

Universidad Nacional de Misiones

Facultad de Ciencias Exactas Químicas y Naturales

**Trabajo Final de Maestría en Tecnología de la
Información**

**Análisis y Gestión de Riesgo en Proyectos
Software**

**Un nuevo modelo integrando la metodología
SEI y Magerit3**

**Caso de estudio Servicio Médico Asistencial de
la Universidad Nacional de Misiones**

Autor: Lic. Sergio Daniel Caballero

Tutor: Dr. Horacio Daniel Kuna

Año: 2021

Agradecimiento

A los que me ayudaron en mi paso por la maestría, y a los que estuvieron siempre.

A mi SENSEI Dr. Horacio Kuna, por empujarme a ser cada vez mejor.

A la Educación Pública por darme la oportunidad de estudiar.

Resumen

Los activos tecnológicos de las organizaciones corren riesgos, estos representan un problema para que los activos se desempeñen con normalidad. El riesgo es la posibilidad de que ocurra una incidencia y este quede inoperativo o no se ejecute de forma óptima, es esencial, analizar los activos y buscar una manera de afrontar los riesgos que corren, gestionarlos para poder actuar, teniendo un plan, restablecer su funcionamiento de una manera rápida y económica.

Para tratar esta problemática, existen metodologías de análisis y gestión de riesgos, las cuales poseen procesos, técnicas y herramientas para su tratamiento. Las metodologías mayormente utilizadas están orientadas a organizaciones que puedan cumplir con las actividades solicitadas por estas metodologías, por lo que se denota, no están orientadas a una organización pequeña, con poco o nulo personal.

Si la organización es grande o pequeña, el problema persiste, no divisar, gestionar y afrontar los riesgos, puede llevar a cualquier tipo de empresas a tomar gastos imprevistos o no generar ganancias establecidas.

Afrontar, controlar y gestionar los riesgos en medianas y pequeñas organizaciones utilizando los recursos adecuados es el foco de este trabajo final de maestría, para lo cual, generar un método 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, es el desafío que propone el trabajo de investigación aplicada.

Se creó el método RIC que toma y combina prácticas de dos de las metodologías más utilizadas y conocidas en la actualidad, genera actividades para el control de las tareas detallando acciones preventivas para cuidar los activos, como así también gestiona las incidencias de la totalidad de los activos tecnológicos informáticos estén o no gestionados por el método, y por último determina la manera de comunicar la información sobre los riesgos, gestión, acciones preventivas e incidencias implicadas. Para lograr agilizar el reconocimiento, tratamiento y seguimiento de los riesgos, además de facilitar el uso del método, se desarrolló una herramienta asistente denominada SCRisk y se generó un caso de estudio real.

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

Abstract

The technological assets of organizations are at risk, these represent a problem for the assets to perform normally, the risk is the possibility that an incident occurs and this is inoperative or is not executed optimally, it is essential to analyze the assets and find a way to face the risks they run, manage them in order to act, having a plan, to restore their operation quickly and economically.

To deal with this problem, there are risk analysis and management methodologies, which have processes, techniques and tools for their treatment. The most commonly used methodologies are aimed at organizations that can comply with the activities requested by these methodologies, so it is denoted, they are not aimed at a small organization, with little or no staff.

If the organization is large or small, the problem persists, not identifying, managing and facing risks, can lead any type of companies to take unforeseen expenses or not generate established profits.

Facing, controlling and managing risks in medium and small organizations using the appropriate resources is the focus of this final master's work, for which, to generate a method developed with the aim of providing simplicity and agility, without losing formality in the tasks analysis and risk management, creating an intuitive framework, which streamlines the recognition of risks, is the challenge posed by applied research work.

The RIC method was created that takes and combines practices from two of the most widely used and known methodologies today, generates activities to control tasks, detailing preventive actions to take care of the asset, as well as managing the incidents of all the IT technology assets are managed or not by the method, and finally determines the way to communicate the information on the risks, management, preventive actions and incidents involved. In order to speed up the recognition, treatment and monitoring of risks, in addition to facilitating the use of the method, an assistant tool called SCRisk was developed and a real case study was generated.

Keywords: risk, risk analysis and management, taxonomy.

Índice

Tabla de contenido

Índice.....	5
Tabla de contenido	5
Índices de Figuras	8
Índice de Tablas	11
Capítulo 1 - Introducción	13
1.1 Objetivo general del trabajo	14
1.2 A quien está dirigido	14
1.3 Organización del Trabajo Final de Maestría	14
Capítulo 2 - Análisis de Riesgos	17
2.1 Riesgo.....	18
2.2 Análisis de riesgo	20
2.3 Clasificar el riesgo	21
2.4 Gestión de Riesgos	24
2.5 Estrategias para Tratar con Riesgos.....	28
2.6 Identificación de Riesgos	29
2.7 Modelo de Gestión de Riesgos SEI – CRM	33
2.7.1 Características	33
2.7.2 Cuestionarios basados en taxonomías	35
2.7.3 Etapa de la Metodología.....	40
2.7.4 Ventajas	43
2.7.5 Desventajas	43
2.8 Metodología Magerit.....	44
2.8.1 Características y objetivos	44
2.8.2 El Método	44
2.8.3 El Catálogo de los elementos	49
2.8.4 Guía de técnicas	50
2.8.5 Herramienta Software PILAR	51
2.8.6 Ventajas	53
2.8.7 Desventaja	54
2.9 Método Octave - S.....	54
2.9.1 Fases de OCTAVE – S	56
2.9.2 Metas del proceso.....	58
2.9.3 Cronograma	59
2.9.4 Ventajas	59
2.9.5 Desventajas	60
2.10 Gestión de Riesgos en Proyectos	60
2.10.1 Planificar la gestión de los riesgos	65
2.10.2 Identificar los Riesgos.....	68
2.10.3 Realizar el Análisis Cualitativo de Riesgos	69
2.10.4 Realizar el Análisis Cuantitativo de Riesgos	71
2.10.5 Planificar la respuesta a los riesgos	73
2.10.6 Implementar Respuestas	75
2.10.7 Monitores de Riesgo	77
2.11 Gestión del Conocimiento	79
2.11.1 Dato, Información y Conocimiento	80
2.11.2 Características de la Gestión del Conocimiento.....	83
2.11.3 Modelos de la Gestión de Conocimiento	86
2.11.4 Gestión de Conocimiento en la empresa	94
2.12 Análisis de Riesgos en Auditoría.....	97
2.12.1 Cobit 5.....	100
2.12.2 COBIT 5 para Riesgos	105

2.12.3 Riesgos en la Nube	112
2.12.4 Estructura del Riesgo en COBIT for Risk	113
Capítulo 3 - Problema encontrado y Solución sugerida.....	115
3.1 Problema Encontrado	116
3.2 Análisis y Gestión de riesgos en las organizaciones	118
3.3 Estado de AGR en las organizaciones.....	119
3.4 Métodos informales del análisis de riesgos	125
3.5 Metodologías poco adaptativas.....	126
3.6 Dificultades de gestionar los riegos en las pequeñas y medianas organizaciones ...	129
3.7 Solución Sugerida	130
Capítulo 4 - El Método RIC	133
4.1 Características.....	134
4.2 Capítulo R – Análisis, Gestión de Riesgos y seguimiento del Riesgo	137
4.2.1 Etapa Análisis	137
4.2.2 Etapa de Gestión	164
4.2.3 Etapa de Seguimiento y Control.....	168
4.3 Capítulo I - Registros de incidencias.....	170
4.3.1 Etapa de Incidencias	170
4.4 Capítulo C – Comunicación.....	178
4.4.1 Etapa Conocimiento Explícito.....	179
4.4.2 Conocimiento Tácito	180
Capítulo 5 -La Herramienta SCRisk	185
5.1 Introducción	186
5.2 Objetivos Generales del prototipo herramienta.....	186
5.3 Metodología elegida	186
5.3.1 AgEnD- Metodología Ágil y evolutiva	186
5.3.2 Justificación de la Elección metodológica	188
5.3.3 Tecnologías	189
5.3.4 Disciplinas de Soporte	190
5.4 Resultados del Proyecto.....	197
Capítulo 6 - Experimentación	199
6.1 Lugar.....	200
6.2 Estado Actual de la Organización	200
6.3 Entorno	200
6.4 Recursos Humanos	201
6.5 Capítulo R – Análisis, Gestión y seguimiento del riesgo.....	202
6.5.1 Etapa de Análisis	202
6.5.2 Etapa de Gestión	205
6.5.3 Etapa de Control y Seguimiento.....	206
6.6 Capítulo I – Gestión de Incidencias.....	207
6.6.1 Etapa de Incidencia	207
6.7 Capítulo C – Gestión del Conocimiento	208
6.7.1 Etapas Conocimiento Explícito y Tácito	208
6.8 Enseñanza.....	209
6.9 Validación del modelo	210
6.10 Conclusión.....	214
Capítulo 7 - Conclusión del trabajo Futuras líneas de investigación	215
7.1 Conclusión.....	216
7.2 Futuras líneas de investigación.....	217
Capítulo 8 - Referencia Bibliográfica	219
8.1 Bibliografía.....	220
8.2 Referencias Bibliográficas	220
Anexo I - Aspectos Particulares del Software y Estudio de Caso Software SCRisk	229
Aspectos particulares del sistema RIC.....	230

Lanzamiento del Estudio de caso	236
Capítulo R – Análisis Gestión y Seguimiento del riesgo	251
Etapa de Análisis	251
Etapa Gestión de los riesgos	265
Etapa - Seguimiento	271
Capítulo I – Gestión de Incidencias	274
Etapa - Incidencias	274
Capítulo C – Gestión de Conocimiento	280
Etapa Conocimiento Explícito	280
Anexo II - Tablas de Elementos y Amenazas	285
Estructura de desarrollo de proyecto	286
Elementos de un Activo	288
Amenazas	291
Anexo III - Artefactos utilizados en el Análisis y Diseño	303
Planificación del Proyecto	304
Modelo de Requisitos	306
Modelo de Casos de Uso	346
Diagramas de secuencia	441
Modelo de Datos	446
Modelo de Pruebas	448
Anexo IV -Encuesta realizada.....	453

Índices de Figuras

Figura 1 -Preocupaciones, Riesgos y Problemas	18
Figura 2- Descripción de Riesgo.....	19
Figura 3 -PA Gestión de Riesgos en CMMI	23
Figura 4 - Modelos de gestión de riesgos	24
Figura 5 -La Incertidumbre Descriptiva.....	29
Figura 6 - SEI Taxonomía	35
Figura 7 -TBQ - Proceso	40
Figura 8 -Etapas de gestión de riesgos SEI.....	43
Figura 9 - Pilar	52
Figura 10 -OCTAVE.....	55
Figura 11 –Fases de OCTAVE-S	58
Figura 12 -Ejemplos de Riesgos en Proyectos.....	61
Figura 13 –Riesgos - Área de conocimiento y Grupo de Procesos	63
Figura 14 -Tabla RBS	67
Figura 15 -Tabla Niveles de impacto	68
Figura 16 -Procesos medulares de la Gestión del Conocimiento.....	83
Figura 17 -El ciclo de la inteligencia	88
Figura 18 - modelo de gestión del conocimiento kpmg.....	90
Figura 19 -Necesidades de las partes Interesadas.	101
Figura 20 -Objetivo de gobierno	102
Figura 21 -Categorías de Habilitadores	103
Figura 22 -Separar Gobierno de Gestión	105
Figura 23 -Procesos	111
Figura 24 -- Estructura del Riesgo – fuente	114
Figura 25 -Tipo de Organizaciones relevados en la encuesta.....	119
Figura 26 -Distribución de las Provincias en la Encuesta.....	120
Figura 27 -Organizaciones que utilizan AGR.....	121
Figura 28 - Tipo de Metodología Utilizada	122
Figura 29 -Tipos de Metodologías de AGR utilizadas.....	123
Figura 30 -Ramas de la TI utilizadas en AGR	124
Figura 31 -Motivo por el cual No se utiliza AGR en las Organizaciones.....	125
Figura 32 - Cuestionario TBQ.....	128
Figura 33 - Método RIC.....	136
Figura 34 - Etapa de Análisis	137
Figura 35 - Etapa Gestión	164
Figura 36 - Etapa Control y Seguimiento	168
Figura 37 - Etapa de Incidencias	171
Figura 38 - Etapa Conocimiento Explícito.....	179
Figura 39 - Etapa Conocimiento Tácito	181
Figura 40 - Requisitos Funcionales.....	196
Figura 41 - Generación de Taxonomía.....	204
Figura 42 - Asignación de % Probabilidad e Impacto	205

Figura 43 - Carga de incidencia	206
Figura 44 - Finalización de Incidencia.....	208
Figura 45 - Informe estadístico de incidencia por activo gestionado.....	208
Figura 46 - Respuesta de coherencia.....	212
Figura 47 - Respuesta de relevancia.....	213
Figura 48 - Respuesta de claridad	213
Figura 49 - Respuesta de suficiencia.....	214
Figura 50 -Login de acceso al sistema	237
Figura 51 -Menú Parámetros.....	238
Figura 52 -Gestión de Tipo de Activos	239
Figura 53 -Gestión de Elementos.....	239
Figura 54 -Gestión de Dimensión	240
Figura 55 -Gestión de Valoración	241
Figura 56 -Tipo de Amenazas	242
Figura 57 - Gestión de Amenazas	243
Figura 58 - Amenazas por tipo de Activo	244
Figura 59 - Amenazas por Dimensión	245
Figura 60 - Gestión de Salvaguardas	246
Figura 61 - Asignación de Dimensiones a la Salvaguarda.....	247
Figura 62 - Gestión de la Organización	248
Figura 63 - Gestión de fuentes de información.....	249
Figura 64 - Gestión de medidas de tiempo.....	250
Figura 65 - Menú Etapa 1.....	251
Figura 66 - Gestión de Activos	252
Figura 67 - Asignación de elementos a un activo	253
Figura 68 - Dependencia de activos	254
Figura 69 - Asignación de fuente de información.....	255
Figura 70 - Gestión de proyectos	256
Figura 71 - Asignación de propósitos y objetivos al proyecto.....	257
Figura 72 - Asignación de activos al proyecto.....	257
Figura 73 - Gestión de equipos	258
Figura 74 -Selección de proyecto para generar la taxonomía.....	259
Figura 75 - Gestión de elementos y fuentes de información.....	260
Figura 76 - Gestión de declaración	261
Figura 77 - Tabla de probabilidad de ocurrencia por riesgo	262
Figura 78 - Impacto de ocurrencia por proyecto	263
Figura 79 - Asignación de probabilidad e impacto	264
Figura 80 - Exposición al riesgo	265
Figura 81 - Información de riesgos	266
Figura 82 - Recursos	267
Figura 83 - Asignación de plan de acción.....	268
Figura 84 - Plan de contingencia.....	269
Figura 85 - Información necesaria	269
Figura 86 - Responsable.....	270
Figura 87 - Recursos	270
Figura 88 - Menú Seguimiento	271
Figura 89 - Plan de seguimiento	272

Figura 90 - Agenda de actividades.....	272
Figura 91 - Gestión de control de Seguimiento	273
Figura 92 - Menú de seguimiento	274
Figura 93 - Carga de incidente	275
Figura 94 - Control de tipo de riesgo	276
Figura 95 - Detalle de riesgos encontrado	277
Figura 96 - Reporte Plan de contingencias	278
Figura 97 - Finalización de un incidente.....	279
Figura 98 - Menú de Informes	280
Figura 99 - Menú de Informes	281
Figura 100 - Parámetros de estadística.....	282
Figura 101 - Estadística de incidentes por activo evaluado	283
Figura 102 - Seguimientos realizados	284

Índice de Tablas

Tabla 1 - Tipo de Organizaciones relevadas en la Encuesta.....	119
Tabla 2 – Distribución de las Provincias participantes de la encuesta.....	119
Tabla 3 - Formulario Relevamiento de Activos.....	139
Tabla 4 - Formulario Dependencia de Activos	140
Tabla 5 - Importancia del Activo	141
Tabla 6 -Valoración del Activo.....	141
Tabla 7 -Dimensiones del Activo.....	143
Tabla 8 - Tipos de Activos	143
Tabla 9 - Formulario de Tipo de Activos.....	144
Tabla 10 - Formulario de Elementos de los Activos.....	145
Tabla 11 - Formulario de Fuentes de Información.....	146
Tabla 12 - Formulario del Proyecto	148
Tabla 13 - Formulario de Objetivos y Límites del Proyecto.....	149
Tabla 14 - Formulario de Activos por Proyectos	149
Tabla 15 - Formulario Equipo de Trabajo.....	150
Tabla 16 - Formulario de Ruta de Acceso a Activos críticos	152
Tabla 17 - Formulario de Activos relacionados.....	153
Tabla 18 - Formulario de Amenazas de tipo Natural	155
Tabla 19 -Formulario de Amenazas de Origen Industrial.....	155
Tabla 20 -Formulario de Amenazas Errores y Fallos No deseados	155
Tabla 21 -Formulario de Amenazas de Ataques Intencionados.....	155
Tabla 22 - Listado de Taxonomía de Riesgos o Amenazas	156
Tabla 23 - Formulario de Declaración del Riesgo	158
Tabla 24 - Tabla de Ejemplo de Probabilidad de Riesgo.....	159
Tabla 25 - Formulario de Probabilidad de Ocurrencia.....	159
Tabla 26 - Formulario de Impacto	161
Tabla 27 - Ejemplo de Estimación de impacto	161
Tabla 28 - Formulario de Impacto del Riesgo	162
Tabla 29 - Formulario de Exposición al Riesgo.....	164
Tabla 30 - Formulario de Gestión del Riesgo	167
Tabla 31 - Formulario de Seguimiento de Plan de Acción	170
Tabla 32 - Formulario de Denuncia de Incidencia.....	172
Tabla 33 - Formulario de Control de Activo.....	173
Tabla 34 -Informe Plan de Contingencia de Activos ANR - AG	175
Tabla 35 -Formulario de Informe al Responsable.....	177
Tabla 36 - Formulario finalización de Incidente.....	178
Tabla 37 - Informe de seguimiento	180
Tabla 38 - Estadística	180
Tabla 39 - Informe del Incidente.....	181
Tabla 40 - Informe de Experiencia Propia de Riesgos.....	182
Tabla 41 - Enseñanzas de la experimentación	210
Tabla 42 - Amenazas Magerit V3	291

Objetivo General

El objetivo de trabajo final de maestría es crear un método para tratar el análisis y gestión de riesgos, planificación de tareas de control, gestionar las incidencias que poseen los activos (pueden ser tangibles (hardware), intangibles (software y datos) o recursos humanos (personas)[85]) y que provoquen una alteración en la gestión del riesgo, y gestionar la comunicación de la información tratada por el método, todo adaptado a los requerimientos y necesidades informáticas y tecnológicas de las pequeñas y medianas empresas, investigando las metodologías más frecuentemente utilizadas de análisis y gestión de riesgos en IT, la metodología SEI CRM la metodología Magerit V3 y OCTAVE-S, los riesgos a los cuales se enfrentan los proyectos y debido a que el ARG¹ es una de las prácticas utilizada por auditores informáticos se estudiará el marco de trabajo COBIT; además analizar la gestión de conocimiento para poder comunicar la información generada por el método.

Para validar el método se plantea generar una herramienta prototipo, que automatice procesos, gestione activos, incidencias y genere información. El método y la herramienta servirán para analizar y gestionar probables riesgos que pueden tener los activos; establecer un procedimiento de monitoreo 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, esto contribuirá a eliminar o minimizar los incidentes ocurridos, además, de proteger los activos de las organizaciones para que estos no estén expuestos a riesgos desconocidos o el impacto sea mínimo y controlado.

¹ Análisis y gestión de riesgos.

Capítulo 1 - Introducción

Este capítulo se presenta brevemente el trabajo a desarrollar y su estructura organizativa.

1.1 Objetivo general del trabajo

Esta Trabajo Final de Maestría trata sobre el desarrollo de un método para el análisis y gestión de riesgos, planificación de tareas de control, gestionar las incidencias que poseen los activos y que provoquen una alteración en la gestión del riesgo, y gestionar la comunicación de la información, para ser implementadas en pequeñas y medianas empresas, el caso de estudio de la aplicación del método es el Servicio Médicos Asistencial de la Universidad Nacional de Misiones.

El objetivo principal del trabajo es proporcionar un método simple, intuitivo y formal, para agilizar el reconocimiento, tratamiento y seguimiento de los riesgos, para agilizar y viabilizar el uso del método se desarrollará una herramienta.

1.2 A quien está dirigido

El presente trabajo de Trabajo Final de Maestría se encuentra dirigido principalmente informáticos que se encuentren al frente o con un rol de encargados o gerentes de TI.²

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 del Trabajo Final de Maestría

El documento se divide en siete capítulos y en cuatro anexos que abarcan la totalidad del Trabajo Final de Maestría.

- El Capítulo 2. Estado del arte investiga, que son los riesgos, sus características, método y metodologías que los tratan, como SEI CMR y Magerit v3, ventajas

² Tecnología de la Información

y desventajas de cada una, software utilizado. Por otro lado, estudia los riesgos en proyectos analizando el PMBOK, auditoría y riesgos, que factores entrelazan la gestión del riesgo con la auditoría y por último la gestión del conocimiento, para poder generar valor de los procesos generados con el método en la empresa.

- El Capítulo 3. Describe los problemas investigados sobre la gestión del riesgo en las organizaciones, describe la encuesta realizada en la investigación y fundamenta una solución con un método adaptativo propio.
- El Capítulo 4. Se expone las características principales, los capítulos, etapas y procedimientos del método desarrollado que lo denominamos “RIC” siglas del título aprobado del proyecto “Un nuevo modelo integrando la metodología SEI y Magerit3”.
- 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 y los aspectos particulares del sistema.
- El Capítulo 6. Se informa sobre la experimentación del método y herramienta, validando el mismo en un caso real, se informa sobre las enseñanzas obtenida de la experimentación.
- El Capítulo 7. Se expone las conclusiones del trabajo realizado y direcciones de investigaciones futuras.
- El Capítulo 8. Muestra la Bibliografía que se utilizó para la realización del presente trabajo.
- Anexo I. Aspectos Particulares del Software y Estudio de Caso Software SCRisk-

- Anexo II. Tablas referencia Elementos y Amenazas.
- Anexo III. Muestra los artefactos utilizados en el análisis, diseño y desarrollo del sistema RIC.
- Anexo IV. Muestra la encuesta realizada a las organizaciones.
- Anexo V. Resultado de la encuesta realizada.

Capítulo 2 - Análisis de Riesgos

2.1 Riesgo

Se puede pensar en un riesgo, como la probabilidad que ocurra una pérdida o que un activo sea afectado en su funcionamiento [1], como así también el impacto asociado.[2]

En muchas ocasiones se confunde preocupación, riesgos y problemas, se debe entender que:

- Preocupación puede ser cualquier situación sobre la cual existen dudas en un delimitado contexto, se valora como un probable riesgo.
- Problema es un riesgo, que ciertamente se ha producido (véase Figura 1 -Preocupaciones, Riesgos y Problemas).

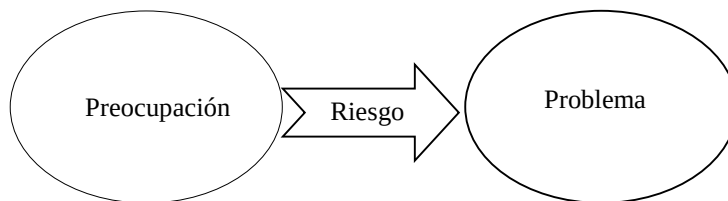


Figura 1 -Preocupaciones, Riesgos y Problemas

Un riesgo es la relación entre una situación real de proyecto y una situación no deseada es decir la condición (estado actual) y la consecuencia (estado de pérdida).

- Condición: constituye una situación existente en el proyecto, prevista por el equipo, que puede significar pérdida o reducción de beneficios.
- Consecuencia: refiere a la situación no buscada para el activo, que podría ser la resultante de la ocurrencia.

Estas dos partes, se articulan 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 2 -Descripción de Riesgos).

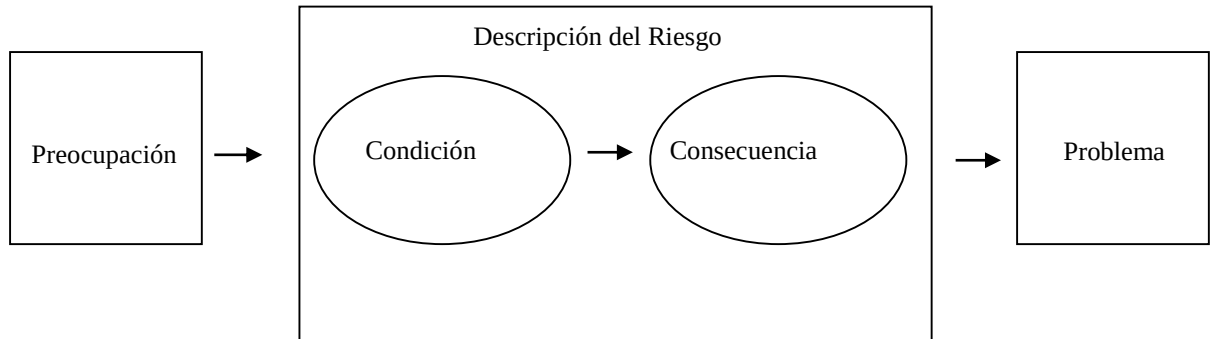


Figura 2- Descripción de Riesgo

El riesgo que nos concierne, es aquel que puede producir a futuro un problema. Lo primordial, es darnos cuenta hoy de los riesgos futuros y tomar acciones de control para que no suceda o realizar tareas en el momento justo, las pérdidas pasadas, son importantes, debido a que se puede prever el margen de ocurrencia de la misma. Todo riesgo implica un cambio de acciones, opiniones y modalidad de trabajo.

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

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

Al definir un riesgo, la expresión debe ser estricta, específica y completa, permitiendo el análisis del origen, el impacto y el despliegue de acciones o respuestas que prevengan y reduzcan los efectos. Es útil añadir información de contenido a un riesgo, siendo obligación para contribuir con las personas, que no conocen los detalles del proyecto, a la comprensión del tema[5].

En la descripción se debe descartar el uso de abreviaturas o acrónimos que impliquen dificultad de comprensión, generalizaciones y detalles irrelevantes. La definición no debe contener razones o características que generen dudas en la comprensión y el entendimiento[6].

Para llevar a cabo una administración eficiente, la descripción de un riesgo no

es la única información que debe estar disponible y cotejada, aunque tiene un grado significativo de importancia, también es necesario considerar una serie de variables componentes. Por lo tanto, normalmente el documento de descripción de riesgos o la Base de Datos de Riesgos se prepara por separado del Plan de Riesgos.

2.2 Análisis de riesgo

La etapa inicial de un análisis de riesgo, comienza generando un proyecto y examinando, los conceptos básicos como ser: los activos, objetivos y límites, equipos de trabajo, clasificación y se prolonga a lo largo de su ciclo de vida, finaliza con la aceptación del resultado del proyecto. Por lo general, se basa en una metodología que utiliza procesos, métodos y herramientas para gestionar los riesgos hallados; además, posee métodos específicos que identifican riesgos más valorados y estrategias de gestión; provee un entorno disciplinado para la toma de decisiones de manera pro activa basándose constantemente en identificar que puede salir mal[7]; la Gestión de Riesgos es importante debido a que ayuda a evitar desastres, re-trabajo y sobre-trabajo, pero aún más importante, porque estimula la generación de situaciones del tipo ganar-ganar[8].

Conocer el riesgo que poseen los activos, el alcance de los mismos, el valor que está en juego si no funciona de forma correcta, es la clave de todo AGR, para lo cual, llevar a cabo una Gestión de Riesgos, para poder entenderlo, interpretarlo y tratarlo de forma eficiente[9].

Analizar correctamente estos riesgos otorga la posibilidad de optimizar los recursos, para incrementar ganancias y minimizar pérdidas. Fundamento demás objetivo para que hacer hincapié en el grado de importancia que posee el análisis de Riesgos, en todo tipo de proyectos y en este trabajo, el foco está puesto en los proyectos de TI.

La importancia de esta práctica queda explícitamente incluida en el CMMI³, que es el 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 PA⁴ primordiales de Nivel 3 análisis y gestión Riesgos[10].

2.3 Clasificar el riesgo

Clasificar los riesgos implica el valerse de una estructura, en la cual los riesgos son agrupados teniendo en cuenta sus diversidades o clasificaciones comunes, sirviendo como base de consulta al momento de llevar a cabo la tarea de Identificación de los Riesgos [11], [12] esta clasificación la llamamos taxonomía o taxonomía de riesgos.

La taxonomía es la clasificación ordenada de los elementos según su relación evidente; esta fundamentación, presenta las taxonomías como un instrumento de utilidad relevante en las diferentes ramas de la ciencia y la industria, tiene el propósito de organizar y dar acceso a numerosos componentes relacionados entre sí de manera trascendental.

Podemos decir que la identificación del riesgo y las taxonomías, adquieren un rol fundamental entre los objetivos vinculado 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).

Los riesgos se clasifican en categorías definidas, que proporcionan un medio para revisarlos de acuerdo con su fuente, taxonomía o componente del proyecto. Los riesgos relacionados o equivalentes se pueden agrupar para un manejo eficiente. Las relaciones de causa y efecto entre los riesgos relacionados están documentadas.[13]

³ Capability Maturity Model Integration, modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software.

⁴ Process Area, Area de procesos

La figura N° 3 muestra los distintos objetivos para la gestión de riesgos en CMMI, que se deben implementar para la gestión de riesgos en CMMI, y se agrupan de acuerdo con el flujo de trabajo propuesto[10].

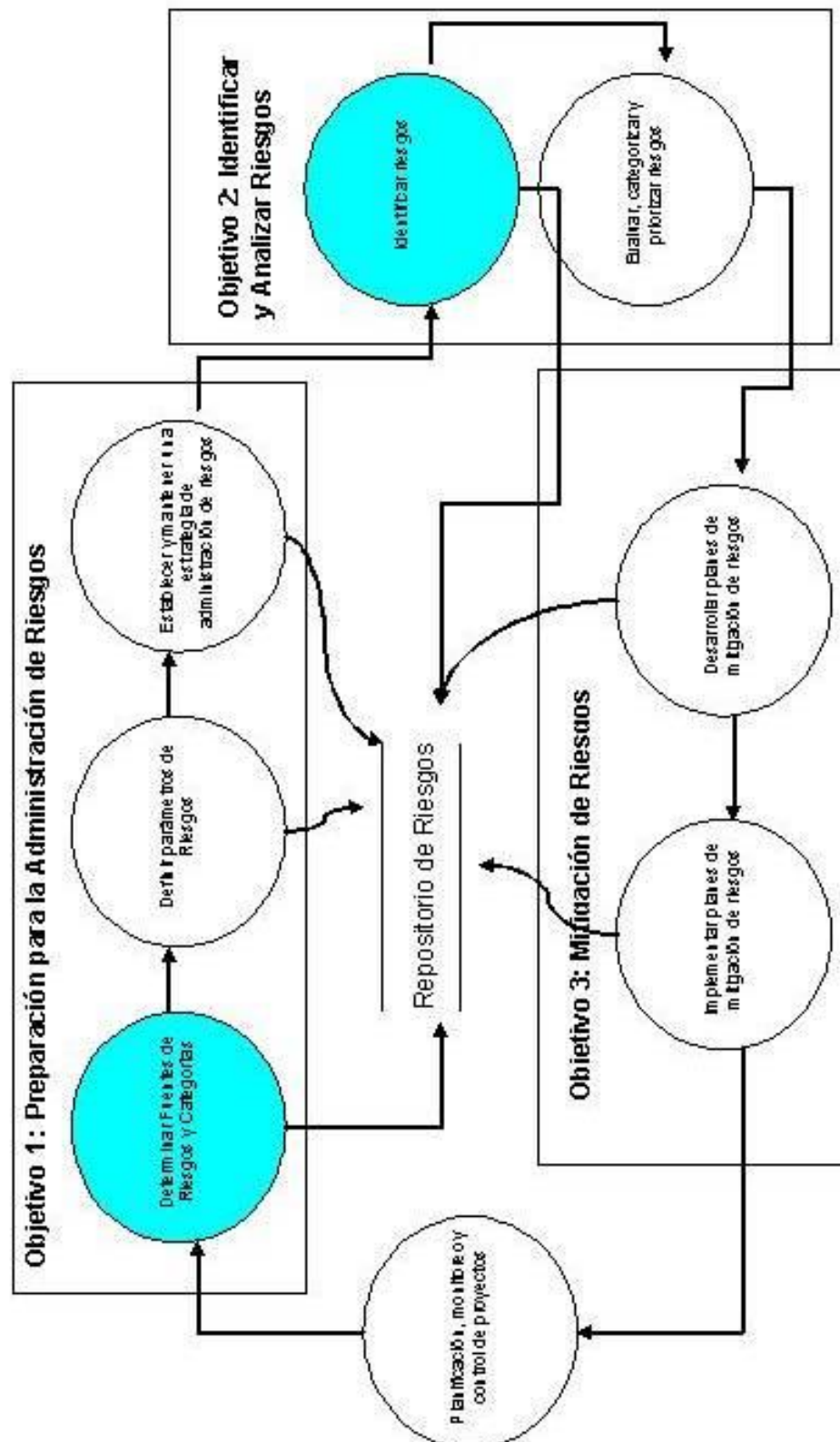


Figura 3 -PA Gestión de Riesgos en CMMI [10]

2.4 Gestión de Riesgos

La gestión del riesgo comienza por lo general, luego de terminada la etapa de exposición, en la cual, la mayoría de las metodologías identifican aquellos riesgos que serán gestionados y los que se desechan.

