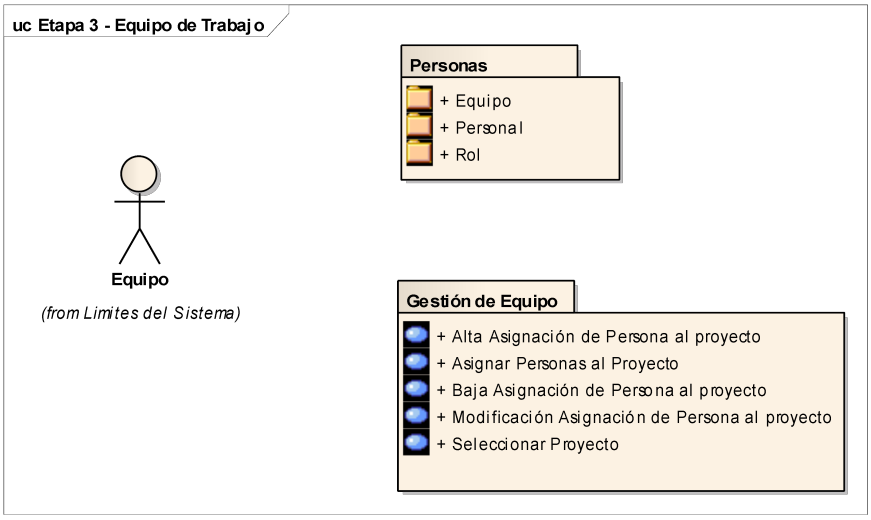


Imagen 10: Etapa 3 - Equipo de Trabajo

1.2.3.1 Gestión de Equipo

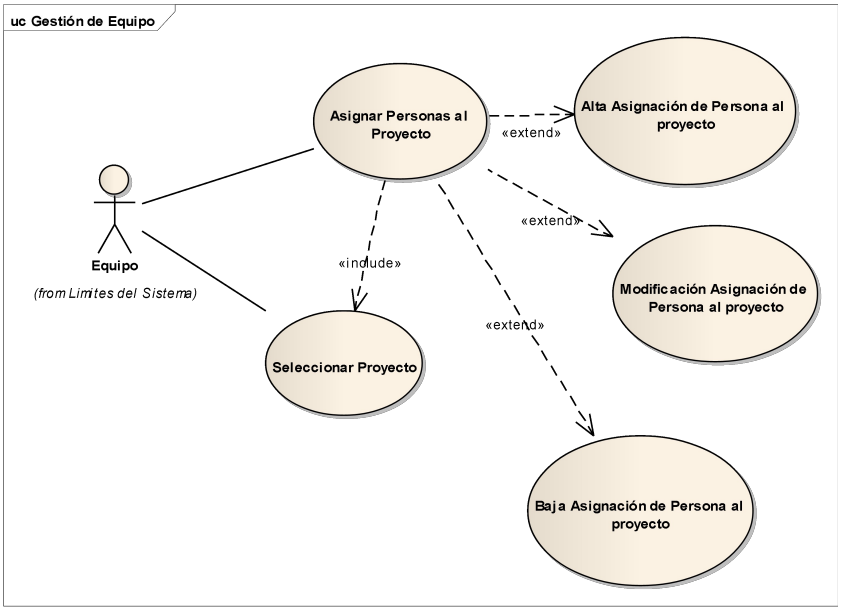


Imagen 11: Gestión de Equipo

1.2.3.1.1 Alta Asignación de Persona al proyecto

Adiciona personas al Proyecto

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde se muestra el Id del Proyecto y el usuario .puede cargar el Id Persona, Id Equipo y Id Rol

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego .devuelve el control a la pantalla grilla

Invariant *Estado:* Approved

"Debe haber seleccionado un Proyecto. Caso de Uso "Seleccionar Proyecto

1.2.3.1.2 Asignar Personas al Proyecto

Asigna Personas al Proyecto

Flujo de Eventos

Basic Path

Paso 1. El caso de uso comienza cuando el usuario presiona el botón "Asignar personas al proyecto"

Basic Path

Paso 2. El sistema muestra una ventana en donde se muestra las personas asignadas al proyecto seleccionado en el Caso de Uso "Seleccionar Proyecto" y muestras los botones de Nuevo, Modificar o Borrar.

1.2.3.1.3 Baja Asignación de Persona al proyecto

Gestiona los Proyectos

Flujo de Eventos

Basic Path

Paso 1 El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2. El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3. El usuario selecciona el botón Aceptar.

Basic Path

Paso 4. El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

PRE-condición *Estado:* Approved

"Debe haber seleccionado un Proyecto. Caso de Uso "Seleccionar Proyecto

1.2.3.1.4 Modificación Asignación de Persona al proyecto

Modifica personas en un proyecto

Flujo de Eventos

Basic Path

Paso 1 El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2. El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path
Paso 3. El usuario modifica los datos y presiona el botón guardar

Basic Path
Paso 4. El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
"Debe haber seleccionado un Proyecto. Caso de Uso "Seleccionar Proyecto

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.3.1.5 Seleccionar Proyecto

Selecciona un Proyecto

Flujo de Eventos

Basic Path
Paso 1
.El caso de uso comienza cuando el usuario carga el Nº de proyecto
Basic Path
Paso 2
.El sistema corrobora que el ID ingresado exista y muestra el nombre del proyecto
Alternate
Sistema
Si el Id No existe el sistema muestra una lista de los datos del almacén proyectos para que el usuario elija una opción

PRE-condición *Estado:* Approved
.Deben existir proyectos

1.2.3.2 Personas

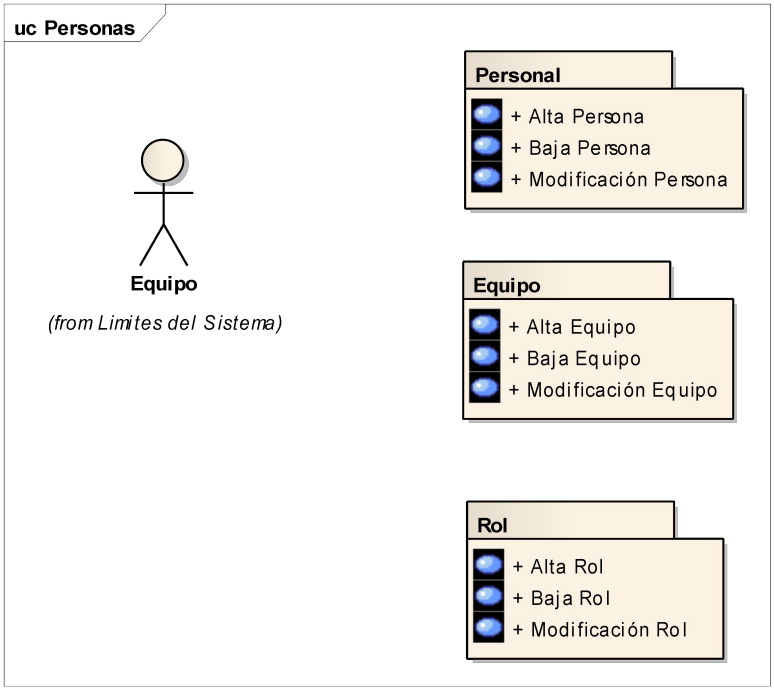


Imagen 12: Personas

1.2.3.2.1Equipo

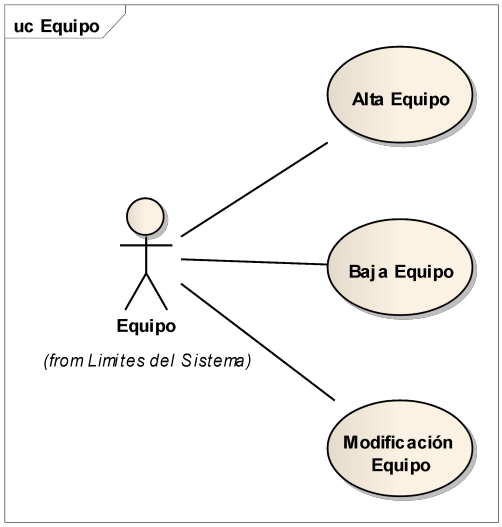


Imagen 13: Equipo

1.2.3.2.1.1 Alta Equipo

Gestión de Equipos del Proyecto

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el Nombre, descripción
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.2.3.2.1.2 Baja Equipo

Gestión de Equipos del Proyecto

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.3.2.1.3 Modificación Equipo

Gestión de Equipos del Proyecto

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.3.2.2Personal

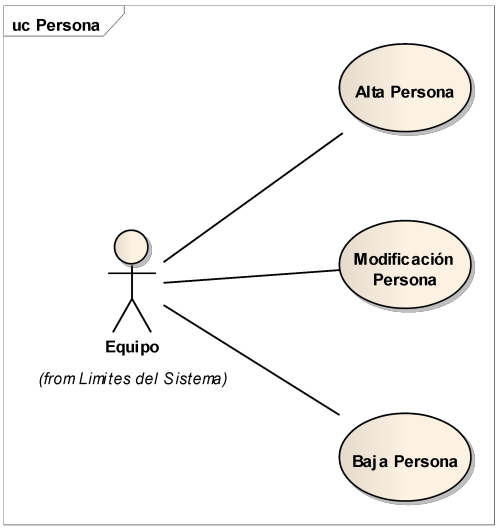


Imagen 14: Persona

1.2.3.2.2.1 Alta Persona

Gestión de Persona asignada al proyecto

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar el Nombre, email y tipo de personal

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.2.3.2.2.2 Baja Persona

Gestiona los Proyectos

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path
Paso 3
El usuario selecciona el botón Aceptar.

Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.3.2.2.3 Modificación Persona

Gestión de Persona asignada al proyecto

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Basic Path
Paso 2.
El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path
Paso 3.
El usuario modifica los datos y presiona el botón guardar

Basic Path
Paso 4.
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.3.2.3Rol

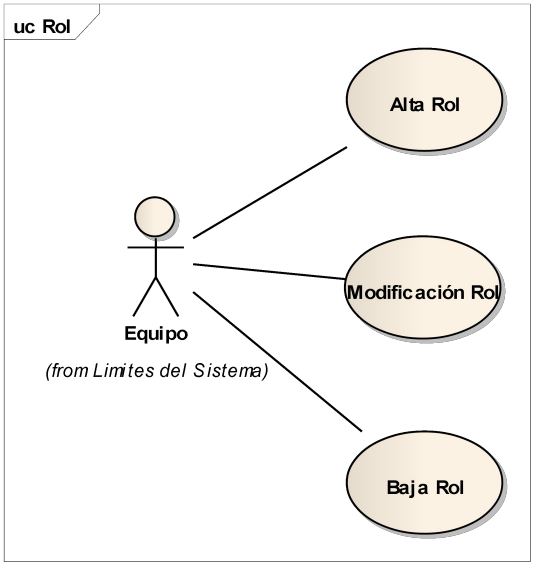


Imagen 15: Rol

1.2.3.2.3.1 Alta Rol

Gestión de Roles dentro del equipo en el Proyecto

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el Nombre, descripción
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.2.3.2.3.2 Baja Rol

Gestión de Roles dentro del equipo en el Proyecto

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path

Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.3.2.3.3 Modificación Rol

Gestión de Roles dentro del equipo en el Proyecto

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.4 Etapa 4 - Taxonomía

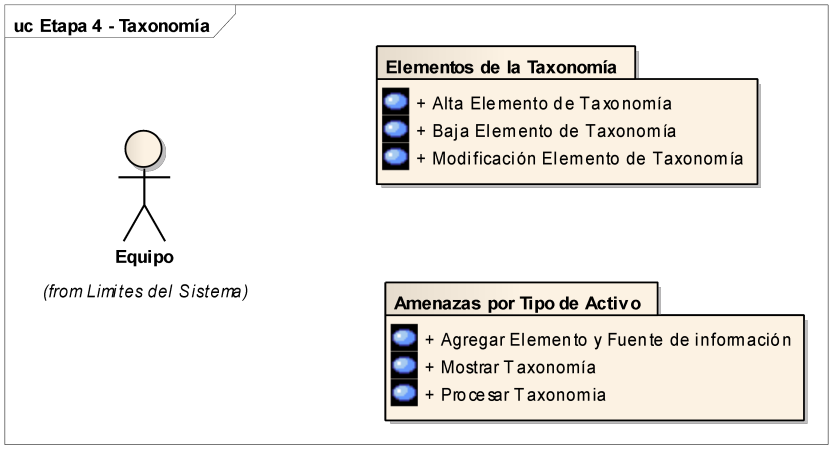


Imagen 16: Etapa 4 - Taxonomía

1.2.4.1 Amenazas por Tipo de Activo

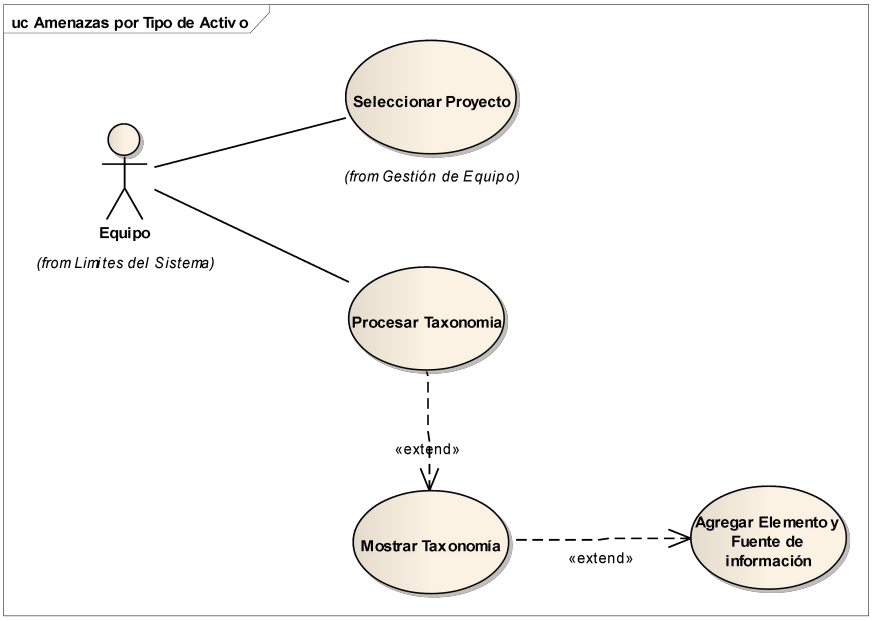


Imagen 17: Amenazas por Tipo de Activo

1.2.4.1.1 Agregar Elemento y Fuente de información

Agrega elemento y fuente de información a cada ítem de la taxonomía.
Una vez agregado Marca la taxonomía para diferenciar los Ítems completos y los incompletos.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el usuario selecciona un ítems y presiona la tecla "Asignar elemento y fuente de información"

Basic Path
Paso 2
El sistema abre una pantalla en la cual se cargan el ID de Elementos de la Taxonomía y Fuentes de información

Basic Path
Paso 3
El usuario carga los Id. luego presiona el botón Aceptar.

Basic Path
Paso 4
El sistema controla que los datos estén correctos y guarda la operación.

PRE-condición *Estado:* Approved
Deben Existir elementos en la grilla

PRE-condición *Estado:* Approved
"Deben existir los elementos de la taxonomía CU "Elementos de la Taxonomía

PRE-condición *Estado:* Approved
Debe existir la fuente de información

1.2.4.1.2 Mostrar Taxonomía

1º Muestra los resultados del proceso de taxonomía
Posee etiquetas de Orden:

- Amenaza
- Activo

Y Filtro muestra solo los Ítems "Completos"

2º Muestra una grilla relacionando los elementos del activo a casa ítems de taxonomía

1.2.4.1.3 Procesar Taxonomía

El caso de uso procesa la taxonomía según el proyecto elegido.
Recorre la base de datos de los activos del Proyecto, tipo de activo y amenaza y lo carga a un almacén de "taxonomía"
Al finalizar Muestra una grilla con los datos cargados en el almacén taxonomía.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el usuario presiona el botón "Procesar taxonomía"
Basic Path
Paso 2
El sistema recorre la base de Activos, filtrado por el proyecto seleccionado en donde carga en el almacén "taxonomía" los datos del proyecto, activos, tipo de activo y amenaza. Al terminar extiende al CU Mostrar Taxonomía.

PRE-condición *Estado:* Approved
Debe seleccionarse un proyecto

1.2.4.2 Elementos de la Taxonomía

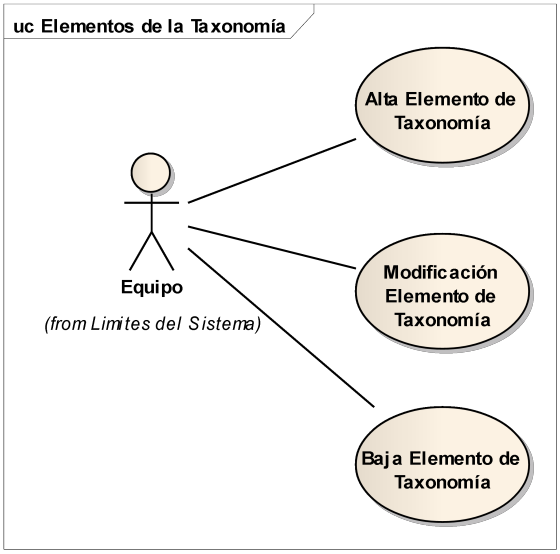


Imagen 18: Elementos de la Taxonomía

1.2.4.2.1 Alta Elemento de Taxonomía

Gestiona el Alta de los elementos ha ser referenciados en la Taxonomía.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar la descripción de los elementos.

Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar

Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.2.4.2.2 Baja Elemento de Taxonomía

Gestiona la baja los elementos ha ser referenciados en la Taxonomía.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.4.2.3 Modificación Elemento de Taxonomía

gestiona la modificación los elementos ha ser referenciados en la Taxonomía.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Alternate
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.5 Etapa 5 - Declaración

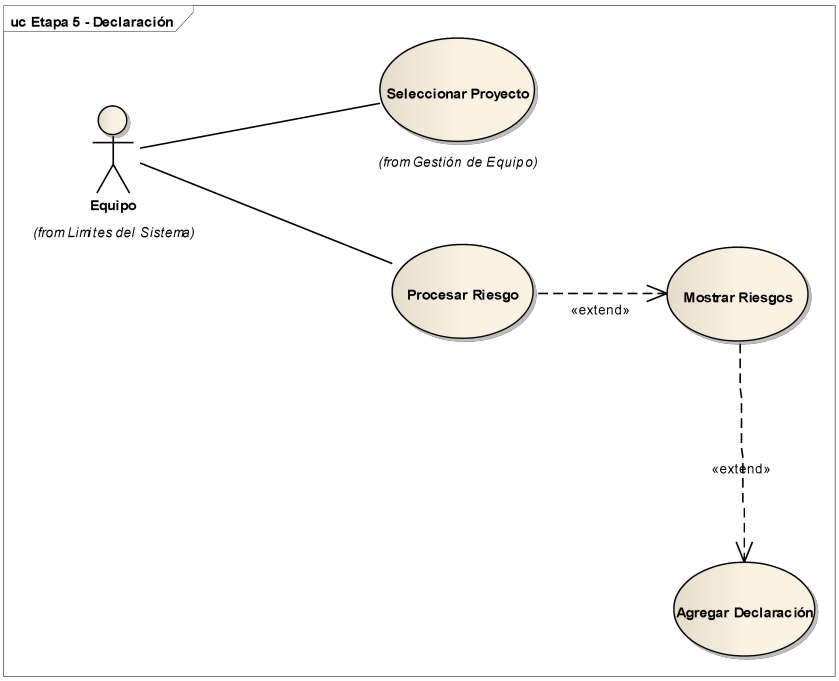


Imagen 19: Etapa 5 - Declaración

1.2.5.1 Agregar Declaración

Agrega la declaración de los riesgos.

- Condición
- Consecuencia
- Efecto.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el usuario selecciona un ítems y presiona la tecla "Agregar declaración"

Basic Path

Paso 2

El sistema abre una pantalla en la cual muestra los datos de la amenaza y sobre que activo impacta y los lugares para cargar la condición, consecuencia y efecto.

Basic Path

Paso 3

El usuario carga los datos y luego presiona el botón Aceptar.

Basic Path

Paso 4

El sistema controla que los datos estén correctos y guarda la operación.

PRE-condición *Estado:* Approved

Deben Existir elementos en la grilla

1.2.5.2 Mostrar Riesgos

Muestra los resultados del proceso de taxonomía
Posee etiquetas de Orden:

- Amenaza
- Activo

Y Filtro muestra solo los Ítems "Riesgos a Evaluar"

1.2.5.3 Procesar Riesgo

El caso de uso procesa los riesgos según el proyecto elegido.
Recorre el almacén de taxonomitas completas y lo carga al almacén de riesgos. Al finalizar Muestra una grilla con los datos cargados en el almacén taxonomía.
SI el Riesgo existe lo actualiza.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el usuario presiona el botón "Cargar Declaración"

Basic Path

Paso 2

El sistema recorre la base de taxonomía, filtrado por el proyecto seleccionado en donde carga en el almacén "taxonomía" y filtra los ítems completos y los carga al almacén Riesgos. Al terminar extiende al CU Mostrar Riesgos

PRE-condición *Estado:* Approved

Debe seleccionarse un proyecto

1.2.6 Etapa 6 - Estimación de Probabilidad e impacto

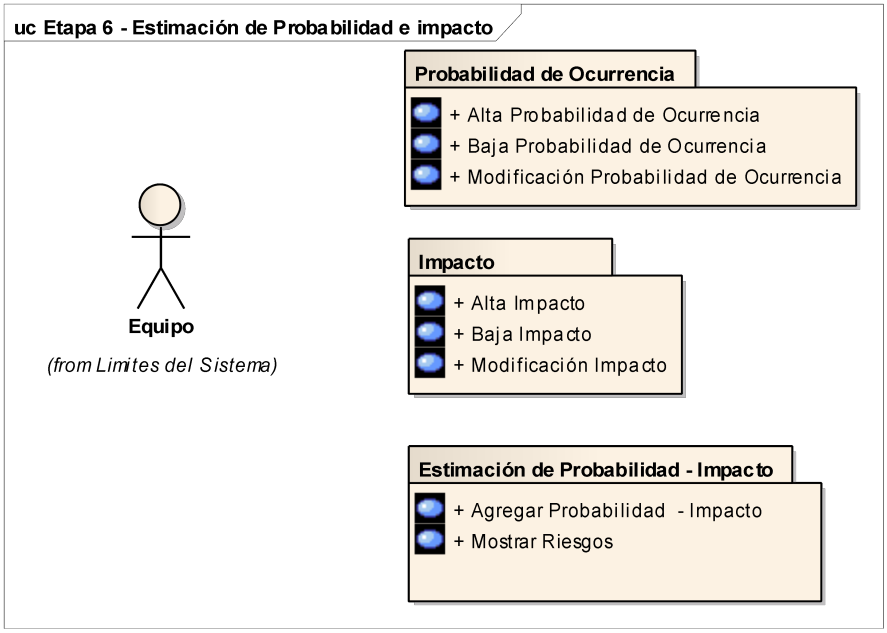


Imagen 20: Etapa 6 - Estimación de Probabilidad e impacto

1.2.6.1 Estimación de Probabilidad - Impacto

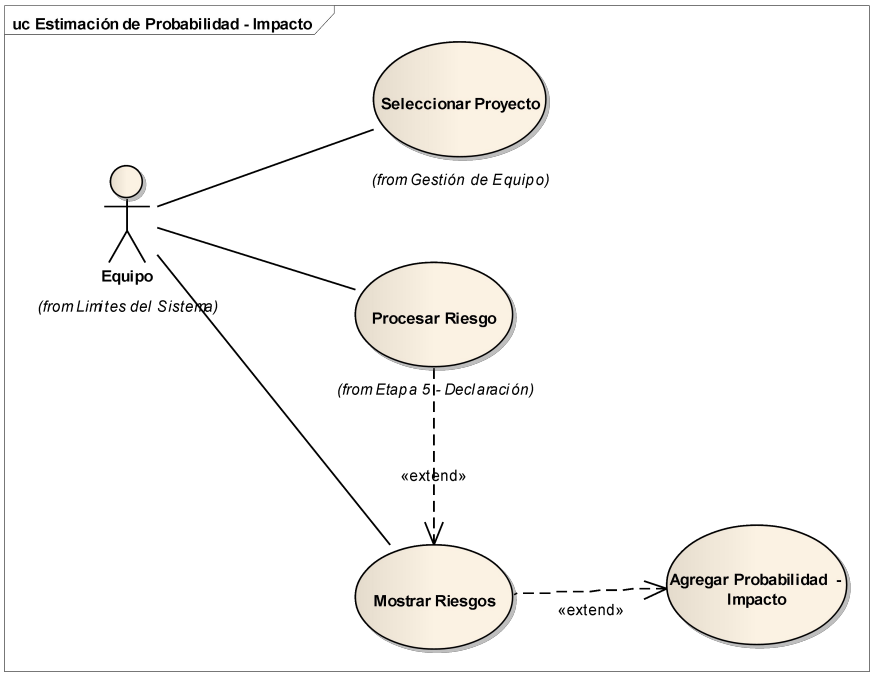


Imagen 21: Estimación de Probabilidad - Impacto

1.2.6.1.1 Agregar Probabilidad - Impacto

Agrega la declaración de los riesgos.

- % Probabilidad de Ocurrencia
- Valor del impacto Medio.

Muestra en los parámetros de probabilidad e impacto generados para el proyecto.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el usuario selecciona un ítems y presiona la tecla "Cargar Probabilidad - Impacto"

Basic Path
Paso 2
El sistema abre una pantalla en la cual muestra los datos de la amenaza y sobre que activo impacta y los lugares para cargar la % de Probabilidad y Valor del Impacto

Basic Path
Paso 3
El usuario carga los datos y luego presiona el botón Aceptar.

Basic Path
Paso 4
El sistema controla que los datos estén correctos y guarda la operación.

PRE-condición *Estado:* Approved
Deben Existir elementos en la grilla

Post-condición *Estado:* Approved
Los Valores de Probabilidad y de Impacto deben estar dentro del rango estipulado .para el proyecto

1.2.6.1.2Mostrar Riesgos

Muestra los resultados del CU "Procesar Riesgos"
Posee etiquetas de Orden:

- Amenaza
- Activo
- Probabilidad
- Impacto

Y Filtro muestra solo los Ítems "Riesgos a Evaluar"

1.2.6.2 Impacto

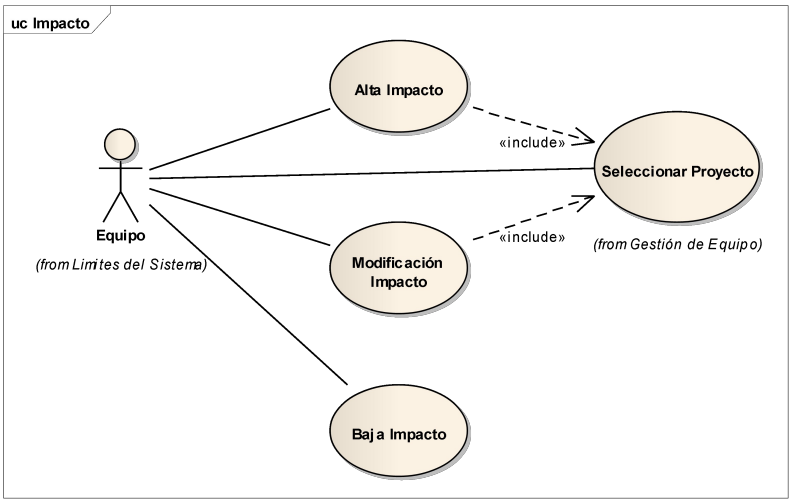


Imagen 22: Impacto

1.2.6.2.1 Alta Impacto

Gestión de Valores de Impacto sobre un proyecto.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar: Id del Proyecto, Criterio, retraso y Valor.

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

.Debe existir cargado los proyectos

1.2.6.2.2 Baja Impacto

Gestión de Valores de Impacto sobre un proyecto.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la

eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.6.2.3 Modificación Impacto

Gestión de Valores de Impacto sobre un proyecto.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.6.3 Probabilidad de Ocurrencia

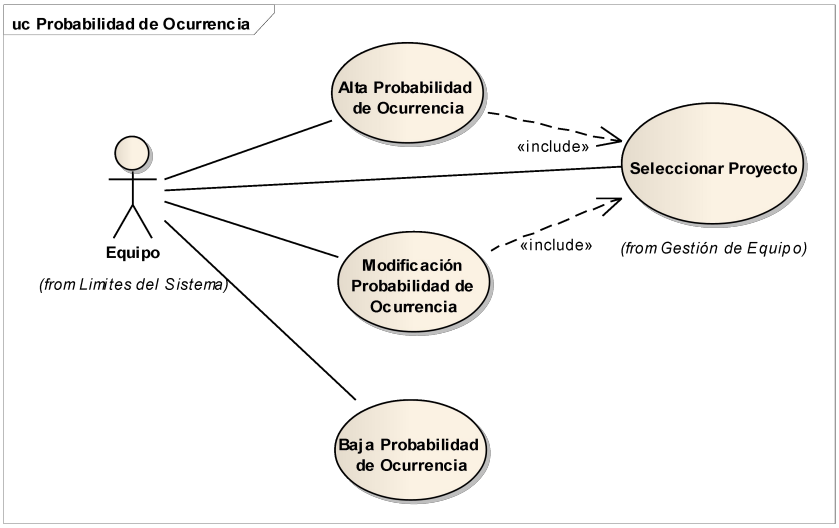


Imagen 23: Probabilidad de Ocurrencia

1.2.6.3.1 Alta Probabilidad de Ocurrencia

Gestión de Valores de Probabilidad de ocurrencia por Proyecto

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar: Id del Proyecto, % Mínimo, % Máximo, % Medio, val. Exposición, Valor Nominal.

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

.Debe existir cargado los proyectos

1.2.6.3.2 Baja Probabilidad de Ocurrencia

Gestión de Valores de Probabilidad de ocurrencia por Proyecto

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.6.3.3 Modificación Probabilidad de Ocurrencia

Gestión de Valores de Probabilidad de ocurrencia por Proyecto

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.7 Etapa 7 - Exposición

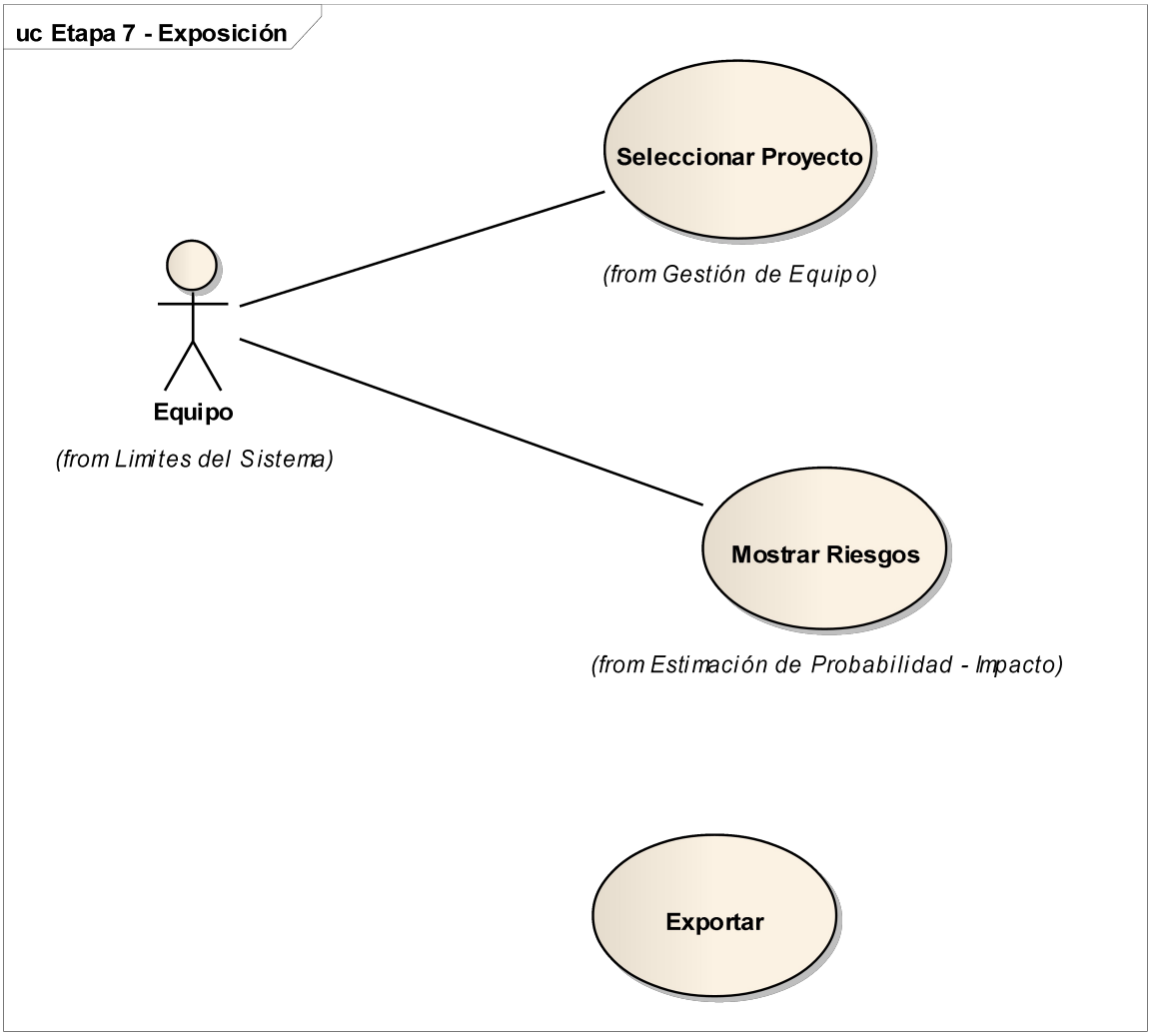


Imagen 24: Etapa 7 - Exposición

1.2.7.1 Exportar

Modulo para exportar datos de una grilla a distintos formatos digitales.