La gestión de riesgos de los proyectos permite, además, definir en forma estructurada, operativa y organizada una serie de actividades de control denominados plan de acción. En la mayoría de los casos, estas prácticas están destinadas a impedir que los riesgos se transformen en problemas.

Existe diversos modelos de Gestión de Riesgos (Ver figura 4), sacando un factor común de pasos para gestionar un riesgo, los diferentes modelos, se pueden enumerar como:

- Identificación: trata sobre la identificación y clasificación de los riesgos, activos.
- Análisis: trata sobre el proceso de análisis de los riesgos, donde se detallan sus características y se realiza la exposición de los mismos.
- Planificación: trata sobre las tareas de control que se deben realizar para evitar que el riesgo no se transforme en un problema.
- Seguimiento y Control: Trata sobre acciones preventivas sobre los riesgos, actividades de control.

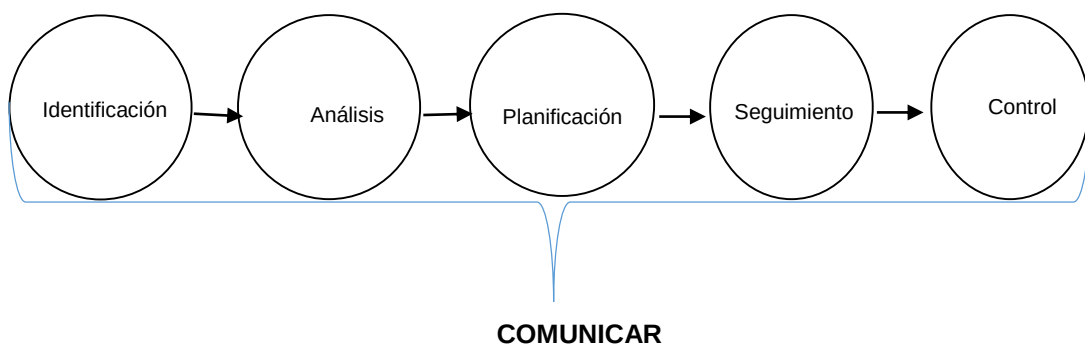


Figura 4 - Modelos de gestión de riesgos

La tecnología informática está impuesta en la totalidad de los negocios y pymes estudiados, todos ellos son activos de la organización, por lo cual para administrarlos se deben generar planes y proyectos de adquisición, mantenimiento y gestión de estos activos, por ser activos poseen riesgos, por ello, la gestión de riesgos, es primordial; dado que, los emprendimientos tecnológicos están caracterizados por una serie de aspectos, que incrementan la presión sobre la TI, 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 normativas legales y técnicas, que podrían resultar en una variación del manejo de los activos.
- 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.

El laboratorio de tecnología de la empresa Motorola en 1999 generó aspectos a tener en cuenta, en la política de gestión de riesgos de la organización exitosa [14]:

1. Los riesgos relacionados con los proyectos de desarrollo de software deben ser reconocidos, examinados, anticipados y estableciendo un Plan de Gestión de Riesgos.
2. El Plan de Gestión de Riesgos debe ser correctamente documentado. Esta documentación podría ser parte del Plan de Proyecto.
3. 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.
4. 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.

La organización American Sistemas Corporation [ASC], también generó unas reglas se describen a continuación:

- ✓ Regla #1:
“Las organizaciones 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, la empresa Microsoft define unos de principios básicos en los cuales asentar los procesos de gestión de riesgos[15]:

- Agilidad: Una visión proactiva logra que un equipo asuma los cambios y los transforme en una oportunidad.
- Potenciar la comunicación: 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 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.
- 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: Los riesgos deben ser considerados como el único modo de crear la ocasión apropiada para conquistar los objetivos del proyecto.
- Valoración continua: Esta consideración se debe, a los continuos cambios en los proyectos y los contextos operativos.
- 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.
- Las situaciones no deben juzgarse sólo por el número de riesgos: Recordar que,

un riesgo es únicamente una probabilidad, no la seguridad de una pérdida ni un resultado por debajo de lo esperado. Por lo cual no se debe considerar la cantidad de riesgos encontrados, si no, la cantidad que se debe gestionar.

Resumiendo, podemos decir que la gestión de riesgos es un proceso pro activo, llevado a cabo por un equipo que investiga los orígenes y tratamientos de los riesgos de una forma cíclica, organizada y ordenada, basándose en una metodología.

2.5 Estrategias para Tratar con Riesgos

Los riesgos deben ser tratados como una actividad ordenada y cualitativa, deben ser individualizados y clasificados, ya que cada uno de ellos representan la posibilidad de un problema, por lo cual existen estrategias comunes para poder administrarlos.

Cada riesgo o conjunto de riesgos, según su clasificación deben poseer una estrategia para su abordaje, las mismas pueden ser diferentes a la hora de su análisis pero también pueden cambiar si es necesario a la hora de la re evaluación o en distintas revisiones del proyecto [16].

Existen diferentes estrategias de respuesta, entre las más reconocidas y utilizadas pueden destacarse[17]:

- Aceptar: Si es riesgo posee baja escala de impacto de producirse en la organización y su gestión genera un costo mayor al del impacto. Una manera es aceptar el riesgo, sin tomar medidas preventivas.
- Evitar: Esta técnica se enfoca en impedir la posibilidad de ocurrencia de un riesgo, por lo contrario, a la aceptación, se emplean mecanismo gestión y control de manera de evitar el riesgo en su máxima expresión, si se trasformara en un problema, el impacto sería preponderante para la organización.
- Controlar: Esta práctica sugiere asegurar mecanismos de control sobre el riesgo para reducir la probabilidad de ocurrencia y por consiguiente su impacto.

- Investigar: Es utilizada cuando no se conoce, el daño exacto que puede producir el riesgo, no existe información de probabilidad de ocurrencia o planes de acción para controlar el mismo.
- Reducir: Esta práctica se adopta activamente con la finalidad de alcanzar una reducción de los riesgos en base a la ejecución de una sucesión de “acciones planificadas y constantes”.
- Transferir: trasladar el riesgo a otro proyecto, persona o institución, es una técnica utilizada para bajar costos de gestión y control. Trasferir un riesgo, no significa transferir la responsabilidad.

2.6 Identificación de Riesgos

La identificación de los riesgos posee el objetivo de adquirir una adecuada identificación de los problemas factibles en el proyecto, y la administración adecuada de los mismos, 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[6], la figura 5 muestra como la identificación es la acción por la cual se conoce al riesgo.

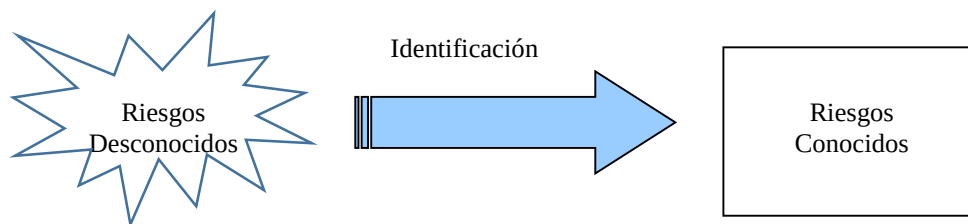


Figura 5 -La Incertidumbre Descriptiva

Si no se identifican de forma correcta los riesgos, los planes para atenuarlos son inservibles, pero esto no significa que se deben identificar todos los riesgos que implican a un activo. La identificación de estos, puede ser gradual y grupal, utilizando técnicas que abarquen mayor generalidad a la hora de la identificación.

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.

Podemos decir que dos de los aspectos principales que gravitan sobre la identificación de riesgos son: la comunicación abierta entre los integrantes del proyecto de AGR y la capacidad de pronosticar problemas futuros, por otro lado, está la experiencia de los agentes junto con la contribución de ideas, que logren como resultado la excelencia en el producto final.

Tal vez el aspecto más relevante en este ciclo, está dado en detectar la mayor cantidad de riesgos posibles, garantizando un proceso de evaluación claro, sobre problemas futuros. Pero no es factible identificar todos los riesgos asociados a un proyecto dentro de un tiempo establecido, por lo que resulta una buena práctica realizar interacciones sobre el tratamiento de los riesgos, y en cada interacción ir profundizando sobre su identificación y su alcance [17].

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[18].

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[19], [20]. Todo lo que sea considerado por el equipo de proyecto, como aporte en la identificación de los riesgos, deberá ser tenido en cuenta como, por ejemplo: 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.

Para la identificación de riesgos se pueden utilizar clasificaciones ya realizadas por algunas metodologías, documentos de fabricación y estándares establecidos por la

industria, lista de control, base de conocimientos específicos o cualquier otro origen de investigación divulgada.

Las actividades de identificación serán asignadas a los miembros que se consideren más 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.

Como resultado de la identificación se espera una declaración clara, consensuada y sin tergiversaciones que se registra a manera de listado, los riesgos se identifican de forma única con algún código establecido que debe analizar el equipo del proyecto. Esa lista se transforma en una tabla que será la entrada principal para la siguiente etapa de estudio del proceso de gestión de riesgos.

Identificar el riesgo, también incluye la individualización de las causas raíz y las consecuencias que provocan, las partes afectadas, el propietario, etc.

Las amenazas de mayor riesgo son las internas. La persona autorizada para realizar ciertas acciones en la organización, administrar la confianza otorgada en contra de la organización.[21].

Técnicas de Identificación de Riesgos

Existe diferentes métodos, técnicas y herramientas para identificar un riesgo y en ocasiones, esta se realiza utilizando varias técnicas para el mismo riesgo, a continuación, se especifican las técnicas más usuales:

- Tormenta de ideas: En este método, los miembros identifican los posibles riesgos en formato libre de ideas expuestas por los participantes y tomada en nota como cuadros sinópticos y no permiten la crítica de las opiniones expresadas por los participantes. El uso de esta técnica suele trasladarse además a otras etapas (por ejemplo, al momento de generar estrategias de mitigación)[22].
- Encuestas: Para conocer un problema del que no se tiene información, lo

principal es realizar una encuesta a los agentes que conviven con el riesgo. Existen métodos para la generación de una encuesta, y es preferible utilizar preguntas de tipo cuantitativas a la cualitativas, ya que la primera son medibles, una ventaja importante es la posibilidad de alcanzar una gran variedad de respuestas e información, evitando reunir a los participantes para lograr el objetivo[23].

- Entrevistas: Es solo un mecanismo de preguntas y respuestas, en donde el resultado final dependerá exclusivamente a la capacidad del entrevistador y de la formulación apropiada de las preguntas.
- Grupos de trabajo: Es un mecanismo muy significativo para el análisis de un área o tema específico, habitualmente los grupos de trabajo se encuentran integrados por individuos especializados en las distintas áreas temáticas referidas al proyecto[22].
- Conocimiento por experiencia o documentado: El conocimiento por experiencia se plantea generalmente a un experto en riesgos, normalmente existen consultores expertos en distintos tipos de riesgos, el conocimiento documentado es la compilación de información que se ha documentado en distintas AGR anteriores.
- Taxonomías de riesgos: Las taxonomías son registros de riesgos que han sido hallados en programas, 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; están agrupadas por áreas temáticas (utilidades, costos, agenda, por ejemplo)[7].
- Salidas del Análisis Orientado a Riesgos: Trata sobre 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.

- Información histórica: Es en esencia 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, aceptada como un hecho efectivo.

2.7 Modelo de Gestión de Riesgos SEI – CRM

2.7.1 Características

El método de Gestión Continua de Riesgos (SEI-CRM), desarrollado por el Instituto de Ingeniería de Software (SEI) de la Universidad de Carnegie Mellow⁵, es una metodología en el campo de la ingeniería de software cuyos conceptos, procesos y herramientas permiten gestionar continuamente los riesgos de un proyecto, proporcionando un entorno disciplinado para la toma de decisiones proactivas a lo largo de todas las fases del proyecto: análisis de los posibles problemas (riesgos), identificación de los riesgos significativos, para desarrollar estrategias y planes de gestión. Además, esta metodología incluye también el concepto de gestionar estas actividades como un ciclo básico, es decir, identificar, analizar, planificar, vigilar, controlar y comunicar los riesgos a lo largo de todo el ciclo de vida del proyecto.

El modelo es un proceso continuo en el gráfico número 10 se muestra con su forma circular, 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.

La comunicación y la documentación en este modelo es importante, por lo cual, su gestión se ubica en el centro de las operaciones, cada una de las tareas, debe además de generar su información específica en forma de documentos, debe comunicar esta información a todos los participantes del proyecto, gerencias y todo personal que fuese necesario para la gestión del activo [11]. 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 está determinado por la comunicación dentro del equipo de proyecto y el tercer nivel por la que surge entre el

⁵ Carnegie Mellow University -<https://www.sei.cmu.edu/>

proyecto y los diferentes participantes del mismo.

Según la información relevada de la metodología SEI- CRM, la misma se basa en la gestión de riesgos orientados a los proyectos software. Al ser un método formal, se puede utilizar en cualquier proyecto de TI.

Etapas del Modelo de Gestión de Riesgos SEI - CRM

1º Identificación: Identificar los riesgos es anticiparse a que estos se ejecuten y pasen a ser un problema. La identificación de los riesgos debe llevarse a cabo de manera disciplinada y coherente, alentando a los miembros del equipo del proyecto a formular sus preocupaciones y facilitando el análisis posterior.

2º Análisis: Su objetivo es transformar una serie de datos obtenidos en la etapa de identificación, en información que permita la toma de decisiones centradas en los riesgos más importantes para el proyecto, en la fase se aplican la declaración del riesgo, estimación de impacto y cálculo de probabilidad de ocurrencia y su exposición. [6].

3º Planificación: Convierte la información relacionada con cada riesgo en medidas y acciones efectivas en un momento inmediato y futuro. Esta fase incluye el proceso de acciones para controlar los riesgos y además la aplicación de un procedimiento de gestión integral de riesgos.

4º Seguimiento: Genera un monitoreo de los riesgos y las tareas de control, para poder evitar que el riesgo se ejecute. Los referentes de la administración del proyecto deben realizar una permanente y precisa revisión de los planes, ajustando los mismos a los a la eficacia de las tareas de control, como los planes correctivos.

5º Control: Etapa en la que se puede corregir las desviaciones que puedan causarse a los planes de gestión efectuados.

2.7.2 Cuestionarios basados en taxonomías

El método de identificación de riesgos basado en taxonomías, genera un cuestionario llamado TBQ⁶ para realizar la identificación y clasificación del riesgo, agrupando las distintas fuentes de riesgos en varias categorías.

La estructura fundamental del método consta de un Cuestionario Basado en Taxonomías y un proceso para su aplicación [24].

La taxonomía organiza los riesgos de desarrollo de software en tres niveles (ver figura 6):

- Clases.
- Elementos.
- Atributos.

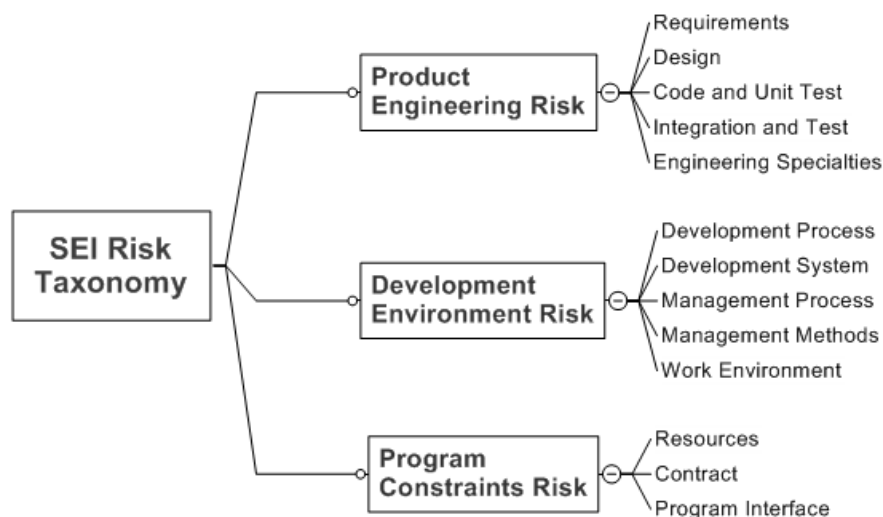


Figura 6 - SEI Taxonomía [24]

Tal como puede observarse, la taxonomía está organizada en tres grandes clases, que contienen elementos y cada elemento está caracterizado por una serie de atributos.

Las tres clases y elementos mencionados son:

⁶ Taxonomy-Based Questionnaire, Cuestionario basado en taxonomías.

Clases

- C.1 Ingeniería de Producto: Incluye los aspectos técnicos del trabajo a realizar.
- C.2 Entorno de Desarrollo: Involucra métodos, procedimientos y herramientas a emplear en la elaboración del producto.
- C.3 Restricciones del Programa: Trata factores contractuales, organizativos y operativos dentro del cual se enmarcar el software.

Elementos

- C.1 Ingeniería del Producto
 - C1.E.1 Requerimientos:
 - C1.E1.A1 Calidad de la especificación de los requisitos
 - C1.E1.A2 Dificultad de implementar un sistema que satisfaga los mismos.
 - C1.E.2 Diseño:
 - C1.E2.A1 Diseño y la viabilidad de los algoritmos
 - C1.E2.A2 Funciones o requerimientos de performance
 - C1.E2.A3 Las interfaces interna y externa del producto.
 - C1.E.3 Código y unidad de Testeo:
 - C1.E3.A1 calidad y estabilidad de las especificaciones del software o sus interfaces,
 - C1.E3.A2 Problemas que se podrían presentar en la implementación o dificultad en el testeo.
 - C1.E.4 Integración y Testeo:
 - C1.E4.A1 integración y la planificación del testeo.
 - C1.E4.A2 Ejecución e instalación del producto y la integración de este, dentro del sistema o el mismo entorno.
 - C1.E.5 Ingeniería Específica:

- C1.E5.A1 Requisitos específicos
- C1.E5.A2 Requisitos generales.

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

- C.2 Entorno de Desarrollo
 - C2.E1 Proceso de Desarrollo:
 - C2.E1.A1 Definición
 - C2.E1.A2 Planificación
 - C2.E1.A3 Documentación
 - C2.E1.A4 Adecuación
 - C2.E1.A5 Aplicación
 - C2.E1.A6 Comunicación de los métodos y procedimientos utilizados para el desarrollo del producto.
 - C2.E2 Proceso de Sistema: Herramientas y equipos de apoyo a utilizar en el desarrollo del producto.
 - C2.E2.A1 ingeniería de software asistida por ordenador (CASE),
 - C2.E2.A2 Herramientas
 - C2.E2.A3 Simuladores
 - C2.A2.A4 Compiladores
 - C2.A2.A5 Alojamiento del sistema.
 - C2.E3 Administración de Procesos:
 - C2.E3.A1 Planificación, seguimiento y control de presupuestos y tiempos.
 - C2.E3.A2 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.

- C2.E4 Administración de Métodos: Métodos, herramientas y equipo de apoyo a utilizar en la gestión y control del desarrollo de productos, tales como:
 - C2.E4.A1 Herramientas de monitoreo
 - C2.E4.A2 Gestión de personal
 - C2.E4.A3 Control de calidad
 - C2.E4.A4 Gestión de configuración.
- C2.E5 Entorno de trabajo: Ambiente general en que se realizara el trabajo incluye
 - C2.E5.A1 Actitudes personales
 - C2.E5.A2 Niveles de cooperación
 - C2.E5.A3 Comunicación, y moral.
- C3 Restricciones de Programas
 - C3.E1. Recursos: Limitaciones externas impuestas por:
 - C3.E1.A1 Horarios.
 - C3.E1.A2 Personal
 - C3.E1.A3 Presupuesto
 - C2.E1.A4 Instalaciones.
 - C3.E2 Contratos:
 - C3.E3.A1 Términos y condiciones del contrato del proyecto.
 - C3.E3.A2 Restricciones
 - C3.E3.A3 Dependencias
 - C3.E3 Interfaces de programas:
 - C3.E3.A1 Interfaces externas a clientes,
 - CE.E3.A2 Contratistas
 - CE.E3.A3 Gestión empresarial
 - CE.E3.A4 Vendedores.

El cuestionario TBQ consiste en una serie de preguntas objetivas relacionadas con cada uno de los atributos referenciados en la taxonomía, está diseñada para deducir un conjunto de riesgos y dudas, que podrían afectar potencialmente al producto o proyecto.

El proceso se desarrolla considerando la posibilidad de llevar a cabo 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 utilizan como instrumento de definición de riesgos, lo que no limita el uso de otras metodologías; además, este cuestionario suele definirse como una lluvia de ideas estructurada.

El TBQ produce mejores resultados, cuando se aplica a través de un equipo independiente.

El proceso de aplicación de TBQ consta de cuatro etapas secuenciales, Figura 7:

- **Compromiso de la Gerencia:** Debe contar con la aceptación y el compromiso de los ejecutivos de la organización, seleccionar el proyecto sobre el cual se ejecutará la técnica, seleccionar los participantes de diferentes áreas.
- **Selección del Equipo y Entrenamiento:** Consta de conformar los equipos del proyecto y 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.
- **Identificación de Riesgos:** Se genera la introducción, el equipo y de la metodología a emplear, además se generan entrevistas las cuales se dividen en 2 etapas. Cada una de las entrevistas, se divide en dos etapas: preguntas y respuestas: Implica el uso explícito de TBQ y clarificación: Implica la aclaración de cualquier situación.
- **Conclusión de la Identificación:** Finalizada la identificación se presenta a los participantes los resultados obtenidos.

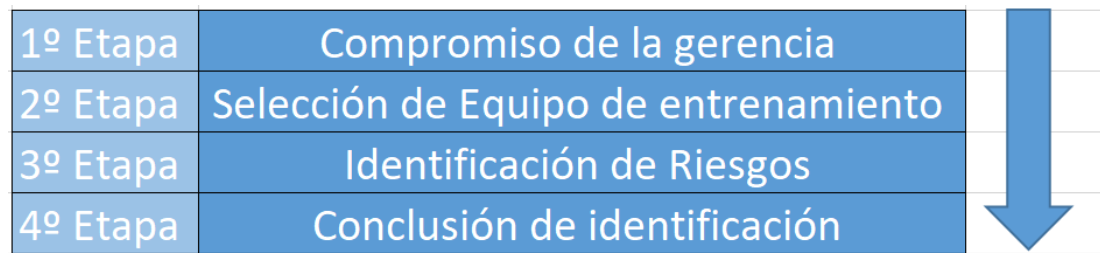


Figura 7 -TBQ - Proceso

En esta metodología, se una amplia gama de riesgos a nivel del sistema y permite destacar las áreas que requieren mayor atención por parte del equipo de proyecto.

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[25].

2.7.3 Etapa de la Metodología

1º Etapa - Inventario de activos:

Se deberá analizar los activos que podrían ser amenazados por algún tipo de riesgo.

2º Etapa - Propósitos y Objetivos del análisis de riesgos

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

3º Etapa - Equipo de Trabajo

Se debe formalizar el equipo de trabajo, definiendo roles a tareas, como funciones dentro del proyecto.

4º Etapa - Taxonomía de Riesgos

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

5º Etapa - Declaración de los Riesgos

Por cada riesgo representado en el cuestionario taxonómico, se debe definir:

- Por qué el riesgo es importante.
 - Que condición posee el riesgo para que se ejecute.
 - La consecuencia que tendrá la organización de ejecutarse el riesgo.
- Además, se incluyen los efectos que tendrían estos riesgos de no controlarse debidamente.

6º Etapa - Estimación de la probabilidad

Se genera un cuadro de referencia donde se implantan los porcentajes de las series en grupos, teniendo como base un porcentaje promedio de la serie como, por ejemplo, serie de porcentajes de 50% a 75% como valor de referencia es 65%, esto se realiza para no tener 100 registros diferentes, luego de crear el cuadro de referencia, se genera un formulario de estimación, donde se estima el porcentaje de ocurrencia por cada riesgo analizado, y se toma el porcentaje de referencia de la tabla anterior.

7º Etapa - Estimación del impacto

El impacto hace referencia a la gravedad de los efectos generados por el riesgo si se activa y cómo impacta este en la organización, al igual que con el porcentaje de ocurrencia, se debe realizar una tabla de referencia donde se expresa en lenguaje natural la importancia del impacto y se le asigna un valor numérico del 1 al 10. Preferiblemente esta tabla utiliza los rangos del 1 al 5 y por cada riesgo se toma un valor de la tabla de referencia de impacto.

8º Etapa - Exposición al riesgo

La exposición al riesgo se calcula tomando el valor del impacto generado si el riesgo se activa, multiplicando por el valor natural del porcentaje de ocurrencia del riesgo. Como resultante se tendrá un formulario donde se expresan valores de exposición negativos y positivos. Solo serán gestionados los riesgos cuyo valor resultante es mayor a 0, o sea positivo. Los riesgos mejoras a cero, solo se expresan como riesgos analizados, pero no se los gestiona.

9º Etapa - Gestión de los Riesgos

Líneas de Acción

Gestionar un riesgo es definir el alcance que puede tomar si se ejecuta, los recursos necesarios para poder controlarlo, y las acciones detectivas denominados plan de acción. Por otro lado, se estudian las tareas a realizar si el riesgo se ejecuta, esto se denomina plan de contingencias.

El Plan de Acción será utilizado para minimizar los riesgos mediante acciones preventivas. Las mismas son una lista de tareas, normalmente ordenadas en secuencia de pasos que deban realizarse sobre el activo evitar que el riesgo se ejecute y pase a ser un problema.

Por otro lado, el Plan de contingencia, implementa 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. La información a incluir en el plan de contingencias es:

- Disparador: Acción o episodio que transforma el riesgo en un problema.
- Responsable: Persona/as que son las encargadas de realizar los pasos necesarios para que el riesgo finalice y el activo vuelva a la normalidad.
- Pasos a seguir: Listado de tareas o pasos ordenados y secuenciales, donde se incorpora toda la información necesaria para ejecutar cada uno de ellos de una forma completa y minuciosa.

En la (figura 8), se muestra de forma gráfica las etapas de la metodología SEI

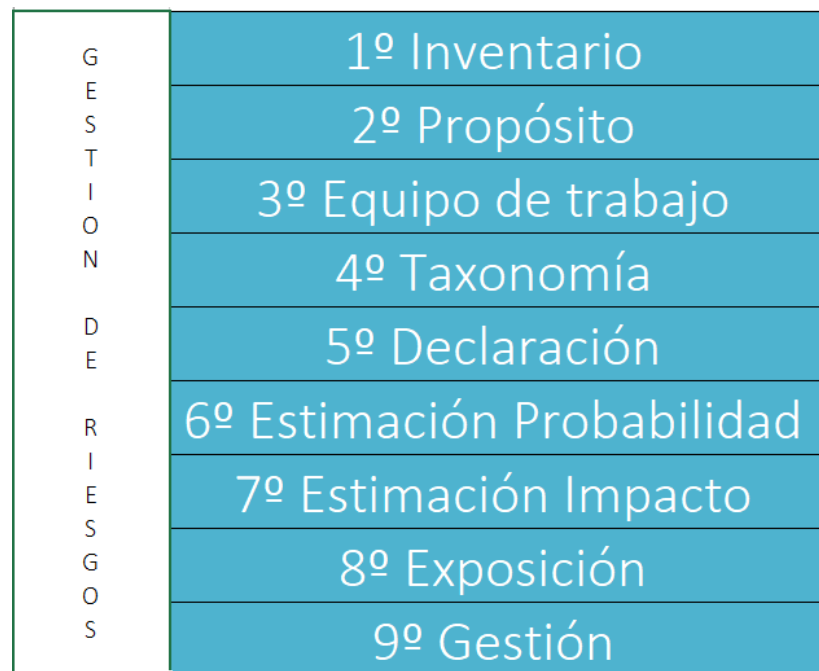


Figura 8 -Etapas de gestión de riesgos SEI

2.7.4 Ventajas

Como ventajas, podemos describir que es un modelo que posee tan solo nueve etapas, simple y claras, su documentación es relevante y posee mucha experimentación dentro de los proyectos de análisis y gestión de riesgos en organizaciones.

El uso de la clasificación taxonómica refuerza el método, ya que se puede utilizar en distintas etapas del proyecto, unificando los riesgos por grupos para ser analizados y tratados agrupando los tipos de riesgos, así se logra unificar la terminología, la cual, puede ser utilizada en la supervisión y control de los riesgos en la vida del proyecto, además de establecer una base de conocimiento dentro de la organización [15].

2.7.5 Desventajas

La principal desventaja, es que el método está fuertemente orientado a la gestión de riesgos en desarrollo de proyecto software, su taxonomía, precisa específicamente, los procesos del ciclo de vida de los proyecto software. Otro aspecto a tener en cuenta, es que el cuestionario TQB expone una clasificación de riesgos, pero

no identifica los mismos. Para la utilización de esta metodología, se debe contar con un equipo de trabajo del proyecto con experiencia en analizar riesgos, y se debe tener en cuenta, la incorporación de personal específico con conocimientos técnicos de los activos como consultores o personal auxiliar, esto encarece el costo del proyecto de AGR.

2.8 Metodología Magerit

2.8.1 Características y objetivos

La metodología Magerit⁷ en su versión 3, 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[4].

Los objetivos principales de Magerit V3 como:

- Concientizar a los dueños del proceso de la existencia de riesgos, 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.

Magerit se compone de tres partes, que se describen a continuación:

2.8.2 El Método

Forma parte del primero de los tres libros que conforman la metodología Magerit, este documento que describe los pasos y tareas básicas a realizar en un

⁷ Metodología de Análisis y gestión de riesgos de los sistemas de información

proyecto, proporciona una serie de aspectos prácticos y además describe la metodología desde un punto de vista de tres ángulos.

Primero Analizar estado de los riesgos: Proporciona una serie de paso para analizar en qué estado se encuentran los activos, de qué tipo son, que dependencia poseen, como se degradan, cuales son las amenazas que activan esos tipos de activos y describe las salvaguardas para realizar el control de los riesgos, además 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 dos etapas[26].

- Etapla 1 - 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. Los activos se definen en tipos de activos y poseen dimensiones.
 - Amenazas: Acciones no esperadas, son los riesgos, que pueden suceder a un activo, causando un perjuicio a la organización.
 - Salvaguardas: Tareas de control preventivas cuyo objetivo es que el riesgo no se ejecute.

Esta etapa posee pasos a seguir y analizar.

1. Determinar los activos relevantes para la organización, la interrelación, tipos, dimensiones y valor.
 2. De acuerdo a los tipos de activos se determinan 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.
- Etapla 2 - Gestión de Riesgos: Permiten organizar la defensa de los activos de manera metodológica, evitando la activación de los riesgos o minimizado el impacto.

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

1. Estimar el impacto, Es el daño sobre el activo, derivado de la materialización de la amenaza.
2. Estimar el riesgo, conforma el impacto ponderado con el porcentaje de ocurrencia.
3. Seleccionar salvaguarda, para cada riesgo, el plan de control y seguimiento de los controles.
4. Establecer normas, con el objeto de afirmar con propiedad que la amenaza ha sido ejecutada.
5. Establecer procedimientos paso a paso, actividades en forma de tareas para 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.

Magerit define como la gestión de seguridad, es la correcta gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

Como complemento para la etapa de análisis y la etapa de gestión de riesgos, la metodología presenta las tareas fundamentales y prioritarias para poder abordar un proyecto, para lo cual define los: roles, actividades, hitos y documentación.

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: Formaliza los roles que deben tener los integrantes del grupo de gestión de riesgos. Al ser una metodología los roles que se definen a continuación son obligatorios.

- Comité de Dirección: Recursos Humano con perfil de líder del proyecto que debe 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. La responsabilidad 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

El detalle del desarrollo del proyecto propuesto por el método, se define en el anexo II, a continuación, solo se enumera los procesos y actividades, para demostrar la estructura la cual posee Magerit. Como resumen podemos definir que la metodología posee 3 procesos, 11 actividades y 27 tareas las cuales se muestran a continuación.

 - Proceso P1: Planificación
 - Actividad A1.1: Estudio de oportunidad.
 - Tarea T1.1.1: Determinar la oportunidad
 - Actividad A1.2: Determinar el alcance del proyecto.
 - 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.
 - 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.
 - 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.
 - Actividad A2.1: Caracterización de los activos.
 - 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: Definir las amenazas
 - Tarea T2.2.1: Identificar de las amenazas
 - Tarea T2.2.2: Valorar las amenazas
 - Actividad A2.3: Definir las salvaguardas.
 - Tarea T2.3.1: Identificar las salvaguardas existentes.
 - Tarea T2.3.2: Valorar las salvaguardas existentes.
 - Actividad A2.4: Estimación del estado de riesgo.
 - 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.
 - 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.
 - Tarea T3.2.1: Programas de seguridad
 - Tarea T3.2.2: Plan de ejecución
 - Actividad A3.3: Ejecución del 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.

2.8.3 El Catálogo de los elementos

Manual que especifica los elementos utilizados por la metodología, define y clasifica cada uno de estos, incorporando ejemplos con respecto a:

- Tipos de activos: Los activos pueden tener distintos tipos como, por ejemplo, un servidor, puede ser del tipo hardware, pero también del tipo comunicación, y del tipo datos, si es un servidor que posee sistemas de gestión web.
- Dimensiones de valoración: Un activo puede poseer distintas dimensiones. Las dimensiones se utilizan para caracterizar los activos y pueden ser Autenticidad, Confidencialidad, Integridad y Disponibilidad
- Criterios de valoración: Valorar a un activo por su importancia.
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información.

Persigue dos objetivos por un lado facilitar la labor de las personas que acometen el proyecto, definiendo un catálogo elementos estándares, a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis. y por otro lado busca como objetivo 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.

En este manual expresa en ejemplos y datos específicos, sobre valores, formas e información específica para tratar los riesgos, y es una herramienta esencial para su tratamiento de forma manual[27].

2.8.4 Guía de técnicas

Describe las técnicas donde se aplican los datos e información del catálogo de elementos, son técnicas comunes de tratamiento de datos como ser árboles de ataque, análisis costo beneficio, análisis mediante tablas, análisis algorítmico, técnicas generales, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi⁸[28].

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.

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 deben ser considerados desde el primer momento, en un proyecto software, además de los riesgos al que se expone el 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 desgana una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo, para la realización de un análisis y gestión realmente efectivos.

La evolución de la versión 3 con respecto a la versión 2:

⁸ 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.

- Alinearse mejor con las regulaciones ISO y buscar integrar las tareas de análisis de riesgos dentro de un marco organizacional de gestión de riesgos dirigido desde los órganos de gobierno.
- El texto es mucho más simple.
- se normalizan las diferentes actividades como:
 - MAR – Método de Análisis de Riesgos
 - PAR – Proyecto de Análisis de Riesgos
 - PS – Plan de Seguridad

2.8.5 Herramienta Software PILAR

La metodología Magerit propone la utilización de un software realizado en el lenguaje JAVA. Para el presente trabajo se obtuvo una versión 7.3.1

Las herramientas EAR⁹ soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit y está desarrollada y financiada parcialmente por el Centro Criptológico Nacional (CCN) el cual es el Ente responsable de coordinar la acción de los diferentes organismos de la Administración, que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

El software completo, es de utilización libre únicamente para las organizaciones públicas pertenecientes al gobierno español. Las demás organizaciones privadas, que trabajan o poseen relación 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.

⁹ Entorno de Análisis de Riesgos

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.

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, Linux, IOS Apple. La figura 9 muestra la pantalla de inicio del Upilar.

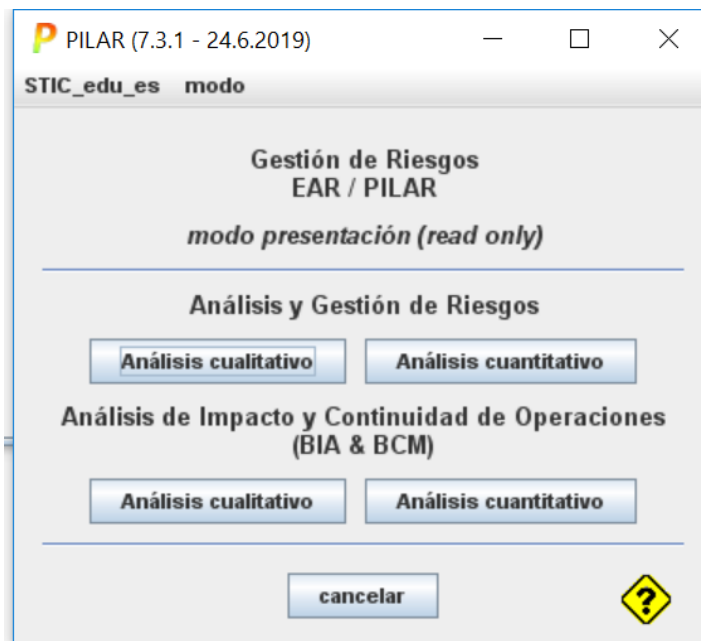


Figura 9 - Pilar

Posee 3 versiones

Versión 1 - μ PILAR - Análisis y Gestión de Riesgos: PILAR reducida a la mínima expresión, realiza 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. μ PILAR es distribuido con perfiles específicos. Sólo se pueden analizar los perfiles de la distribución.

Versión Gratuita

Versión 2 - PILAR Basic - Análisis y Gestión de Riesgos: Versión sencilla enfocado para PYME y Administración local, 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: 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 y Analiza el riesgo residual en diversas etapas de tratamiento.

Costo: 1500 Euros

2.8.6 Ventajas

Método orientado a toda la gestión de las Tics en la organización además posee catálogos, datos, ejemplos y técnicas, por lo cual, hace de esta, un modelo completo y organizado, con acceso a toda la información para realizar AGR. El equipo de riesgos, no necesita poseer amplia experiencia en gestión de riesgos, ya que posee los catálogos.

Los activos se clasifican en tipos y poseen dimensiones, esto genera claridad a la hora de gestionar las amenazas, ya que, ellas dependen del tipo de activo y no del activo en sí, esto quiere decir, que los riesgos, están ligados a las características operacionales de los activos, antes que al activo por sí mismo. Por otro lado, anexa salvaguardadas o planes de acción, que los incorpora a las dimensiones de los activos.

Con referencia a las técnicas utilizadas en la estimación del impacto del riesgo es de fácil comprensión y semejante a la propuesta por la metodología SEI.

Posee un software de soporte.

2.8.7 Desventaja

Como toda metodología, propone actividades y pasos a seguir, y en la versión 3, esta versión 3 procesos, 11 actividades y 27 tareas, las cuales están conformada de actividades por tareas, representa una gran cantidad de trabajo a realizar para poder utilizar este método.

Está orientada a gestionar los riesgos de grandes organizaciones, que para esta investigación es una desventaja, debido a la alta carga de actividades que posee y la carga de tiempo de gestión de recursos humanos, que en una pyme es escaso.

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.

2.9 Método Octave – S

OCTAVE¹⁰ es una metodología desarrollada por el Instituto de ingeniería de software de la Universidad de Carnegie Mellon, está basada en el método SEI CRM y se utiliza para definir una evaluación estratégica basada en el riesgo y una técnica de planificación de seguridad que incorpora el análisis de comportamiento de la organización y las debilidades de la tecnología. OCTAVE es un analizador de componentes importantes que pueden construir un equipo interno de la empresa en sí que tiene las habilidades técnicas y capacidad de organización relacionados a la práctica de negocio[21].

El método es un enfoque auto dirigido, las personas de una organización asumen la responsabilidad de establecer la estrategia de implementación de la seguridad en la empresa.

¹⁰ Operationally Critical Threat, Asset and Vulnerability Evaluation

Características

- Posee una evaluación de la organización a contraparte de la evaluación del Sistema.
- Se centra en las prácticas de seguridad frente a enfocarse en la tecnología.
- Se concentra en los puntos estratégicos ante los tácticos.
- Sugiere la autodirección del recurso humano establecido en el proyecto ante de la dirección de expertos.

La figura 10 muestra los ejes de las características del OCTAVE.

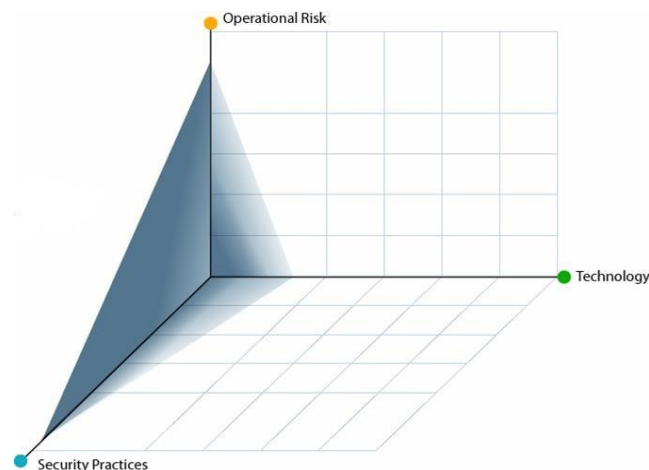


Figura 10 -OCTAVE [21]

El enfoque de evaluación de vulnerabilidades, activos y amenazas operacionalmente críticas, el método define una técnica de planificación y evaluación estratégica basada en riesgos para la seguridad.

OCTAVE-S es una variación del enfoque adaptado a los medios limitados y las limitaciones únicas que se encuentran típicamente en organizaciones pequeñas con menos de 100 personas, está orientado a ser dirigido por un pequeño equipo interdisciplinario compuesto de tres a cinco personas, del personal de una

organización, que recopila y analiza información, generando una estrategia de protección y planes de mitigación basados en los riesgos de seguridad operacional únicos de la organización.

2 aspectos únicos del método:

1. Un pequeño equipo de análisis interdisciplinario de tres a cinco personas, en conjunto, los miembros del equipo de análisis deben tener una visión amplia de los procesos comerciales y de seguridad de la organización, lo suficiente para realizar todas las actividades propuestas por el método. Por esta razón, no requiere capacitación formal de recopilación de datos para iniciar la evaluación.

2. Incluye una exploración limitada de la infraestructura informática durante la Fase 2. Dado que las organizaciones pymes frecuentemente tercerizan sus servicios y funciones de TI, los cuales, no poseen conocimiento profundo de la gestión organizacional de la empresa, del valor del activo y de activos específicos. Sin embargo, la falta de capacidad organizacional para ejecutar tales herramientas no impide que una organización establezca una estrategia de protección. En lugar de utilizar datos de vulnerabilidad para refinar su visión de sus prácticas de seguridad actuales, una organización, puede examinar los procesos empleados para configurar y mantener de forma segura su infraestructura informática. Cualquier deficiencia en la capacidad organizacional se observa y se considera durante la Fase 3, cuando la organización desarrolla su estrategia de protección.

Cada método es único, ya que se adapta al entorno de riesgos de la organización, sus objetivos de seguridad, la capacidad de recuperación y el nivel de habilidad del personal de la empresa. Se centra en las amenazas y riesgos de seguridad de información, pero mira más allá del nivel del sistema ya que se enfoca en las personas y los procesos

2.9.1 Fases de OCTAVE – S

El Proceso cuenta con 3 fases las cuales son:

1. Construcción de perfiles de amenazas basados en los activos[29].

Esta fase cuenta con los siguientes procesos:

- Identificar la información organizacional
- Crear perfiles de amenazas.

Para los que se desarrollan las siguientes actividades:

- Establecer el impacto de los criterios de la evaluación.
- Identificar activos organizaciones.
- Evaluar prácticas de seguridad organizacionales
- Seleccionar activos críticos.
- Identificar requerimientos de seguridad
- Identificar amenazas a los activos críticos.

2. Identificación de las vulnerabilidades de la infraestructura.

Cuenta con un solo proceso en el que se examina la infraestructura computacional en relación a los activos críticos para lo que se definen las siguientes actividades:

- Examinar rutas de acceso.
- Analizar los procesos relacionados con tecnología.

3. Desarrollo de estrategia y planes de seguridad.

En la Fase Tres se desarrollan planes y estrategias de seguridad a través de los siguientes procesos: identificar y analizar los riesgos y desarrollar estrategias y planes de mitigación.

Se cuenta con las siguientes actividades:

- Evaluar el impacto de las amenazas.
- Establecer criterios basados en la frecuencia.
- Evaluar probabilidades de amenaza.
- Describir la estrategia de protección actual.

- Desarrollar un plan de mitigación.
- Identificar cambios a la estrategia de protección e identificar siguientes pasos.

La documentación incluye hojas de trabajo y orientaciones para cada actividad, así como una introducción, la guía de preparación, y un ejemplo completo. [30]. La figura 11 muestra las 3 fases del proceso OCTAVE. -S



Figura 11 –Fases de OCTAVE-S [30]

2.9.2 Metas del proceso

- En la fase 1, se conoce a la organización, sus prácticas y activos; los activos pueden ser la información, hardware, sistemas o personas[31].
- En la fase 2, hasta 5 de los activos relacionados a la información de la organización han sido designados como críticos y se ha documentado por qué se los ha elegido. Se han creado perfiles de amenazas para cada activo, cada perfil contiene: un conjunto de árboles de amenazas, ejemplos específicos de amenazas humanas, la fuerza del motivo si aplica y el nivel de confianza asociada, la historia de cada amenaza.

- En la fase 3, se tiene un entendimiento amplio de cómo se usa la tecnología de la información, y el ambiente de negocio. Se identifican los sistemas para cada activo, puntos de acceso de red, administradores, y se examina la resistencia a ataques.
- En la fase 4, se identifica y analiza riesgos basándose en el impacto, la historia y la probabilidad tomando valores cuantitativos como alto bajo y medio.
- En la fase 5, se planifican las estrategias de mitigación contra las amenazas encontradas.

2.9.3 Cronograma

El método se lleva a cabo mediante una serie de reuniones; el horario para la realización de estas reuniones es flexible. El marco de tiempo más breve posible para completar una evaluación en su conjunto es de aproximadamente dos días. Esta estimación asume un tiempo completo, con un equipo de análisis dedicado que tiene experiencia con el proceso y una evaluación cuyo ámbito es estrecho. Al programar las actividades de evaluación, se debe:

Considerar las limitaciones de la organización[32].

- Asignar tiempo suficiente para completar todas las actividades de preparación.
- Recordar que todos los planes son estimaciones.
- Revisar el plan del proyecto para reflejar los cambios apropiados.

2.9.4 Ventajas

El método OCTAVE – S como mayor característica posee flexibilidad, ya que cada método se puede adaptar al entorno de riesgos que es único para su organización a comparación con el método SEI – CRM que está orientado a desarrollo de software,

además de los objetivos de seguridad y capacidad de recuperación y el nivel de habilidad.

Posee una fase de análisis de vulnerabilidades tecnológicas, la cual, es importante, ya que se muestran los activos el cual afecta, estas vulnerabilidades.

Los escenarios de los talleres abarcan una amplia gama de posibles incidentes de seguridad, lo que ayuda a prever y planear distintas acciones y medidas de seguridad en caso de que se presente alguna amenaza.

2.9.5 Desventajas

La metodología fallará si las personas involucradas no tienen un amplio conocimiento de los procesos operativos y de seguridad de la organización.

No permite modelar matemáticamente el riesgo, ya que no es de interés de la Unidad de Negocio.

No se incluye aún la adaptación de orientación a reuniones o de información.

No posee software herramienta para su implementación.

Está basado en la seguridad de los activos y no en los riesgos propios de cada uno.

2.10 Gestión de Riesgos en Proyectos

Para los proyectos de software, una crisis es un freno denominado como show-stopper que detiene o impide seriamente el progreso.

El riesgo en un proyecto es la oportunidad de que algo malo ocurra, puede suceder un problema potencial que aún no ha sucedido, si ocurre tendrá un impacto negativo en algunos o todos los recursos del presupuesto, el cronograma o la totalidad de los mismos, costo, características del producto y atributos de calidad. Las consecuencias del impacto negativo podría ser la pérdida de vidas humanas,

propiedades, información, dinero, reputación, tardanza, etc. entrega de un producto inaceptable, costo inaceptable, o su trabajo[33].

El riesgo de tiempo calendario inadecuado puede ser el resultado de como muestra la figura 12, Ejemplo de riesgos en proyectos:

- Comprometerse con una mala estimación
- Compresión del cliente o de la administración de un cronograma sin un ajuste correspondiente a los recursos y / o requisitos
- Adicionar requisitos sin los ajustes correspondientes al cronograma y los recursos, o reducción de los recursos planificados sin los ajustes correspondientes.

Factores de riesgo	Ejemplos
Programar	Tiempo de calendario inadecuado
Presupuesto	Fondos insuficientes cuando sea necesario
Requisitos	Inviabile, inestable, incorrecto, incompleto, inconsistente
Personal	Reclutamiento, habilidad, retención
Proceso	Procedimientos ineficientes y / o ineficaces.
Recursos	Máquinas host y de destino; organizaciones de apoyo
Tecnología	Plataforma y dominio
Geografía	Múltiples sitios de desarrollo
Factores externos	Vendedores y subcontratistas.
Riesgos operacionales	Funciones faltantes, rendimiento inadecuado
Calidad	Insatisfacción del usuario y del cliente
Mantenimiento	Correcciones, características faltantes

Figura 12 -Ejemplos de Riesgos en Proyectos

El riesgo de fondos insuficientes para llevar a cabo un proyecto puede implicar la falta de suficiente dinero en el presupuesto para realizar todas las actividades de trabajo necesarias, este error puede ser causado por una mala estimación o por aceptar un presupuesto impuesto o con pocas márgenes de negociación, o puede involucrar no recibir el dinero de manera oportuna. En el último caso, por ejemplo, el cliente que está pagando un proyecto puede retrasar el pago incremental de fondos o su administración puede diferir la asignación de los fondos necesarios hasta el próximo trimestre fiscal o año fiscal en casos de organizaciones gubernamentales.

La ingeniería del Software, sugiere la utilización de técnicas y herramientas para el desarrollo de software en todo el ciclo de vida del proceso software[34], la gestión de proyectos y su dirección es parte de la ingeniería del software, en su libro PMBOK sexta edición, recibió valiosas recomendaciones para mejorar esta guía del Project Manager Institute en adelante PMI[35] se especifica los fundamentos para la dirección de proyectos, generalmente reconocido como buenas prácticas, además proporciona y promueve un vocabulario común en el ámbito de la dirección de proyectos.

Sin ahondar en esta guía, es importante resaltar que un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único, al decir temporal, no se especifica necesariamente que sea de corta duración, pero la naturaleza temporal de los proyectos indica un principio y un final definidos. El final se logra cuando se alcanzan los objetivos del proyecto, o cuando se termina el proyecto cuando los objetivos no pueden ser cumplidos, cuando ya no existe la necesidad que dio origen al proyecto[19].

Por otra parte, es necesario para lograr ejecutar un proyecto, personas o grupo de personas que puedan dirigir, controlar, realizar y auditar los procesos en los cuales se desplaza el proyecto. Por lo cual la dirección del proyecto podríamos definir como la aplicación de los conocimientos, habilidades, técnicas y herramientas a las actividades del proyecto para cumplir con los objetivos del mismo. La guía PMBOK cuenta con 49 procesos de dirección de proyectos o actividades agrupados por un grupo de 5 procesos. El proceso número 11 es el proceso de riesgos del proyecto, como muestra la figura 13.

Áreas de Conocimiento	Grupos de Procesos de la Dirección de Proyectos				
	Grupo de Procesos de Inicio	Grupo de Procesos de Planificación	Grupo de Procesos de Ejecución	Grupo de Procesos de Monitoreo y Control	Grupo de Procesos de Cierre
4. Gestión de la Integración del Proyecto	4.1 Desarrollar el Acta de Constitución del Proyecto	4.2 Desarrollar el Plan para la Dirección del Proyecto	4.3 Dirigir y Gestionar el Trabajo del Proyecto 4.4 Gestionar el Conocimiento del Proyecto	4.5 Monitorear y Controlar el Trabajo del Proyecto 4.6 Realizar el Control Integrado de Cambios	4.7 Cerrar el Proyecto o Fase
5. Gestión del Alcance del Proyecto		5.1 Planificar la Gestión del Alcance 5.2 Recopilar Requisitos 5.3 Definir el Alcance 5.4 Crear la EDT/WBS		5.5 Validar el Alcance 5.6 Controlar el Alcance	
6. Gestión del Cronograma del Proyecto		6.1 Planificar la Gestión del Cronograma 6.2 Definir las Actividades 6.3 Secuenciar las Actividades 6.4 Estimar la Duración de las Actividades 6.5 Desarrollar el Cronograma		6.6 Controlar el Cronograma	
7. Gestión de los Costos del Proyecto		7.1 Planificar la Gestión de los Costos 7.2 Estimar los Costos 7.3 Determinar el Presupuesto		7.4 Controlar los Costos	
8. Gestión de la Calidad del Proyecto		8.1 Planificar la Gestión de la Calidad	8.2 Gestionar la Calidad	8.3 Controlar la Calidad	
9. Gestión de los Recursos del Proyecto		9.1 Planificar la Gestión de Recursos 9.2 Estimar los Recursos de las Actividades	9.3 Adquirir Recursos 9.4 Desarrollar el Equipo 9.5 Dirigir al Equipo	9.6 Controlar los Recursos	
10. Gestión de las Comunicaciones del Proyecto		10.1 Planificar la Gestión de las Comunicaciones	10.2 Gestionar las Comunicaciones	10.3 Monitorear las Comunicaciones	
11. Gestión de los Riesgos del Proyecto		11.1 Planificar la Gestión de los Riesgos 11.2 Identificar los Riesgos 11.3 Realizar el Análisis Cualitativo de Riesgos 11.4 Realizar el Análisis Cuantitativo de Riesgos 11.5 Planificar la Respuesta a los Riesgos	11.6 Implementar la Respuesta a los Riesgos	11.7 Monitorear los Riesgos	
12. Gestión de las Adquisiciones del Proyecto		12.1 Planificar la Gestión de las Adquisiciones	12.2 Efectuar las Adquisiciones	12.3 Controlar las Adquisiciones	
13. Gestión de los Interesados del Proyecto	13.1 Identificar a los Interesados	13.2 Planificar el Involucramiento de los Interesados	13.3 Gestionar la Participación de los Interesados	13.4 Monitorear el Involucramiento de los Interesados	

Figura 13 –Riesgos - Área de conocimiento y Grupo de Procesos [33]

El riesgo en un proyecto es un actor clave, que debe ser divisado, analizado, controlado, y la guía PMBOK, posee un capítulo y actividades exclusivas para ellos.

La gestión de los riesgos en un proyecto incluye tareas y actividades que tienen por objetivo, la identificación, el análisis, la planificación de la respuesta a los riesgos,

el control y monitoreo de los mismos. Esta guía define los objetivos de la gestión de riesgos en un proyecto, como aumentar la probabilidad y el impacto de eventos positivos y disminuir la probabilidad y el impacto de eventos negativos, como metodología de análisis y gestión de riesgos.

Aumentar la probabilidad y el impacto de eventos positivos, hace referencia a eliminar, controlar o aceptar los riesgos que puedan ejecutarse en un futuro. Por lo cual, es importante visibilizar el riesgo, para que no represente un obstáculo en la búsqueda del objetivo del proyecto.

La guía propone 6 actividades en distintos procesos en donde se evalúan los riesgos, cada una de ellas poseen entradas, que son tomadas de las salidas de otros procesos y actividades. Con estas entradas se ejecutan técnicas y herramientas y se generan salidas que son tomadas como información para el AGR en proyectos, ellas son:

- Planificar la gestión de riesgos.
- Identificar los riesgos
- Realizar el análisis cualitativo de los riesgos
- Realizar el análisis cuantitativo de los riesgos
- Planificar la respuesta a los riesgos
- Implementar la respuesta a los riesgos.
- Monitorear y controlar los riesgos.

Estos procesos interactúan unos con otros además con procesos de otras áreas de conocimiento de esta guía. Cada proceso puede ser realizado por una o muchas personas, dependiendo de las necesidades del proyecto. Cada proceso se ejecuta por lo menos una vez en cada proyecto en una o más fases del proyecto, en el caso de que este contemple varias fases.

Los riesgos en el proyecto, así como los riesgos en general, se presentan en un futuro, como un evento o condición incierta, como se plantea en la sección 2.2. Que si sucede posee un efecto en por lo menos uno de los objetivos del proyecto. Los objetivos pueden incluir, alcance, cronograma, costo y calidad. Por lo que, analizando

las características de los riesgos, se puede plantear que el mismo puede tener una o más causas y si se transforma en un problema puede llevar a uno o más impactos.

Los proyectos poseen riesgos conocidos y desconocidos, los conocidos son aquellos que han sido identificados, analizados y por lo cual se puede planificar una respuesta, los riesgos desconocidos, no puede gestionarse de manera pro activa, lo que sugiere que el equipo de proyecto debe crear un plan de contingencias.

Las empresas y/o organizaciones ven a los riesgos como el efecto de una incertidumbre sobre los objetivos del proyecto y de la misión o visión de la organización, pero es imposible que el riesgo sea nulo, pero no todos los riesgos son catastróficos. Existen distintos tipos de niveles de riesgos, los cuales, para las organizaciones son conocidos y aceptados, esto se conoce como niveles de tolerancia al riesgo.

2.10.1 Planificar la gestión de los riesgos

Es el proceso donde se define como realizar las actividades de gestión de los riesgos para un proyecto. Planificar correctamente la gestión de los riesgos en un proyecto mejora la probabilidad de éxito de los otros cinco procesos de gestión de riesgos[36].

Planificar los procesos de gestión de riesgos, asegura que el nivel, tipo y visibilidad de la gestión de riesgos sean acordes, tanto en el nivel de riesgos. como en la importancia para del proyecto en la organización. Planificar proporciona los recursos y tiempo suficientes para las actividades de gestión y establece una base acordada para evaluar los riesgos. Este proceso debe iniciarse tan pronto como se concibe el proyecto y debe contemplarse en las fases tempranas de la planificación.

La información que se obtiene como salida de este proceso son:

- Plan de gestión de riesgos: El plan de gestión de riesgos, describe la manera en la cual se realizarán las actividades de gestión de riesgos en el proyecto, y pasa a ser parte de un plan general en la dirección del proyecto, en otra área

denominada “Desarrollar el plan para la dirección del proyecto”, este plan de gestión que incluye:

- Metodología: Define los métodos, las técnicas, herramientas y fuentes de datos que se pueden utilizar para llevar a cabo la gestión de riesgos del proyecto, cuando hablamos de metodología, se orienta a los métodos de planificación y gestión de proyectos, y una de las gestiones que hay que atacar son los riesgos.
- Roles y Responsabilidades: Se definen los roles del líder, el equipo y el personal de apoyo para cada tipo de actividad en el plan de gestión de riesgos, delimita sus responsabilidades.
- Presupuesto: El costo, tanto de la gestión de los riesgos como así también de los planes de contingencias son definidos en esta sección, estimando los fondos necesarios, y se incluyen en la línea de base del desempeño de costos, se establece los protocolos para la aplicación de la reserva presupuestaria para activar los planes de contingencia. -
- Calendario: Establece cuando y con qué frecuencia se realizarán los procesos de gestión de riesgos a lo largo del ciclo de vida del proyecto, y prevé las actividades de gestión de riesgos que serán incluidas en el área cronograma de proyecto.
- Categoría de Riesgos: Genera una estructura que asegura un completo proceso de identificación de los riesgos a nivel de detalle coherente, y contribuye a la efectividad y calidad del proceso de identificación de riesgos. Para lograr visualizar de manera ordenada y verificar las prioridades de los riesgos, se recomienda utilizar una tabla RSB¹¹ (figura 14) que define una estructura jerárquica de los riesgos identificados en el proyecto, organizándolos por categoría y sub categorías, donde se identifican las distintas áreas y causas de posibles riesgos.

¹¹RBS: Risk Breakdown Structure, Estructura de Desglose del Riesgo.

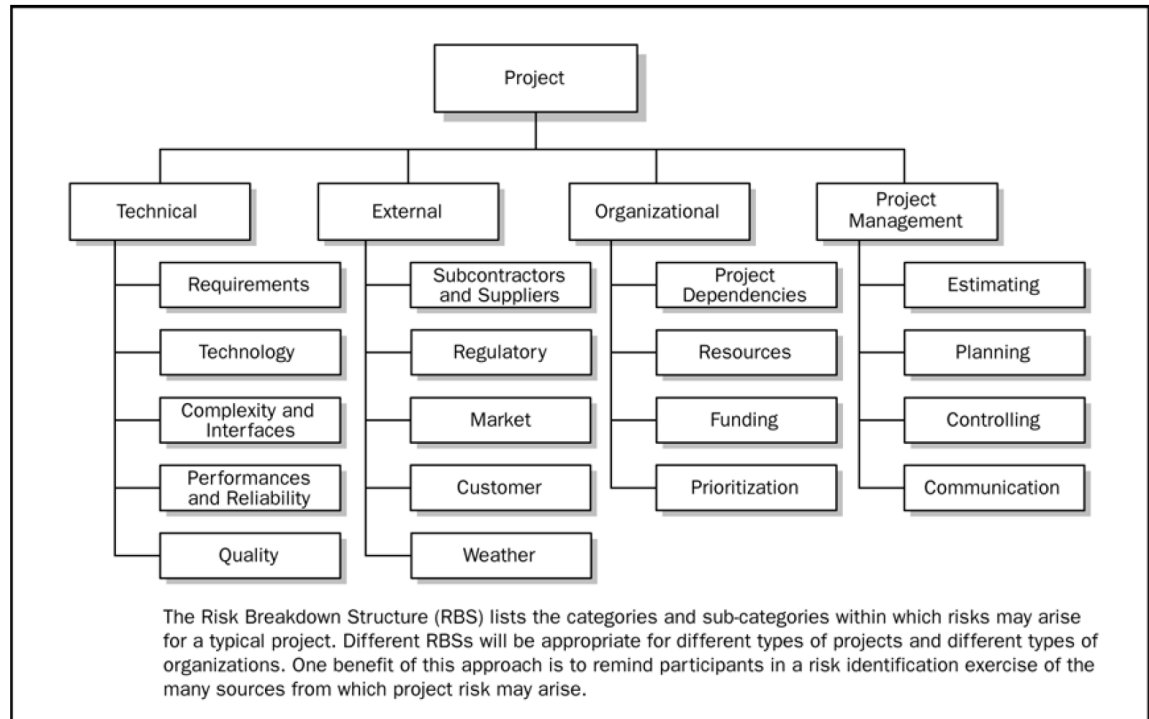


Figura 14 -Tabla RBS [22]

- Definiciones de Probabilidad e impacto de los riesgos: definen los niveles de probabilidad e impacto de los riesgos, en forma de tablas de doble entrada como los utilizan otras metodologías de análisis y gestión de riesgos. En este proceso, solo se definen, las tablas y las unidades que se evaluarán más adelante en el análisis cuantitativo de los riesgos. Estas tablas se adaptan a cada proyecto individualmente, se puede tomar de ejemplo la tabla de niveles de impacto como muestra la figura 15.

Defined Conditions for Impact Scales of a Risk on Major Project Objectives (Examples are shown for negative impacts only)					
Project Objective	Relative or numerical scales are shown				
	Very low /.05	Low /.10	Moderate /.20	High /.40	Very high /.80
Cost	Insignificant cost increase	<10% cost increase	10-20% cost increase	20-40% cost increase	>40% cost increase
Time	Insignificant time increase	<5% time increase	5-10% time increase	10-20% time increase	>20% time increase
Scope	Scope decrease barely noticeable	Minor areas of scope affected	Major areas of scope affected	Scope reduction unacceptable to sponsor	Project end item is effectively useless
Quality	Quality degradation barely noticeable	Only very demanding applications are affected	Quality reduction requires sponsor approval	Quality reduction unacceptable to sponsor	Project end item is effectively useless
This table presents examples of risk impact definitions for four different project objectives. They should be tailored in the Risk Management Planning process to the individual project and to the organization's risk thresholds. Impact definitions can be developed for opportunities in a similar way.					

Figura 15 -Tabla Niveles de impacto [33]

- Matriz de Probabilidad e impacto: Los riesgos se clasifican por orden de prioridad, dependiendo de las implicaciones potenciales de tener efecto sobre los objetivos del proyecto. Se utiliza el método típico de una matriz de probabilidad – impacto donde se clasifican en Alta – media y baja.
- Tolerancias revisadas de los interesados: Las tolerancias de los interesados según aplican al proyecto, están implementados en el marco del proceso planificar la gestión del riesgo.
- Formato de los Informes: Se define como se documentará, se analizará y como se comunicará los resultados de los procesos de gestión de riesgos, se visualiza la estructura y el contenido de los informes, y cualquier otro informe necesario o requerido
- Seguimiento: Generación de un documento donde expresa de qué manera se registrarán la gestión de riesgos, necesidades futuras, lecciones aprendidas y si los procesos de gestión de riesgo se auditarán y de qué manera

2.10.2 Identificar los Riesgos

Es el proceso por el cual se determina los riesgos que pueden afectar al proyecto y se documentan sus características. Esto es un proceso iterativo e incremental, debido

a que, en el trayecto de avance del proyecto, se pueden encontrar nuevos riesgos o estos pueden evolucionar. Las interacciones y los equipo que integran la gestión de riesgos pueden variar de una situación a otra, dentro del mismo proyecto. El formato de la declaración de riesgos debe ser consistente para asegurar la capacidad de comparar el efecto relativo de un evento de riesgo con los otros eventos del marco del proyecto.

La información que se obtiene como salida de este proceso son:

- Registro de Riesgos: Las salidas principales del proceso de identificación de riesgos, son las entradas iniciales al registro de riesgos. El registro de riesgos contiene los resultados de los demás procesos de gestión de riesgos a medida que se llevan a cabo, dando como resultado un incremento en el nivel y tipo de información contenida en el registro de riesgos conforme a transcurre el tiempo.
 - Lista de riesgos identificados: Los riesgos identificados se describen en su totalidad con un nivel de detalle razonable, y se incorpora la fecha y versión de la última modificación de los detalles.
 - Lista de respuestas potenciales: Se pueden dar respuestas potenciales en la sección de registro de los riesgos, si la identificación del mismo y la experiencia del equipo así lo considera, estas respuestas que se identifican en este proceso pueden utilizarse en las entradas del proceso de Planificar la respuesta a los riesgos.

2.10.3 Realizar el Análisis Cualitativo de Riesgos

Consiste en priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando la probabilidad de ocurrencia y el impacto de dicho riesgo.