- XLS
- XML
- TXT
- HTML

1.2.8 Etapa 8 - Gestión de los Riesgos

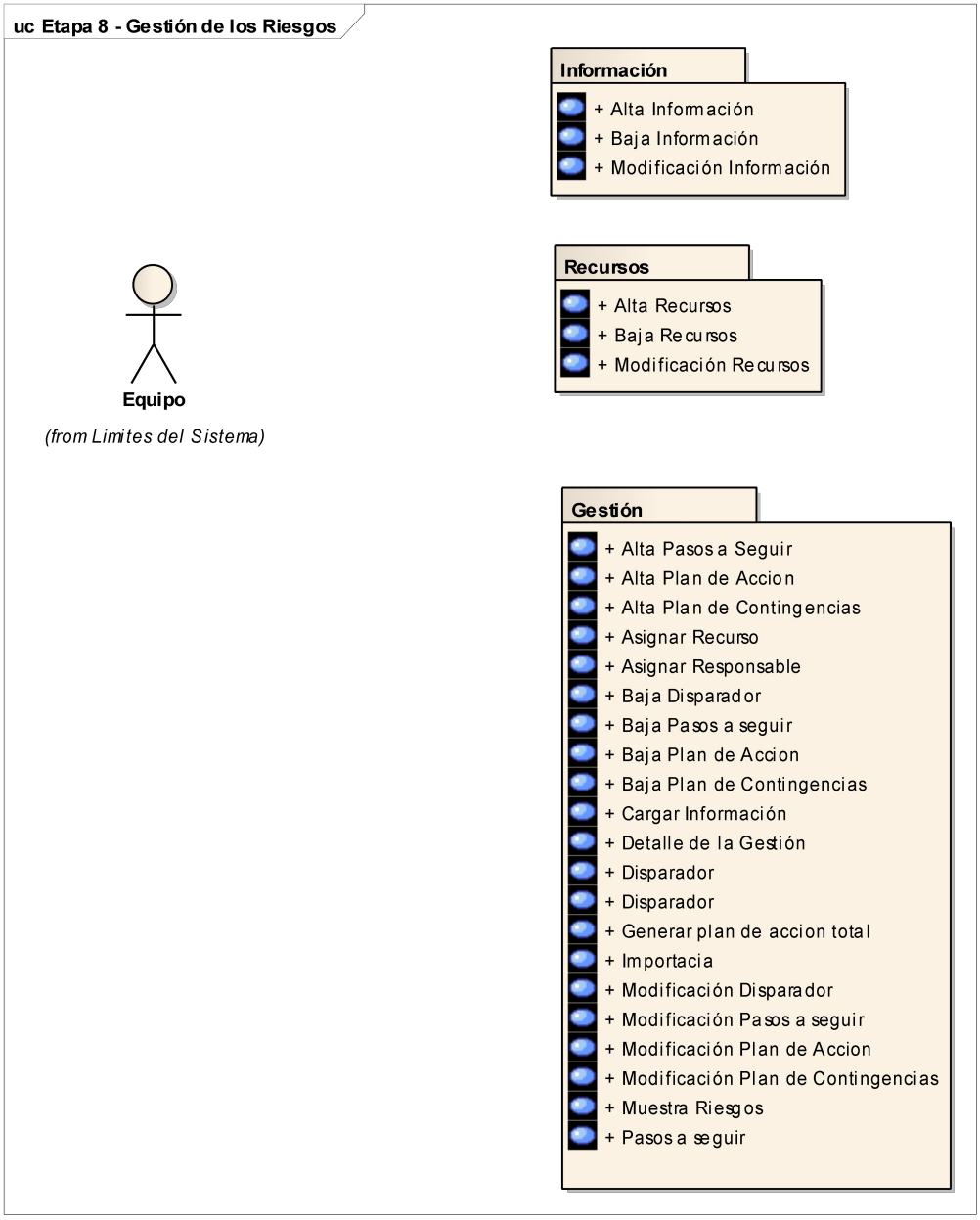


Imagen 25: Etapa 8 - Gestión de los Riesgos

1.2.8.1 Gestión

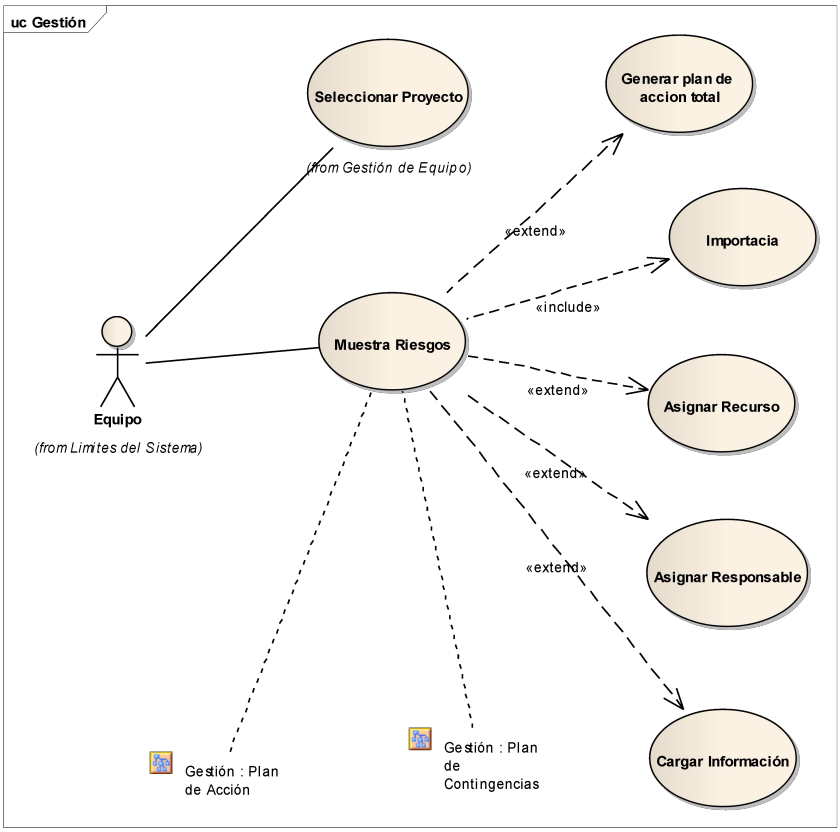


Imagen 26: Gestión

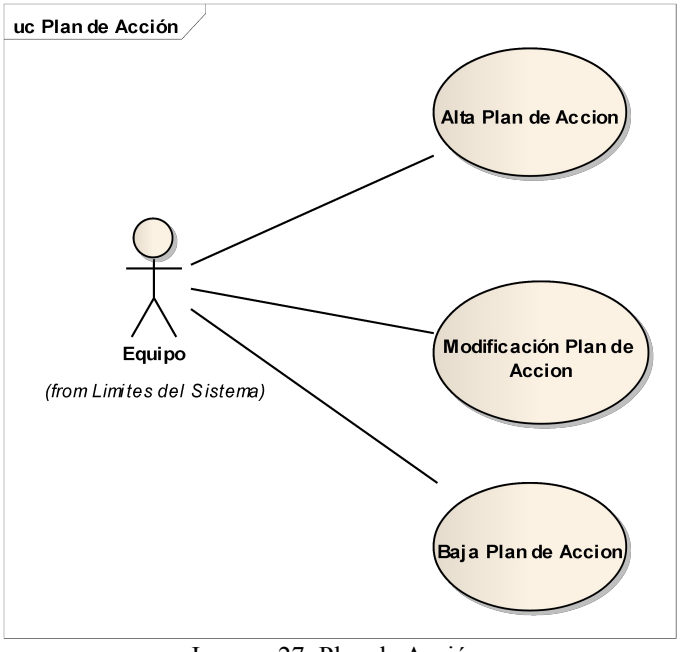


Imagen 27: Plan de Acción

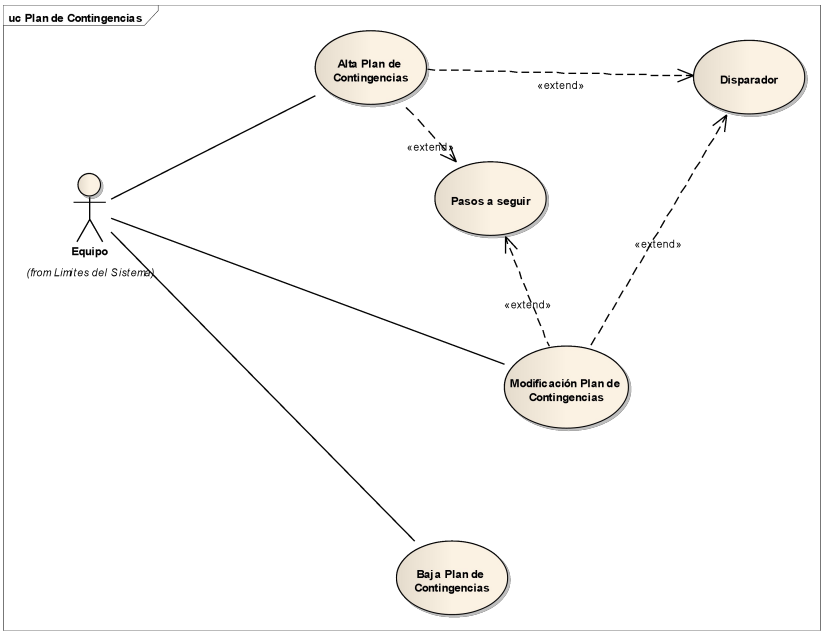


Imagen 28: Plan de Contingencias

1.2.8.1.1 Alta Pasos a Seguir

Se establecen los pasos secuenciales a seguir para poder minimizar o eliminar el problema

1.2.8.1.2 Alta Plan de Acción

Alta del Plan de acción para el riesgo seleccionado.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar: Id de la Amenaza, Id Dimensión, Id. Salvaguarda, Id Responsable, Paso, Descripción y Observación.

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

.Debe existir cargado los proyectos

1.2.8.1.3 Alta Plan de Contingencias

Gestión de contingencias para el riesgo seleccionado.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario cargará: Id Disparador, Id responsable, Pasos a seguir Caso de Uso (Pasos a Seguir), Observación

Alternate

Paso 3. El usuario cargar los datos y presiona el botón guardar

Alternate

Paso 4. El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

.Debe existir Disparador

PRE-condición *Estado:* Approved

.Debe existir responsables asignados al proyecto

1.2.8.1.4Asignar Recurso

Gestión de recursos para el Riesgo analizado.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo, Modificar o eliminar.

Basic Path

Paso 2

- Si la opción es Nuevo o Modificar, el sistema muestra una ventana en donde el usuario puede cargar o modificar: Id Recurso, Descripción, Observación.

- Si es Eliminar Pregunta si el usuario está seguro de la acción.

Basic Path

Paso 3

Opción Nuevo o modificación

- El usuario cargar o modifica los datos y presiona el botón guardar

Opción Borrar

- El usuario presiona Aceptar.

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

Basic Path

Alternativa 1
Si el recurso No existe CU Alta Recursos.

PRE-condición *Estado:* Approved
.Debe existir el recurso

1.2.8.1.5 Asignar Responsable

Gestiona Responsables para el Riesgo.

Flujo de Eventos

Alternate
Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo, Modificar o eliminar.

Basic Path
Paso 2
Si la opción es Nuevo o Modificar, el sistema muestra una ventana en donde el usuario puede cargar o modificar: Id Persona
Si es Eliminar Pregunta si el usuario está seguro de la acción.

Basic Path
Paso 3
Opción Nuevo o modificación
- El usuario cargar o modifica los datos y presiona el botón guardar

Opción Borrar
- El usuario presiona Aceptar.

Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Dichos responsables deben estar asignados al proyecto en curso

1.2.8.1.6 Baja Disparador

Gestión de Valores de Impacto sobre un proyecto.

Flujo de Eventos

Alternate
Paso 1 El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Alternate
Paso 2. El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Alternate

Paso 3. El usuario selecciona el botón Aceptar.

Alternate
Paso 4. El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.8.1.7 Baja Pasos a seguir

Pasos secuénciales a seguir para la solución del problema.

Flujo de Eventos

Alternate
Paso 1 El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Alternate
Paso 2. El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Alternate
Paso 3. El usuario selecciona el botón Aceptar.

Alternate
Paso 4. El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.8.1.8 Baja Plan de Acción

Baja del Plan de acción para el riesgo seleccionado.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.8.1.9 Baja Plan de Contingencias

Gestión de contingencias para el riesgo seleccionado.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path
Paso 3
El usuario selecciona el botón Aceptar.

Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos.

Basic Path
Alternativa
Si no lo puede realizar la eliminación por restricciones genera un informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.8.1.10 Cargar Información

Cargar información necesaria para la gestión del riesgo

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo, Modificar o Eliminar.

Basic Path
Paso 2

- Si la opción es Nuevo o Modificar, el sistema muestra una ventana en donde el usuario puede cargar o modificar: Id Información.

- Si es Eliminar Pregunta si el usuario está seguro de la acción.

Basic Path
Paso 3
Opción Nuevo o modificación

- El usuario cargar o modifica los datos y presiona el botón guardar

Opción Borrar

- El usuario presiona Aceptar.

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

Basic Path

Alternativa 1

Si la información No existe, Accionar CU Alta Información

PRE-condición *Estado:* Approved

.Debe existir la información

1.2.8.1.11 Detalle de la Gestión

Gestiona los activos con exposición al Riesgo.

Por cada Riesgo se establecen

- Información necesaria sobre el riesgo.
- Responsable de los riesgos.
- Recursos para el seguimiento y control de riesgo.
- Plan de acción
- Plan de Contingencias.

1.2.8.1.12 Disparador

Gestión de Disparador del Riesgo.

Flujo de Eventos

Alternate

Paso 1 El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Alternate

Paso 2. El sistema muestra una ventana en donde el usuario puede cargar: Id del Proyecto, Criterio, retraso y Valor.

Alternate

Paso 3. El usuario cargar los datos y presiona el botón guardar

Alternate

Paso 4. El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

.Debe existir cargado los proyectos

1.2.8.1.13 Disparador

Gestión de disparador.
Acción o causa que dispara la transformación del Riesgo en Problema.
El CU gestiona los disparadores Alta, Baja y modificación de los mismos.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el usuario selecciona una de las 4 opciones que ofrece "Nuevo", "Modificación", "Baja" y "Elegir"

Basic Path

Paso 2

Si la opción es:

- "Elegir" muestra el dato seleccionado en el CU "Alta de Plan de Contingencias" o "Modificación de Plan de Contingencias".
- "Nuevo" Muestra una ventana en donde se carga la descripción del Disparador.
- "Modificar" Muestra una ventana en donde se puede modificar el valor de la descripción del Disparador.
- "Eliminar" Muestra un mensaje al usuario si está seguro de la acción, controla si se puede eliminar el dato y lo elimina.

Post-condición *Estado:* Approved

No se puede dar de baja a un disparador asignado

PRE-condición *Estado:* Approved

.No se puede repetir un disparador

1.2.8.1.14 Generar plan de acción total

Generación del plan de Acción basado en las Salvaguardas para todos los activos del proyecto seleccionado.
Se podrá generar plan de acción total para actualizar las bases de plan de acción, cuando existe una salvaguarda nueva o un activo nuevo.

Flujo de Eventos

Alternate

Paso 1

El caso de uso comienza cuando el usuario presiona el botón "Generar por defecto el Plan de acción"

Alternate

Paso 2

El sistema recorre los activos por proyecto, dimensión por activo y salvaguardas por dimensión y va cargando las salvaguardas en el almacén plan de acción

PRE-condición *Estado:* Approved

Existencia de las Salvaguardas

1.2.8.1.15 importancia

Se carga la importancia de que el riesgo se trasforme en un problema.

Flujo de Eventos

Alternate

Paso 1

El caso de uso comienza cuando el usuario seleccionar un riesgo y presiona el botón "Cargar detalle del riesgo"

Alternate

Paso 2

El sistema abre una pantalla en donde muestra los el campo Importancia.

Alternate

Paso 3

El usuario carga el campo importancia y presiona el botón aceptar.

Alternate

Paso 4

El sistema corrobora la correcta carga y guarda en la BD.

1.2.8.1.16 Modificación Disparador

Gestión de Valores de Impacto sobre un proyecto.

Flujo de Eventos

Alternate

Paso 1 El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Alternate

Paso 2. El sistema muestra una ventana en donde el usuario puede modificar los datos.

Alternate

Paso 3. El usuario modifica los datos y presiona el botón guardar

Alternate

Paso 4. El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.8.1.17 Modificación Pasos a seguir

Pasos secuénciales a seguir para la solución del problema.

Flujo de Eventos

Alternate

Paso 1 El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Alternate

Paso 2. El sistema muestra una ventana en donde el usuario puede modificar los datos.

Alternate
Paso 3. El usuario modifica los datos y presiona el botón guardar

Alternate
Paso 4. El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.8.1.18 Modificación Plan de Acción

Modificación del Plan de acción para el riesgo seleccionado.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar.
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.8.1.19 Modificación Plan de Contingencias

Gestión de contingencias para el riesgo seleccionado.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego

devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.2.8.1.20 Muestra Riesgos

Muestra los riesgos correspondientes al proyecto seleccionado en el CU "seleccionar proyecto"

Flujo de Eventos

Alternate

Paso 1
El caso de uso comienza cuando el usuario ingresa a la aplicación "Gestión de Riesgos"
Luego de haber seleccionado un proyecto en el CU "Seleccionar Proyecto"

Alternate

Paso 2
El sistema filtra los riesgos declarados y muestra en pantalla.

1.2.8.1.21 Pasos a seguir

Gestión de Pasos a seguir.
Pasos secuénciales a seguir para la solución del problema.

Flujo de Eventos

Basic Path

Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo, Modificar o eliminar.

Basic Path

Paso 2
Si la opción es Nuevo o Modificar, el sistema muestra una ventana en donde el usuario puede cargar o modificar: Nº de Paso, código, nombre, descripción, realiza control, realiza seguimiento, observaciones.
Si es Eliminar Pregunta si el usuario está seguro de la acción.