Por lo general este proceso tiene por objetivo evaluar la prioridad de los riesgos detectados, utilizando la probabilidad relativa de ocurrencia, el impacto correspondiente sobre los objetivos del proyecto si los riesgos pasan a ser un problema,

se evalúa además otros factores como restricción del proyecto en cuando a cronograma, costo, alcance y calidad. Esta evaluación muestra una prioridad en los riesgos lo cual refleja la actitud que debe tomar el equipo de proyecto como los interesados. Realizar el análisis cualitativo es un medio rápido y económico para planificar la respuesta a los riesgos con mayor prioridad de ocurrencia y sienta las bases para realizar el análisis cuantitativo, si así se requiera.

Uno de las características singulares que posee el análisis cualitativo, es que se deben evaluar durante todo el ciclo de vida del proyecto, en la cual, se debe ir ajustando la probabilidad relativa de los riesgos, además de incorporar nuevos riesgos identificados, en esto se diferencia de las demás metodologías, debido a su carácter dinámico e interactivo.

Como entrada se utiliza:

- Registro de los riesgos, que es una de las salidas de la identificación de los riesgos.
- Plan de Gestión de Riesgos: se utiliza la salida del proceso de planificar los riesgos. Si no se realizó esta salida en el plan de gestión, se puede realizar en el análisis cualitativo, teniendo en cuenta los roles y las responsabilidades de la gestión de riesgos, el factor económico exployado en los presupuestos y costos, el cronograma de actividades relativa a la gestión de los riesgos, las categorías de los riesgos y las definiciones de probabilidad e impacto.
- Enunciado del Alcance del Proyecto: Marcar los límites del proyecto, asegura identificar el alcance, y con ellos visualizar la complejidad del proyecto, si es de baja complejidad o es de uso común en la organización, los riesgos tienen a ser conocidos y comprendidos, en tanto que, si el proyecto se realiza por primera vez, o es de alta complejidad tienen a poseer mayor incertidumbre.
- Activos de los procesos de la organización: Este es un punto que influye en el proceso de realizar este análisis, debido a que, si se posee información que provenga de otros proyectos similares finalizados, evaluación de expertos en análisis y gestión de riesgos o la utilización de base de

conocimientos, como posee la metodología Magerit, ayuda a entender y evaluar los riesgos conocidos.

Las salidas que posee este proceso son los siguientes:

- Actualización al Registro de Riesgos: el inicio del registro de riesgos se realiza en el proceso de identificación de riesgos, en este proceso de análisis cualitativo se enriquece esta identificación con:
 - Lista de prioridades de los riesgos del proyecto.
 - Riesgos Agrupados por categorías
 - Riesgos con mayor prioridad o más sensibles
 - Lista de riesgos a atender a corto plazo
 - Lista de riesgos que necesitan mayor análisis o son más complejos.
 - Riesgos de baja prioridad

2.10. 4 Realizar el Análisis Cuantitativo de Riesgos

Consiste en analizar numéricamente, el efecto de los riesgos encontrados sobre los objetivos del proyecto.

Es similar al estudio realizado por otras metodologías, se establecen valores numéricos y además se utilizan rangos como alto, bajo o medio.

Las entradas de este proceso son:

- Registro de riesgos: tomados de la salida del proceso identificar los riesgos.
- Plan de Gestión de riesgos.
- Plan de Gestión de Costos: En este análisis, proceso mayormente datos numéricos, se establecen los formatos de criterios para planificar, estructurar, estimar los costos del proyecto, tal como se especifica en el proceso de Costos de la guía PMBOK.
- Plan de Gestión del Cronograma: Define formatos y criterios para generar y controlar el cronograma del proyecto, esto se expresa en la sección Cronograma de la guía PMBOK. Los controles y el cronograma ayudan a

generar la estructura o el método de la aplicación del análisis cuantitativo del cronograma.

- Activos de los procesos de la Organización: Listado generado como entrada en el análisis cualitativo de los riesgos.

De este proceso se obtiene:

Dentro de los documentos que pueden ser considerados como salida del análisis cuantitativo están:

Informe de Riesgos: Presentado en el punto anterior donde expresa la de riesgos generales del proyecto y riesgos individuales del mismo.

Evaluación de exposición general a los riesgos del proyecto: esta evaluación se obtiene de dos (2) mediciones, la probabilidad de éxito de proyecto elaborado alcance los objetivos claves y la segunda opción de medición es el grado de variabilidad inherente del proyecto, tomado al momento que se realizó el análisis, indicando las posibles modificaciones al proyecto, en el tiempo que reste en el desarrollo del mismo.

Análisis probabilístico detallado de proyecto: Se presentan las salidas de la información con mayor importancia del análisis cuantitativo.

Tomando técnicas y herramientas con las curvas S, utilidades para obtener la probabilidad acumulada, que representa, la probabilidad de lograr cualquier resultado en particular o menor, también el diagrama de tornado, que constituye un análisis de sensibilidad, con la finalidad de colaborar en la determinación de cuales riesgos individuales del proyecto, tienen un impacto con mayor potencial sobre los resultados del mismo.

Lista priorizada de riesgos individuales del proyecto: Corresponde a una lista de riesgos individuales que representan mayor amenaza o muestran una mayor oportunidad para el proyecto.

Tendencias en los resultados del análisis cualitativo: Muestra una lista de tendencias que aparecen luego de repetir el análisis de riesgo en distintos momentos ciclo de un proyecto.

Respuesta recomendada a los riesgos: Trata de un informe de recomendaciones que se utilizan como entrada para el proceso de planificarla respuesta a los riesgos, este informe representa, respuestas sugeridas a nivel de exposición general del riesgo o riesgos claves sobre la base de los resultados del análisis cualitativo.

2.10.5 Planificar la respuesta a los riesgos

La exposición al riesgo conlleva un conjunto de actividades, tanto para el proyecto en general, como para tratar individualmente cada riesgo. Se deben desarrollar opciones, estrategias y acordar acciones para identificar la manera más adecuada de abordar los riesgos, asignar recursos e incorporar actividades. Este proceso se desarrolla a lo largo del ciclo de vida del proyecto.

El correcto proceso del manejo de riesgo reduce al mínimo las amenazas, maximiza las oportunidades de éxito y minimiza la exposición total al riesgo del proyecto.

Se deben dar respuestas y priorizar los riesgos con mayor importancia, los que posean mayor rentabilidad con respecto al cumplimiento, deben ser realistas dentro del contexto de proyecto, y todos los participantes deben estar de acuerdo con la forma y los riesgos a dar respuestas.

Desarrollar acciones específicas para implementar estrategias de respuestas a los riesgos, se deben incluir además de las estrategias principales, las estrategias de refuerzos con un plan de contingencias, por si la estrategia principal no tuviera éxito, además se deben identificar los riesgos secundarios que surjan de la aplicación de la respuesta a los riesgos.

Entradas

Plan de Dirección del Proyecto

Considera la gestión de los recursos, donde se observa la coordinación de los recursos asignados a Gestión de Riesgos con otros recursos del proyecto, además contempla el plan de gestión de riesgos obtenido como salida del análisis cualitativo de los riesgos y por último se cuenta con la información de la línea base de costos donde poder ver el fondo asignado para las contingencias del proyecto.

Documentos del Proyecto:

Se obtiene como salida, que alguno de ellos, puede ser utilizado como entrada en las siguientes etapas.

Registro de Lecciones Aprendidas

Se basa en un registro de repuestas efectivas utilizadas en fases anteriores para afrontar los riesgos.

Cronograma y Calendario del Proyecto:

Asignación de tiempo programado para ejecutar respuestas a los riesgos.

Asignación de Equipo de Proyecto

Según las respuestas a los riesgos individuales en el cronograma se muestran los recursos con que se cuentan, para conformar el equipo del proyecto que trabajara en la planificación de respuestas.

Registro de Riesgo:

El nivel de prioridad de cada riesgo individual ayuda a orientar la selección de las respuestas apropiadas. Además, identifica al responsable y dueño del riesgo.

Informe del Riesgo:

Presenta el nivel de exposición general a los riesgos del proyecto.

Registro de Interesados:

Identifica a los responsables y a los dueños de la respuesta a los riesgos.

Salidas

Solicitud de Cambio:

Cualquier solicitud de cambio conlleva una modificación en la línea de base de costos y cronogramas, la respuesta planificada a los riesgos se procesa y se revisan dentro del proceso integrado de cambios en PMBOK.

Actualización del Plan para la Dirección del Proyecto

Cualquier actualización o cambio en el plan de proyecto pasa por el proceso de control de cambio. Una respuesta a los riesgos puede llevar a un cambio en el plan del proyecto por lo cual pueden requerir una solicitud de cambio en el plan gestión del cronograma, gestión de costos, gestión de calidad u otros.

Actualización de Documentos del Proyecto

Los riesgos ejecutados pueden llevar a modificar la documentación de los procesos del proyecto.

2.10.6 Implementar Respuestas

Para asegurar que la respuesta a los riesgos que se acordaron en la planificación se debe realizar:

El proceso de Implementación de respuesta a los riesgos. Este proceso también llevado a cabo durante toda la vida del Proyecto.

Realizar de forma adecuada este proceso garantiza que las respuestas acordes a los riesgos se ejecuten realmente.

El problema común con los riesgos del proyecto es que no se toman medidas para gestionar el riesgo. Se invierte un gran esfuerzo en todos los demás procesos.

Para obtener éxito en el manejo de la gestión y exposición general al riesgo, es imprescindible que el nivel de esfuerzo sea acorde a los requerimientos de riesgo,

como así también una acción pro-activa ante las amenazas y oportunidades individuales.

Entradas

Los componentes del plan para la dirección del proyecto incluyen el plan de Gestión de Riesgos, el cual enumera los roles y las acciones los miembros del equipo. Esta información se utiliza para asignar los dueños para las respuestas acordadas de riesgo.

El plan de gestión de Riesgos define detalladamente la metodología de gestión.

Activos de los procesos de la Organización

Poseer un repositorio de riesgos resguardados de proyectos terminados favorece la efectividad de la respuesta a los riesgos, los mismo se encuentran en el Registro de Lecciones Aprendidas.

Salidas

La implementación de las respuestas a los riesgos, pueden dar lugar a modificaciones en el cronograma y costos del proyecto. Las solicitudes se procesan para su revisión y tratamiento por medio del proceso Control de cambios Integrados, proceso incluido en la Gestión de Integración del proyecto del PMBOK VE

Los documentos que se pueden actualizar como resultado de este proceso son

- Registro de incidentes: Cuando los incidentes son identificados como parte del proceso.
- Registro de Lecciones Aprendidas: Se actualiza con información de las dificultades encontradas y como podrían haberse evitado.
- Asignaciones del equipo: Una vez que se confirma la respuesta a los riesgos, se deberá asignar los recursos necesarios para cada acción asociada con un plan de respuesta. Incluye personal técnico y asesoría externa de ser necesario.

- Registro de Riesgos: Finalizada la implementación de la respuesta a los riesgos el registro puede ser actualizado para reflejar los cambios en la respuesta a los riesgos.
- Informe de Riesgo: Al igual que el registro de riesgo, el informe de Riesgo puede ser actualizado para incluir cualquier cambio en la respuesta a los riesgos.

2.10.7 Monitores de Riesgo

Corresponde a realizar un seguimiento a los riesgos identificados, identificar y analizar nuevos riesgos y evaluar la efectividad del proceso a lo largo de la vida del proyecto.

Monitorear los riesgos posee grandes beneficios ya que permite que las decisiones del proyecto se basen en información actual sobre la exposición al riesgo.

Garantizar el acceso a la información detallada al nivel de exposición al riesgo es preponderante para que los interesados tomen conciencia y tengan acceso a toda la información, por lo cual el proyecto deberá poseer un monitoreo continuo en busca de riesgos individuales, nuevos, cambiantes y obsoletos. El proceso de Monitorear los riesgos utiliza información de desempeño para determinar si:

- Las respuestas a los riesgos implementadas son efectivas.
- Han cambiado el nivel de riesgo general o el estado de los riesgos.
- Se encontraron nuevos riesgos.
- El enfoque de gestión de riesgo sigue siendo el adecuado.
- Los supuestos del proyecto siguen siendo validos
- Se respetan los procedimientos y políticas de la Gestión de Riesgos.
- La estrategia del proyecto sigue siendo válida.

Entrada:

Plan Dirección de Proyecto:

Proporciona información orientativa sobre cómo y cuando

revisar los riesgos, las políticas y procedimientos que deberán seguirse, los roles y responsabilidades en el proceso de seguimiento.

Datos de Desempeño del trabajo:

Contienen datos sobre el estado del proyecto, riesgos implantados y producidos, riesgos activos y cerrados.

Informes del Desempeño del Trabajo:

Aportan datos e información de las mediciones del desempeño. Se utilizan para brindar información del desempeño del trabajo del proyecto, incluido el análisis de variación, los datos sobre el valor ganado y los datos para proyecciones.

Salidas:

Información de Desempeño del Trabajo

Incluye información sobre el estado actual de la gestión de los riesgos del proyecto, mediante la comparación de los riesgos individuales, producidos y como debieron producirse. Esta información muestra si el proceso de planificación de la respuesta y de implementación han sido efectivizados.

Solicitudes de Cambio:

Incluyen acciones correctivas y preventivas recomendadas para hacer frente al actual nivel de riesgo general del proyecto, para afrontar los riesgos individuales.

Actualización del Plan para la Dirección del Proyecto:

Cualquier cambio en el plan para la dirección del proyecto pasa por el proceso de control de cambios de la organización.

Actualización de los Documentos del Proyecto:

Registro de Supuestos: se pueden identificar nuevas restricciones y los supuestos existentes pueden ser revisados o modificados.

Registro de Incidentes: Se actualiza el registro cuando los incidentes son identificados como parte de estos procesos.

Registros de lecciones aprendidas: Se actualizan con cualquier lección relacionada con el riesgo aprendido durante las revisiones del riesgo. Serán utilizadas en las fases posteriores del proyecto o futuras del proyecto.

Registro de Riesgo: Incluye la inclusión o adición de nuevos riesgos, la actualización de los riesgos obsoletos, la actualización de la respuesta a los riesgos.

Informe de los riesgos: Incluye detalle de los riesgos individuales, las respuestas acordadas, las conclusiones y recomendaciones.

Además, incluye las conclusiones de los auditores de riesgos sobre la afectividad de los procesos de Gestión de Riesgos.

Actualizaciones a los activos de los procesos de la organización: Los activos de los procesos de la organización que son actualizados como resultados del proceso son:

- Planillas para el plan de Gestión de Riesgos, registros de riesgos o informes de riesgos.
- Estructura de desglose de riesgo

Resultados del cronograma y costo de proyecto, esta salida muestra una distribución acumulativa, se utiliza la cuantificación de las reservas para contingencias de costo y tiempo.

- Probabilidad de alcanzar los objetivos de costo y tiempo:
- Lista priorizada de los riesgos cuantificados
- Tendencia en los resultados de análisis cuantitativo.

2.11 Gestión del Conocimiento

Una nueva generación tecnológica, que se inicia a finales del siglo XX, se destaca en las organizaciones y empresas, cuyo núcleo principal del flujo de datos por la mismas, era la información digital.

Las diferentes ramas económicas, políticas y sociales, y los procesos de globalización dieron origen a la aparición de nuevos estilos y métodos de dirección. Estos componentes contribuyeron a que la información, se convirtiera en el medio económico y estratégico más relevante para las organizaciones, permitiendo que estas, obtengan inmejorables ventajas competitivas y la vía fundamental para lograrlo, fue sin duda, la gestión de dicho recurso.

Emerge, en ese momento la Sociedad de Información y del conocimiento, que orienta a la información como el elemento principal y recurso económico para las organizaciones. [37]

2.11.1 Dato, Información y Conocimiento

Dar una breve definición de los términos básicos analizados en este artículo: dato, información y conocimiento, arrojará más claridad sobre las palabras que se utilizan.

Para tener claridad sobre las palabras antes de usarlas, es útil dar, de modo breve, una definición para los términos básicos analizados en este artículo: dato, información y conocimiento. Términos relacionados como aptitud, capacidad, habilidad, destreza y competencia origina ocasionalmente un problema recurrente al tratar de definirlos, dado que. algunos de ellos se explican apelando a los otros y es difícil lograr una clara diferenciación entre ellos o precisar la forma en que se vinculan o complementan.

- Datos: Representan la materia prima y un dato como tal, no tiene significado para un ser humano, ejemplo calor, calor = ausencia del frío, a una persona común le resulta complejo o imposible interpretar este dato.
- Información: es algo con significado “ahora hace calor” y el individuo puede interpretarlo. La actividad de interpretar es subjetiva y, esto hace que, la información sea subjetiva. Es decir, cada sujeto construye su “propio mundo” a través de la interpretación y la percepción.

- Conocimiento: es más relevante que información, a partir de los datos y la información, se origina el conocimiento; y este genera las decisiones necesarias, cuyo resultado es la obtención del aprendizaje necesario, para producir de forma reiterada, más conocimiento. En otras palabras, el conocimiento es el resultado de un proceso de aprendizaje, y de una experiencia.

Así, el conocimiento existe en el contexto personal [38]

Se pueden precisar tres tipos diferentes, de conocimientos, el denominado tácito, el conocimiento explícito y por último el conocimiento organizacional.

La gestión del conocimiento como encuadre gerencial otorga la posibilidad de transformar el conocimiento tácito en explícito y estos en el denominado organizaciones o culturales, por medio de diferentes estrategias que permitan su identificación, posibilitando que las habilidades, competencias y experiencias de los integrantes de una organización sean puestas a disposición de todos sus miembros. con el objetivo de lograr el éxito de la empresa y un apropiado proceso de toma de decisiones. [37]

El conocimiento tácito es aquel que existe en la mente humana, que no resulta sencillo de plantear a través del lenguaje formal, consecuentemente se dificulta transmitirlo y compartirlo con otros, se requiere una estrecha relación y confianza para que la transmisión detente eficacia. Este tipo de conocimiento puede ser engorroso de adquirir pues físicamente, es desconocido hasta por el propio individuo que lo posee, se considera de gran valor dado que proporciona contextos, ideas y experiencias propias de la persona.

El conocimiento explícito es aquel que permite ser documentado y escrito, expresar con palabras y números, así como transmitir y compartir fácilmente, es aquel que está soportado en un recurso tangible, disponible en documentos, bases de datos, formulas científicas, etc., expresado mediante códigos y datos concretos que permiten

ser descodificados. Su gestión puede llegar a ser menos engorrosa que la del conocimiento tácito. [39]

El conocimiento organizacional establece el pilar más significativo para las organizaciones, es el valor anexado del resultado de la aplicación de los conocimientos tácitos y explícitos reconocidos tanto en el ámbito interno como en su contexto. El conocimiento organizacional se puede hallar en patentes, procesos, comportamiento de los individuos de una organización, los productos y servicios, procesos de innovación tecnológica. [40], además es la integración del explícito, el tácito, no se pueden ver desvinculados, el estudio de los conocimientos de los miembros de una organización, sus conocimientos expresados, su situación social, sus creencias, la manera de afrontar los problemas que hacen en conjunto la formación del conocimiento organizacional.

El conocimiento organizacional asocia también el aprendizaje que se logra adquirir a nivel de grupo o división. Esta mirada permite dimensionar los conocimientos que se forman escala de los grupos o de las organizaciones, se podría decir que es, el resultado de todos los conocimientos individuales que se emplean para conquistar el éxito de la organización.

Estos tipos de conocimiento no permiten ser diferenciados tan fácilmente, dado que existe entre ellos un nexo que los hace dependientes uno del otro, a pesar de sus diferenciaciones y especificidades.

Este proceso, contienen desarrollos organizativos que procuran la combinación sinérgica de la capacidad de procesamiento de datos e información, con la capacidad innovadora y creativa de los seres humanos, es decir, está localizado esencialmente en las personas, por lo cual, para que estas herramientas funcionen, se deberá tener como premisa, considerar la manera en que las personas piensan y se comportan, como muestra la figura 16.

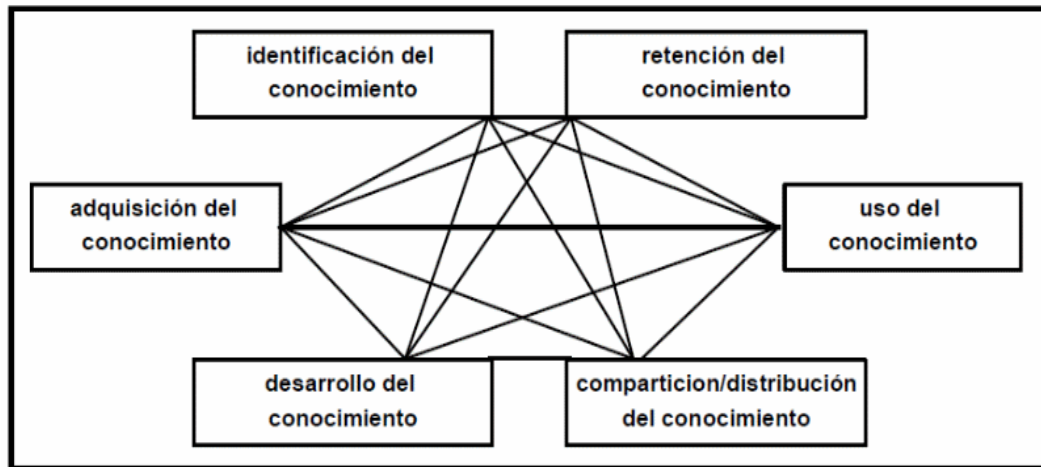


Figura 16 -Procesos medulares de la Gestión del Conocimiento[41]

2.11.2 Características de la Gestión del Conocimiento

La gestión de conocimiento encierra varios conceptos, unos autores hablan de Gestión del Conocimiento, otros de aprendizaje organizacional, algunos de Capital Intelectual, e incluso de activos intangibles.

Las organizaciones, poseen activos físicos y financieros, estos activos no poseen la capacidad de gestar ventajas competitivas sustentadas en el tiempo, poseen, además, activos intangibles que aportan verdadero valor a las organizaciones. [42]

Las organizaciones, hace cierto tiempo tomaron conciencia de que sus activos físicos y financieros no tienen la capacidad de generar ventajas competitivas sostenibles en el tiempo, y descubren que los activos intangibles son los que aportan verdadero valor a las organizaciones.

La conceptualización de aprendizaje organizativo, se funda en el análisis de la envergadura de los intangibles, es menester recordar que la mayoría de ellos suelen estar sustentados en la información, el conocimiento y el aprendizaje.

La Gestión del Conocimiento, tal como su nombre lo indica es la gestión de los activos intangibles que originan valor para la organización. La gran mayoría de estos intangibles tienen que ver con procesos relacionados de una u otra forma con la

captación, estructuración y transmisión de conocimiento, donde el aprendizaje organizacional, es su principal herramienta. Es un concepto dinámico o de flujo, como lo es el aprendizaje del ser humano.

Plantear la diferencia entre dato, información y conocimiento, hace a la comprensión del principio de la gestión del conocimiento. Una primera aproximación podría ser la siguiente: los datos se encuentran localizados en el mundo y el conocimiento localizado en agentes como personas y organizaciones, en tanto que la información adopta un papel mediador entre ambos conceptos.

Hay que considerar que, en realidad, lo que fluye entre agentes distintos nunca es el conocimiento como tal, sino datos que al procesarlo lo transformamos en información.

Es posible aproximar el conocimiento de dos agentes que comparten los mismos datos, pero a causa de sus experiencias anteriores y a las diferencias en el modo de procesar los datos (modelos mentales, modelos organizacionales), no tendrán nunca la misma inclinación para la acción, tampoco estados idénticos de conocimiento. Sólo se lograría aproximaciones, a razón de que el contexto interno y externo de un agente siempre es diferente a otro, porque el conocimiento es información puesta dentro de un contexto (experiencia). Como conclusión, los datos, una vez asociados a un objeto y estructurados se convierten en información. La información asociada a un contexto y a una experiencia se transforma en conocimiento. El conocimiento asociado a una persona y a una serie de habilidades personales se transforma en sabiduría, y finalmente el conocimiento asociado a una organización y a una serie de capacidades organizativas se convierte en Capital Intelectual.

La práctica de gestionar el conocimiento para lograr la utilidad para las personas y la organización mediante las modalidades de conocimiento aplicables a la formación de las capacidades organizativas [43].

- Know-what: se refiere a saber qué es lo que se gestionará
- Know-how: saber el cómo se realizará la gestión, es decir, los procedimientos.

- Know-why: responde a conocer por qué se gestiona.

Se diferencia de forma explícita el conocimiento, de los motivos y de los supuestos que subyacen a las prácticas laborales de las organizaciones.

Capital Intelectual:

Es un concepto casi contable. La idea es implementar modelos de medición de activos intangibles, denominados habitualmente modelos de medición del Capital Intelectual. La dificultad de estos modelos radica en que dichos intangibles no pueden ser valorados mediante unidades de medida uniformes, y por lo cual, no se puede exhibir una contabilidad de intangibles como tal, si permite tener una foto aproximada del valor de los intangibles de una organización [44].

El objetivo es, precisar cuáles son los intangibles que aportan valor a la organización y posteriormente elaborar un seguimiento de los mismos.

Una vez que hemos incluido el concepto de Capital Intelectual, se podrá definir de nuevo el concepto de Gestión del Conocimiento de un modo más preciso: conjunto de procesos y sistemas que permiten que el Capital Intelectual de una organización aumente de forma significativa, mediante la gestión de sus capacidades de resolución de problemas de forma eficiente, con el objetivo final de generar ventajas competitivas sostenibles en el tiempo [45].

Capital Intelectual como material intelectual, información, conocimiento, propiedad intelectual, experiencia, que pueden aplicarse para crear valor, es fuerza cerebral colectiva. Dificultoso de identificar y más aún de distribuir eficazmente, pero quien lo encuentra y explota, triunfa. El mismo autor afirma que en la nueva era, la riqueza es producto del conocimiento y conjuntamente con la información, se han convertido en las materias primas esenciales de la economía y los productos más importantes. En definitiva, El Capital Intelectual lo podemos definir como el conjunto de Activos Intangibles de una organización que, pese a no estar reflejados en los estados contables tradicionales, en la actualidad genera valor o tiene potencial de generarlo en el futuro [46].

2.11.3 Modelos de la Gestión de Conocimiento

La gestión de Conocimiento como práctica dentro las organizaciones requiere la formalidad de los procesos por lo tanto se deben utilizar modelos estándares para su implementación, por lo cual, se investigaron 4 modelos de implementación de GC.

Modelo conceptual de Nonaka y Takeuchi

Es un modelo que responde a mejorar los modelos categóricos o taxonómicos planteados por McAdam y McCreedy en el año 1999 [47]. Esta tipología es más teórica y comparte una índole mecanicista; las propuestas categorizadas parten de elementos moderados, conocimiento tácito y explícito, para comprender como se da el proceso de transformación del conocimiento. El modelo alude a dos tipos de conocimiento: el conocimiento tácito y el explícito.

El conocimiento explícito, o articulado, se puede separar del individuo que lo posee, mediante una apropiada interpretación, que se transfieren a formas de externalizar dicho conocimiento, de una manera verbal, escrita o en un lenguaje científico. El conocimiento tácito, no puede ser apartado de la persona que lo conoce, este conocimiento se va radicando a través de la experiencia y no puede separarse del individuo, dada su complejidad [48].

Como se alegó precedentemente el modelo de Nonaka y Takeuchi ha dado la base para el desarrollo de otros; desde esta perspectiva se comprenden 4 actividades importantes:

- Fase 1: Fase de socialización, ocurre la interacción, lo que permite que el conocimiento se traslade de individuo a individuo, es decir que, se comparte de una persona a otra.
- Fase 2: Fase de externalización, el conocimiento, de estar en las personas de modo tácito pasa a ser explícito: es decir que, a través la reflexión colectiva se articula el conocimiento tácito, en la creación de información.
- Fase 3: Fase de combinación, el conocimiento explícito se intercambia entre los miembros de la organización.

- Fase 4: Fase de internacionalización, se busca que el conocimiento explícito, se transforme a conocimiento tácito mediante la creación de la acción; por lo tanto, constituye crecimiento operacional, y se corresponde con el aprendizaje organizacional.

Este modelo, establece la piedra angular sobre la cual se han desarrollado otros modelos de la gestión del conocimiento, incluso de otras categorías, como por ejemplo, la herramienta KMAT (Knowldge Managment Assesment Tool) desarrollado por Andersen y donde se plantean cuatro factores facilitadores de la administración del conocimiento: Liderazgo, Cultura, Medición y Tecnología, influyentes en el proceso de captura, almacenamiento y transferencia del conocimiento, propuesto inicialmente por Nonaka y Takeuchi.

Modelo cognoscitivo de Choo

Choo propone un modelo de la organización inteligente, en él se refiere un tipo de gestión de conocimiento que también puede ser apreciado dentro de la categoría de modelos cognoscitivos y de capital intelectual. En su modelo se destaca el sentido común, la creación del conocimiento y la toma de decisiones como sus bases, y está centrado en la selección e incorporación de elementos de información, dentro de las acciones de la organización, lo cual es posible, dada la concentración y asimilación de la información proveniente del entorno.

Las organizaciones que buscan “hacer un uso y aplicación intensiva del conocimiento con la finalidad de generar valor para sus productos y procesos” [47], implementan este modelo

La vinculación de la teoría de la organización, las ciencias cognoscitivas y las de la información, a los propósitos de la gestión del conocimiento; del modelo Choo define tres metas fundamentales:

- Meta 1: Generar sentido: crear una identidad y un contexto compartido de acción y reflexión, se asienta en la construcción de la identidad, que es necesaria para que el individuo mantenga una opinión coherente de sí mismo.

El medio ambiente actúa como espejo que confirma o retroalimenta este proceso. La misma es retrospectiva, de manera selectiva, los sujetos rastrean en su memoria los sucesos pasados. En esta exploración, se establecen interpretaciones y significados a las experiencias pasadas, de modo de formar un “mapa mental”, generado a partir de ellas. También es representativa y frecuentemente, simboliza parte del medio ambiente en el que se desenvuelve, se podría decir que es social, dado que es el medio a partir del cual, se edifican las representaciones colectivas.

- Meta 2: Crear conocimiento: desplegar nuevas capacidades y conocimientos, Transformación del conocimiento personal, a través del diálogo y la compartición de información entre individuos.
- Meta 3: Toma de decisiones; en la que se comprometen recursos y capacidades para una acción intencionada, Identificar y evaluar alternativas mediante el proceso de análisis de información y conocimiento.

Así, el autor refiere tres procesos estratégicos (figura 17) en la gestión del conocimiento que, se extra ponen y son recíprocos; siendo estos: la percepción, la creación de conocimiento y la toma de decisiones. Actividades, que a su vez configuran lo que el autor señala como ciclo continuo de aprendizaje y adaptación o ciclo del conocimiento [49].

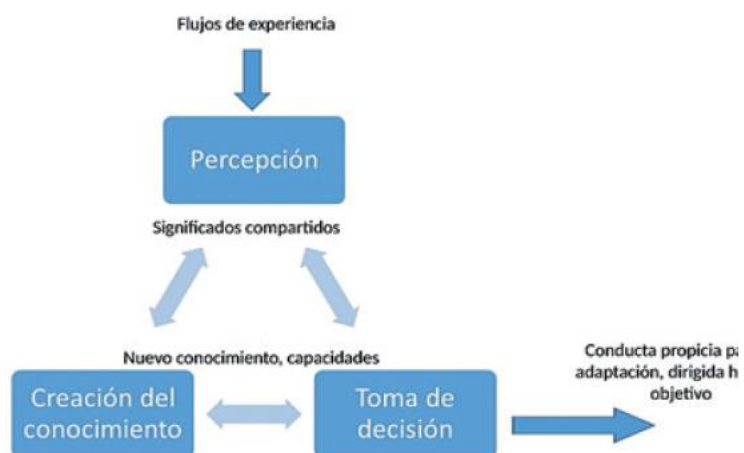


Figura 17 -El ciclo de la inteligencia[46]

Choo estima que el éxito de la gestión del conocimiento, lleva a la organización a una fase superior, donde se originan las denominadas organizaciones inteligentes y las precisa, como aquellas aptas para percibir y procesar información, crear conocimiento a partir de la información procesada y utilizar el conocimiento para la toma de decisiones de manera eficaz.

Modelo socio construccionista KPMG

El modelo parte de la pregunta: ¿qué factores condicionan el aprendizaje de una organización y qué resultados produce dicho aprendizaje?

KPMG para responder a esta pregunta efectúa un esfuerzo que produce un modelo cuya finalidad es la exposición clara y práctica de los factores que determinan la capacidad de Aprendizaje de una organización, además de los resultados esperados del aprendizaje.

La interacción de todos sus elementos, es una de las características esenciales del modelo, que se exhiben como un sistema complejo, en el cual las influencias se producen en todos los sentidos [50].

La estructura organizativa, la cultura, el liderazgo, los mecanismos de aprendizaje, las actitudes de las personas, la capacidad de trabajo en equipo, etc., no son independientes, sino que están conectados entre sí, se muestra en la figura 18 el modelo kmpg.



Figura 18 - modelo de gestión del conocimiento kpmg[51]

Los factores condicionantes del aprendizaje.

Son aquellos que conforman la capacidad de aprender de una empresa, se han dispuesto en los tres bloques siguientes, atendiendo a su naturaleza:

1.- Compromiso firme y consciente de toda la empresa, en especial de sus líderes, con el aprendizaje generativo, continuo, consciente y a todos los niveles.

Para el éxito de una iniciativa de gestión del conocimiento, se ha de reconocer manifiestamente, que el aprendizaje es un proceso que debe ser gestionado y comprometer para ello todos los recursos disponibles.

2.- Comportamientos y mecanismos de aprendizaje a todos los niveles. La organización como entidad no humana, sólo obtiene aprendizaje en la medida en que, las personas y equipos que la integran sean capaces de aprender y posean deseo de hacerlo.

Disponer de personas y equipos aptos es condición necesaria pero no suficiente para poseer una organización capaz de generar y utilizar el conocimiento mejor que las demás. Para lograr que la organización aprenda es preciso desarrollar mecanismos de creación, captación, almacenamiento, transmisión e interpretación del conocimiento, permitiendo el aprovechamiento y utilización del aprendizaje que se da en el nivel de las personas y equipos [51].

Los comportamientos, actitudes, habilidades, herramientas, mecanismos y sistemas de aprendizaje que el modelo considera son:

- La responsabilidad personal sobre el futuro (proactividad de las personas).
- La habilidad de debatir los supuestos (modelos mentales).
- La visión sistémica (ser capaz de analizar las interrelaciones existentes dentro del sistema, entender los problemas de forma no lineal y ver las relaciones causa-efecto a lo largo del tiempo).
- La capacidad de trabajo en equipo.
- Los procesos de elaboración de visiones compartidas.
- La capacidad de aprender de la experiencia.
- El desarrollo de la creatividad.
- La generación de una memoria organizacional.
- Desarrollo de mecanismos de aprendizaje de los errores.
- Mecanismos de captación de conocimiento exterior.
- Desarrollo de mecanismos de transmisión y difusión del conocimiento.

Si se logra que las personas aprendan, pero no transforman ese conocimiento en activo útil para la organización, no se puede hablar de aprendizaje organizacional. La empresa inteligente practica la comunicación a través de diversos mecanismos, tales como reuniones, informes, programas de formación internos, visitas, programas de rotación de puestos, creación de equipos multidisciplinarios

3.- Desarrollo de las infraestructuras que determinan el funcionamiento de la empresa y el comportamiento de las personas y grupos que la integran, para favorecer el aprendizaje y el cambio permanente.

Pero, debemos tener en cuenta que las condiciones organizativas pueden actuar como obstáculos al aprendizaje organizacional, bloqueando las posibilidades de desarrollo personal, de comunicación, de relación con el entorno, de creación.

Las características de las organizaciones tradicionales que dificultan el aprendizaje:

- Estructuras burocráticas.

- Liderazgo autoritario y/o paternalista.
- Aislamiento del entorno.
- Autocomplacencia.
- Cultura de ocultación de errores.
- Búsqueda de homogeneidad.
- Orientación a corto plazo.
- Planificación rígida y continuista.
- Individualismo.

En conclusión, la forma de ser de la organización no es neutra y exhorta cumplir una serie de condiciones para que las actitudes, comportamiento y procesos de aprendizaje definidos puedan desarrollarse.

El modelo considera los elementos de gestión que influyen directamente a la forma de ser de una organización: cultura, estilo de liderazgo, estrategia, estructura, gestión de las personas y sistemas de información y comunicación.

Los resultados del aprendizaje.

Una vez examinados los factores que condicionan el aprendizaje, el modelo refleja los resultados que debería producir ese aprendizaje. La capacidad de la empresa para aprender se debe traducir en:

- La posibilidad de evolucionar permanentemente (flexibilidad).
- Una mejora en la calidad de sus resultados.
- La empresa se hace más consciente de su integración en sistemas más amplios y produce una implicación mayor con su entorno y desarrollo.
- El desarrollo de las personas que participan en el futuro de la empresa.

Modelo de comunidades de práctica KMAT de Andersen

El KMAT es un instrumento de evaluación y diagnóstico construido sobre la base del Modelo de Administración del Conocimiento Organizacional desarrollado

conjuntamente por Arthur Andersen y la American Productivity & Quality Center (apqc) [52].

Este modelo considera necesario acelerar el flujo de información que tiene valía, desde los individuos a la organización y de vuelta a los individuos, de modo que estos la empleen, creando valor para los clientes. También destaca la responsabilidad que poseen los trabajadores de hacer explícito el conocimiento llamándolos facilitadores; para ello, la organización debe establecer infraestructuras de apoyo que lo permitan [53].

Propone, en este modelo dos tipos de sistemas o mecanismos para favorecer el flujo de información: en primer lugar, sharing Networks o comunidades de práctica que pueden ser virtuales o reales, el propósito es generar reflexiones conjuntas sobre un tema determinado; y en segunda instancia el conocimiento empaquetado, considerado como la espina dorsal de la GC, en donde a través de un sistema interno, se implantan las mejoras prácticas, metodologías, informes y herramientas, con la finalidad de colocarlas a disposición de los colaboradores [54].

Este mismo autor Andersen en el año 1999 desarrolló una herramienta de evaluación y diagnóstico construida por este autor y APQC, copropietaria del modelo. El modelo KMAT es una herramienta de benchmarking colaborativo, que está diseñado para ayudar a las organizaciones a tomar conocimiento sobre forma que gestionan el conocimiento, basado en 5 factores esenciales a saber:

Liderazgo: Comprende la estrategia y cómo la institución define su negocio y el uso del conocimiento para reforzar sus competencias críticas.

Cultura: Refleja cómo se enfoca, favorece el aprendizaje y la innovación, conteniendo acciones que fortalecen el comportamiento abierto al cambio y al nuevo conocimiento.

Tecnología: Analiza cómo equipa a sus miembros, porque posean una fácil comunicación y de mayor rapidez.

Medición: Incluye la medición del capital intelectual y la forma en que se distribuyen los recursos, potenciando el conocimiento que fomenta el crecimiento.

Procesos: Contienen los pasos mediante los cuales la empresa identifica las brechas de conocimiento y ayuda a capturar, adoptar y transferir el conocimiento necesario, agregando valor al cliente y potenciar los resultados.

2.11.4 Gestión de Conocimiento en la empresa

El conocimiento es, la capacidad de actuar, procesar e interpretar información generando más conocimiento o dando solución a un determinado problema [55]. La dificultad radica, en cómo las organizaciones incorporan en sus procedimientos la gestión del conocimiento, y esta tributa de forma práctica, al desarrollo de sus procesos, al fomento de sus competencias, a la calidad en la toma de decisión y en su sentido más amplio, a su gestión [56].

Vamos camino hacia una sociedad impulsada por el conocimiento, donde los activos tangibles habituales están perdiendo valor a favor de los intangibles. Teniendo en cuenta lo antes dicho, se puede pensar al conocimiento como, el principal ingrediente intangible tanto en las empresas, como en la economía en su conjunto [57].

La gestión de conocimientos extiende en el ámbito de la organización el uso de prácticas difíciles de observar y manipular, a veces incluso son desconocidas para los que las poseen. Esto presenta un inconveniente para las empresas más familiarizadas con la gestión y contabilidad del capital fijo.

Todas las perspectivas de la gestión del conocimiento, basándose en unos principios y unas prácticas, en muy pocas ocasiones son adscritas a la parte donde se almacena mayor nivel de conocimiento tácito dentro de las organizaciones tanto industriales como ser también de servicios, como pueden ser los aspectos tácticos de mantenimiento, montaje y proyectos, y actividades en general de difícil documentación, que normalmente se basan en gran parte en la experiencia de los empleados

Las estructuras de conocimiento se fundan sobre experiencias pasadas y son utilizadas para ordenar datos, su consiguiente interpretación y acción. De aquí que el conocimiento individual se orienta a las estructuras de conocimiento individual, mientras que el conocimiento grupal, se relaciona a las estructuras de conocimiento organizacional [58].

La organización generadora de conocimiento, tiene que delinear formas de trabajo y establecer políticas que generan condiciones que se puede caracterizar en tres facilitadores básicos, como ser la equidad, reconocimiento del esfuerzo y los méritos de cada miembro de la organización.

El fomento de la confianza en los miembros y entre cada uno de ellos, es un requisito para delegar en ellos la autonomía necesaria en el trabajo cualificado, adquirir la cooperación en la creación de conocimiento y la congruencia entre los objetivos e intereses de la empresa y los trabajadores, son las que producen la creación de conocimiento.

Se trata de instaurar un espacio organizativo, donde los miembros de la organización, basando sus relaciones en las condiciones básicas expuestas, compartan información, objetivos e intereses. De este modo, aseguramos la cooperación voluntaria de los miembros de la organización y la contribución de su inteligencia que, son necesarias para la organización creadora de conocimiento [59].

El proceso de gestión del conocimiento, debe ser establecido como una misión de grupo o equipo, y donde debe haber una sensibilización y pro-actividad para la captura de ese conocimiento, y como en todos los grupos de sujetos, existe relación entre la competitividad y la cooperación entre sus miembros.

Si puntualizamos la gestión del conocimiento dentro del contexto de una empresa, se muestra como un proceso, un enfoque de este, podría estar integrado básicamente, por la generación, la codificación, la transferencia y la utilización del conocimiento [60].

- Generación del conocimiento: estudia los procesos de adquisición de conocimiento externo y de creación del mismo en las organizaciones, poniendo en acción los conocimientos poseídos por las personas [61].
- Codificación, almacenamiento o integración del conocimiento: poner al alcance de todos los conocimientos organizativos, ya sea de forma escrita o localizando a la persona que lo concentra.
- Transferencia del conocimiento: analiza los espacios de intercambio del conocimiento y los procesos técnicos o plataformas que lo hacen posible. Esta fase puede realizarse a través de mecanismos formales y/o informales de comunicación.
- Utilización del conocimiento: la aplicación del conocimiento recientemente adquirido en las actividades rutinarias de la empresa.

La generación y transferencia del conocimiento son procesos que cuenta con una mayor cantidad de conocimiento tácito. Tanto en la etapa de codificación como en la de utilización, el conocimiento tácito es convertido en conocimiento explícito para la comprensión y disposición de todos los miembros de la empresa [61].

Es conveniente definir el concepto de pérdida o fugas de conocimiento, donde nos encontramos con la extensa problemática de la pérdida del personal importante para la organización, este es un factor que se produce con gran incidencia entre el personal de planta, debido a la rotación de dicho personal o por las políticas de subcontratación de las empresas. Claramente se demuestra que el abandono de los individuos claves, resulta una pérdida neta de conocimiento, limitando el grado al acceso del conocimiento y al aprendizaje para los empleados que los sustituyen al no poder contratar un nuevo trabajador igualmente rentable. Una alta tasa de abandono, rompe la continuidad en la organización y provoca un entorno social, en el que los trabajadores desconfían de sus compañeros [62].

Por lo cual, debemos capturar estos conocimientos para evitar que se pierdan con el personal que ha dejado su vínculo con la organización, podemos aplicar herramientas tecnológicas, que produzcan un abaratamiento y confiera una evidente

fiabilidad y eficiencia en la difícil tarea de capturar el conocimiento estratégico y que genera valor para la organización.

Capturar el conocimiento y evitar su pérdida

- Instrucciones de trabajo: Generar una documentación explícita del conocimiento referente a un proceso o producto, facilitando su comprensión.
- Listas de comprobación: El conocimiento se representa a través de una serie de elementos que se comprueban antes de finalizar un trabajo.
- Formación de paquetes: Se recopilan los puntos o aspectos fundamentales de un proceso. Puede registrarse a través de algún programa de formación.
- Puesto de trabajo: Relacionada con la formación en el puesto de trabajo, el mentor traslada el conocimiento y experiencia implícita a otros RRHH de la organización, surge como conocimiento indocumentado para los demás.
- Base de conocimiento: Confeccionar lecciones aprendidas a lo largo del proceso. Se propone capturar el conocimiento, los logros y fracasos generados a partir de un producto o servicio, expuestos en una base de datos para su revisión durante el diseño. El conocimiento a disposición de próximos procesos.

2.12 Análisis de Riesgos en Auditoría

La auditoría informática y el análisis de riesgos son los métodos usados comúnmente de forma independiente para evaluar los sistemas de información, cada una de ellas con un enfoque diferente. Por un lado, la auditoría informática, es un proceso de revisión y verificación y por el otro, el análisis de riesgos que es un proceso de diagnóstico y revisión. La auditoría informática sólo identifica el nivel de exposición por la falta de controles, mientras que el análisis de riesgos facilita la evaluación de los riesgos y recomienda acciones en base al coste/beneficio de las mismas.

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la

evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. Proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado[4]. Por otra parte, el auditor de sistemas de información, debe utilizar una técnica o enfoque apropiado de evaluación de riesgos, al desarrollar el plan general de auditoría de sistemas de información, y al determinar prioridades para la asignación eficaz de los recursos de auditoría de los sistemas. Además, al planear revisiones individuales, el auditor debe identificar y evaluar los riesgos relevantes al área bajo revisión[63].

Debido a los cambios en los modelos de operación de los negocios, impulsados por los avances en las tecnologías de información -que hemos indicado anteriormente- el surgimiento de normativas nacionales e internacionales en el ámbito de las tecnologías de información, relacionadas con el procesamiento, explotación, entrega de información y servicios basados en dichas tecnologías, los nuevos modelos de control interno impulsados por ejemplo, por marcos de trabajo ampliamente conocidos y aceptados como COBIT 5. La auditoría informática se ha enfrentado a la necesidad de evolucionar de un enfoque de verificación efectuado a posteriori, a uno preventivo y proactivo basado en la valoración de los riesgos, la evaluación de la eficacia y la eficiencia de los procedimientos, y los controles establecidos en las organizaciones, todo ello, orientado a mejorar las características de seguridad, calidad, eficiencia y eficacia de los sistemas de información y las tecnologías asociadas.

Para incorporar el análisis de riesgos en la auditoría informática, se recurre a algunas metodologías y/o estándares que consideran el análisis de riesgos como parte de una auditoría informática.

“Una auditoría puede servirse de un análisis de riesgos que le permita 1º saber qué hay en juego, 2º saber a qué está expuesto el sistema y 3º valorar la eficacia y eficiencia de las salvaguardas.”[26]

De acuerdo a lo expuesto, se observa que el papel que puede desempeñar un análisis de riesgos dentro de una auditoría informática, está orientado a valerse de la información proveniente de dicho análisis, relativa al valor que posee el o los sistemas

o procesos a auditar, las amenazas y sus salvaguardas, lo que permitirá al auditor, focalizar su trabajo y priorizar las áreas o procesos a auditar.

La organización ISACA, proporciona una serie de estándares, guías y procedimientos al respecto del tema que nos ocupa, el estándar S11: Uso de la evaluación de riesgos en la planeación de auditoría[64], proporciona las siguientes líneas básicas:

El auditor de SI debe recurrir a una técnica o enfoque apropiado de evaluación de riesgos al desarrollar el plan general de auditoría de SI y al determinar prioridades para la asignación eficaz de los recursos de auditoría de SI. Al planear revisiones individuales, el auditor de SI debe identificar y evaluar los riesgos relevantes al área bajo revisión.

Para la aplicación de este estándar, ISACA recomienda el uso de la guía G13: Uso de la evaluación de riesgos en la planeación de auditoría, que da las claves para la aplicación del estándar y el procedimiento de auditoría de SI P1: Medición de la evaluación de riesgos de SI que proporciona ejemplos de procedimientos a seguir.

A través de este estándar se advierte un enfoque de auditoría que hace uso del análisis de riesgos. El papel principal del análisis de riesgos es suministrar la base para la selección de las áreas a revisar, que posean una mayor exposición a riesgos, e incluirlas en un plan general de auditoría o en una auditoría puntual.

Con la aplicación de este guía, es posible identificar los riesgos y vulnerabilidades, que le permitirán al auditor establecer que controles son necesarios para mitigar esos riesgos. En este sentido es importante determinar una clara relación entre riesgo y control, así como conocer los tipos de riesgos y los controles a recurrir, es quizás, este un punto clave para el uso de este enfoque de auditoría, dado que establece las áreas con mayor exposición a riesgos y su respectivo control.

Como resultado de la auditoría se obtendrá un informe que expondrá las inconsistencias, entre las necesidades identificadas en el análisis de riesgos y la realidad detectada durante la inspección del sistema, área o proceso.

En la actualidad, existen organizaciones que utilizan un enfoque de auditoría basada en el análisis de riesgos, como una visión de auditoría moderna, que les permite desarrollar y mejorar su proceso de auditoría continua. Es importante puntualizar que en un proceso de auditoría que emplee este enfoque, los auditores pueden partir de un análisis de riesgos ya elaborado o realizar un análisis propio.

El desarrollo de una auditoría bajo esta orientación, basado en riesgos, puede alinearse con metodologías, estándares y marcos de trabajo, nacionales e internacionales de control interno, auditoría, gestión de riesgos y seguridad informática tales como Mageritv3, ISO 27005, ISO 27002, COBIT5, Esquema Nacional de Seguridad, entre otros, los cuales han sido tratados en capítulos anteriores.

De lo expuesto anteriormente, podemos concluir que, los principales usos que pueden hacerse del análisis de riesgos dentro de una auditoría informática son, por un lado, la planificación de la auditoría, definiendo su alcance y por otro, la verificación de los controles implementados frente a los riesgos identificados.

2.12.1 Cobit 5

Control Objectives for Information and related Technology o COBIT 5, se define como un conjunto de herramientas de soporte empleadas por los gerentes, para reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Es un marco de trabajo o framework¹², en el que se puede desarrollar una política clara que permite el control de las TI en la organización. La aplicación de este marco, incide especialmente en el cumplimiento regulatorio y se basa específicamente a la creación de valor asociado al área de TI de la organización.

Las organizaciones poseen muchas partes interesadas en crear valor y esa premisa pueden ser objetivos diferentes para cada parte de la organización o área, y en algunos casos contradictoria[65].

¹² Entorno de trabajo es una estructura conceptual y tecnológica de asistencia definida, normalmente, con artefactos o módulos concretos de *software*

Desde su inicio, COBIT 5 ha evolucionado a partir de su uso para la auditoría de TI, para luego pasar por el control, la gestión de TI, el gobierno de TI, llegando a su versión actual, que es un enfoque holístico de gobierno corporativo de TI.

Este marco de trabajo cuenta con cinco principios que una organización debe seguir para adoptar la gestión de TI:

1. Satisfacción de las necesidades de los accionistas: se alinean las necesidades de los accionistas con los objetivos empresariales específicos, objetivos de TI y objetivos habilitadores. Se optimiza el uso de recursos, cuando se obtienen beneficios con un nivel aceptable de riesgo. Las actividades y objetivos de gobierno, tratan de negociar y decidir entre los diferentes intereses, el valor de las partes interesadas, en consecuencia, los sistemas de gobierno consideran las necesidades de todas las partes, al tomar decisiones sobre beneficios, evaluación de riesgos y recursos. Para cada una de las decisiones por lo general, se realizan tres cuestionamientos (figura19):

- a. ¿Para quién son los beneficios?
- b. ¿Quién asume el riesgo?
- c. ¿Qué recursos se requieren?

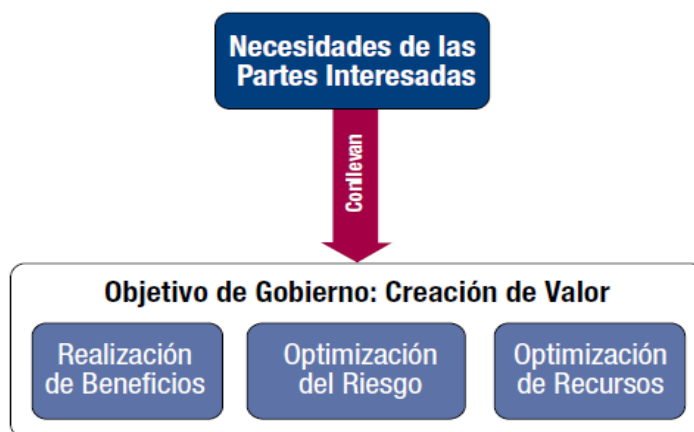


Figura 19 -Necesidades de las partes Interesadas.[61]

2. Considerar la empresa de punta a punta: el gobierno de TI y la gestión de TI son asumidos desde una perspectiva global, como muestra la figura 20; de tal

modo que se cubren todas las necesidades corporativas de TI. Esto se aplica desde una perspectiva "de punta a punta" basada en los 7 habilitadores de COBIT. Integra el gobierno de la empresa TI en el gobierno corporativo. Es decir, el sistema de gobierno para la empresa TI propuesto por COBIT 5 se integra sin problemas en cualquier sistema de gobierno. COBIT 5 se alinea con las últimas visiones sobre gobierno. Cubre todas las funciones y procesos dentro de la organización; no se focaliza solamente en la función de TI, pero trata la información y tecnologías relacionadas, como activos que necesitan ser tratados como cualquier otro activo dentro de la empresa.

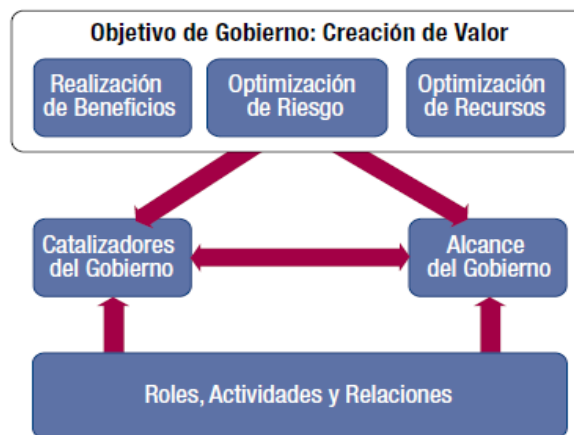


Figura 20 -Objetivo de gobierno [61]

3. Aplicar un único modelo de referencia integrado: COBIT 5 integra los mejores marcos de Information Systems Audit and Control Association en inglés ISACA como Val IT, que relaciona los procesos de COBIT con los de la gerencia requeridos para conseguir un buen valor de las inversiones en TI. También se relaciona con Risk IT, lanzado por ISACA para ayudar a organizaciones a equilibrar los riesgos con los beneficios. Se considera el uso de Business Model for Information Security o BMIS e IT Assurance Framework con sus siglas ITAF. Permite además, alinearse con los principales estándares o marcos como Information Technology Infrastructure Library - ITIL, The Open Group Architecture Forum -TOGAF, Project Management Body of Knowledge -PMBOK, PProjects IN Controlled Environments 2 -PRINCE2, Committee of Sponsoring Organizations of the Treadway Commission - COSO y estándares ISO.

4. Posibilitar un enfoque holístico: los habilitadores de COBIT 5 están identificados en siete categorías (figura 21) que abarcan la empresa de punta a punta. Individual y colectivamente, estos factores influyen para que el gobierno de TI y la gestión de TI operen en función de las necesidades del negocio.

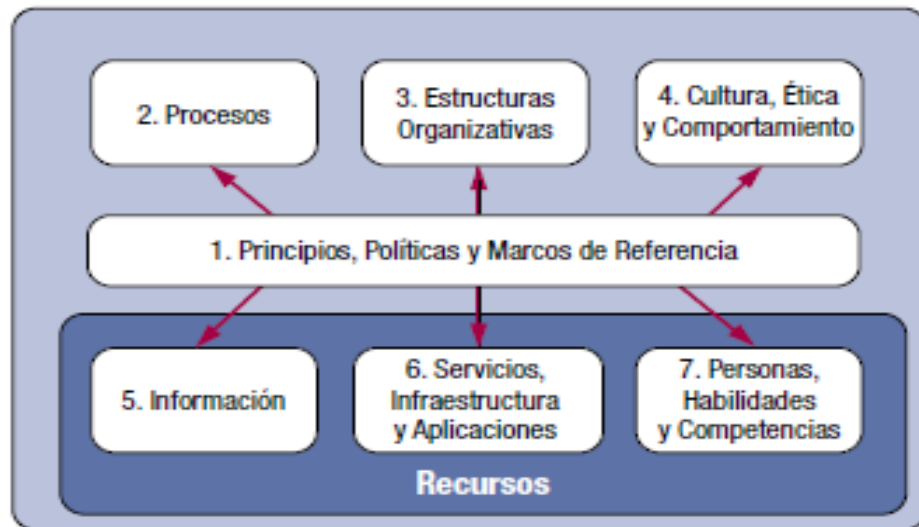


Figura 21 -Categorías de Habilitadores [62]

1. Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas, para la gestión del día a día.
2. Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI
3. Las estructuras organizativas son las entidades de toma de decisiones clave en una organización
4. La Cultura, ética y comportamiento de los individuos y la empresa son muy a menudo subestimados como factor de éxito en las actividades de gobierno y gestión.
5. La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es

necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es a menudo el producto clave de la empresa en sí misma.

6. Los servicios, infraestructuras y aplicaciones incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
7. Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades para la correcta toma de decisiones y de acciones correctivas.

Cualquier organización debe siempre considerar un conjunto interconectado de habilitadores, se necesita del resultado de otros catalizadores para ser completamente efectivo, por ejemplo, los procesos necesitan información, las estructuras organizativas necesitan habilidades y comportamiento, además de proporcionar una salida para beneficio de otros catalizadores. Por ejemplo, los procesos proporcionan información, habilidades y el comportamiento hace los procesos eficientes.

5. Separar el gobierno de la gestión: COBIT 5 distingue con claridad los ámbitos del gobierno de TI y la gestión de TI (figura22). Se entiende por gobierno de TI las funciones relacionadas con la evaluación, la dirección y el monitoreo de las TI. El gobierno busca asegurar el logro de los objetivos empresariales y también evalúa las necesidades de los accionistas, así como las condiciones y las opciones existentes. La dirección se concreta mediante la priorización y la toma efectiva de decisiones. Y el monitoreo abarca el desempeño, el cumplimiento y el progreso en función con los objetivos acordados. La gestión, está más relacionada con la planificación, la construcción, la ejecución y el monitoreo de las actividades, alineadas con la dirección establecida por el organismo de gobierno, para el logro de los objetivos empresariales.

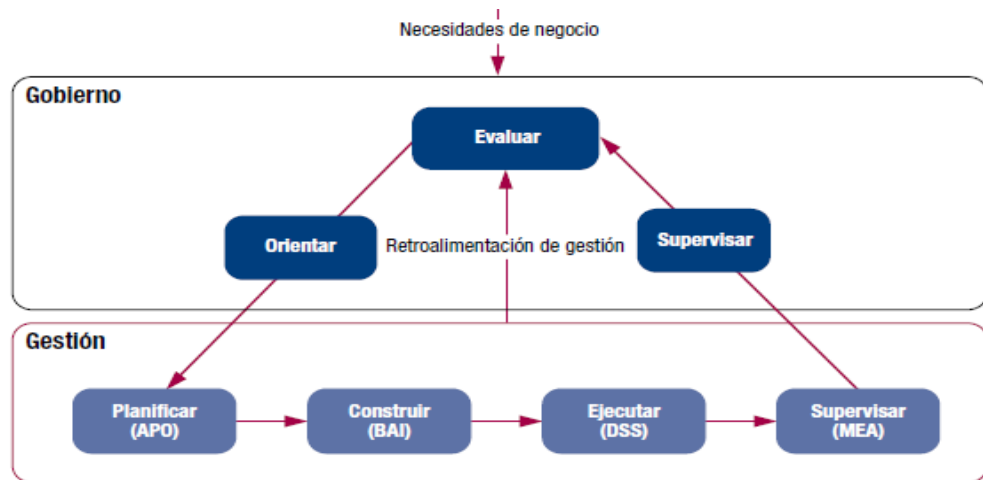


Figura 22 -Separar Gobierno de Gestión [63]

Este método propone ordenar las metas de la organización con las metas de TI. Para lo cual el marco de trabajo propone 7 habilitadores.

Los Procesos, son una categoría y una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. Empresas más pequeñas pueden tener pocos procesos; empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas.

COBIT 5 incluye un modelo de referencia de procesos (PRM), el cuál define y describe en detalle una cantidad de procesos de gobierno y gestión. El detalle de este modelo se encuentra en COBIT 5: Enabling Processes volume.

2.12.2 COBIT 5 para Riesgos

Los riesgos de TI engloban a toda la organización, si bien en el marco de trabajo se enfocan en 2 habilitadores, los procesos, controles, actividades y tareas relacionadas con los riesgos, se realizan en todos los procesos de la gestión. Se puede decir que, todos los departamentos o áreas de las organizaciones están vinculadas con la TI. Por lo tanto, si existe una falla, relacionado con TI, la misma, afectará a toda la organización, y el departamento TI no está desconectado, sino que, generalmente

posee una acción de trabajo transversal a la organización, por lo cual, decimos que un riesgo que afecta a TI, afecta directamente a toda la organización.

COBIT plantea 3 categorías de riesgos en TI.

1. Habilitación de Valor: Trata sobre poder medir a la totalidad de los servicios que presta TI, y cuanto valor genera para la organización, servicios como por ejemplo el catalizador tecnológico para las nuevas iniciativas del negocio o los catalizadores tecnológicos para las operaciones eficientes.

2. Entrega de Programas y Proyectos de TI: Trata sobre los riesgos sobre la entrega en tiempo y forma de los proyectos y programas que poseen soporte de TI, cumplir con los tiempo, cronogramas y presupuestos, es cumplir con la planificación y costos, por lo cual los riesgos de atrasos de los productos y servicios de TI son críticos para una organización. Para afrontar estos tipos de riesgos es fundamental el conocimiento sobre riesgos en proyectos, expresados en el tema anterior de este Trabajo Final de Maestría. Para la evaluación del riesgo en la entrega de programas y proyectos, podemos tomar a manera de ejemplos, el factor de calidad que debe poseer el proyecto, los sobre costos que llevan al atraso en el cronograma de entrega de los productos o servicios de TI entre otros.

3. Entrega de Operaciones y Servicios de TI: Trata sobre los procesos, productos y servicios que la organización requiere para su trabajo, funcionen de manera adecuada. Por ejemplo, como las interrupciones en el servicio de TI, problemas de seguridad, falla en sistemas etc.

Este modelo, está orientado para generar una clasificación del riesgo dentro de lo que corresponda a TI, una taxonomía de los posibles problemas que engloban a toda la organización, clasificar los riesgos e implantar soluciones diferentes, dependiendo de la categoría a la cual pertenece.

Dualidad del Riesgo

La información y la tecnología, bien gobernada y gestionada confieren beneficios a la organización, debido a que, si se evalúan los riesgos correctos, se genera conocimiento del estado de activos, esto conlleva una ventaja positiva para la

organización, por eso decimos, a mayores riesgos obtenemos mayores ventajas y nuevas oportunidades de negocios habitadas para la TI. Por contraparte el desconocimiento de ellos o la información y la tecnología pobremente gobernada y gestionada destruyen el valor o fallarán en la entrega de beneficios.

Perspectivas

Función del Riesgo

La perspectiva de la función del riesgo, se centra en lo que se necesita para construir y mantener la función de los riesgos en la empresa. -

Gestión del Riesgo

La perspectiva de la gestión del riesgo se centra en los procesos básicos del gobierno y gestión del riesgo para optimizar el riesgo y en cómo identificar, analizar, responder y reportar sobre riesgos a diario.

Modelo de las 4 T

1. Terminar: Trata sobre la eliminar el riesgo, existen tipos de riesgos que pueden ser eliminados, por ejemplo, el corte de suministro electro, si bien, no podemos controlar que la empresa de energía corte el servicio, el riesgo de que la organización quede sin energía se puede eliminar, incorporando una unidad de energía ininterrumpida, o grupo electrógeno.

2. Trasferir: Podemos realizar un outsourcing o tercerización de los riesgos, por ejemplo, al tener un servidor web en la empresa, podemos contratar un hosting web y transferir todo el riesgo de infraestructura y TI que la misma necesita, pero se debe tener en cuenta que, transferir el riesgo no significa transferir la responsabilidad de que el activo funcione correctamente.

3. Tolerar: Asumir el riesgo y sus consecuencias, analizar, investigar y conocer el riesgo es beneficioso, para poder evaluar si el mismo podría ser tolerado por la organización, y el costo que conlleva. Por ejemplo, en el sector de TI contratar personal de soporte auxiliar para tener de reserva, ante la falta de algún empleado, o

asumir el riesgo de la inasistencia de personal y no brindar correctamente el servicio ante alguna falla el día de la inasistencia.

4. Tratar: Conocer y tratar el riesgo, significa, realizar la gestión del riesgo elaborando un plan de control y tratamiento del mismo, más comúnmente llamando plan de acción, y un plan de contingencias por si el riesgo se activa como indica el modelo SEI.

Principios para la Gestión del Riesgo

- Conexión Objeto Corporativo: Trata sobre el nivel de riesgo que está dispuesto a aceptar en la empresa.
- Alinear con ERM: Generar un análisis y gestión de riesgos en la organización, y tratar las 4 T.
- Balance Costo / Beneficio de Riesgo en TI: Generar un análisis de riesgos balanceado, de acuerdo a las metas de la organización, estableciendo que la inversión y el costo que se dará al tratamiento de los riesgos sea correspondiente a los beneficios que se espera de la utilización de los activos.
- Promover comunicación justa y abierta: Comunicar es un punto primordial de la gestión del riesgo, aquí es donde se lo conoce, por lo cual, comunicar a los agentes de la organización sobre cómo tratar los riesgos y capacitarlos para ello, en un lenguaje claro donde el objetivo es, que el personal comprenda el riesgo y tome conciencia de la gestión del mismo. Esta comunicación debe ser constante en el tiempo.
- Establecer enfoque directivo y responsabilidades: Definir los roles que cumple cada agente dentro del plan de gestión de riesgos.
- Funcionan como parte de las actividades diarias: Gestionar los riesgos es trabajo diario y persistente en el tiempo, al igual que ajustar los modelos y proyectos de riesgos en TI.
- Enfoque consistente: Trata sobre realizar una planificación coherente del tratamiento de los riesgos en TI que sean consistentes en el tiempo, y basándose en el costo / beneficio de los mismos.