Basic Path

Paso 3
Opción Nuevo o modificación

- El usuario cargar o modifica los datos y presiona el botón guardar

Opción Borrar

- El usuario presiona Aceptar.

Basic Path

Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
.Debe existir cargado los proyectos

1.2.8.2 Información

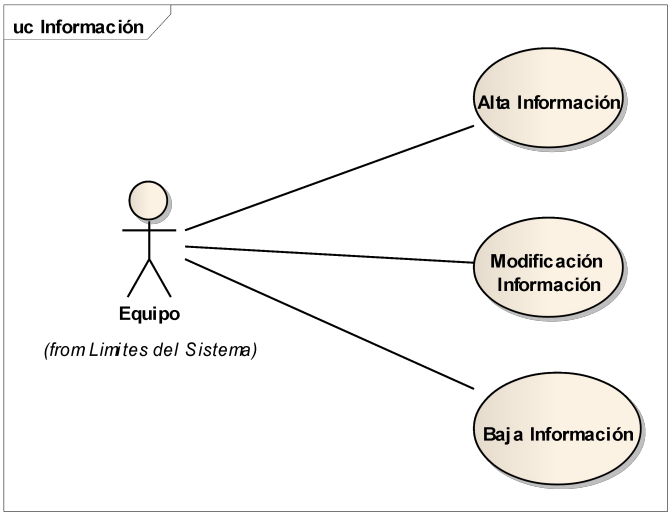


Imagen 29: Información

1.2.8.2.1 Alta Información

Gestión de información necesaria para la gestión del riesgo.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el código, nombre y descripción de la información
Basic Path
Paso 3.
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4.
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.2.8.2.2 Baja Información

Gestión de información necesaria para la gestión del riesgo.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.8.2.3 Modificación Información

Gestión de información necesaria para la gestión del riesgo.

Flujo de Eventos

Alternate

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Alternate

Paso 2.

El sistema muestra una ventana en donde el usuario puede modificar los datos.

Alternate

Paso 3.

El usuario modifica los datos y presiona el botón guardar

Alternate

Paso 4.

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.8.3 Recursos

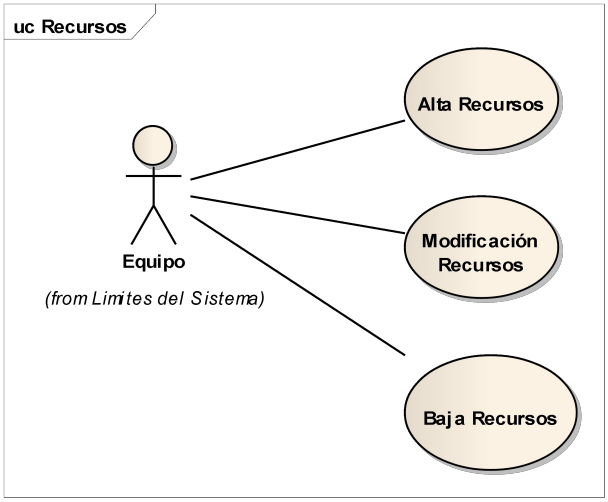


Imagen 30: Recursos

1.2.8.3.1 Alta Recursos

Gestión de recursos utilizados para la gestión del riesgo

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario presiona el botón Nuevo

Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el nombre y descripción de la información

Basic Path
Paso 3.
El usuario cargar los datos y presiona el botón guardar

Basic Path
Paso 4.
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.2.8.3.2 Baja Recursos

Gestión de recursos utilizados para la gestión del riesgo

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path
Paso 3
El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.2.8.3.3 Modificación Recursos

Gestión de recursos utilizados para la gestión del riesgo

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2.

El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path

Paso 3.

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4.

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.3 Incidencias

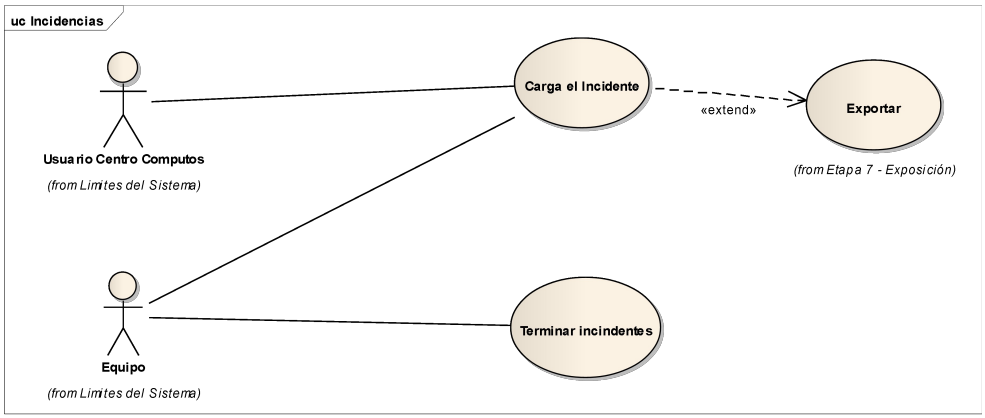


Imagen 31: Incidencias

1.3.1 Carga el Incidente

Se cargan los incidentes.

- El sistema controla si el activo con incidente:

1. Está analizado y gestionado
2. Está analizado
3. No esta analizado.

- Si está analizado y gestionado genera un reporte del plan de contingencia que se debe realizar.

- Envía un e-mail al encargado de corregir el incidente y al Líder del proyecto.

Posee dos partes.

1. Incidentes Activos
2. Incidentes Finalizados

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Nuevo, Modificar.

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar o modificar: Id Activos, Id Amenaza, Id responsable, Fecha incidente, hora incidente, acción a tomar.

Basic Path

Paso 3

El usuario cargar o modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos.

Controla si el riesgo esta:

- Analizado y gestionado.
- Analizado.
- No analizado.

Envía un email al responsable de la incidencia y al líder del proyecto.

Luego devuelve el control a la pantalla grilla.

Alternate

Alternativa 1

Si el riesgo esta analizado y gestionado el sistema genera un reporte con el plan de contingencia detallado.

1.3.2 Terminar incidentes

Se acciona la finalización del incidente.

El usuario cargará los parámetros de finalización del incidente.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el usuario presiona el botón terminar incidente.

Basic Path

Paso 2

El sistema muestra una pantalla con los siguientes datos a cargar:

- Observación
- El incidente se solucionó correctamente?
- Fecha de Fin del incidente.
- El plan de contingencia es adecuado ?
- Se debería mejorar ?

Basic Path

Paso 3

El usuario carga los datos y presiona el botón Aceptar.

Basic Path

Paso 4

El sistema controla los datos cargados y guarda los mismos en los almacenes correspondientes.

Luego imprime un reporte y vuelve a la pantalla anterior.

PRE-condición *Estado:* Approved

El incidente debe estar cargado y No finalizado.

1.4 Informes

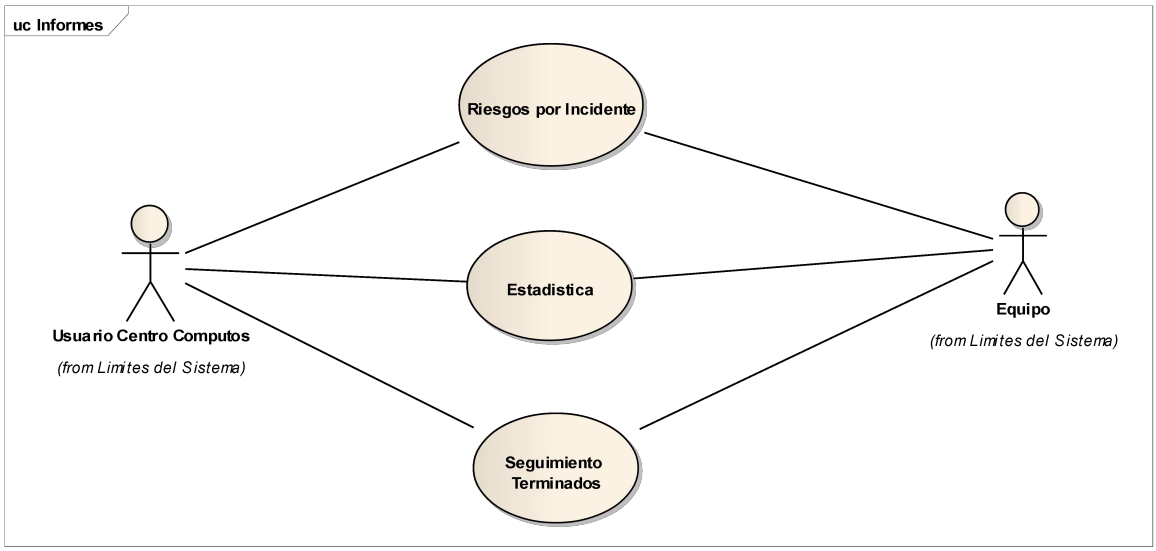


Imagen 32: Informes

1.4.1 Estadística

Informe de Ranking estadístico por tipo de incidente y fecha con gráfico de torta.

Características

- Incidentes Terminados

- Total de Incidentes.

1.4.2 Riesgos por Incidente

Informe de Incidentes con las siguientes características

- Terminados Bien
- Terminados Mal
- Pendientes
- Activos con AGR
- Activos con Análisis
- Activos sin análisis

1.4.3 Seguimiento Terminados

Informe de Seguimientos terminados.
Características:

- Ordenado por Fecha
- Por Amenaza
- Por Salvaguarda
- Por Dimensión
- Terminado Bien
- Terminado Mal.

1.5 parámetros

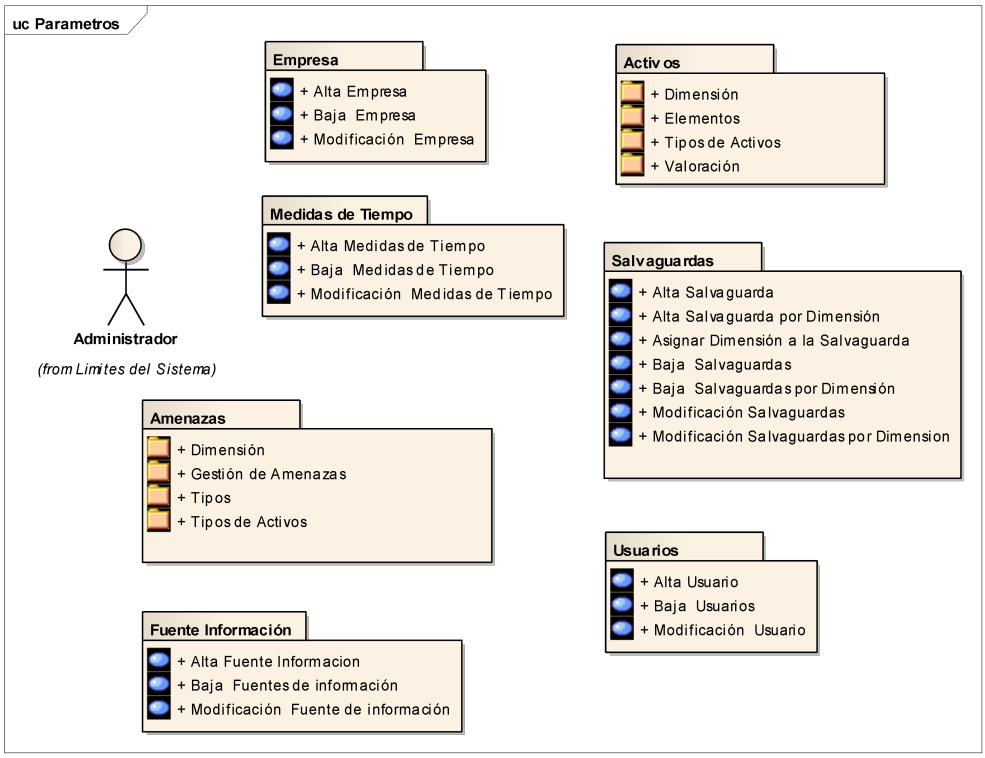


Imagen 33: parámetros

1.5.1 Activos

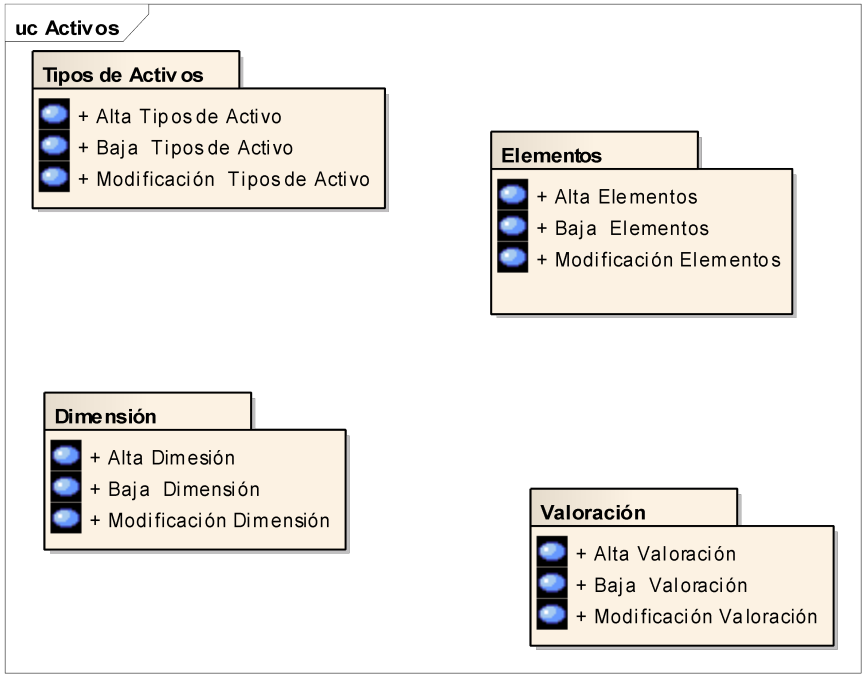


Imagen 34: Activos

1.5.1.1 Dimensión

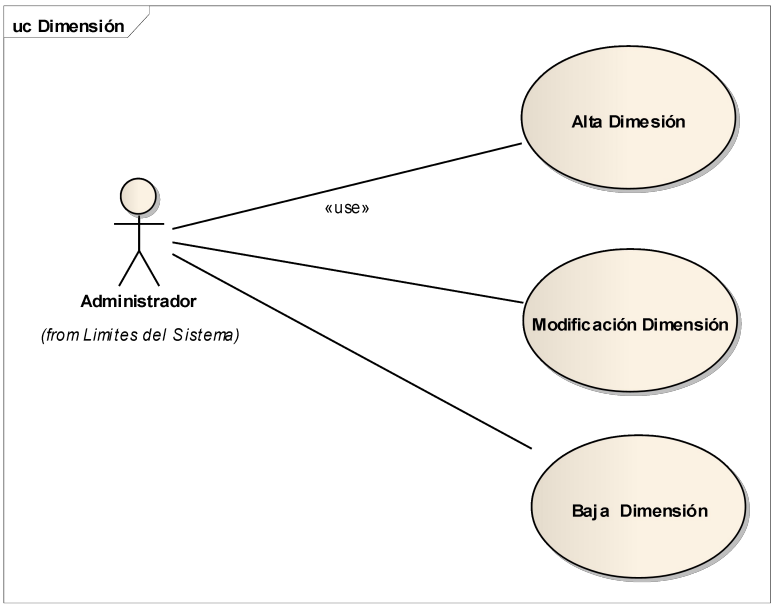


Imagen 35: Dimensión

1.5.1.1.1 Alta Dimensión

Gestión de Dimensión, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar el código, nombre, pregunta y descripción

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.1.1.2 Baja Dimensión

Gestión de Dimensión, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.1.1.3 Modificación Dimensión

Gestión de Dimensión, según parámetros propuestos por Magerit v2.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.1.2 Elementos

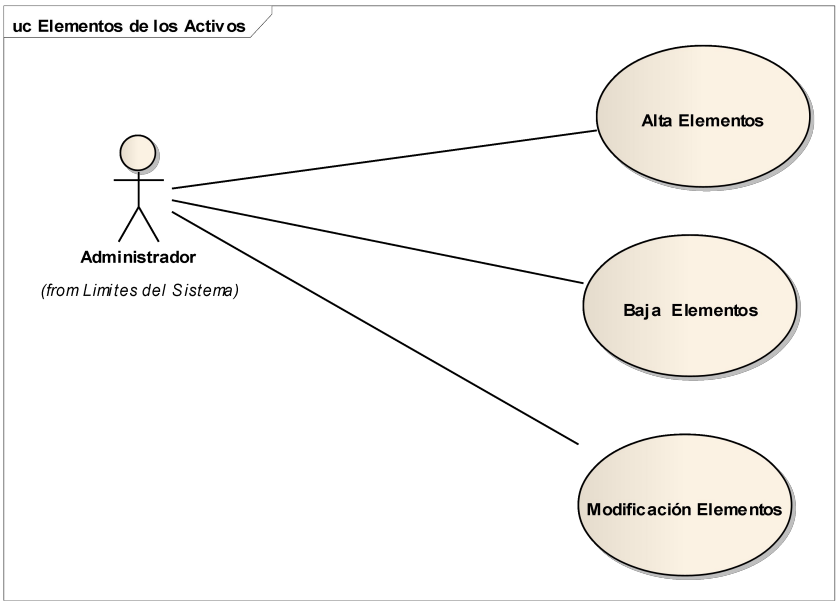


Imagen 36: Elementos de los Activos

1.5.1.2.1 Alta Elementos

Gestión de Elementos, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar el código, nombre y tipo de activo.

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

Invariant *Estado:* Approved

.Deben estar cargados los tipos de activos

1.5.1.2.2 Baja Elementos

Gestión de Elementos, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a

Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.1.2.3 Modificación Elementos

Gestión de Elementos, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.1.3 Tipos de Activos

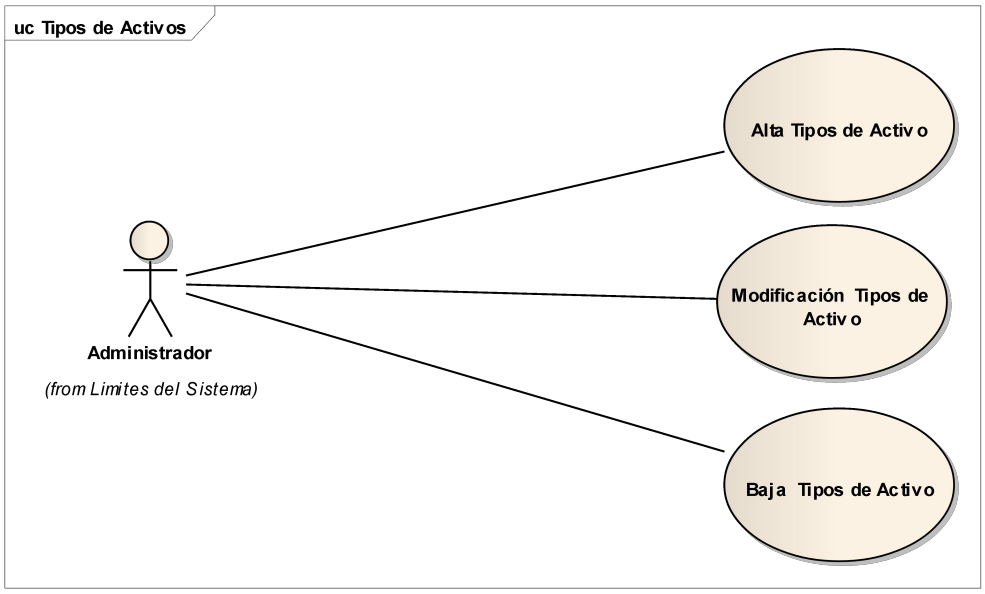


Imagen 37: Tipos de Activos

1.5.1.3.1 Alta Tipos de Activo

Gestión de tipo de activos, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar el Nombre y la descripción del Tipo de Activo

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.1.3.2 Baja Tipos de Activo

Gestión de tipo de activos, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.1.3.3 Modificación Tipos de Activo

Gestión de tipo de activos, según parámetros propuestos por Magerit v2.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar el Nombre y la descripción del Tipo de Activo
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos.
Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.1.4 Valoración

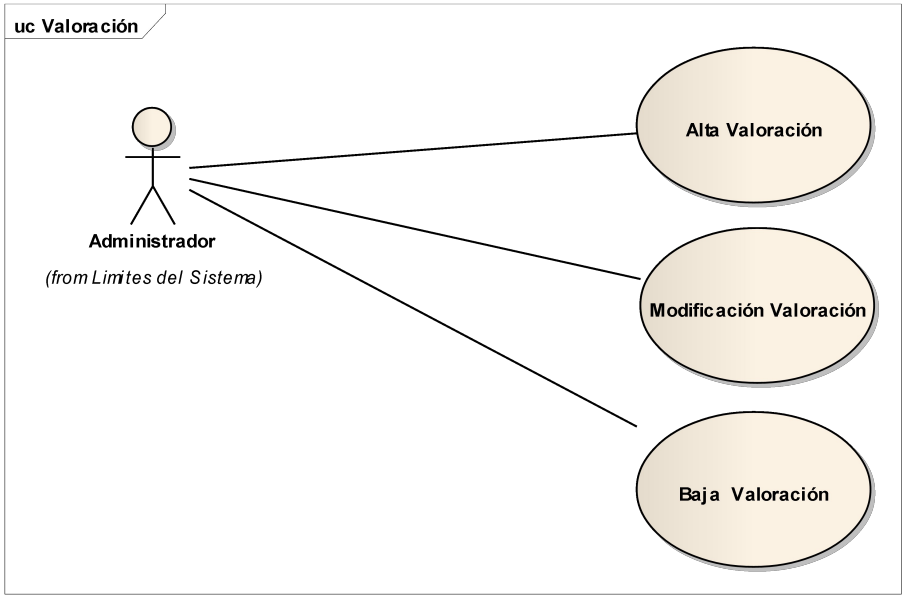


Imagen 38: Valoración

1.5.1.4.1 Alta Valoración

Gestión de Valoración de Activos.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar el valor, tipo valor, criterio y descripción

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.1.4.2 Baja Valoración

Gestión de Valoración de Activos.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.1.4.3 Modificación Valoración

Gestión de Valoración de Activos.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados
Basic Path
Paso 3

Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.2 Amenazas

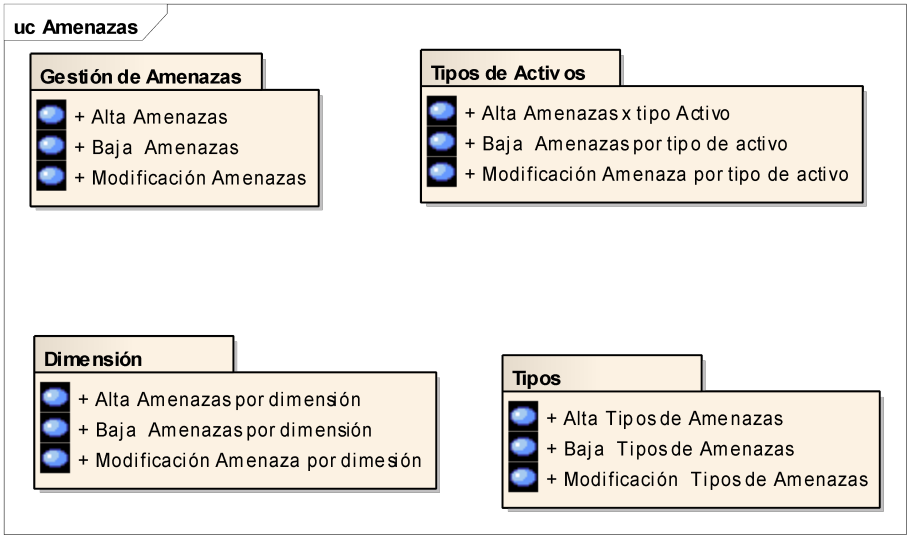


Imagen 39: Amenazas

1.5.2.1 Dimensión

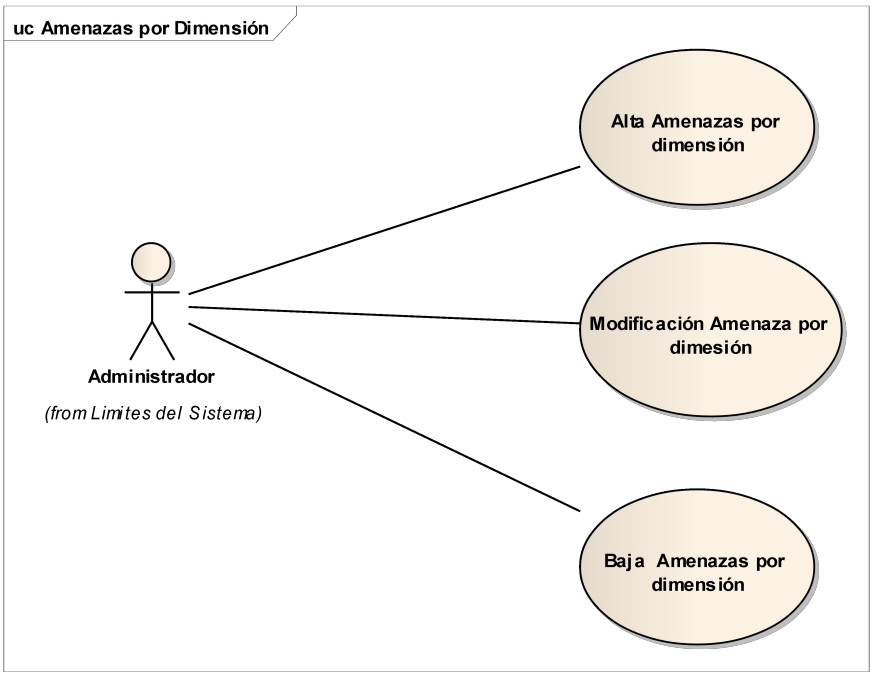


Imagen 40: Amenazas por Dimensión

1.5.2.1.1 Alta Amenazas por dimensión

Asignación a cada Dimensión una o mas amenazas.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario selección una dimensión y una Amenaza.
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

Invariant *Estado:* Approved
.Deben estar cargados de las amenazas y las dimensiones

1.5.2.1.2Baja Amenazas por dimensión

Asignación a cada Dimensión una o mas amenazas.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.2.1.3Modificación Amenaza por dimensión

Asignación a cada Dimensión una o mas amenazas.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados.

Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.2.2 Gestión de Amenazas

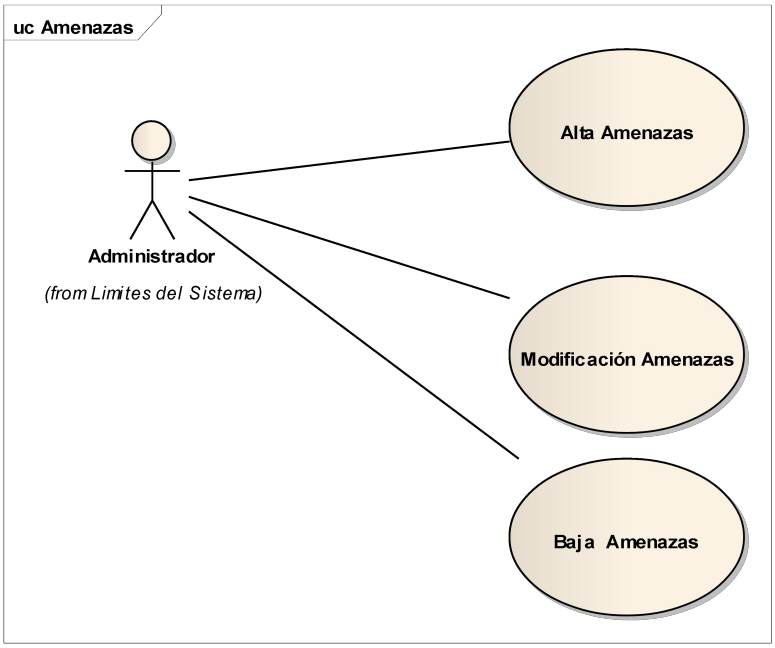


Imagen 41: Amenazas

1.5.2.2.1 Alta Amenazas

Gestión de Amenazas, según parámetros propuestos por Magerit v2.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el código, nombre , descripción, detalle y tipo de amenazas
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path

Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos.
Luego devuelve el control a la pantalla grilla.

Invariant *Estado:* Approved
.Deben estar cargados los tipos de Amenazas

1.5.2.2.2Baja Amenazas

Gestión de Amenazas, según parámetros propuestos por Magerit v2.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.2.2.3Modificación Amenazas

Gestión de Amenazas, según parámetros propuestos por Magerit v2.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.2.3 Tipos

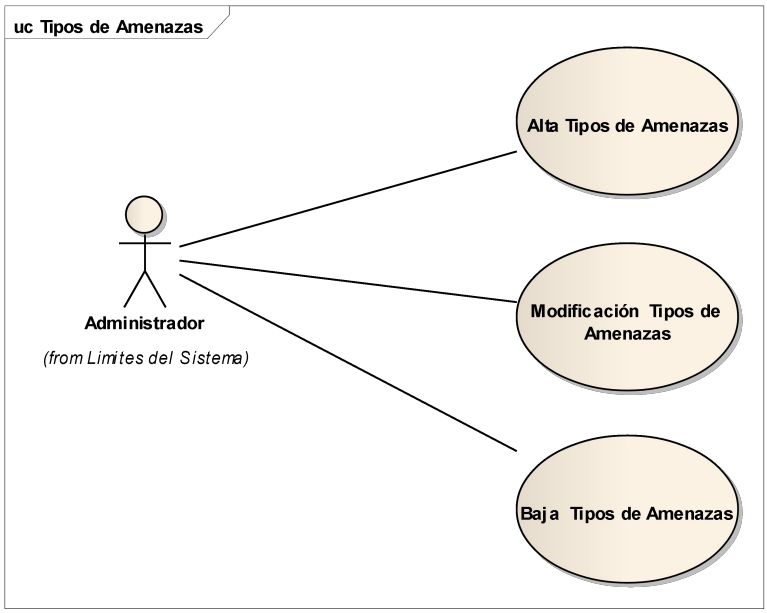


Imagen 42: Tipos de Amenazas

1.5.2.3.1 Alta Tipos de Amenazas

Gestión de tipo de Amenazas, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el código, Nombre y la descripción
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.2.3.2 Baja Tipos de Amenazas

Gestión de tipo de Amenazas, según parámetros propuestos por Magerit v2.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar
Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.2.3.3 Modificación Tipos de Amenazas

Gestión de tipo de Amenazas, según parámetros propuestos por Magerit v2.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.2.4 Tipos de Activos

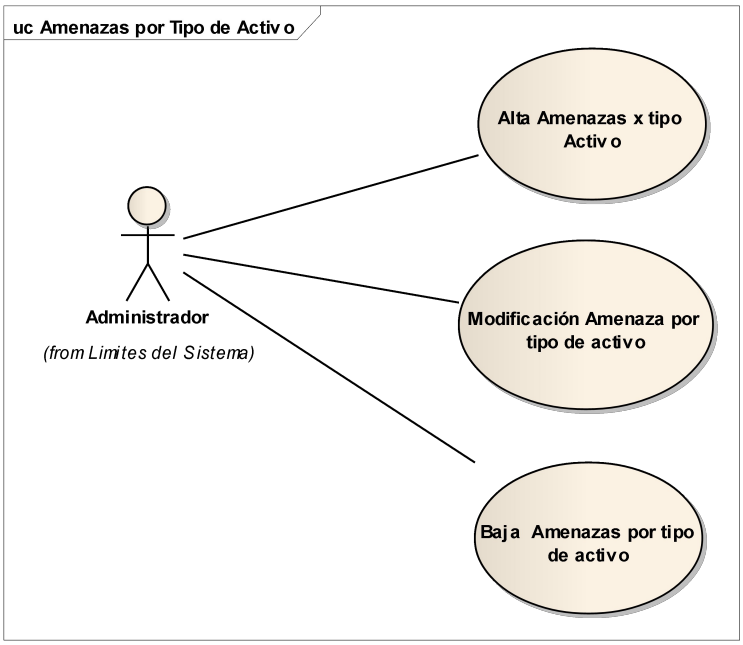


Imagen 43: Amenazas por Tipo de Activo

1.5.2.4.1 Alta Amenazas x tipo Activo

Asignación a cada tipo de activo una amenaza.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario selección una Tipo de activo y una Amenaza.

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

Invariant *Estado:* Approved

.Deben estar cargados de las amenazas y los Tipos de activos

1.5.2.4.2 Baja Amenazas por tipo de activo

Asignación a cada tipo de activo una amenaza.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.2.4.3 Modificación Amenaza por tipo de activo

Asignación a cada tipo de activo una amenaza.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.3 Empresa

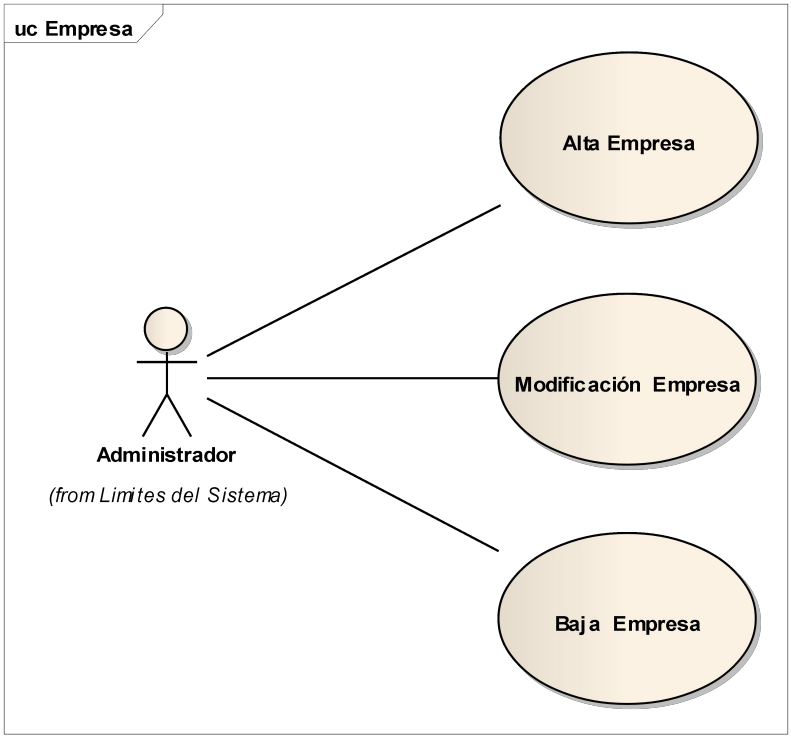


Imagen 44: Empresa

1.5.3.1 Alta Empresa

Datos de la Organización en donde se utilizará el Sistema

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar la descripción, dirección y cuit.