Políticas de Riesgos

Para tratar correctamente los riesgos se deben seguir políticas generadas para ello, las políticas ayudan a ordenar la gestión, ser consistentes en el tratamiento de riesgos, COBIT 5 para riesgos nos define un conjunto de políticas, las cuales, cada organización deberá ajustar a sus necesidades, deben ser precisas y entendibles por los agentes de la organización. A continuación mostramos las políticas y un resumen breve de su referencia[66]

Políticas:

- Principal de Riesgos de TI: Define el nivel estratégico, táctico y operativo como se requiere gestionar y gobernar los riesgos de la empresa. -
- Seguridad de la Información: Pautas de trabajo de gestión y gobierno sobre el comportamiento de la protección de la información. -
- Gestión de Crisis: Establece las directrices de cómo actuar en un entorno de crisis.
- Gestión de Entrega de servicios de TI por terceros: Establece un marco de referencia de expectativas y comportamiento de las precauciones de seguridad tomadas por terceros proveedores de servicios de TI.
- Continuidad de Negocios: Gestiona el plan de contingencias de la empresa referida a los activos de TI.
- Gestión de Programas y Proyectos: Establece la gestión de riesgos de los programas y proyectos tomando a PMBOK como marco de referencia de los mismos.
- Recursos Humanos: Establece y gestiona el riesgo que está relacionado con una persona.
- Riesgo de Fraude: Establece orientación a todo el personal de la empresa de como resguardar los datos de las mismas, datos sensibles e importantes para la empresa, además de gestionar las denuncias o alertas cuando la importación no está segura.
- Cumplimiento: Explica el proceso de evaluación de cumplimiento de requisitos regulatorios, contractuales e internos.
- Ética: Define elementos esenciales de la interacción de las personas en una organización. -

- Gestión de Calidad: Detalla la visión de la organización sobre los objetivos de calidad de la empresa.
- Gestión de Servicio: Directivas definidas en ITIL¹³ para la optimización de servicios y gestión de riesgos de servicios de TI.
- Gestión de Cambios: Gestiona los proyectos de cambios de infraestructura o componentes de TI dentro de la organización, minimizando los riesgos que lleva todo cambio, analizando los activos que se verán afectados.
- Delegación de Autoridad: Establece los perfiles de los agentes de la organización, responsabilidad de cada uno, sobre los datos y la tecnología y su delegación cuando este no esté activo en la empresa, ejemplo vacaciones o licencias.
- Denuncias: Estimula a que los agentes de la organización puedan plantear libremente inquietudes y preguntas, resguardar de represalias al mismo, cuando se plantean problemas.
- Control Interno: Establece parámetros de control interno, métricas, y estándares para su control.
- Propiedad Intelectual: El propósito es asegurar los activos intangibles de la organización como software, métodos, datos etc. Y la propiedad de ellos.
- Privacidad de los Datos: Trata de establecer un contrato de privacidad en el cual se establecen pautas bien definidas sobre acceso, manipulación y resguardo de activos tangibles e intangibles de la empresa.

Procesos principales de la Gestión del Riesgo

COBIT for Risk define 37 procesos y justifica cada uno de ellos en el marco de su implementación se puede utilizar como una guía para gestionar eficazmente los riesgos empresariales. Pero hay dos procesos que son claves para la gestión de los riesgos, que son el EDM03 y el APO12 como muestra la figura 23.

¹³ La Biblioteca de Infraestructura de Tecnologías de Información es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

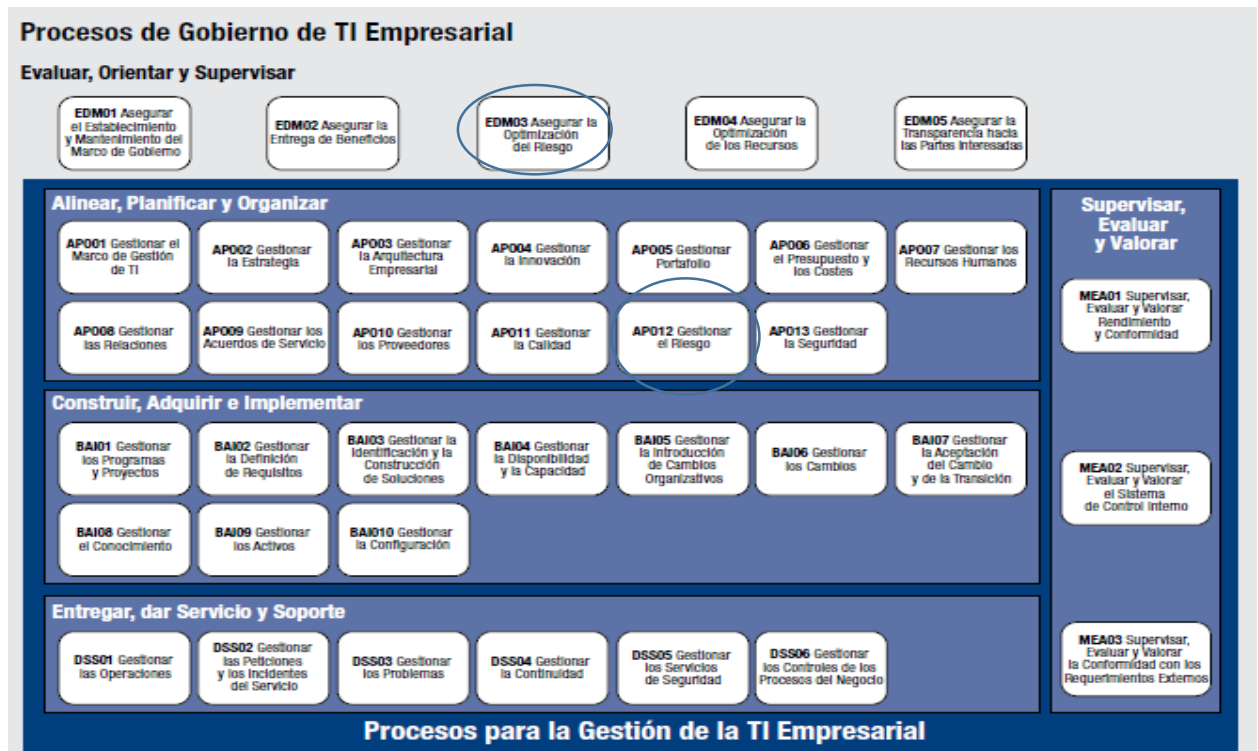


Figura 23 -Procesos [64]

ADM03 - Asegurar la optimización del riesgo: asegura que los riesgos relacionados con TI no excedan los umbrales de riesgo de la empresa. También aseguran que el potencial de falla sea mínimo en todas las etapas.

APO12- Gestionar Riesgo: trabaja para equilibrar los costos y beneficios de administrar los riesgos relacionados con TI de la empresa. También integran la gestión de riesgos con Enterprise Risk Management.

Estos procesos ayudan a desarrollar una estrategia de gestión de riesgos, a desarrollar un plan de comunicación de riesgos y a responder y mitigar los riesgos. También ayudan en el monitoreo de métricas y objetivos de riesgo.[67]

EDM03: "Asegúrese de que se entienda, articule y comunique el apetito y la tolerancia al riesgo de la empresa, y que se identifiquen y gestionen los riesgos para el valor de la empresa relacionados con el uso de TI".

Los procesos son:

- EDM03 -04 - Riesgos empresariales gestionados relacionados con TI
- EDM03 -06 - Transparencia de costos, beneficios y riesgos de TI

APO12: "Identifique, evalúe y reduzca continuamente los riesgos relacionados con TI dentro de los niveles de tolerancia establecidos por la administración ejecutiva de la empresa".

Los procesos cubiertos son:

- APO12-06 - Transparencia de costos, beneficios y riesgos de TI
- APO12-07 - Entrega de servicios de TI en línea con los requisitos comerciales
- APO12-09 - Agilidad informática
- APO12-10 - Seguridad de la información y la infraestructura de procesamiento y aplicaciones
- APO12-15 - Cumplimiento de TI con políticas internas

2.12.3 Riesgos en la Nube

En la perspectiva de la nube, los riesgos a considerar están cubiertos por DSS05 - Gestionar servicios de seguridad de procesos COBIT 5. Los riesgos de la nube pueden ser riesgos de cumplimiento, riesgos de análisis de incidentes, riesgos de manejo de datos, protección de datos, privacidad del usuario, pérdida o pérdida de datos, eliminación de datos insegura o incompleta durante la migración, interfaces inseguras, pérdida de claves de cifrado, seguridad de infraestructura, denegación distribuida de Servicio (DDoS), pérdida o compromiso de registros, etc. La mayoría de estos riesgos están cubiertos por los procesos de COBIT en su totalidad y algunos en parte específicamente por APO12, EDM03 y DSS05[68].

Las 3 líneas de Defensa contra el Riesgo

COBIT for Risk definen 3 líneas de defensa para analizar y gestionar los riesgos:

1. Línea de Defensa – Es la Defensa operativa, donde se gobiernan y gestionar los riesgos corporativos.
2. Línea de Defensa – Es la defensa que implica la función del riesgo y su cumplimiento. -
3. Línea de Defensa – Auditoría, donde ya el riesgo se ejecutó y los auditores tiene que verificar y validar las pistas de auditoría y buscar evidencias de los controles y acciones que no se realizaron o se realizaron erróneamente.

2.12.4 Estructura del Riesgo en COBIT for Risk

Por ultimo COBIT for Risk nos proporciona un marco simple para mejorar el entendimiento sobre el manejo de los riesgos, generando una estructura del escenario del riesgo, compuesta por 5 factores, como muestra la figura 24:

1. Actor: Se clasifican en:
 - a. Interno: Empleado o contratista
 - b. Externo que puede ser el competidor externo.
2. Tipo de Amenaza: pueden ser:
 - a. Malicioso: un riesgo provocado.
 - b. Accidental: un riesgo que no se puede controlar y se ejecuta por accidente.
 - c. Fracaso: riesgo generado por riesgos externos o errores.
 - d. Naturales: riesgos que de origen natural que no se pueden manejar.
3. Acción: acción que genera el riesgo ejecutado
 - a. Divulgación: Los datos se hacen públicos.
 - b. Interrupción: Se interrumpe el servicio.
 - c. Modificación: El software se modifica sin controles o versiones.
 - d. Robo: Pérdida de activo.
 - e. Destrucción: sustracción de activos.
 - f. Diseño Ineficaz: Error de diseño.

- g. Ejecución Ineficaz: Problemas con la ejecución
 - h. Regulación: El activo o resultante de su utilización es regulada por estándares.
 - i. Uso inadecuado: El activo se utiliza de una manera ineficaz.
4. Activos y Recursos:
- a. Personas y Organización
5. Procesos:
- a. Infraestructura: Instalaciones, infraestructura de TI.
 - b. Arquitectura de componentes de la organización: información, tecnología y aplicaciones.
6. Tiempo: Duración que tendrá el riesgo activo o problemas que este genere.
- a. Duración
 - b. Calendario de Incidencias
 - c. Momento de ejecución del riesgo.



Figura 24 -- Estructura del Riesgo – fuente [65]

Capítulo 3 - Problema encontrado y Solución sugerida

El análisis y gestión de riesgos es una práctica conocida dentro del ámbito de las ciencias informáticas, y por los profesionales graduados de altas casas de estudios, se utiliza en metodologías de desarrollo de software, auditoría y gestión de TI.

En este capítulo se define el problema encontrado dentro del ámbito tecnológico de las pymes y cuál es el estado actual de las organizaciones respecto al AGR; se analiza la informalidad en la práctica, acciones para gestionar riesgos, la escasa utilización de metodologías existentes, y las dificultades por lo cual no se utilizan; al final se propone una solución metodológica, adaptada a las necesidades de las pequeñas y medianas organizaciones de las región.

3.1 Problema Encontrado

El uso de la tecnología de la información ha crecido considerablemente en los últimos años y las organizaciones medianas y pequeñas denominadas pymes, cada vez dependen más de ella, de sus avances, actualizaciones, soporte, mantenimiento, el uso de la nube como plataforma de comunicación y resguardo de datos.

En la informática actual, la utilización de software como servicio en su acrónimo en inglés SaaS, permite que los sistemas de información de intercomuniquen entre sí automáticamente, y en su mayoría el resultado de estas conexiones pueden ser críticas aumentando el riesgo de TI[69] .

Para garantizar el éxito en el entorno de negocios actual; la habilidad que tenga la pyme para implantar las tecnologías modernas, que soporten de manera eficiente y controlada los procesos de negocios críticos, tiene un gran impacto en su grado de competitividad, ya que debe administrar los costos y recursos .

En respuesta a los cambios de mercado, las compañías han invertido en tecnología y en revisar las formas de administrar sus negocios, con la introducción de la robótica en los procesos, costear bienes y servicios se ha convertido en una tarea básica, pero ha cobrado mayor importancia la administración de los costos y la administración de la información como base para la toma de decisiones, permitiendo

a las empresas direccionar sus negocios en pos de un posicionamiento más ventajoso y competitivo basado en costos[70].

En las pymes la información de costos se vuelve cada vez más crucial, pues los precios de los servicios en TI tienden a ser fijados por el mercado.

La presión ejercida por la globalización desencadena guerras de precios que al final se convierten en guerras de costos, haciendo que las pymes exitosas sean aquellas que tienen la capacidad de mantener o reducir sus costos a una velocidad mayor que la de sus competidores; si bien actualmente en la Argentina servicios como conectividad a Internet están reguladas por el DNU 690/2020¹⁴, se considera a estas conexiones como servicio esencial y su costo está regulado por el estado Argentino, al momento de la escritura de este trabajo final de maestría no se ha convertido en ley.

Por otro lado el costo de los servicios de TI cuyas empresas son extranjeras, se ha incrementado exponencialmente, debido a los gravámenes e impuestos a la moneda extranjera, la cual es el método de pago de la mayorías de las empresas que brindan SaaS, por lo que podemos decir que dentro de los componentes del costo de hacer negocios o de producir bienes y servicios, los costos indirectos han llegado a representar una gran parte del costo de estas inversiones tecnológicas.

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.

Si bien en TI siempre existen riesgos, investigando para este trabajo de tesis de maestría, se observó un incremento en la complejidad de las arquitecturas tecnológicas y en los procesos para su implantación y administración; arribándose a la conclusión de que existen nuevos riesgos que deben ser mitigados de forma efectiva y eficiente para mantener el cumplimiento de los objetivos de control. Dichos riesgos se

¹⁴ Establece que Se establece que los Servicios de las Tecnologías de la Información y las Comunicaciones (TIC) y el acceso a las redes de telecomunicaciones para y entre licenciatarios y licenciatarias de servicios TIC son servicios públicos esenciales y estratégicos en competencia.

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 en general.

3.2 Análisis y Gestión de riesgos en las organizaciones

En el año 2001 en su investigación Peter Kulik y Catherine Weber[71] , realizaron 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, 28% en forma periódica y solo el 14% utilizaban un enfoque formal de AGR[71]. 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 Jyrki Kontio en su tesis doctoral[72], cree 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.

Las amenazas de mayor riesgo son las amenazas internas, para superar estos riesgos, se debería considerar varios métodos de evaluación de riesgos para calcular el impacto de las amenazas internas y analizar las brechas actuales en el método de evaluación de riesgos.

3.3 Estado de AGR en las organizaciones

Para este trabajo de Trabajo Final de Maestría se realizó una encuesta sobre el estado de situación del análisis y gestión de riesgos y se invitó a participar de la misma a los directores de TI de las organizaciones y empresas del ramo local de la provincia de Misiones y del ramo nacional a empresas de origen y base en todo el país Argentina y otros países de América Latina, en su totalidad fueron pymes y organizaciones (figura 25) estatales como muestra el siguiente cuadro.

Tipo Organización	Cantidad
Pyme	18
Organización Estatal	16

Tabla 1 - Tipo de Organizaciones relevadas en la Encuesta

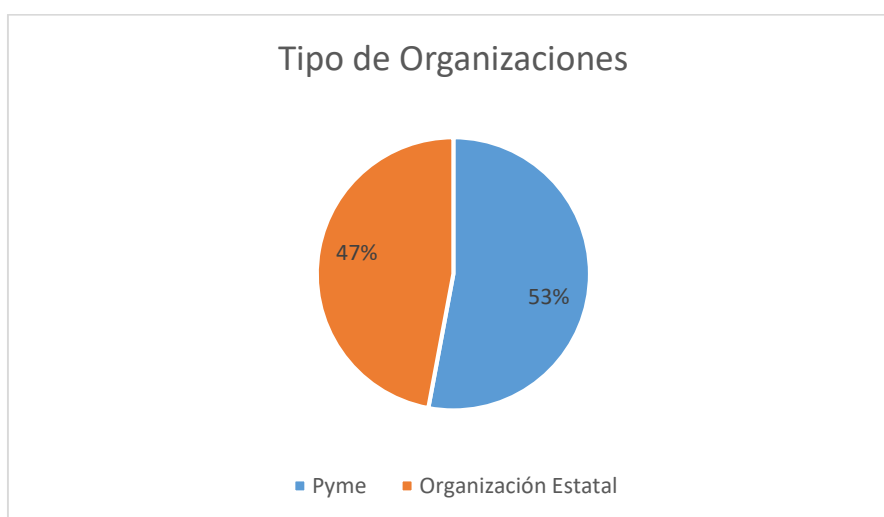


Figura 25 -Tipo de Organizaciones relevados en la encuesta

País	Provincia	Cantidad
Argentina	Misiones	28
Argentina	CABA	3
Argentina	Córdoba	2
Argentina	Salta	2
Argentina	Corrientes	2
Argentina	Santa Fe	1
Argentina	La Rioja	1
Argentina	San Juan	1
Argentina	Neuquén	1
Otros Países	-	1

Tabla 2 – Distribución de las Provincias participantes de la encuesta

La figura 26 muestra la distribución de las respuestas de la encuesta por provincias en el país.

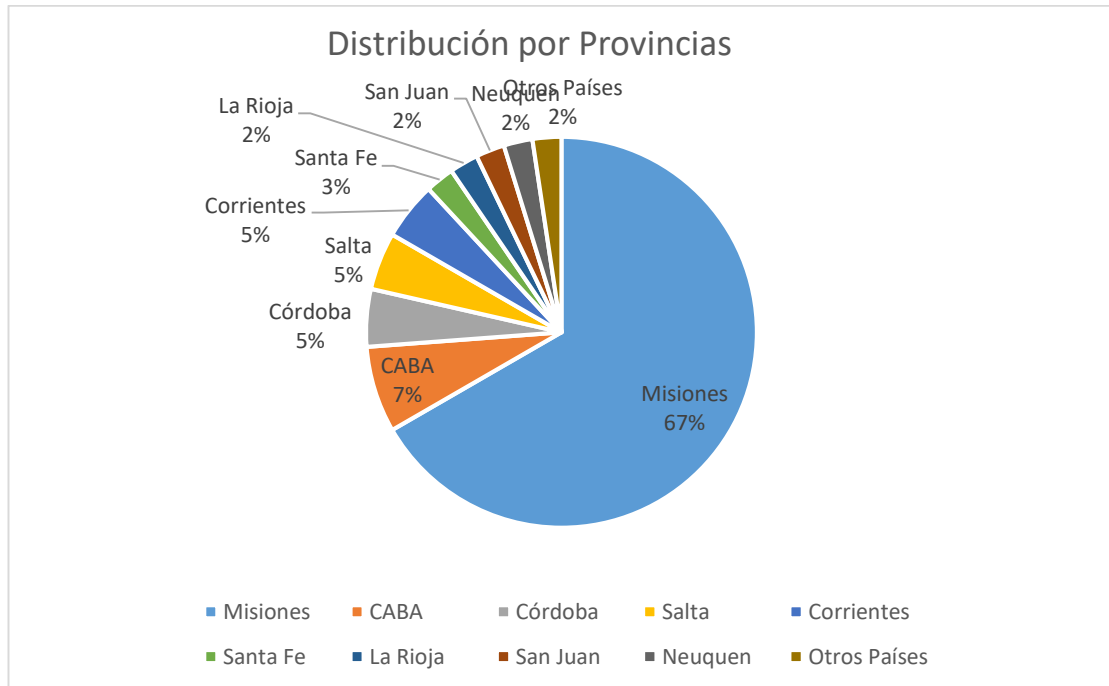


Figura 26 -Distribución de las Provincias en la Encuesta

El objetivo principal de la encuesta fue identificar el porcentaje de organizaciones que utilizan AGR, y dentro de los que lo utilizan, la formalidad de los mismos, en que rama de la TI lo utilizan, como ser desarrollos de software, gestión de proyectos, equipamientos y tecnología entre otros, y por último, el nivel del éxito que obtuvieron en utilizar AGR; por otro lado también, se relevó las organizaciones que no utilizan metodología o método de análisis y gestión de riesgos y los motivos por el cual no lo utilizan.

De un total de 53 datos procesados, el 77% No utiliza análisis y gestión de riesgos en TI (figura27). Y un 6 % no contestó esta pregunta.

En la organización/empresa que Ud trabaja, utilizan análisis y gestión de riesgos en TI ?

Opción	Cuenta
Sí (Y)	9
No (N)	41
Sin respuesta	3

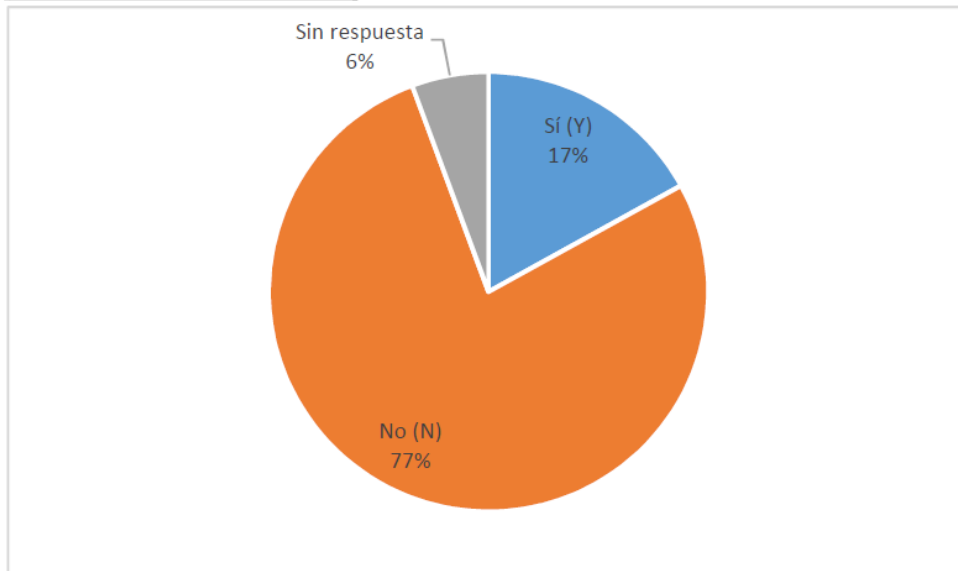


Figura 27 -Organizaciones que utilizan AGR

Del 17% que utiliza algún método de AGR, el 55% emplea métodos mixtos, tomando prácticas de alguna metodología específica, mientras que el 45% se dividen entre método totalmente formales e informales (figura 28).

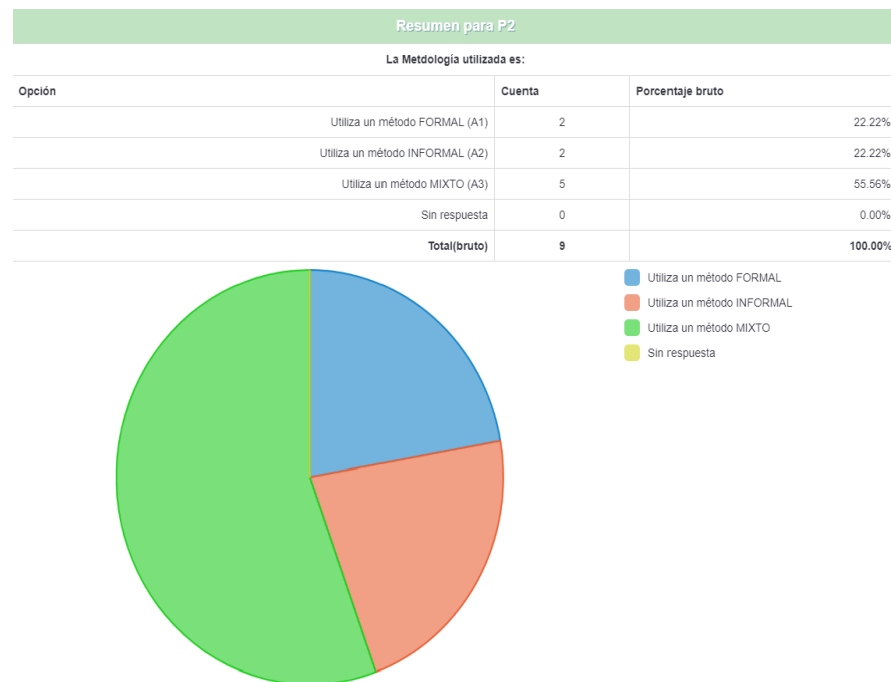


Figura 28 - Tipo de Metodología Utilizada

Para obtener conocimiento específico sobre los métodos estudiados en el transcurso de este trabajo, se consultó a los que utilizaban métodos formales, si aplicaban algunos de los descriptos en el estado del arte, como información, se obtuvo que el 60% utiliza PMBOK, en gestión de proyectos, mientras que otro 20% utiliza SEI y 20% otros métodos, como muestra la figura 29.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

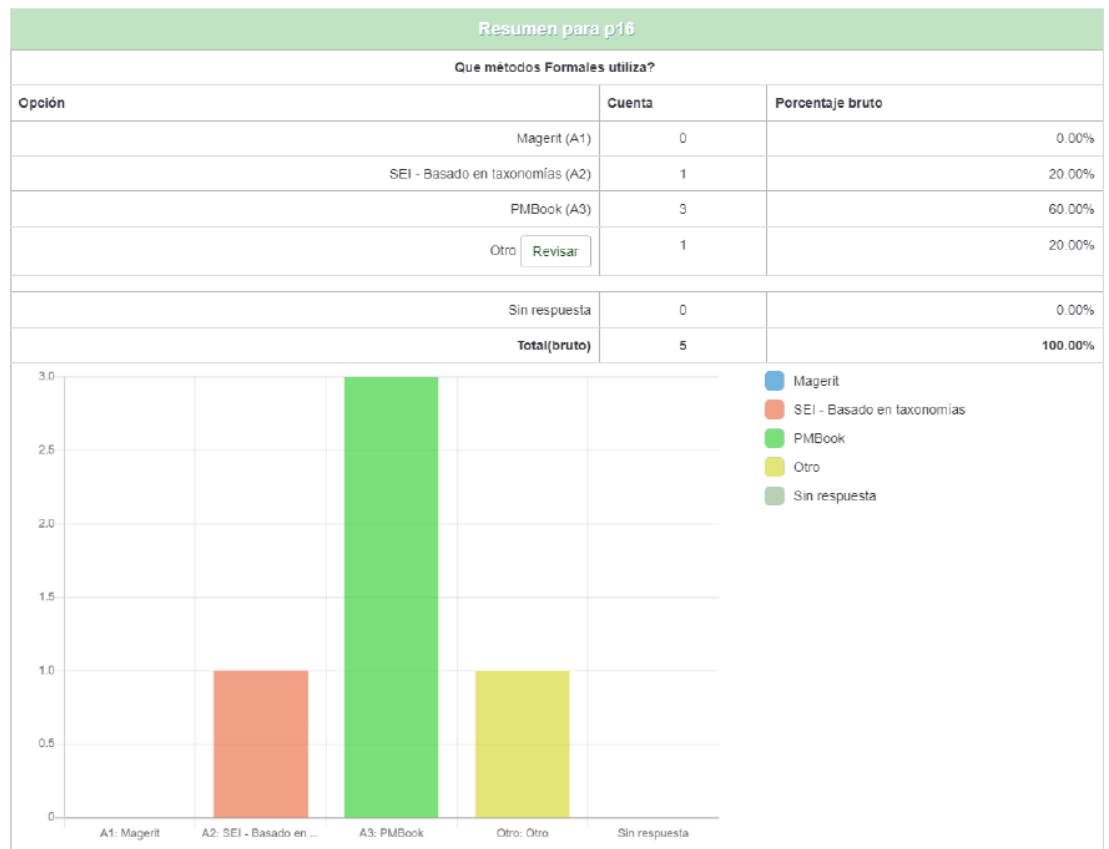


Figura 29 -Tipos de Metodologías de AGR utilizadas

Dentro del entorno de TI la rama que mayor uso de AGR es la de equipamientos, seguido de los datos, proyectos, comunicaciones y por último el desarrollo de software, se muestra en la figura 30.

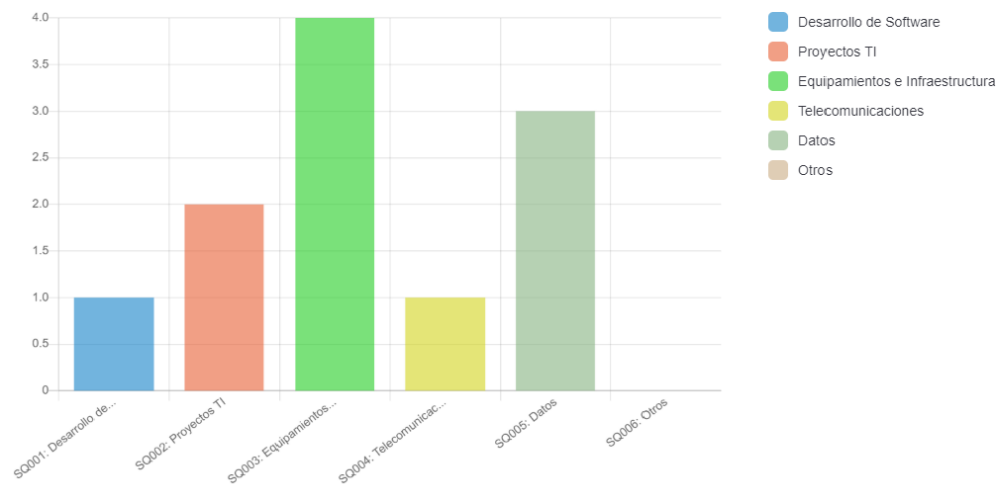


Figura 30 -Ramas de la TI utilizadas en AGR

Debido a que la investigación se basa en generar un método para ser utilizado por las pymes más pequeñas, se hizo foco en aquellos que no utilizan AGR en sus organizaciones y se indagó por qué no lo utilizan. Ante la consulta “Por que no utilizan Análisis y Gestión de Riesgos en TI? “ la respuesta fue que 45% por desinterés institucional, 27% por falta de recursos, humanos, económicos y otros; y un 28% por desconocimiento de una metodología formal para realizar AGR. (figura 31).

Cual cree que es la causa por la cual No realiza Análisis y Gestión de Riesgos en TI?

Opción	Cuenta
Falta de Recursos (Presupuesto/RRHH/Tiempo) (A1)	13
Desconocimiento de Metodologías (A2)	13
Falta de Interés Organizacional (A3)	21

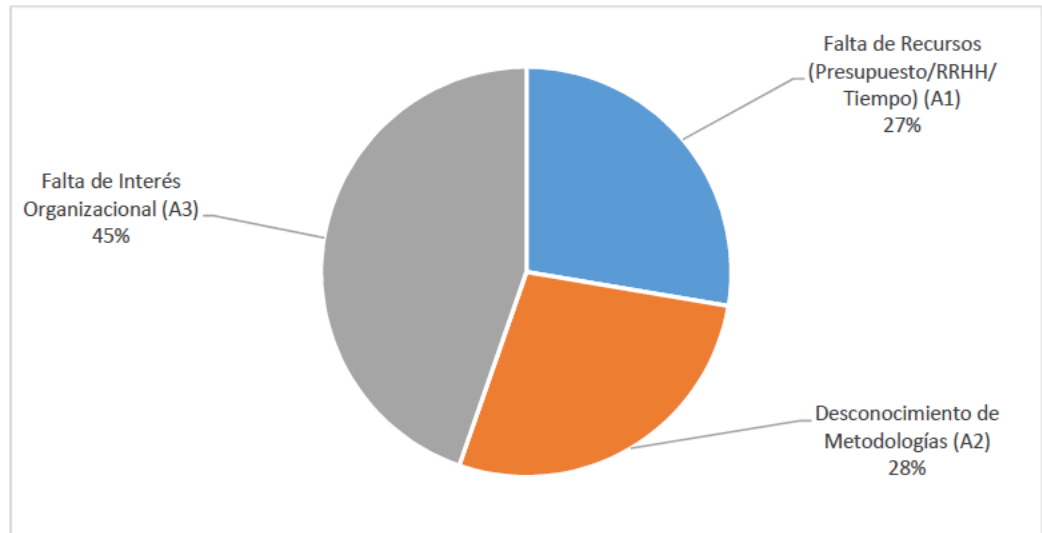


Figura 31 -Motivo por el cual No se utiliza AGR en las Organizaciones

3.4 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 UPS¹⁵ etc.

La mayoría de las personas y las organizaciones toman como práctica resguardar estos activos, que inconscientemente 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:

¹⁵ Servicio de energía ininterrumpida

- ¿Tenemos varias copias, cuál es la última?
- El dispositivo 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 cambió 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 expresa el plan de acción, que es, el método que abarca el seguimiento y control del riesgo, o el plan de contingencia, para poder generar acciones controladas cuando el riesgo se transforme en un problema.

3.5 Metodologías poco adaptativas

Normas como ISO / IEC 27001 y 27002 no definen pasos detallados de evaluación de riesgos, por lo que si queremos utilizar dichas normas tenemos que definir nuestro propio método de evaluación de seguridad o podemos utilizar métodos que se han desarrollado por otras organizaciones.

No hay prueba formal de que siguiendo esos cuatro pasos, identificación de amenazas, identificación de vulnerabilidades, determinación del riesgo y recomendación y control, que proponen Syalim Amril, Hori Yoshiaki y Sakurai Kouichi en su artículo “Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide”[73]; se logre obtener una lista de todos los riesgos de seguridad que amenazan a un sistema y obtener todas las medidas de control apropiadas.

En realidad, se pueden utilizar métodos formales para probar adecuadamente los resultados de la evaluación de riesgos, sin embargo, el uso de métodos formales para la evaluación de riesgos es complejo, requiere mucho tiempo y requiere una gran experiencia en programación formal. Además, los métodos formales no muestran un avance convincente para comprobar la seguridad de un sistema complejo, porque hay demasiados objetos y aspectos que deben analizarse[73].

Para la gestión de riesgos además existen otros estándares como el ISO 3100:2009 que establece un conjunto de principios para la gestión de los riesgos, establece recomendaciones de desarrollo e implementación de mejoras continuas en el proceso de gobierno, políticas, valores y cultura de la organización, promueve la integración de estrategias, planificación, gestión y elaboración de informes, que pueden ser utilizadas por organizaciones públicas o privadas, las misma, como todo estándar, agrupa buenas prácticas, pero al no ser una metodología, no contiene método y pasos a seguir para tal efecto.

Existen metodologías como Octave, Mehari, NIST SP 800:30, Coras, Cramm y Ebios entre otras, por lo general son aplicadas en el ámbito de la seguridad informática, que permiten contextualizar y concientizar a las organizaciones en la necesidad mecanismos de seguridad de acuerdo con los riesgos y amenazas identificados.

Las metodologías mencionadas y las estudiadas en profundidad en este trabajo de maestría, buscan integrar los procesos de análisis de riesgos en las normas y estándares existentes, se considera que no se adaptan al objeto de estudio de este trabajo, que son las pymes pequeñas y medias; si bien cada una está orientada a un ámbito específico, poseen sus propias características y herramientas, pero en su mayoría precisan un ámbito de conocimiento experto en el manejo y gestión de riesgos y se basan, en su mayoría en la seguridad de la información.[74]

De las metodologías estudiadas en el capítulo 2 las desventajas son:

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.

Taxonomía TBQ: como se demostró en el capítulo 2, el método SEI – CRM posee una taxonomía específica que se deberá cumplir, la misma que consiste en 194 preguntas muy abstractas clasificadas en tres grandes clases, las que a su vez se subdividen en subclases, por lo que se denota su extensión y dificultad, para ser

realizado en organizaciones con poco personal o persona sin mucho conocimiento de la gestión de riesgos, la figura 32, muestra el modelo de cuestionario TBQ.

Development Taxonomy

- | A. Product Engineering | B. Development Environment | C. Program Constraints |
|--|---|---|
| 1. Requirements <ul style="list-style-type: none">a. Stabilityb. Completenessc. Clarityd. Validitye. Feasibilityf. Precedentg. Scale | 1. Development Process <ul style="list-style-type: none">a. Formalityb. Suitabilityc. Process Controld. Familiaritye. Product Control | 1. Resources <ul style="list-style-type: none">a. Scheduleb. Staffc. Budgetd. Facilities |
| 2. Design <ul style="list-style-type: none">a. Functionalityb. Difficultyc. Interfacesd. Performancee. Testabilityf. Hardware Constraintsg. Non-Developmental Software | 2. Development System <ul style="list-style-type: none">a. Capacityb. Suitabilityc. Usabilityd. Familiaritye. Reliabilityf. System Supportg. Deliverability | 2. Contract <ul style="list-style-type: none">a. Type of Contractb. Restrictionsc. Dependencies |
| 3. Code and Unit Test <ul style="list-style-type: none">a. Feasibilityb. Testingc. Coding/Implementation | 3. Management Process <ul style="list-style-type: none">a. Planningb. Project Organizationc. Management Experienced. Program Interfaces | 3. Program Interfaces <ul style="list-style-type: none">a. Customerb. Associate Contractorsc. Subcontractorsd. Prime Contractore. Corporate Managementf. Vendorsg. Politics |
| 4. Integration and Test <ul style="list-style-type: none">a. Environmentb. Productc. System | 4. Management Methods <ul style="list-style-type: none">a. Monitoringb. Personnel Managementc. Quality Assuranced. Configuration Management | |
| 5. Engineering Specialties <ul style="list-style-type: none">a. Maintainabilityb. Reliabilityc. Safetyd. Securitye. Human Factorsf. Specifications | 5. Work Environment <ul style="list-style-type: none">a. Quality Attitudeb. Cooperationc. Communicationd. Morale | |

© 2005 by Carnegie Mellon University

Figura 32 - Cuestionario TBQ [75]

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 están orientados a las grandes corporaciones.

Amplio conocimiento de Riesgos: Utilizando esta metodología, el equipo encargado de cumplir con el AGR debe poseer gran experiencia sobre el tratamiento de riesgos e ingeniería del software, debido a la complejidad y amplitud del cuestionario.

Enfoque basado en la creación y mantenimiento de software: La metodología está orientada hacia el análisis de riesgos en desarrollos y mantenimiento de software y como complemento la tecnología informática añadida a ese proyecto. Si bien, se puede utilizar antes cualquier proyecto de riesgos, si abstracción dificulta su implementación.

Desventaja MageritV3

Una de las principales características de esta metodología es que está orientada a una extensa variedad de organización y exclusivamente direccionada a las organizaciones gubernamentales de la república de España, por ser una metodología que sugiere seguir todos los procesos para obtener un resultado exitoso: como hemos definido en el capítulo 2 la principal desventaja de Magerit V3 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, aplicar de esta metodología sea realmente costoso.

Herramientas con alto costo económico: Como se presentó al final del capítulo 2, el software existente para gestionar esta metodología es costosa de 500 Euros en su versión Basic, y aquellas versiones que se pueden conseguir gratuitamente, son solo formatos de visión de ejemplos.

3.6 Dificultades de gestionar los riesgos 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:

- *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, significa una erogación

económica, 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, sin tomar en cuenta todos los componentes comunes como el outsourcing de múltiples software actuales, como plugins de las páginas webs, dominios externos y otros, en donde se aprecian la falta de conocimientos de las metodologías de AGR.
- *Falta de Compromiso:* Es usual por parte de los directivos de las organizaciones en base al AGR, en la mayoría de los casos, al iniciar un proyecto están de acuerdo en 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, el compromiso asumido se diluye.
- *Falta de Recursos Humanos:* Debido a la tecnificación y automatización de las empresas, el recurso humano que trabaja en TI, está sobre pasado de tareas, por el cual, el ARG no es prioritario.

3.7 Solución Sugerida

Luego de haber realizado el estudio de las metodologías SEI –CRM, Magerit V3, OCTAVE-S, se denota que las dos primeras son conocidas por el ámbito profesional y en el contexto del ambiente informático de las pequeñas y medianas empresas en las encuestas analizadas, mientras que OCTAVE-S, está basado en ámbitos de pequeñas organizaciones de no más de 100 personas, e implementa procedimientos sencillos y específicos apoyándose en procesos como la gestión de los activos vulnerables.

Investigado en detalle las 3 metodologías antes mencionadas y posteriormente al analizar las encuestas realizadas, se manifiesta la falta de éxito en la práctica formal y metodológica del AGR.

Se concluye en generar un método adaptado, denominado “RIC - Un nuevo modelo integrando la metodología SEI y Magerit3”, este método propio toma los simples pasos de la metodología SEI – CRM, y aplica la base de conocimiento de las amenazas y salvaguardas de la metodología Magerit V3, incorporando como innovación, procedimientos de control de tareas de los planes de acción, gestión de incidentes y la implementación de conceptos de la gestión de conocimiento, con el objetivo de agregar valor al AGR aumentando su conocimiento colectivo dentro de la organización.

A modo de aclaración expreso que, si bien en el título del TFM no lo expresa, se incorporó además una fase de la metodología OCTAVE-S, por considerarla importante para el análisis de riesgos en un proyecto TIC.

De la metodología SEI se utilizarán las nueve etapas propuestas, de OCTAVE-S la etapa de identificar vulnerabilidades de estructura y de la metodología Magerit V3 las técnicas de clasificación y elementos.

El método posee tres etapas externas, el seguimiento de los planes de acción, que es un proceso orientado al control del auditor interno, la gestión de incidencias, y la gestión de conocimiento, que no existe dentro de ninguna de las metodologías antes mencionadas. Ello generará un alto valor agregado al método desarrollado, incorporando técnicas de gestión del conocimiento a la organización, ya que podrán conocer de forma detallada los riesgos a los que se exponen, y los planes de acción y contingencias.

Junto a la metodología RIC, se desarrollará un software herramienta denominado “SCRisk”, cuyo objetivo es impulsar la utilización de análisis y gestión de riesgos en las Tics incorporadas a las pymes, dando un marco formal, a muchas prácticas de riesgos que se llevan hoy día, de una manera informal.

Capítulo 4 - El Método RIC

4.1 Características

El Método RIC fue desarrollado con el objetivo de brindar un formalismo a muchas prácticas realizadas en las pymes que carecen de una organización formal, se busca crear un método simple, intuitivo y que agiliza el reconocimiento de los riesgos, incorporando elementos ya definidos y clasificados por otros métodos y trabajos de investigación, como el presentado por este mismo autor, en su trabajo de tesis de grado[76].

El método RIC tiene por objetivo ayudar a la organización de las empresas pymes a generar su propia gestión de riesgo, incrementando el valor del conocimiento de la implementación y resultante de los procesos del método, además de aplicar un diseño que se base en estándares, para mejorar y facilitar la auditoría del mismo, así también posee etapas exclusivas para la gestión de incidencias y conocimiento, siempre orientadas a las pequeñas y medianas organizaciones.

La metodología se distribuye en tres capítulos R, I y C cada uno de ellos, poseen Etapas y las etapas poseen procesos:

- **Capítulo R – Análisis, Gestión y Seguimiento del Riesgo**
 - Etapas de Análisis: Se implementa 9 procesos o actividades secuenciales, en los procesos como inventario de activos, propósitos y objetivos e identificar vulnerabilidad se incluyeron subprocesos o tareas. En esta etapa, se evalúan los riesgos de un activo y sus características específicas, la relación entre ellos, la taxonomía y analiza los posibles riesgos, además incorpora las mejoras prácticas de las metodologías Magerit v3 y CRM – SEI, y OCTAVE-S, generando una integración propia de este método, mediante formularios sugeridos y simples de administrar.
 - Etapas Gestión: Se realiza la actividad de gestión del riesgo, especificando la importancia del riesgo, la información requerida para

su seguimiento, el responsable de las tareas de control y los recursos necesarios para llevar dichos controles. Se especifican además el plan de acción y el plan de contingencia

- Etapa Seguimiento y Control: Esta etapa es creada por el maestrando y un plan de seguimiento de 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.

- **Capítulo I – Gestión de Incidencias**

- Etapa de Incidencias: Cuando ocurre un problema hay que buscar una solución rápida y práctica, para reducirlo o controlarlo. La característica de esta etapa es el control y gestión de las incidencias ocurridas, creada exclusivamente para este método. Dicha gestión posee la particularidad de registrar los activos afectados, estén o no en el AGR, 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. Y como valor a la gestión de incidentes, se puede divisar los activos que tuvieron incidentes y no fueron gestionados por los riesgos, se detallan las tareas para la resolución de problemas que puede ser útil para alimentar con información real de los riesgos en la etapa de análisis de riesgo.

- **Capítulo C – Gestión del Conocimiento**

- Etapa Conocimiento Explícito: El conocimiento se incrementa utilizando métodos específicos de la comunicación, con datos cuantitativos y parametrizables
- Etapa Conocimiento Tácito: Incorpora conocimiento cualitativo, en lenguaje natural, para obtener conocimiento desestructurado.

En la figura 33 se muestra el método RIC, donde muestras sus 3 capítulos, etapas y procedimientos.

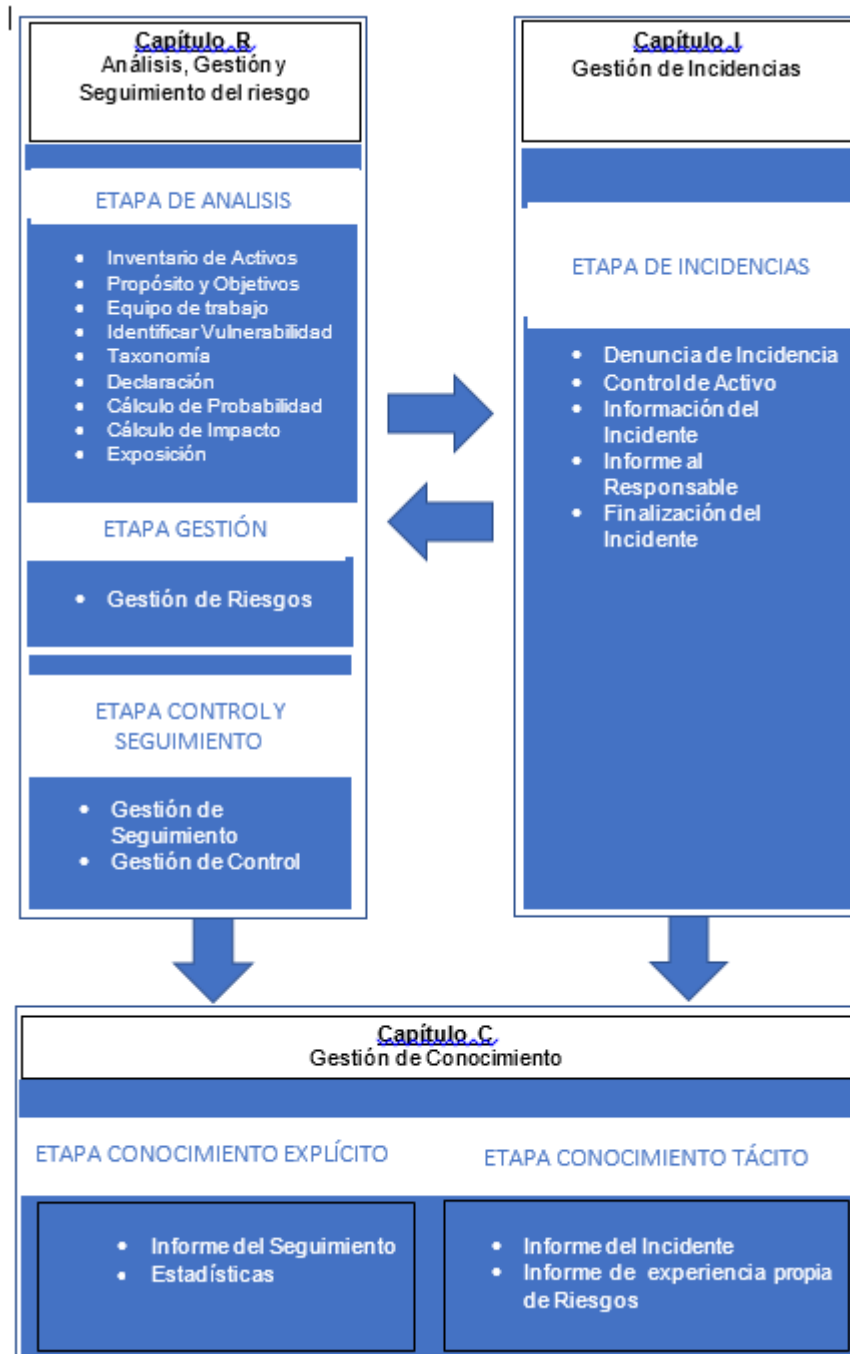


Figura 33 - Método RIC

En la descripción de tallada del método, se incorporan formularios de carácter orientativo para la empresa, entrada de datos de estos formularios, responsables y

salida de los mismos, para la aplicación del método, dichos formularios pueden ser modificados, ampliados o ajustados a las necesidades de las organizaciones.

4.2 Capítulo R – Análisis, Gestión de Riesgos y seguimiento del Riesgo

4.2.1 Etapa Análisis

La etapa de análisis del riesgo, se combinan las metodologías SEI-CRM, Magerit y OCTIVE-S.

Está compuesta por 9 (nueve) procesos y alguno de ellos poseen subprocesos, a continuación, en la figura 34, se representa su estructura:

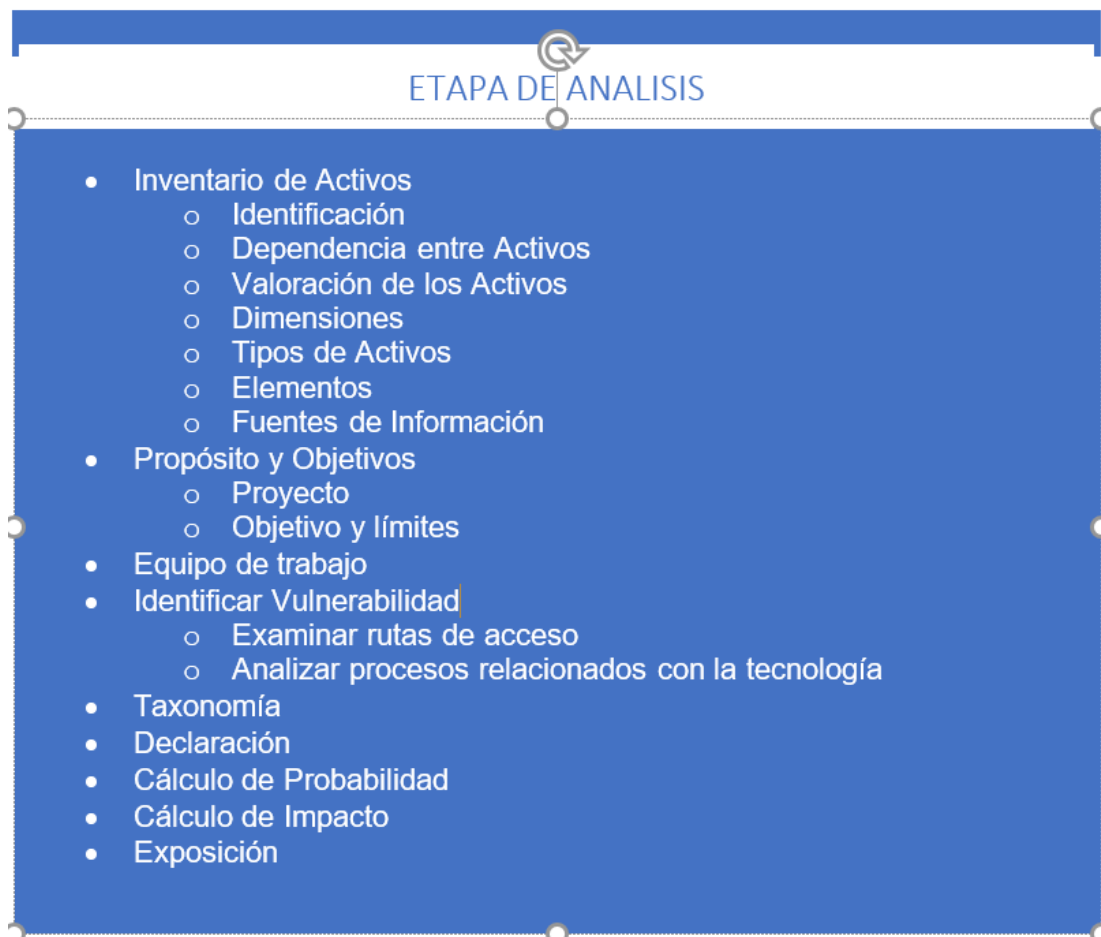


Figura 34 - Etapa de Análisis

Inventario de activos

El inventario de activos, se realiza llevando un relevamiento de todos los activos TIC de la empresa, activos tangibles e intangibles, como el recurso humano que realiza sus actividades con desarrollando o gestionado las Tics. Se detallan además

las características específicas que posee un activo, como ser su tipo, valoración, dimensión, elementos, fuentes de información y su criticidad para la organización.

Identificación de Activos

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

- Servicios: se proporcionan a partir de los datos, y son necesarios 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 el demás activo nombrado.

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.

Formulario de relevamiento de Activos

Entradas: Como entrada de datos del formulario se incluirán:

- Código del Activo: Dato Único y definido por el usuario
- Descripción: Descripción del Activo, nombre por el cual se lo reconoce en la organización
- Contenido: Parte o partes del activo.

- Propietario: Persona responsable del activo.
- Crítico: Para saber si un activo es crítico, se deberá responder a la siguiente pregunta: El activo tendría un efecto adverso en la organización si:
 - ¿Es divulgado a personas no autorizadas?
 - ¿Es modificado sin autorización?
 - ¿Se pierde o es destruido?
 - ¿El acceso al activo es interrumpido?

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, como ser contratos, hardware, software, personal etc.

Código Activo	Descripción	Contenido	Propietario	Crítico
A01	[nombre del activo]	[Descripción del activo]	[identificar]	[S/N]
[...]	[...]	[...]	[...]	[...]

Tabla 3 - Formulario Relevamiento de Activos

Salida: Como salida se obtiene un formulario con el listado de los activos de la organización y el campo de criticidad, será utilizado en el formulario de identificación de vulnerabilidades de infraestructura.

Dependencias entre Activos

En un sistema de información los activos son dependientes y dependen de otros activos o servicios. No se aprecia un activo tecnológico, que no posea vinculación dependiente de otro.

Se define a activos superiores a los datos y servicios, pero estos son dependientes de los denominados activos inferiores, que se describen como equipos, comunicaciones o personas.

Formulario propuesto por el maestrando de Dependencias entre Activos

Entradas: Como entrada de datos de este formulario, se utilizará el formulario de relevamientos de activos y se incluirán:

- Código del Activo: Dato Único y definido por el usuario
- Código Activo Dependiente: código del activo el cual depende.

Los datos se toman de la columna Código de Activo de la tabla Relevamiento de Activos.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, y preferentemente haber realizado el formulario de relevamiento de activos.

Código Activo	Código Activo Dependiente
A01	[A0D]
[...]	[...]

Tabla 4 - Formulario Dependencia de Activos

Salida: Como salida se obtiene un formulario que evidencia la dependencia entre los activos, en el lado izquierdo aparecen los activos dependidos y los que se ubican en la parte derecha son los dependientes.

Valoración de los activos

Un activo es más importante por su valor, que por su costo económico. Si un activo está en desuso o no vale nada es prescindible y hay que dar de baja en el inventario, si no se puede prescindir de él es porque algo vale y esto es lo que hay que investigar (su valor) y protegerlo.

Se propone una tabla con datos de valoración, la cual, se podría ajustar a las necesidades de la organización

Tabla de Importancia

Valor	Tipo
0	Prescindible
1	Bajo
2	Medio
3	Alto
4	Muy Alto

Tabla 5 - Importancia del Activo

Formulario propuesto de Valoración del Activo

Entradas: Como entrada de datos de este formulario, se utilizará el formulario de relevamientos de activos y se incluirán:

- Código del Activo: Dato Único y definido por el usuario
- Valor o Importancia: Valor o importancia que la organización le asigna al activo, el mismo es obtenido de la tabla de Importancia.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, y preferentemente haber realizado el formulario de relevamiento de activos.

Código Activo	Valor o Importancia
A01	[0...4]
[...]	[...]

Tabla 6 -Valoración del Activo

Salida: Como salida se obtiene un formulario que muestra por cada activo relevado la importancia o valor que posee para la organización.

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 [A]: 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 [C]: Que problemas originaría el conocimiento de los datos por parte de quien no debe? Valoración típica de los datos.
- Integridad [I]: Si el activo está dañado o corrupto ¿qué problemas ocasionaría? Valoración de datos y de soporte informático (Discos).
- Disponibilidad [D]: Que problemas traería aparejado “no” poder contar o “no” poder utilizar un activo. Valorización típica de servicio (telecomunicaciones etc.)
- Trazabilidad de acceso a los datos [TAD]. ¿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. -

Formulario propuesto de Dimensiones del Activo

Entradas: Como entrada de datos de este formulario, se utilizará el formulario de relevamientos de activos y se incluirán los datos de las dimensiones:

- Código del Activo: Dato Único y definido por el usuario
- Dimensiones: Se ingresan las siglas de las dimensiones, por cada código de activo se ingresan el conjunto de dimensiones que este posee.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, y preferentemente haber realizado el formulario de relevamiento de activos.

Código Activo	Dimensiones
A01	[A, C, I, D, TUS, TAD]
[...]	[...]

Tabla 7 -Dimensiones del Activo

Salida: Como salida se obtiene un formulario que muestra por cada activo relevado las dimensiones que este posee, su importancia radica en su utilización para la automatización de las acciones necesarias para realizar el control de los riesgos.

Tipos de Activos

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.

Un Activo puede ser de muchos tipos de activo (TA), para este método definir correctamente los tipos de activo, por activo es de carácter preponderante e importante.

Tabla de tipo de activos Sugeridos

IDTA	Tipo de activo
SR	Servicios
DI	Datos / Información
AP	Aplicaciones
EI	Equipos Informáticos
RC	Redes de Comunicación
SI	Soporte Informático
EA	Equipamiento Auxiliar
IN	Instalaciones
PR	Personal

Tabla 8 - Tipos de Activos

Formulario Tipos de Activos

Entradas: Como entrada de datos de este formulario, se utilizará el formulario de relevamientos de activos y se incluirán:

- Código del Activo: Dato Único y definido por el usuario.
- Tipo de Activo: Identificar con siglas los tipos de activos al cual pertenece el activo, se debe generar un IDTA por cada reglón.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, y preferentemente haber realizado el formulario de relevamiento de activos.

Código Activo	Tipo de activo (IDTA)
A01	[SR,DI,AP, EI, RC, SI,EA,IN,PR]
[...]	[...]

Tabla 9 - Formulario de Tipo de Activos

Salida: Como salida se obtiene un formulario que muestra por cada activo relevado y de qué tipo de activo es, cada activo puede ser de muchos tipos de activos, por lo cual el código de Activo, puede repetirse tantas veces como tipos de activo conlleve.

Elementos

Una vez identificados los activos, dependencias, valoración y dimensiones, se debe asignar el elemento en el que el activo es importante. La tabla de elementos propuestas por Magerit se expone en el anexo II, las mismas pueden ser ajustadas a la organización.

Formulario propuesto de Elementos del Activo

Entradas: Como entrada de datos de este formulario, se utilizará el formulario de relevamientos de activos y se incluirán:

- Código del Activo: Dato Único y definido por el usuario.

- **Elementos:** Se definen los elementos de los activos incluyendo por cada activo el conjunto de elementos el cual posee. La definición de los elementos propuesto por Magerit V3 se encuentran en la tabla de Anexo I.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, y preferentemente haber realizado el formulario de relevamiento de activos, y basto conocimiento de equipamientos, software, se recomienda la asistencia de un experto de cada activo, debido a que el análisis de elementos, con lleva a un conocimiento profundo del activo.

Código Activo	Elementos
A01	Código Elemento1,.....,CódigoElementoX
[...]	[...]

Tabla 10 - Formulario de Elementos de los Activos

Salida: Como salida se obtiene un formulario que muestra por cada activo relevado y el conjunto de elementos a los cuales ayuda a evaluar, debido a la cantidad de elementos que posea, la valoración que posee cada uno, un activo que posee muchos elementos, debería tener una valoración mayor a un activo con pocos elementos, pero no es directamente proporcional, ya que la cantidad de elementos no refiere a su importancia.

Fuentes de información

Si el riesgo se transforma en un problema, se debe acudir e informar al área o personas de las cuales obtuvimos la información del activo. Dado que en teoría son los que más saben de su funcionamiento, para ello se debe asignar al activo los que utilizan y se responsabilizan de este en forma directa, denominados las fuentes de información.

Formulario propuesto de Fuentes de Información del Activo

Entradas: Como entrada de datos de este formulario, se utilizará el formulario de relevamientos de activos y se incluirán:

entrada de datos del formulario se incluirán:

- Código del Activo: Dato Único y definido por el usuario utilizando el formulario de activos.
- Fuente de Información: Se identifica el área, departamento, gerencia o dependencia en la cual se la encargada de custodiar o tener a cargo el activo.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, conocimiento de gestión de activos y gestión de la organización e información.

Código Activo	Fuente de Información (Área, Departamento, Gerencia)
A01	[Gerencia de Sistemas Gerencia General]
[...]	[...]

Tabla 11 - Formulario de Fuentes de Información

Salida: Como salida se obtiene un formulario, que muestra por cada activo relevado y la fuente de información en la cual se utilizará en la medida que sea necesaria, si el activo es alcanzado por un riesgo, se debe identificar el lugar donde se pueden obtener información exacta sobre el activo.

Observación:

La dimensión es un factor cuantitativo, obligatoriamente requerido por este método, los demás factores como: Dependencia entre activos, Valoración de los activos, Elementos y Fuentes de información son importantes, pero no obligatorios.

Propósitos y Objetivos del análisis de riesgos

Por cada proyecto se incorpora claramente los propósitos, objetivos y límites que tendrá el proyecto de análisis de riesgos. Además, se asignan los activos evaluados en la etapa anterior. Se realizan 3 Formularios correspondientes al proyecto, el cual puede poseer muchos objetivos y límites y además cada proyecto posee uno o muchos activos.

Proyecto

Se define las características básicas del proyecto, fecha de inicio y si posee fin, y se define un responsable del proyecto

Formulario de Proyecto

Formulario dinámico donde se explyea los proyectos con sus fechas de inicio y estado, el cual, este último es dinámico.

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Proyecto: Dato Único y definido por el usuario.
- Nombre: Se define un nombre para el proyecto, el cual, se sugiere sea identificadorio para el personal, ej. Sala de Servidores, Sistemas de Gestión, Redes planta Alta etc.
- Descripción: Observación general aclaratoria del proyecto.
- Fecha Inicio: Fecha en la cual se comienza con el proyecto.
- Finalizado: Variable S/N Si o No
- Fecha Fin: Fecha de finalización del proyecto.
- Responsable: Personal, área o gerencia responsable del proyecto

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento sobre gestión de proyectos, se sugiere sea el personal que utilice el rol de líder del proyecto.

Código Proyecto	Nombre	Descripción	Fecha Inicio	Finalizado	Fecha Fin	Responsable
01	[Texto de indentificación del proyecto]	[Texto en lenguaje natural]	XX/XX/XX XX	[S/N]	XX/XX/XX XX	[Identificación]
[...]	[...]	[...]	[...]	[...]		

Tabla 12 - Formulario del Proyecto

Salida: Como salida se obtiene un formulario, que muestra los proyectos elaborados en la organización, los proyectos activos, finalizados y sus responsables. Este último campo se puede obviar si la pyme posee un área de sistemas que realiza todos los proyectos.

Objetivos y Límites

Se establecen el o los objetivos del proyecto, estos pueden ser detallados y se demarcan los límites.

Formulario de Objetivos y Limites del Proyecto

Se carga un registro por cada propósito.

Entradas: Como entrada de datos de la identificación del formulario del proyecto y además en el siguiente formulario se incluirán:

- Código de Proyecto: Dato Único y definido por el usuario, obtenido del formulario del proyecto.
- Propósito: Define el o los propósitos para el proyecto, porque es importante el proyecto para la organización.
- Objetivo: Definición de los objetivos generales del proyecto.
- Límites: Alcance y límites que posee el proyecto.

Responsable: El responsable del confeccionar este formulario, debe haber confeccionado el formulario del proyecto.

Código Proyecto	Propósito	Objetivo	Límites
01	[Texto en lenguaje natural]	• [Objetivo 1] • [Objetivo X]	[Texto en lenguaje natural]
[...]	[...]	[...]	[...]

Tabla 13 - Formulario de Objetivos y Límites del Proyecto

Salida: Como salida se obtiene un formulario que muestra el propósito del proyecto, su importancia, por qué es importante para la organización, además detalla los objetivos del proyecto y delimita el alcance del mismo.

Formulario de Activos incluidos en el Proyecto

Se carga un registro por cada activo asignado a un proyecto.

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Proyecto: Dato Único y definido por el usuario obtenido del formulario del proyecto.
- Código del Activo: Dato Único y definido por el usuario del formulario de activos.

Responsable: Los responsables de realizar este formulario, son los encargados de generar el formulario de activos y el formulario del proyecto.

Código Proyecto	Código Activo
01	A01
[...]	[...]

Tabla 14 - Formulario de Activos por Proyectos

Salida: Como salida se obtiene un formulario, que detalla todos los activos que son incorporados al proyecto, es importante verificar que los activos incluidos en el proyecto, no hayan sido incluidos en otros proyectos.