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.3.2 Baja Empresa

Corresponde al Área y Departamentos en donde se obtiene la información correspondiente al activo.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.3.3 Modificación Empresa

Datos de la Organización en donde se utilizará el Sistema.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.4 Fuente Información

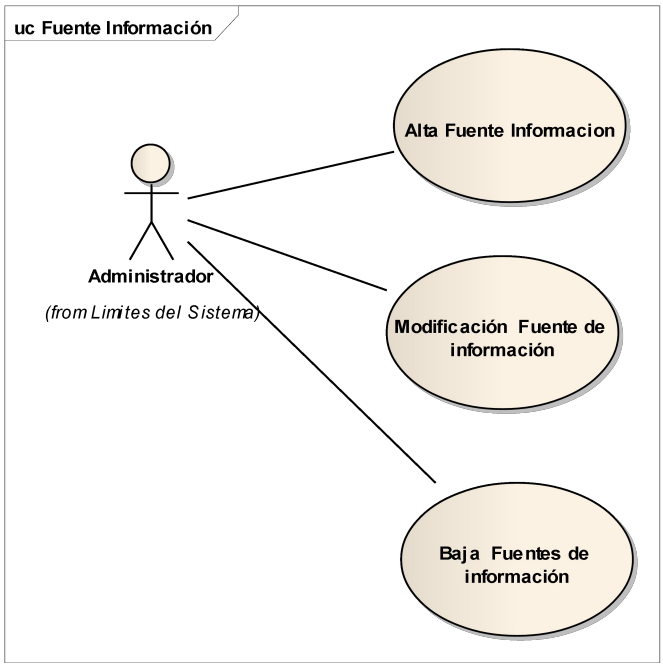


Imagen 45: Fuente Información

1.5.4.1 Alta Fuente Información

Corresponde al Área y Departamentos en donde se obtiene la información correspondiente al activo.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el Nombre y la descripción de la Fuente de Información
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.4.2 Baja Fuentes de información

Corresponde al Área y Departamentos en donde se obtiene la información correspondiente al activo.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a

Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.4.3 Modificación Fuente de información

Corresponde al Área y Departamentos en donde se obtiene la información correspondiente al activo.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.5 Medidas de Tiempo

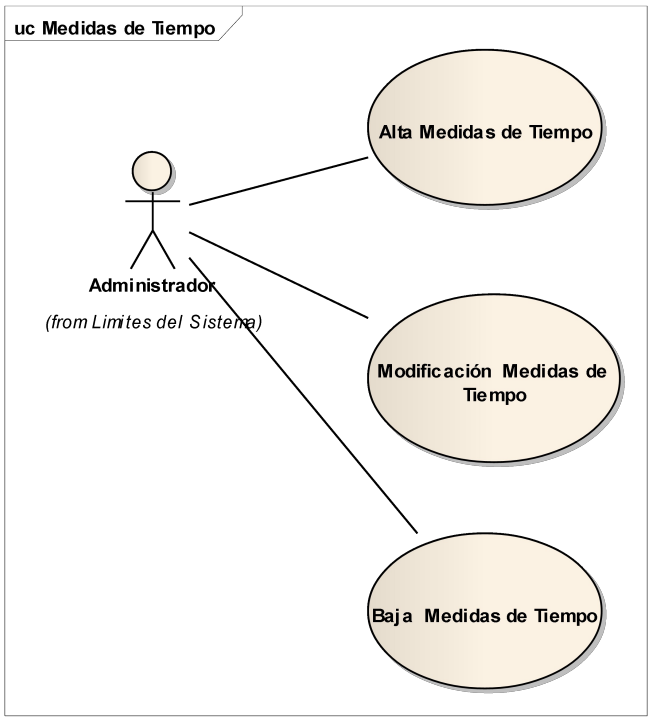


Imagen 46: Medidas de Tiempo

1.5.5.1 Alta Medidas de Tiempo

Unidad propia de medida de tiempo en días para el control de las salvaguardas.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede cargar la descripción de la unidad de tiempo, cantidad al año y distancia entre días.

Basic Path

Paso 3

El usuario cargar los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.5.2 Baja Medidas de Tiempo

Corresponde al Área y Departamentos en donde se obtiene la información correspondiente al activo.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a

Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.5.3 Modificación Medidas de Tiempo

Corresponde al Área y Departamentos en donde se obtiene la información correspondiente al activo.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos.

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.6 Salvaguardas

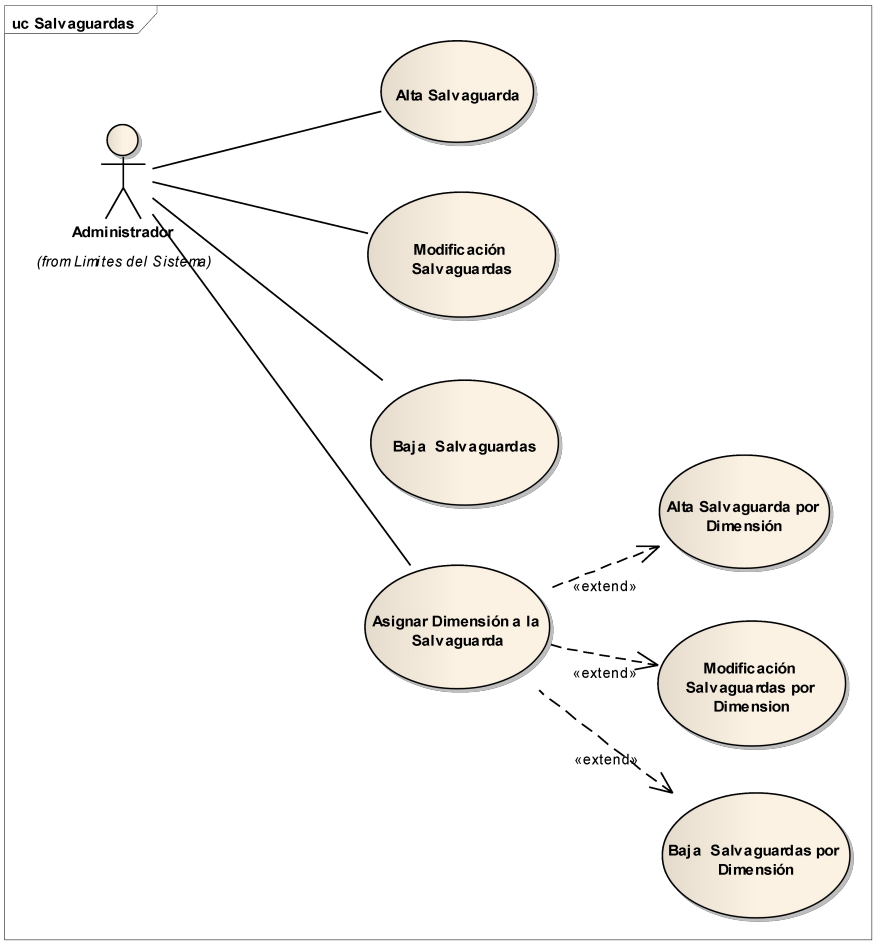


Imagen 47: Salvaguardas

1.5.6.1 Alta Salvaguarda

Gestión de salvaguardas propuestas por Magerit 2.
El modelo permite incluir salvaguardas propias de cada proyecto que no estén dentro de los sugeridos por Magerit2.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el usuario preciona el botón Nuevo
Basic Path
Paso 2
El sistema muestra los campos ha ser cargados por el usuario. Descripción, Observación, seguimiento, Control y Aplicar a todas las dimensiones.
Basic Path
Paso 3
El usuario carga los datos
Basic Path
Paso 4
El sistema verifica los parámetros de los datos y graba los mismos.

1.5.6.2 Alta Salvaguarda por Dimensión

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el usuario presiona el botón nuevo en el caso de Uso "Asignar Dimensión a la Salvaguarda"

Basic Path

Paso 2

El sistema muestra una ventana con los siguientes campo: dimensión, descripción y observación

Basic Path

Paso 3

El usuario carga los datos y presiona el botón guardar.

Basic Path

Paso 4

El sistema procesa y guarda la transacción y devuelve el control al Caso de uso "Asignar Dimensión a la Salvaguarda"

PRE-condición *Estado:* Approved

Deben existir las dimensiones

1.5.6.3 Asignar Dimensión a la Salvaguarda

Flujo de Eventos

Alternate

Paso 1. El caso de uso comienza cuando el usuario selecciona una salvaguarda y presiona el botón "Asignar Dimensión"

Alternate

Paso 2. El sistema muestra una grilla de las dimensiones asignadas a la salvaguarda selecciona y en donde se puede seleccionar Nuevo, Modificar y Borrar.

Alternate

Paso 3. El usuario selecciona una opción

PRE-condición *Estado:* Approved

Deben Existir las dimensiones

PRE-condición *Estado:* Approved

Deben existir las salvaguardas

1.5.6.4 Baja Salvaguardas

Gestión de salvaguardas propuestas por Magerit 2.

El modelo permite incluir salvaguardas propias de cada proyecto que no estén dentro de los sugeridos por Magerit2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.6.5 Baja Salvaguardas por Dimensión

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar en el Caso de Uso "Asignar Dimensión a la Salvaguarda"

Basic Path

Paso 2

El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro

Basic Path

Paso 3

El usuario selecciona el botón Aceptar.

Basic Path

Paso 4

El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.6.6 Modificación Salvaguardas

Gestión de salvaguardas propuestas por Magerit 2.

El modelo permite incluir salvaguardas propias de cada proyecto que no estén dentro de los sugeridos por Magerit2.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.6.7 Modificación Salvaguardas por Dimensión

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar en el Caso de uso "Asignar Dimensión a la salvaguarda"

Basic Path

Paso 2

El sistema muestra una ventana en donde el usuario puede modificar los datos mostrados

Basic Path

Paso 3

El usuario modifica los datos y presiona el botón guardar

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control al Caso de Uso "Asignar Dimensión a la Salvaguarda"

PRE-condición *Estado:* Approved

Deben Existir datos Cargados

1.5.7 Usuarios

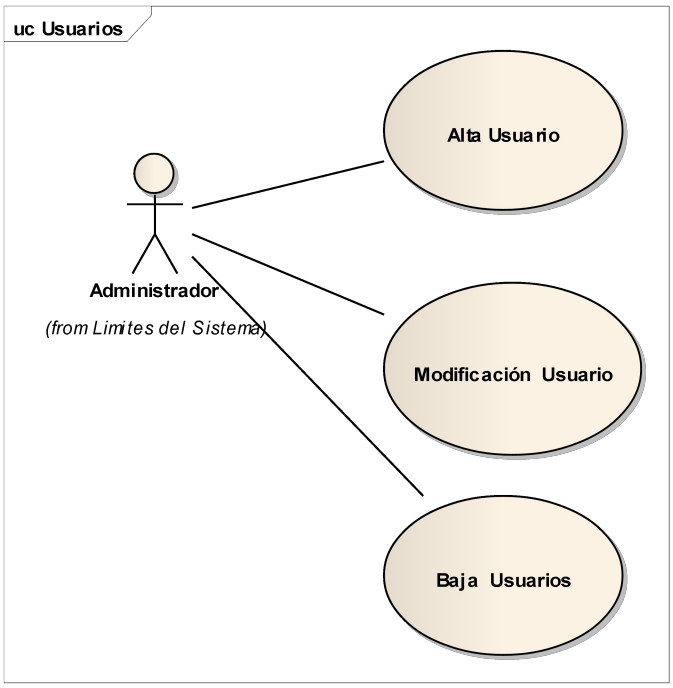


Imagen 48: Usuarios

1.5.7.1 Alta Usuario

Gestión de datos de Usuarios del Sistema.
Posee Niveles de Acceso al sistema y grupos.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador presiona el botón Nuevo
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede cargar el usuario, la contraseña y el nivel de seguridad.
Basic Path
Paso 3
El usuario cargar los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

1.5.7.2 Baja Usuarios

Gestión de datos de Usuarios del Sistema.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a Eliminar y presiona el botón Borrar

Basic Path
Paso 2
El sistema muestra una ventana en donde pregunta al usuario si está seguro de la eliminación del registro
Basic Path
Paso 3
El usuario selecciona el botón Aceptar.
Basic Path
Paso 4
El sistema verifica que el dato se puede eliminar y lo borra de la base de datos, si no lo puede hacer informa al usuario.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.5.7.3 Modificación Usuario

Gestión de datos de Usuarios del Sistema.

Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario Administrador selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón guardar
Basic Path
Paso 4
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved
Deben Existir datos Cargados

1.6 Seguimiento

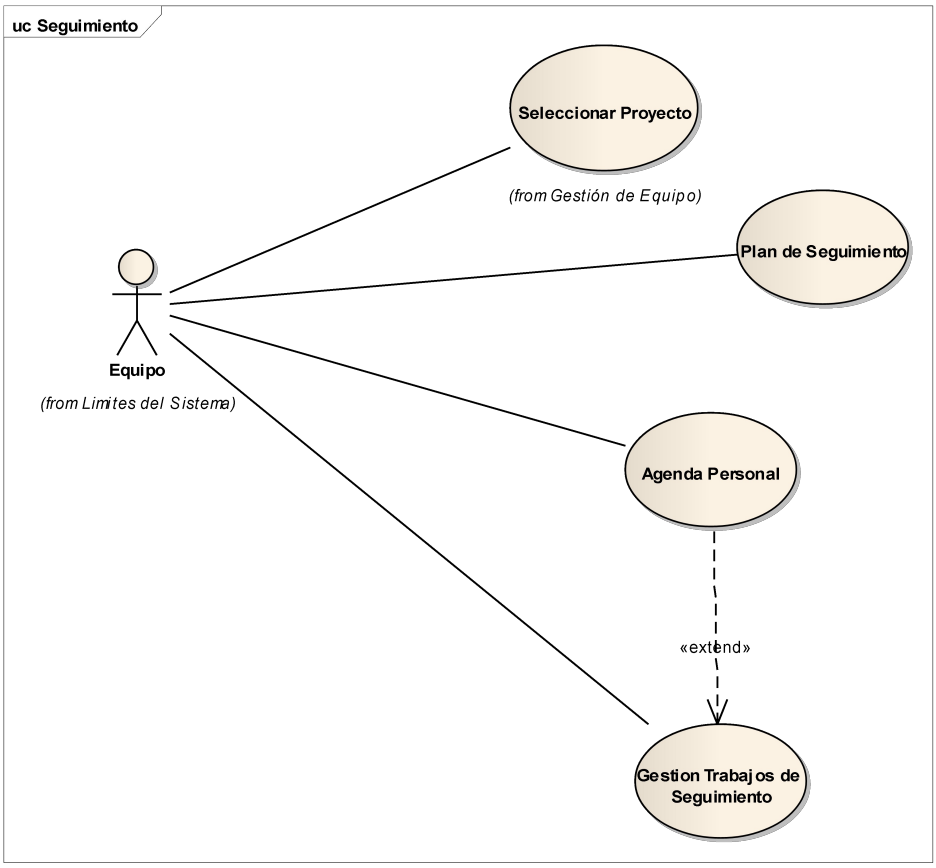


Imagen 49: Seguimiento

1.6.1 Agenda Personal

Agenda de tareas por persona.
Muestra según una persona específica participe del proyecto, todas las tareas que se tiene asignada en base a las salvaguardas por riesgo.
Características:

- Porcentaje de Finalización de Tareas: si la tarea realizada no se completa en un 100%.
- Observación
- Termino Bien. Se carga si la tarea de seguimiento termino con los objetivos estipulados.

Flujo de Eventos

Basic Path
Paso 1
El caso de uso comienza cuando el usuario elige la opción Agenda personal.
Basic Path
Paso 2
El sistema muestra una ventana en donde se ingresa el id de la persona
Basic Path
Paso 3
El sistema muestra en una ventana una lista con:

- las tareas a realizar por el personal seleccionado.

- Las tareas realizadas por el personal
- Las tareas faltantes.

Alternate

Alternativa 1

Si no se conoce el Id de la persona, CU "Seleccionar Persona"

1.6.2 Gestión Trabajos de Seguimiento

Gestión de Trabajo de Seguimiento del personal.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el Usuario presiona el botón Agregar, Modificar o eliminar.

Basic Path

Paso 2

- Si la opción es Nuevo o Modificar, el sistema muestra una ventana en donde el usuario puede cargar o modificar: % de Finalización de tarea, Observación de tarea, Observación de tarea.

- Si es Eliminar Pregunta si el usuario está seguro de la acción.

Basic Path

Paso 3

Opción Nuevo o modificación

- El usuario cargar o modifica los datos y presiona el botón Control. Si el % de Finalización es de 100%, el usuario marca la opción si la tarea termino bien.

Opción Borrar

- El usuario presiona Aceptar.

Basic Path

Paso 4

El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición *Estado:* Approved

Deben existir los seguimientos cargados.

PRE-condición *Estado:* Approved

Solo se muestran las tareas NO estén finalizadas a un 100%.

1.6.3 Plan de Seguimiento

Procesa el Plan de seguimiento para los riesgos en los cuales las salvaguardas poseen activado el parámetro de seguimiento.

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el usuario selecciona la opción "Plan de Seguimiento"

Basic Path

Paso 2

El sistema abre una ventana en donde muestra el CU "Seleccionar Proyecto"

Basic Path

Paso 3

El usuario seleccionar el proyecto y presiona el botón Aceptar.

Basic Path

Paso 4

El sistema genera un proceso en donde:

Carga en la base de datos el seguimiento del riesgo basado en las salvaguardas por el periodo de tiempo preestablecido.

Alternate

Alternativa

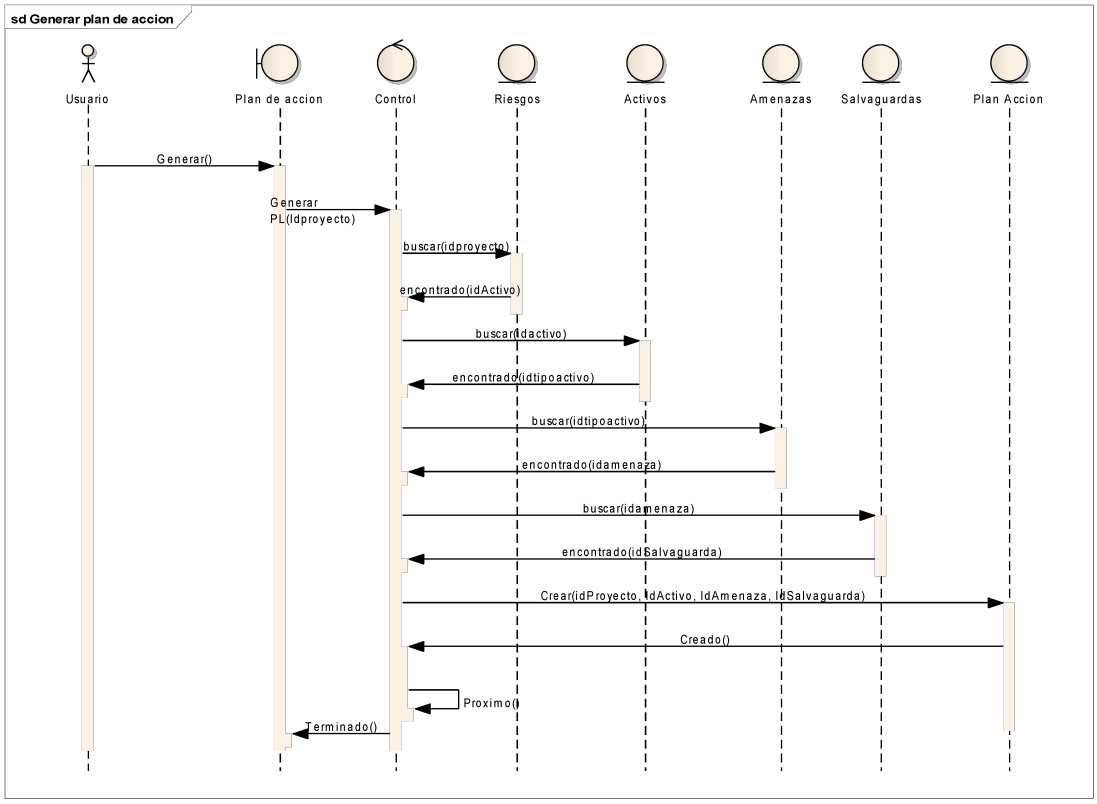
Si el dato ya existe en la base de dato, el sistema no lo incluye.

PRE-condición *Estado:* Approved

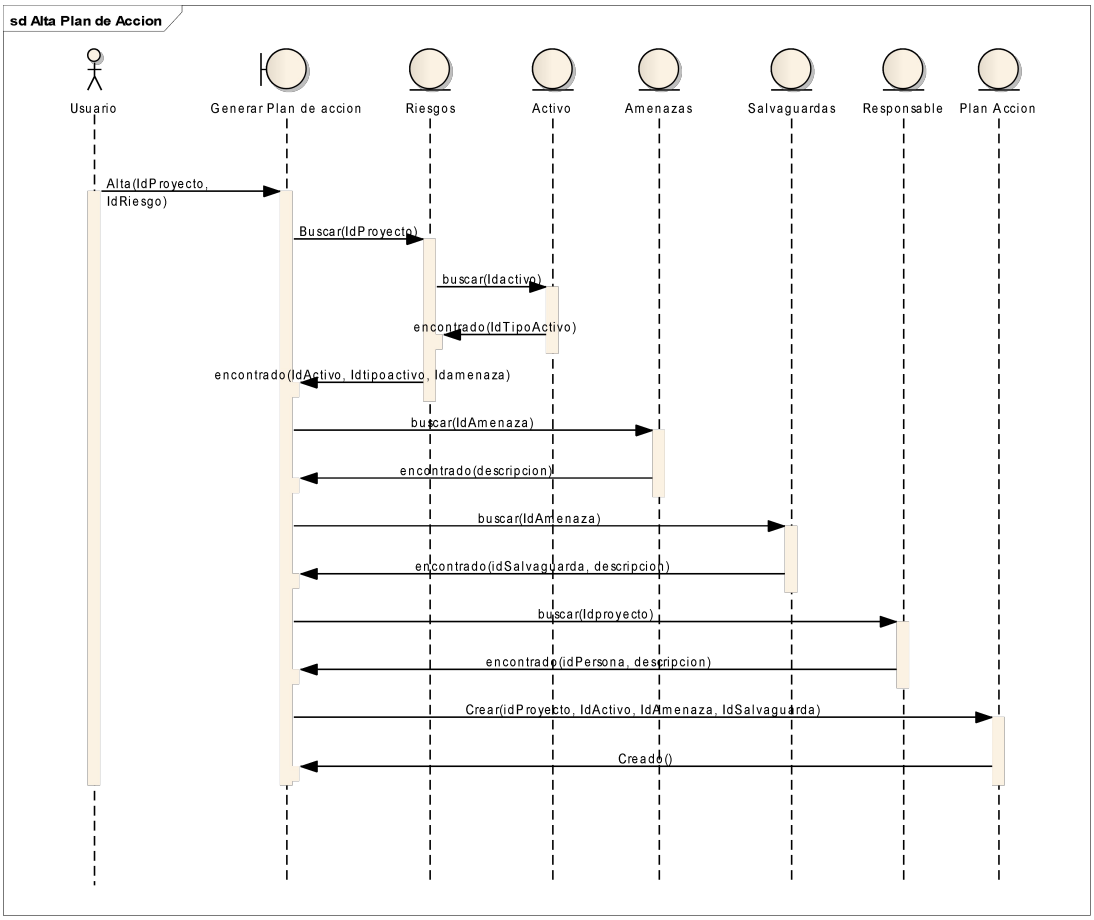
Es necesario que estén cargadas las salvaguardas.

Diagramas de secuencia

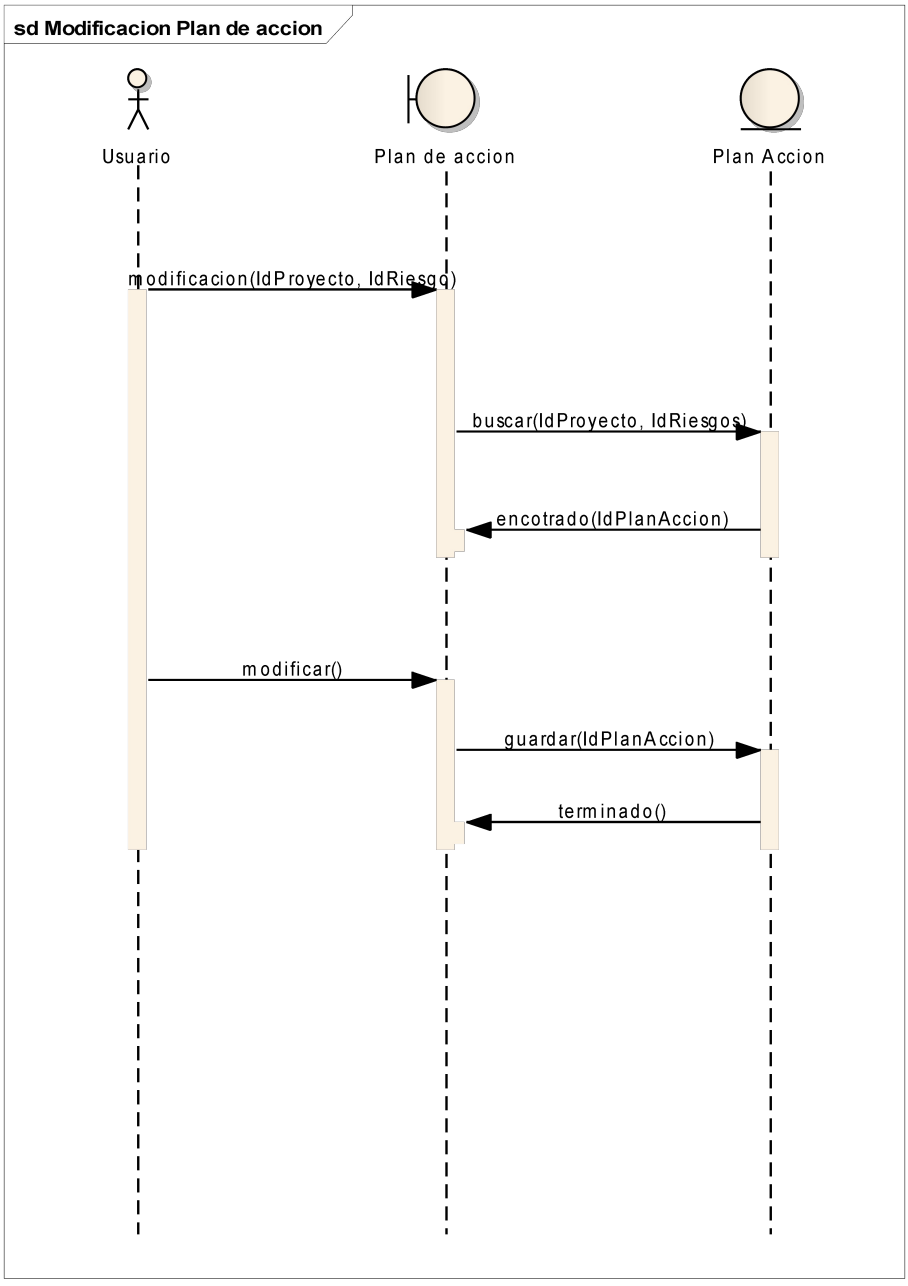
Generar plan de acción



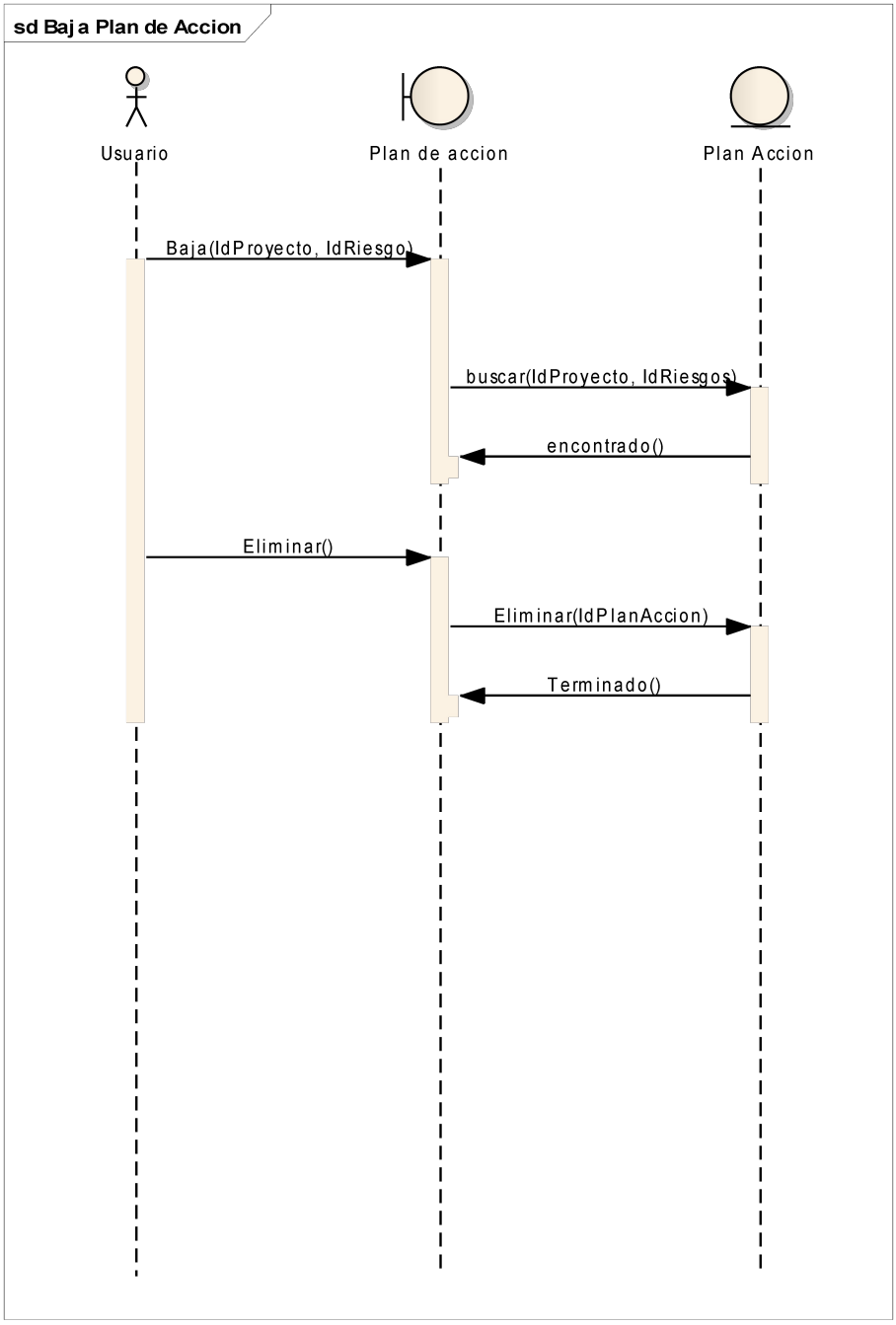
Alta plan de Acción



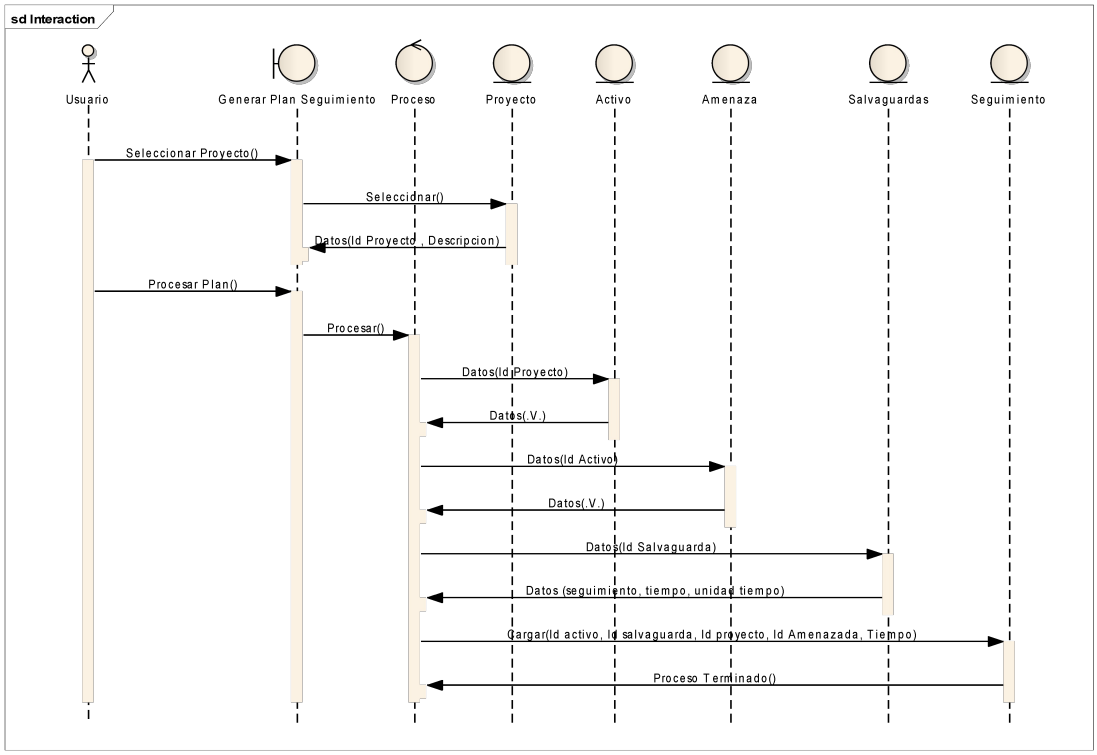
Modificación plan de acción



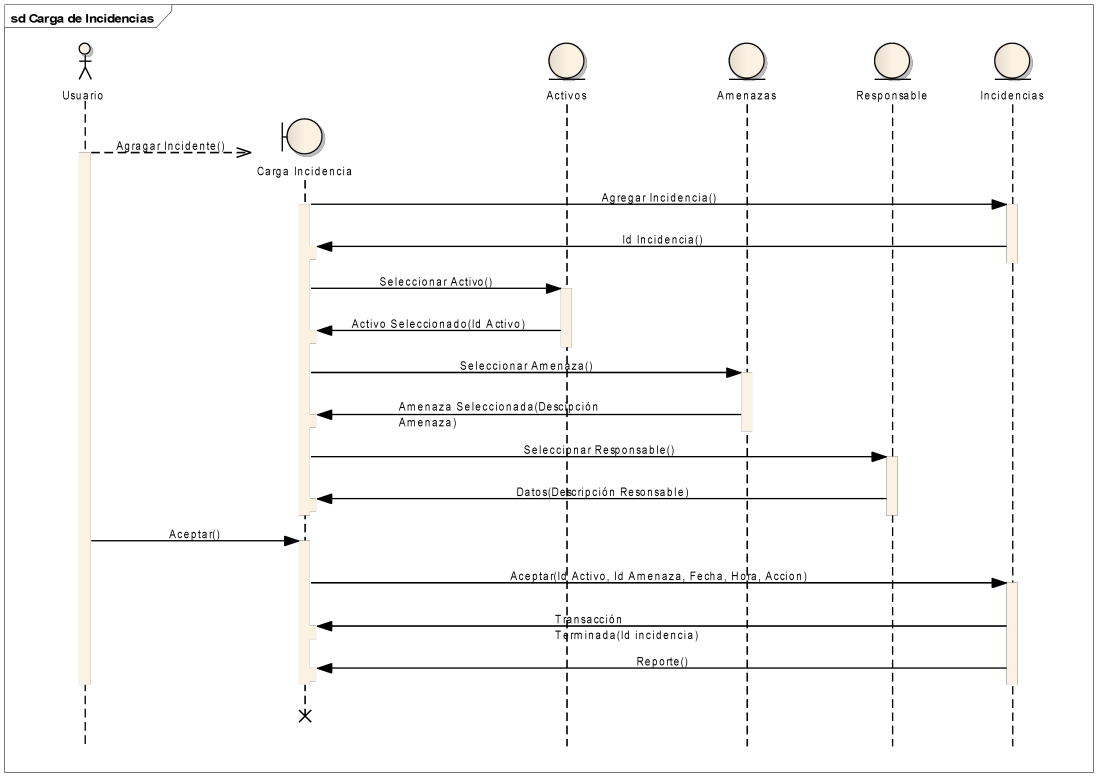
Baja Plan de acción



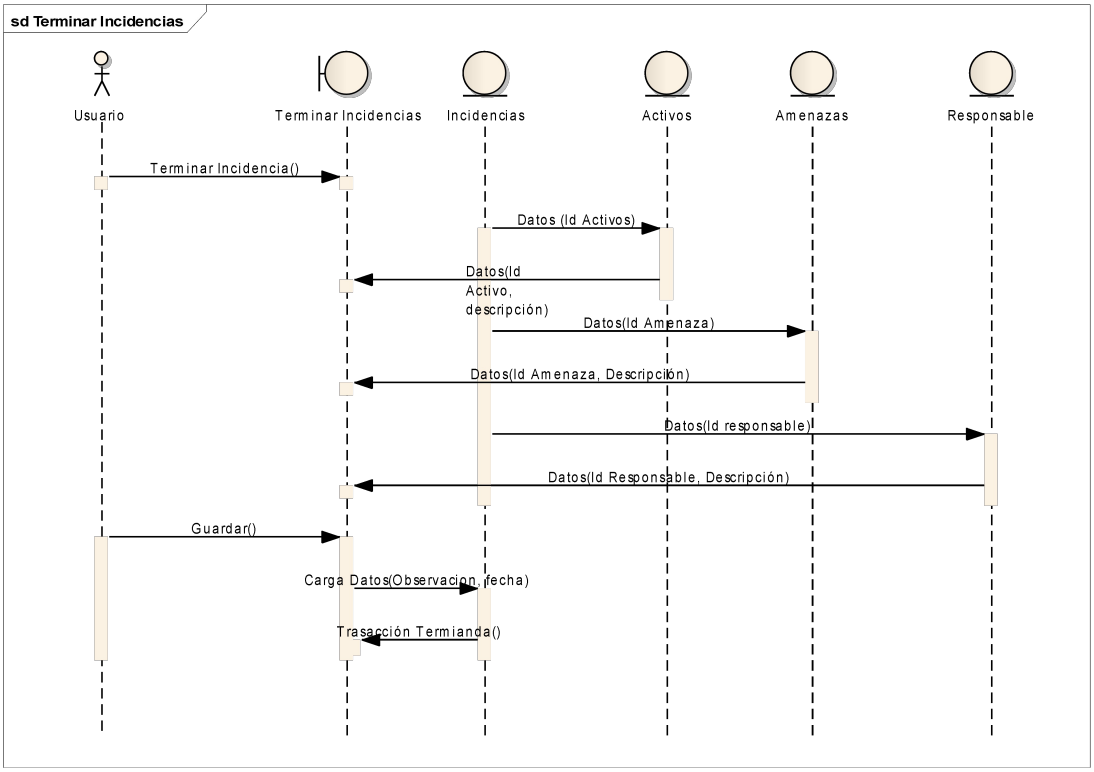
Plan de seguimiento



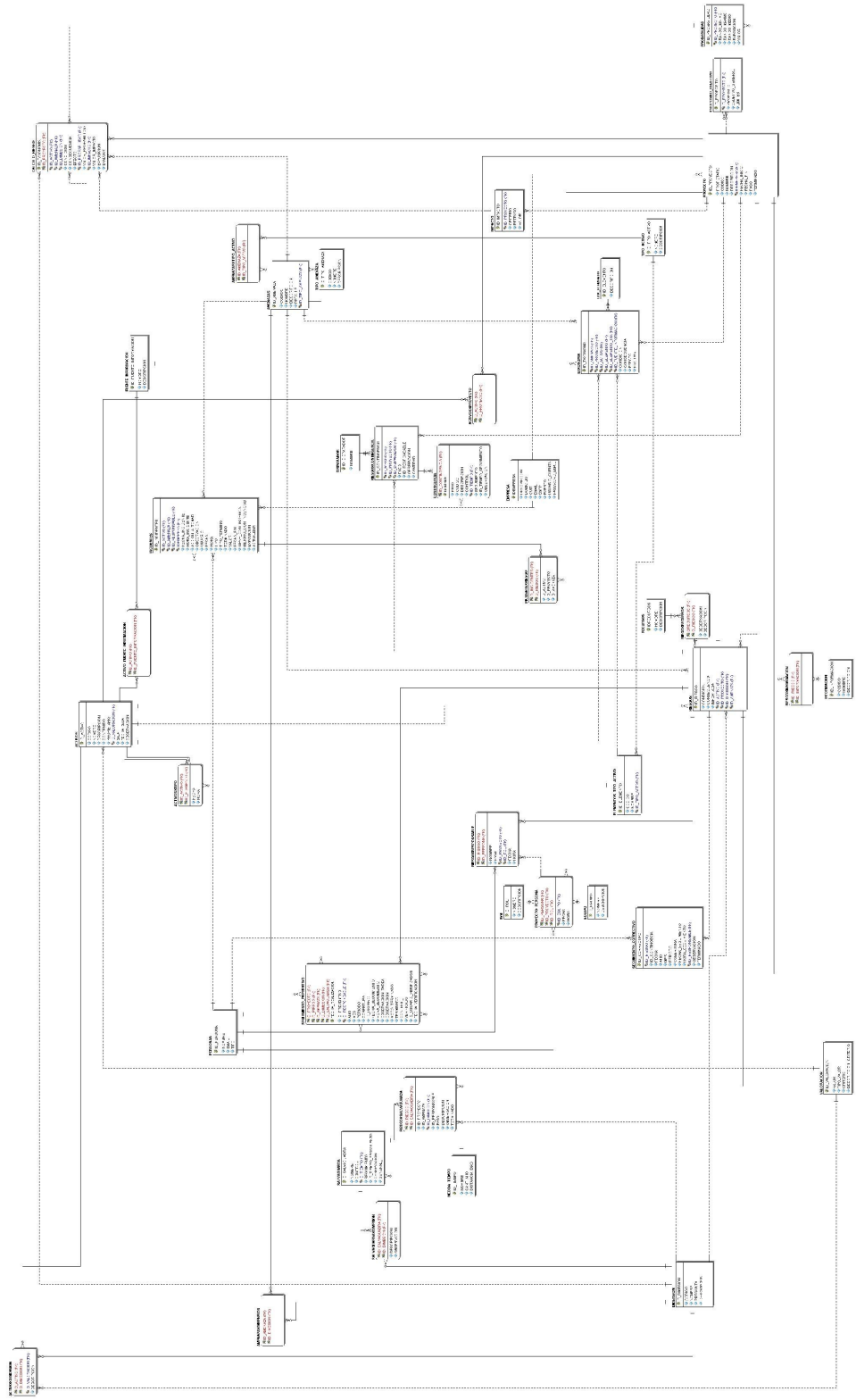
Carga de incidencias



Terminar incidencias



Modelo de Datos



Modelo de Pruebas

Casos de Pruebas

Modelo de pruebas

Agenda Personal

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	**Descripciones**	**Criterios Resultados**	**Detalles del Estado**
Nombre: PR101 *Clase: Sistema* *Tipo: Load*	*Descripción:* Probar % de fin de actividad *Entrada:* % de fin de acividad	*Criterio:* *Resultado:* El sistema debe mostrar un icono en el browse y cambiar el % de actividad por el nuevo.	*Estado: Pasó* *Fecha de Ejecucioón: 09/10/2010* *Ejecutado por:* *Controlado:*
Nombre: PR91 *Clase: Sistema* *Tipo: Load*	*Descripción:* Filtro de actividades por personal *Entrada:* Id persona	*Criterio:* Mostrar unicamente las actividades de = Idpersona *Resultado:* Todas las actividades de Id persona ordenadas por fecha	*Estado: Pasó* *Fecha de Ejecucioón: 06/10/2010* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:* *Sergio Daniel Caballero*

Carga Incidente

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	**Descripciones**	**Criterios Resultados**	**Detalles del Estado**
Nombre: PR111 *Clase: Sistema* *Tipo: Load*	*Descripción:* Controlar el tipo de riesgo. *Entrada:* Id Riesgo	*Criterio:* Tipo de riesgo correcto *Resultado:* No econtró ningun tipo de riesgo	*Estado: Falló* *Fecha de Ejecucioón: 15/09/2010* *Ejecutado por: Sergio Daniel Caballero* *Controlado: Sergio Daniel Caballero*
Nombre: PR131 *Clase: Sistema* *Tipo: Load*	*Descripción:* Controlar el tipo de riesgo. *Entrada:* Id Riesgo	*Criterio:* Tipo de riesgo correcto *Resultado:* Encontró el tipo de riesgos correcto	*Estado: Pasó* *Fecha de Ejecucioón: 22/09/2010* *Ejecutado por: Sergio Daniel Caballero* *Controlado: Sergio Daniel Caballero*

Nombre: *PR141* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Informar Plan de contingencias *Entrada:* Id Riesgo	*Criterio:* Plan_Contingencias.idriesgo = Riesgo.idriesgo *Resultado:* Reporte del plan de contingencias	*Estado:* *Pasó* *Fecha de Ejecucioón:* *20/10/2010* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:*

Estadísticas

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	**Descripciones**	**Criterios Resultados**	**Detalles del Estado**
Nombre: *PR161* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Generación de renkin estadistico por tipo de riesgo *Entrada:* IdRiesgo	*Criterio:* Cantidad de tipos de riesgos *Resultado:* Tabla con ranking de tipo de riesgos. Gráfico de torta expresando datos de la tabla.	*Estado:* *Pasó* *Fecha de Ejecucioón:* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:* *Sergio Daniel Caballero*

Generación Automática de Plan de Acción

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	**Descripciones**	**Criterios Resultados**	**Detalles del Estado**
Nombre: *PR61* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Se genera automaticamente el plan de acción para el riesgo seleccionado *Entrada:* Id de Riesgo	*Criterio:* cargar unicamente las salvaguardas para aquellos casos que cumplan con • El riesgo indicado • Amenaza del riesgo • tipo de activo • dimensión • salvaguarda *Resultado:* Solo muestra lo indicado	*Estado:* *Pasó* *Fecha de Ejecucioón:* *19/10/2010* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:* *Sergio Daniel Caballero*

Generación de seguimiento

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	Descripciones	Criterios Resultados	Detalles del Estado
Nombre: *PR71* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Generar automaticamente el seguimiento por cada id del plan de contingencia por proyecto *Entrada:* Id riesgo Id Proyecto	*Criterio:* Unicamente tiene que cargar a la base las salvaguardas que cumplan con la condición *Resultado:* Tabla de Salvaguardas por riesgo y proyecto	*Estado:* *Falló* *Fecha de Ejecucioón:* *20/10/2010* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:* *Sergio Daniel Caballero*
Nombre: *PR81* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Generar automaticamente el seguimiento por cada id del plan de contingencia por proyecto *Entrada:* Id riesgo Id Proyecto	*Criterio:* Unicamente tiene que cargar a la base las salvaguardas que cumplan con la condición *Resultado:* Tabla de Salvaguardas por riesgo y proyecto	*Estado:* *Pasó* *Fecha de Ejecucioón:* *08/10/2010* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:* *Sergio Daniel Caballero*

Gestion de Usuarios

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	Descripciones	Criterios Resultados	Detalles del Estado
Nombre: *Gestion de Usuarios* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Carga de usuarios , contraseñas y nivel de acceso al sistema. Modificación de contraseñas Modificación de nivel de acceso Baja de un usuario *Entrada:* Cargar tres usuarios distintos Modificar 2 contraseñas Modificar 1 nivel de acceso.	*Criterio:* *Resultado:* Funcionó ok	*Estado:* *Pasó* *Fecha de Ejecucioón:* *18/10/2010* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:* *Sergio Daniel Caballero*

	dar de baja el ultimo usuario cargado		

Loguin del sistema

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	**Descripciones**	**Criterios Resultados**	**Detalles del Estado**
Nombre: *Ingreso al sistema* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Probar que el sistema unicamente deje ingresar al mismo a los usuarios cuyo loguin coincidan en usuario y contraseña. *Entrada:* Se prueba ingresar 3 usuarios Juan Pedro Marcos	*Criterio:* Solo juan es el correcto *Resultado:* Deja el ingreso solo al usuario juan	*Estado:* *Pasó* *Fecha de Ejecucioón:* *Ejecutado por:* *Controlado:* *Sergio Daniel Caballero*
Nombre: *Nivel de acceso del usuario* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Probar que el nivel el sistema muestre unicamente los módulos cuyo nivel de acceso sea el correcto. *Entrada:* Marcos	*Criterio:* *Resultado:* La prueba no fue correcta.	*Estado:* *Falló* *Fecha de Ejecucioón:* *18/10/2010* *Ejecutado por:* *Controlado:*

Taxonomía

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	**Descripciones**	**Criterios Resultados**	**Detalles del Estado**
Nombre: *PR01* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* Cargar un proyecto *Entrada:* Se carga el proyecto 3	*Criterio:* unicamente se mostrará los activos del proyecto 3 *Resultado:* Muestra todos los resultados	*Estado:* *Pasó* *Fecha de Ejecucioón:* *04/10/2010* *Ejecutado por:* *Sergio Daniel Caballero* *Controlado:* *Sergio Daniel Caballero*
Nombre: *PR51* *Clase:* *Sistema* *Tipo:* *Load*	*Descripción:* *Entrada:* se ingresa el proyecto 3	*Criterio:* unicamente mostrar activos del proyecto 3 *Resultado:* Solo muestra activos del proyecto 3	*Estado:* *Pasó* *Fecha de Ejecucioón:* *Ejecutado por:* *Controlado:*

Terminar Incidencia

Tipo: CasoDeUso__
Estado: Proposed. *Versión* 1.0. *Fase* 1.0.

Nombre	**Descripciones**	**Criterios Resultados**	**Detalles del Estado**
Nombre: PR151 *Clase: Sistema* *Tipo: Load*	*Descripción:* Cambio de estado de la incidencia *Entrada:* Aceptación del fin de la incidencia	*Criterio:* Si cambia el estado a FIN *Resultado:* Cabio de estado a Estado = 'FIN'	*Estado: Pasó* *Fecha de Ejecucioón: 19/10/2010* *Ejecutado por: Sergio Daniel Caballero* *Controlado: Sergio Daniel Caballero*

Anexo III

Encuesta realizada

Cuestionario

Datos de la Organización

Razón Social: …OSPRERA……
Localidad | Provincia: ……Ciudad Autónoma de Bs.As. – Bs.As……
Su organización es de origen Privado o Estatal:…privada……

En la Organización posee un Plan de Gestión de Riesgos para lo referente al IT[1]

1. NO
   a. Causas (Marcar con una X)
      i. No se de que se trata:…..
      ii. Problemas de Inversión económica:…….
      iii. Falta Personal:…..
      iv. No cree necesario:…..
   b. Le interesaría poseer una metodología de gestión de riesgos basada en sus necesidades y con una software de apoyo: SI …. | NO …..

2. Si
   a. Que metodología Utiliza. ISO/ICC 27005:2008 para dar cumplimiento a la ISO 27.001……..
   b. ¿Posee un control de seguimiento?
      SI……
      ……
   c. ¿Posee Manuales actualizados?
      SI……
      ……
   d. ¿Se Actualizan periódicamente los posibles riegos que No estén en los manuales? SI, Bimestralmente……
   e. Se aplica a (Marcar con una X):
      i. Desarrollo de Software: ….X
      ii. Software en Gral. :…..
      iii. Hardware: …..X
      iv. Comunicaciones : …..X
      v. Personal de IT: …..X
      vi. Otros: …. ¿Cuál?
      .....
   f. Posee Plan de Contingencias básicas: SI…X NO …. ¿Cuál?
      ……
      ……
3. Es necesario mantener en reserva el nombre de la organización? :SI…X | NO…

[1] Tecnología Informática (Software, Hardware, Comunicaciones etc.)