Equipo de Trabajo

La actividad de esta etapa consiste en designar el recurso humano que serán parte del equipo de AGR, asignando roles que se utilizarán en el proyecto y conformar equipos de trabajo.

Formulario de Equipo de Trabajo

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Proyecto: Dato Único y definido por el usuario dato obtenido del formulario de proyectos.
- Persona: Nombre o Identificación de la persona.
- Equipo: Área, departamento o gerencia a la cual pertenece, se puede incluir si es parte de un equipo ya formado, interno o externo.
- Rol: Rol que desempeña dentro del Proyecto.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento sobre gestión de proyectos, se sugiere sea el personal que utilice el rol de líder del proyecto, con asistencia del área de recursos humanos de la organización, ya que conoce los perfiles profesionales del personal, como así también aptitudes de cada uno.

Código Proyecto	Persona	Equipo	Rol
01	[Nombre personal]	[Equipo de AGR]	[Rol dentro del equipo]
[...]	[...]	[...]	[...]

Tabla 15 - Formulario Equipo de Trabajo

Salida: Como salida se obtiene un formulario que detalla la función y rol que cumple cada persona dentro del proyecto, en el caso de las pequeñas empresas, una persona puede ocupar diferentes roles, pero es imprescindible que se realice la segregación de funciones, por más que sea la misma persona.

Identificación de vulnerabilidad de los Activos

En este proceso, el equipo de trabajo conduce una revisión de alto nivel de la infraestructura computacional, debe enfocarse en la seguridad, y se debe analizar cómo la gente utiliza la infraestructura computacional para acceder a los activos críticos, y conociendo quién es responsable de configurar y dar mantenimiento a dichos activos críticos.[29]

Examinar rutas de acceso

Tomando los activos críticos, se debe analizar la ruta de acceso a ellos, para lograr identificar los tipos de acceso, si son accedidos de forma interna o externa, los roles de las personas que acceden a ellos, se deberá identificar, si es personal a cargo del activo o usuario del mismo, para llevar una identificación de las rutas de acceso, se deberá rellenar el siguiente formulario:

Formulario de Ruta de Acceso a Activos críticos

Entradas: Como entrada se toman los activos que fueron declarados como críticos en el Formulario de relevamiento de Activos:

- Código de Activo Crítico: Dato Único y definido por el usuario.
- Descripción de Accesos al Activo: Descripción en forma de texto en lenguaje natural de los accesos que se tiene al activo, sean de tipo hardware, software o de recursos humanos.
- Tipo de Acceso: Se debe asignar uno o varios tipos de activo utilizando los siguientes códigos:
 - HW: Equipamiento tangible
 - SW: Software o Datos
 - RRHH: Personal de la organización o usuarios de sistemas.
- Tipo relación: Identificar el tipo de relación con la organización, utilizando los siguientes códigos:
 - Interno: Puede ser de tipo de equipamiento tangible, software o datos y personas.

- Externo: Puede ser de tipo de equipamiento tangible, software o datos y personas.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, como ser contratos, hardware, software, personal etc.

Código Activo Crítico	Descripción de Accesos	Tipo de Acceso	Tipo Relación
A01	[Texto en lenguaje natural]	[HW SW RRHH]	[Interno Externo]
[...]	[...]	[...]	[...]

Tabla 16 - Formulario de Ruta de Acceso a Activos críticos

Salida: Como salida se obtiene un formulario en el cual, define, únicamente de los activos críticos que a qué tipo de accesos afronta, y la relación con tipo de acceso.

Nota: Se debe cargar por cada activo crítico un tipo de acceso, ya que se busca identificar los tipos de accesos.

Analizar procesos relacionados con la Tecnología

Los activos no son independientes, como está formulado en el apartado “Dependencia de Activos” podemos observar sus relaciones. Analizar y controlar los activos críticos y sus relaciones, es la característica de esta sección.

Se deberá identificar los activos críticos y los activos dependiente a estos, para jerarquizarlos en la declaración de riesgos posterior, el siguiente formulario establece la relación de ambos y define un tipo de relación.

Formulario Activos relacionados

Entradas: Como entrada se tomas los activos que fueron declarados como críticos en el Formulario de dependencia de Activos:

- Código de Activo Crítico: Dato Único y definido por el usuario.

- Activo Dependiente: Dato Único y definido por el usuario.
- Dependencia Crítica: Se define cuando el activo dependiente también es crítico, los posibles valores a tomar son: S|N
- Tipo de Relación: Especifica la relación que poseen los activos, algunos de ellos pueden tener una relación estricta, como el caso de una Pc y un sistema operativo, y en otro caso puede ser irrelevante, como el caso de una PC y un scanner:
 - Crítica: Se utiliza en el caso de que ambos activos sean críticos.
 - Estricta: Activo con relación estricta a su dependiente.
 - Irrelevante: Relación opcional entre activos.

Responsable: El responsable del confeccionar este formulario, debe tener conocimiento y acceso a todos los aspectos de las Tics de la organización, y preferentemente haber realizado el formulario de relevamiento de activos.

Código Activo Crítico	Activo Dependiente	Dependencia Crítica	Tipo Relación
A01	[A0X]	[S N]	[Crítica Estricta Irrelevante]
[...]	[...]	[...]	[...]

Tabla 17 - Formulario de Activos relacionados

Salida: Como salida se identifica los activos críticos y su relación con sus activos dependientes, se debe priorizar los activos cuya dependencia sea crítica, y establecer una prioridad en la declaración del riesgo.

Taxonomía

La clasificación de los riesgos ayuda a elaborar un enfoque coherente (como se define en el capítulo dos de este TFM), 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[77].

Por lo general, todas las metodologías de ARG proponen su forma de clasificación, para este método se ha escogido la clasificación propuesta por el por la metodología Magerit V3., como hemos visto en capítulos anteriores se definen como amenazas o riesgos.

Para ello, y orientando a las organizaciones de tipo pyme, se creó una taxonomía nueva como aporte del maestrando, la cual se obtiene, procesando las amenazas por el tipo activo. Siendo el tipo de activo, una característica obligatoria para este método.

Para poder lograr esta taxonomía, se deberá identificar por cada activo, cuales son los Tipos de Activos a los cuales se ajusta (TA) y de cada TA a que amenazas (A) está ligada, así se podrán identificar los riesgos o amenazas que son sujetos a los activos, por lo que se deberá generar cuatro formularios, uno por cada tipo de Amenazas, los cuales serán completando con los TA que correspondan por cada activo, los TA no deben repetirse en el mismo formulario, para lo cual, la metodología Magerit V3 provee dicha información y en este método se ajustó el listado de amenazas ajustando dichos riesgos a los que utilizan las pequeñas y medianas empresas. Ver ANEXO II.

Formulario Tipo de Activo por Amenaza

Entradas: Como entrada de datos del formulario se incluirán:

- Tipo de Activo: Dato Único utilizando la tabla 7 que define los tipos de activos.
- Amenaza: Identificación de la amenaza, se debe incluir tipo de amenaza por registro, del tipo A.X, datos obtenido por la tabla ANEXO I.

Responsable: Personal con rol de líder del proyecto, se recomienda posea conocimientos de gestión de riesgos.

[N] Desastres Naturales

Tipo de Activo	Desastre Naturales
[HW]	[N.2] Daños por Agua
[...]	[N.X]

Tabla 18 - Formulario de Amenazas de tipo Natural

[I] De origen Industrial

Tipo de Activo	De Origen Industrial
[HW]	[I.3] Contaminación Mecánica
[...]	[I.X]

Tabla 19 -Formulario de Amenazas de Origen Industrial

[E] Errores y Fallos No Intencionados

Tipo de Activo	Errores a Fallos No Intencionados
[S]	[E.1] Errores de Usuarios
[...]	[E.X]

Tabla 20 -Formulario de Amenazas Errores y Fallos No deseados

[A] Ataques Intencionados

Tipo de Activo	Ataques Intencionados
[SW]	[A.5] Suplantación de la Identidad del Usuario
[...]	[A.X]

Tabla 21 -Formulario de Amenazas de Ataques Intencionados

Salida: Como salida se obtiene 4 formularios en los cuales se agrupan los tipos de amenazas por los tipos de riesgos, donde se mostrarán el listado del total riesgos que posee todos los tipos de activos, y por consiguiente los activos del proyecto, estos formularios serán la puerta de entrada para poder lograr la taxonomía de los mismos.

Una vez identificado los tipos de activos por amenazas se genera el Listado Taxonómico de Riesgos, para lo cual se deberá enumerar los riesgos con la amenaza identificada. Aquí también la amenaza debe ser de tipo único.

Formulario Taxonómico de riesgos

Entradas: Como entrada de datos del formulario se incluirán:

- **Identificador:** Identificador del Riesgo o Amenaza, dato único y definido por el Usuario.
- **Amenaza:** Identificación de la amenaza, se debe incluir un tipo de amenaza por registro, del tipo N.X, datos obtenidos por la tabla ANEXO II.
- **Vinculación:** Identificar que vínculo posee el riesgo o amenaza con la organización, pueden ser:
 - **Negocio:** Riesgo o Amenaza correspondiente a la Organización como ser riesgos de presupuestos, o riesgos de cambios estructurales organizacionales.
 - **Producto:** Riesgo o amenaza, con respecto a los activos de la organización, equipos, redes, telecomunicaciones etc.
 - **Proyecto:** Riesgo o amenaza, que representa a un proyecto o tareas dinámicas, como ser, desarrollo de software, mantenimiento de equipos etc.

Responsable: Personal con rol de líder del proyecto en conjunto con el equipo de riesgos.

Identificador	Amenaza /Riesgo	Vinculación
R1	[N.X] o [I.X] o [E.X] o [A.X]	[Negocio Producto Proyecto]
[...]	[...]	[...]

Tabla 22 - Listado de Taxonomía de Riesgos o Amenazas

Salida: Como resultante se obtendrá un listado de todos los riesgos o amenazas a los cuales se podrían enfrentar los activos.

Declaración

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 más 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.

Formulario de Declaración del Riesgo

Entradas: Como entrada de datos del formulario se incluirán:

- Identificador: Identificador del Riesgo o Amenaza, dato único y definido por el Usuario.

- Condición: Especificar que condición deber ser dada para que el riesgo pase a ser un problema o se ejecute.
- Consecuencia: Definir qué consecuencias ocasiona la ejecución del riesgo para la organización, activos dependientes entre otros.

Responsable: Líder del proyecto en conjunto con el Equipo de gestión de riesgo y los responsables de los activos.

R1 - [...]	
Condición	[...]
Consecuencia	[...]
Efecto	[...]

Tabla 23 - Formulario de Declaración del Riesgo

Salida: Se obtiene como salida un registro claro de todos los conjuntos de riesgos a los que se ve afrontado los activos que se incluyen en el proyecto. El formulario resultante posee información de importancia, para la gerencia de la organización debido a que se divisan los efectos para la organización si el riesgo se activa.

Cálculo de probabilidad

La probabilidad del riesgo es el porcentaje de que la situación descrita 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. Si bien existen indefinidos métodos de valoración de probabilidades, el siguiente cuadro es propuesto basándose en las características de probabilidades de una pequeña o mediana empresa:

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

Tabla 24 - Tabla de Ejemplo de Probabilidad de Riesgo[77]

Tomando la totalidad de riesgos del listado de taxonomía se realiza el formulario de probabilidad de Ocurrencia.

Formulario de Probabilidad de Ocurrencia

Entradas: Como entrada de datos del formulario se incluirán:

- **Identificador:** Identificador del Riesgo o Amenaza, dato establecido en el formulario de declaración de riesgo.
- **Amenaza o Riesgo:** Identificación de la amenaza expresado en el formulario taxonómico de riesgo, se debe incluir un solo tipo de amenaza por registro, del tipo N.X, datos obtenido por el listado de taxonomías.
- **Expresión:** Expresión en lenguaje natural que expresa el porcentaje de ocurrencia del riesgo.
- **Probabilidad:** Porcentaje de probabilidad promedio de la ocurrencia. Se calcula tomando la probabilidad real, y situándola en el período que registra la tabla de muestra. Como expresa la tabla 21 de ejemplo.

Responsable: Líder del proyecto en conjunto con el Equipo de gestión de riesgo y los responsables de los activos.

Identificador	Amenaza /Riesgo	Expresión	Probabilidad promedio
R1	[N.X] o [I.X] o [E.X] o [A.X]	[expresión en lenguaje natural según tabla previa]	[% de probabilidad de ocurrencia]
[...]	[...]	[...]	[...]

Tabla 25 - Formulario de Probabilidad de Ocurrencia

Salida: Se obtiene como salida un formulario, donde se observa además de los riesgos la probabilidad promedio que se utilizará como dato de entrada, en el formulario de exposición al riesgo.

Cálculo del Impacto

Se establece un Impacto, cuando un ataque exitoso perjudica la confidencialidad, integridad, disponibilidad y autenticidad de los datos, información o equipamiento tecnológico dentro de una organización, cuando un riesgo se transforma en un problema, por ello, a cada riesgo se le asigna un valor denominado valor de impacto. Este valor, aporta una medida de importancia sobre la no disponibilidad de los activos o problemas que ellos pueden padecer. Debido a que los activos afectados por el riesgo son diferentes, los proyectos determinan distintos grados de impactos, por lo cual, debemos generar y utilizar una tabla de valoración de impacto por proyecto.

Tabla de Impacto del Riesgo en la Organización

Entradas: Como entrada de datos del formulario se incluirán:

- Criterio: Identificador en lenguaje natural, que identifica la importancia de la consecuencia que representa si el riesgo se ejecuta.
- Periodo: Periodo de tiempo en el que el proyecto será afectado de producirse el riesgo o amenaza, hasta lograr solucionar el mismo. El periodo para todo el formulario debe poseer la misma unidad de tiempo.
- Valor: Valor numérico que expresa el criterio. Por cada criterio similar debe ir el mismo valor. Se sugiere que se implemente valores ascendentes a nivel de criticidad. En el caso de que la criticidad sea la menor de la lista iría el valor 1, e incrementando el valor cuando se incrementa la criticidad.

Criterio	Período	Valor
Insignificante	[tiempo en horas, días o semanas]	1
Marginal	[tiempo en horas, días o semanas]	2
Medio	[tiempo en horas, días o semanas]	3
Crítico	[tiempo en horas, días o semanas]	4
Catastrófico	[tiempo en horas, días o semanas]	5

Tabla 26 - Formulario de Impacto

A modo de ejemplo se muestra la tabla de impacto orientado a un desarrollo de un producto software.

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

Tabla 27 - Ejemplo de Estimación de impacto[77]

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.

Por cada amenaza o riesgo se deberá generar un registro de impacto, utilizando el siguiente formulario

Formulario de Estimación de Impacto por Riesgo

Entradas: Como entrada de datos del formulario se incluirán:

- Identificador: Identificador del Riesgo o Amenaza, dato establecido en el formulario de declaración de riesgo.
- Amenaza o Riesgo: Identificación de la amenaza expresado en el formulario taxonómico de riesgo, se debe incluir un solo tipo de amenaza por registro, del tipo N.X, datos obtenido por el listado de taxonomías.

- **Impacto:** Identificador en lenguaje natural, que identifica la importancia de la consecuencia que representa si el riesgo se ejecuta.

Responsable: Líder del proyecto en conjunto con el Equipo de gestión de riesgo y los gerentes o encargados de áreas o departamentos, que logren cuantificar el impacto que genera la ejecución de un riesgo.

Identificador	Amenaza /Riesgo	Impacto
R1	[N.X] o [I.X] o [E.X] o [A.X]	[criterio correspondiente al impacto según la tabla anterior]
[...]	[...]	[...]

Tabla 28 - Formulario de Impacto del Riesgo

Salida: Se obtiene como salida un formulario, donde se observa además de los riesgos, el valor de impacto que se utilizará como dato de entrada en el formulario de exposición al riesgo.

Exposición

Si bien todos los activos poseen riesgos que lo pueden afectar, gestionar todos los activos de una organización es improbable debido al costo y el tiempo, por lo cual se genera la exposición al riesgo, ésta 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.

$$\text{Riesgo} = \text{Probabilidad promedio de ocurrencia} \times \text{Impacto}$$

Únicamente serán gestionados los riesgos que posean un positivo, 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 tres grupos de activos:

AGR, activos analizados, cuyo tipo de activo posea una amenaza con exposición positiva y que deberán ser gestionados.

AR, activos analizados, cuyo tipo de activo posea una amenaza con exposición negativa.

N/A Activos no incluidos en proyectos AR y AGR.

Formulario de Exposición al Riesgo

Entradas: Como entrada de datos del formulario se incluirán:

- **Identificador:** Identificador del Riesgo o Amenaza, dato establecido en el formulario de declaración de riesgo.
- **Amenaza o Riesgo:** Identificación de la amenaza expresado en el formulario taxonómico de riesgo, se debe incluir un solo tipo de amenaza por registro, del tipo N.X, datos obtenido por el listado de taxonomías.
- **Impacto:** Valor numérico que expresa el criterio extraído del formulario de estimación del impacto por riesgo.
- **Probabilidad:** Porcentaje de probabilidad promedio de la ocurrencia. Se obtiene del formulario de probabilidad de ocurrencia.
- **Exposición:** Valor resultante del cálculo: Impacto X % probabilidad.

Responsable: Líder del proyecto en conjunto con el Equipo de gestión de riesgo y los gerentes o encargados de áreas o departamentos, que logren cuantificar el impacto que genera la ejecución de un riesgo.

Identificador	Amenaza /Riesgo	Impacto	Probabilidad	Exposición
R1	[N.X] o [I.X] o [E.X] o [A.X]	[expresión]	[%]	[0,00]
[...]	[...]	[...]	[...]	[...]

Tabla 29 - Formulario de Exposición al Riesgo

Salida: Como resultado se obtiene el formulario de exposición al riesgo, que es la resultante del proceso de análisis y gestión de riesgos, será utilizando en diferentes etapas y procedimientos del método.

4.2.2 Etapa de Gestión

Esta etapa está compuesta por un solo proceso, figura 35, gestión de riesgos.



Figura 35 - Etapa Gestión

Gestión de los Riesgos

El riesgo expuesto, se debe gestionar utilizando métodos de control denominados planes de acción como lo define SEI- CRM o Salvaguardas como lo define Magerit el cual define una salvaguarda como “un procedimiento o mecanismo tecnológico que reduce un riesgo al cual se expone un activo” [78].

La correcta planificación de un conjunto de salvaguardas conlleva a reducir el impacto, reducir el riesgo y reducir la degradación¹⁶ del activo minimizando el daño y/o la frecuencia de ocurrencia del mismo.

Como hemos visto anteriormente el riesgo se puede minimizar, reducir o aceptar, pero no eliminarse, por ello, debemos generar tareas de control, para verificar periódicamente el estado del activo, sea tangible, intangible o de recursos humanos.

Los planes de acción deberán ser adecuada para cada activo y para cada tipo del activo. Además, se deberá ajustar a la tecnología vigente, debido a que todos los activos de la IT, incluyendo al personal, están en constante cambio y actualización, por lo cual estos planes de control, deberán ser revisadas con periodicidad y actualizadas de ser necesario.

Las salvaguardas, deben ser ejecutadas para los activos internos y servicios tercerizados, por lo cual, se debe expresar en las contrataciones, los artículos que incluyan este tipo de controles.

Para lograr una gestión de los riesgos establecidos se deben identificar claramente, cuatro aspectos fundamentales de cada uno de los que se pretenda gestionar y generar un plan de acción .

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.

¹⁶ Degradación: La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

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 riesgos, 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 recursos extras, tanto económicos (planificación presupuestaria) como no (asesoramiento externo, asignación de personal interno etc.), la cual se debe incluir en este punto.

Formulario de Gestión de riesgos

Entradas: Como entrada de datos del formulario se incluirán:

- **Importancia del Riesgo o Amenaza**: Se debe describir claramente por que la amenaza es importante para la organización en un lenguaje natural.
- **Información de seguimiento**: Enumerar la información necesaria para el seguimiento del riesgo, se debe describir todos los aspectos relevantes para el seguimiento tanto sea utilizando las Tics como así también información física, informes técnicos entre otros.
- **Responsable**: Persona responsable del seguimiento y control del riesgo.

- **Recursos Necesario:** Enumerar los recursos se necesitan para realizar las actividades de control del riesgo, se detallan los recursos humanos, recursos técnicos, recursos tecnológicos, recursos de terceros etc.
- **Plan de Acción para Controlar el Riesgo:** Enumerar las acciones de control necesarias para vigilancia del riesgo.
- **Plan de Contingencia:** Definir el o los disparadores que llevan a la ejecución del riesgo o amenaza, por cada uno de los disparadores se deberá generar la lista de tareas para desactivar el riesgo en búsqueda instaurar el activo.

Responsable: Líder del proyecto en conjunto con el Equipo de gestión de riesgo y los gerentes o encargados de áreas o departamentos, que logren cuantificar el impacto que genera la ejecución de un riesgo.

R1	[Descripción del Riesgo]
Importancia del riesgo	□
Información requerida para su seguimiento	• □
Responsable	□
Recursos necesarios	• □
Plan de Acción	•
Plan de contingencia	Disparador1: □ • Tareas 1 • Tarea 1..X Disparador N: □ • Tareas N • Tarea N..X

Tabla 30 - Formulario de Gestión del Riesgo

Salida: Se obtiene el formulario de gestión de riesgos, que es la culminación de la etapa II, es el documento principal de este capítulo R, donde se pueden expresar los riesgos a gestionar, la tarea de realizar como acciones preventivas que son denominadas planes de acción y las acciones a realizar si el riesgo se ejecuta, que se denomina plan de contingencia.

El plan de contingencia puede ser afectado en el transcurso del proyecto o vida del activo, debiendo ajustar el plan si fuese necesario. La etapa de incidencias gestiona la incidencia que puede afectar a dichos planes.

4.2.3 Etapa de Seguimiento y Control

Esta etapa posee dos procesos, figura 36, gestión de seguimiento y gestión de control.



Figura 36 - Etapa Control y Seguimiento

Gestión de Seguimiento

Los riesgos gestionados contienen un plan de acción, que son tareas de control que se debe realizar en un lapso determinado de tiempo, por un personal de la empresa, estos controles, utilizando términos de auditoría informática se denominan “preventivos” y “detectivos”.

Para una pyme, contener una agenda de actividades de mantenimiento de activos es esencial, debido que, por lo general, dichas organizaciones cuentan con poco personal asignado a la gestión de las Tics, y teniendo un plan de tareas específico, la empresa, puede capacitar al personal no informático de la organización para realizar las tareas de control o subcontratar mano de obra para realizar dichas tareas. Las mismas son fácilmente controlables y rutinarias.

El plan de seguimiento y control, es una etapa que se crea en este Trabajo Final de Maestría y posee características específicas tanto de control como de seguimiento sobre las actividades indicadas en el plan de acción.

El seguimiento de un plan de acción se asignará a un miembro del equipo de ARG, un personal capacitado o podrá contratar la tarea en un personal externo, en un proyecto establecido, el cual verificará las tareas asignadas y realizar los controles pertinentes generando por cada riesgo una planilla informando:

Formulario de Seguimiento

Entradas: Para realizar este formulario se realizará un formulario de seguimiento de los planes de acción tomado los datos del formulario de gestión de riesgo.

- Proyecto: Identificador del proyecto, dato obtenido del formulario de proyecto.
- Identificador: Identificación del riesgo, dato obtenido del formulario de exposición al riesgo.
- Descripción: Descripción del Riesgo en código y lenguaje natural.
- Fecha: Fecha que se realizó la actividad de control.
- % de Finalización: 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.
- Obs Tarea: Observación de la Tarea el encargado de la tarea deberá incorporar notas de observación sobre la tarea realizada.

- **Obs Tareas Finalizada:** Observación de tarea finalizada lenguaje natural, el resultado de la finalización de la tarea.
- **Terminado:** Forma en la que finalizó la tarea B= Bien, M = Mal.
- **Persona:** Persona que realizó esta tarea.

Responsable: El responsable de generar los formularios de seguimiento, es el líder del proyecto en conjunto con el área o departamento de recursos humanos.

Proyecto:					
[R1]	[Descripción del Riesgo N.X – Texto]				
Fecha	% de Finalización	Obs tarea	Obs. Tarea Finalizada	Terminado	Persona
[XX/XX/XXXX]	[%]	[Texto]	[Texto]	[B/M]	[Nombre Persona]
[...]	[...]	[...]	[...]	[...]	

Tabla 31 - Formulario de Seguimiento de Plan de Acción

Salida: Como salida se obtiene las fichas o formularios de tareas de control a realizar por cada riesgo por proyecto.

Gestión de Control

- Control: El director del proyecto controlará las tareas de seguimiento del plan de acción o 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.

4.3 Capítulo I - Registros de incidencias

4.3.1 Etapa de Incidencias

Es etapa posee 5 (cinco) procesos, que se muestran en la figura 37.

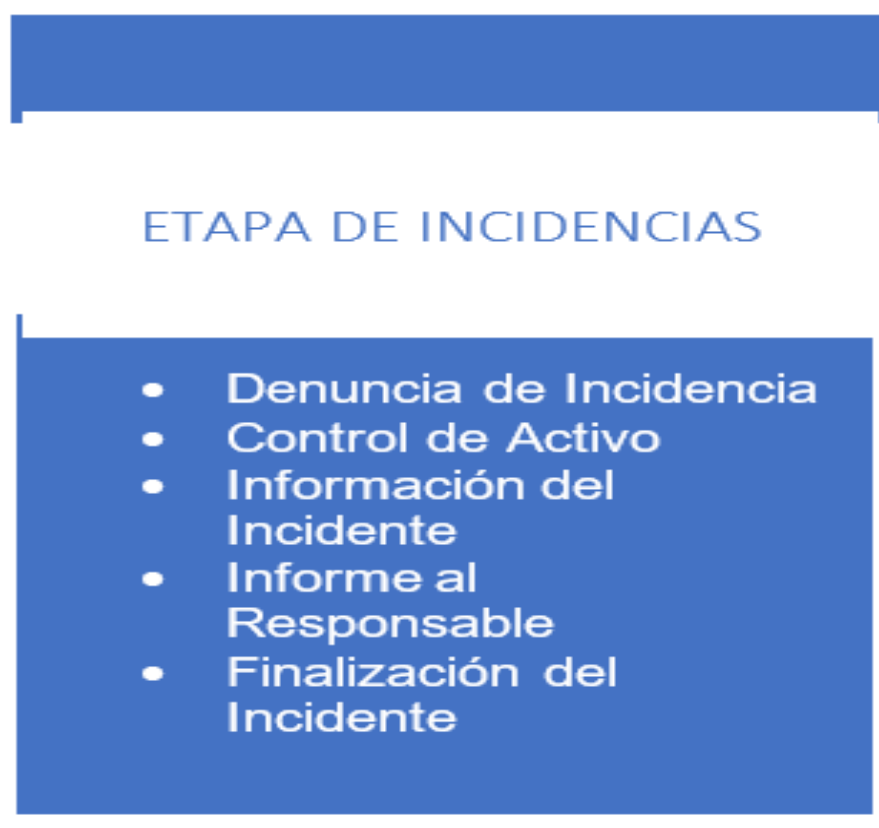


Figura 37 - Etapa de Incidencias

Todos los activos corren riesgos, pero no todo son analizados y gestionados, esta etapa proporciona una gestión de incidencias para identificar los problemas (riesgos ejecutados) que poseen los activos, un elemento clave para el mejoramiento funcional y operacional de la evolución de riesgos, además de brindar a la organización de una herramienta para el fortalecimiento de la gestión del conocimiento.

De ella se desprende información vital para el proyecto, a partir del cual 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.

Denuncia de la incidencia

Se carga una incidencia, la cual puede ser registrada por cualquier miembro de la organización que esté a cargo del activo, se debe registrar: el activo en el cual, se ejecutó el riesgo, el riesgo que disparó el incidente, la fecha - hora del mismo y las

acciones primarias a tomar por parte del usuario denunciante. Por ejemplo: se apagó el equipo.

Formulario de Denuncia de Incidencia

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Incidencia: Dato Único y definido por el usuario.
- Código Activo: Identificación del Activo.
- Amenaza/Riego: Identificación de la amenaza, se debe incluir tipo de amenaza por registro, del tipo N.X, datos obtenido por el listado de taxonomías, si no tuviera un riesgo asignado debe ir la sigla N/A.
- Responsable: Recurso Humano Responsable del Activo
- Fecha del Incidente: Fecha de estado de conocimiento de la incidencia.
- Hora del Incidente: Hora del estado de conocimiento del incidente.
- Acciona a Tomar: Lista de tareas para desactivar el riesgo en búsqueda instaurar el activo.

Responsable: Personal afectado a la gestión de activos, y los agentes que intervengan en la solución del problema, deberán por cada riesgo o problema ejecutado en un activo, cargar el formulario.

Código de Incidencia	Código Activo	Amenaza /Riesgo	Responsable	Fecha Incidente	Hora Incidente	Acción a Tomar
I01	A01	[N.X] o [I.X] o [E.X] o [A.X]	[Nombre y Apellido]	[DD/MM/AAAA]	[HH:MM]	• [Tarea 1] • [Tarea N]
[...]	[...]	[...]	[...]	[...]	[...]	[...]

Tabla 32 - Formulario de Denuncia de Incidencia.

Salida: Formulario de Denuncia, detalla los activos que fueron afectados por un incidente, el riesgo el cual lo afectó, el responsable del activo, fecha y hora. Detalla además el plan de acción realizado para la solución del problema.

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 capítulo.
- b) Activo analizado, pero no gestionado (AR): Esto ocurre cuando en el cálculo de la exposición del riesgo es negativo y no se tomó 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.

Formulario de Control de activo

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Incidencia: Dato Único y definido por el usuario
- Código Activo: Dato Único y definido por el usuario
- Registro de Activo: Identificación si el activo es un
 - Activo No Registrado [ANR]
 - Activo Analizado, pero No registrado [AR].
 - Activo Analizado y Gestionado [AGR]

Responsable: Líder del proyecto. Deberá generar por cada incidencia finalizada, los datos del activo involucrado en el incidente.

Código de Incidencia	Código Activo	Registro Activo
I01	A01	[ANR] o [AR] o [AGR]
[...]	[...]	[...]

Tabla 33 - Formulario de Control de Activo.

Salida: Como salida se obtendrá un listado de activos que fueron alcanzados por un problema, este listado se deberá tener como elemento de consulta para:

- Si el activo posee AGR: contrastar el plan de contingencia incorporado al formulario de gestión del riesgo, con la acción a tomar expresado en el formulario de denuncia del incidente, y si son diferentes, se deberá ajustar el plan de contingencia y evaluar si el plan de acción es coherente o hay que modificarlo, ya que el activo tuvo un incidente. Además de modificar el % de ocurrencia de dicho riesgo.
- Si el activo fue relevado, pero No gestionado AR: se deberá tener en cuenta el % de ocurrencia del mismo para la próxima iteración del proyecto donde se ve reflejado el activo, y si se tomará las acciones realizadas para solucionar el riesgo, como plan de contingencia en un futuro en el Plan de Contingencia de Activos ANR - AG.
- Si el activo no fue declarado ANR: se deberá generar un informe puntal sobre la incidencia en el Plan de Contingencia de Activos ANR - AG.

Nota: Se sugiere identificar este formulario, como formulario principal en las evaluaciones de futuros riesgos y actualizar el listado de amenazas ubicadas en el en el anexo II con los datos de los incidentes que no estuvieran dentro de las amenazas actuales.

Información del Incidente

En este proceso se informan los resultados obtenidos del control del incidente, de activos se trata y consta de dos partes.

- I. Informe Plan de Contingencias: Si el riesgo que generó el incidente no ha sido evaluado o no está gestionado se deberá generar un informe en el cual se reflejen:
 - a. El plan de contingencias realizado para la solución del riesgo.
 - b. El responsable de ejecución del plan.
 - c. Pasos a seguir establecidos en el plan.

Formulario de Informe Plan de Contingencia de Activos ANR - AG

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Incidencia: Dato Único y definido por el usuario dato incluido en el Formulario Denuncia de Incidencias.
- Identificador: Identificación de la amenaza, se debe incluir tipo de amenaza por registro, del tipo N.X, datos obtenido por el listado de taxonomías, si no tuviera un riesgo asignado debe ir la sigla N/A, las amenazas registradas se encuentran en ANEXO II.
- Responsable: Persona responsable de la ejecución del plan de contingencia.
- Fecha: Fecha del Incidente.
- Plan de Contingencia: Disparador y pasos a seguir, si el riesgo no está analizado o gestionado se deberá describir los pasos realizados para la solución del riesgo en formato de pasos a seguir.

Responsable: Personal afectado a la gestión de activos, y los agentes que intervengan en la solución del problema, deberán por cada riesgo o problema ejecutado en un activo, cargar el formulario.

Código de Incidencia	Identificador	Responsable	Fecha	Plan de Contingencia
I01	R1	[Nombre y Apellido]	[DD/MM/AA AA]	Disparador1: [] • Tareas 1 • Tarea 1..X Disparador N: [] • Tareas N Tarea N..X
[...]	[...]	[...]	[...]	[...]

Tabla 34 -Informe Plan de Contingencia de Activos ANR - AG

Salida: Como salida se obtiene un formulario, con datos de los incidentes que no están siendo gestionados por un proyecto de AGR.

Nota: Este formulario es documento importante, para ser evaluado en la próxima iteración del proyecto, debido a que, si el riesgo se gestiona, se toma la información del incidente como datos para genera el de contingencias que logro

revertir el riesgo. Si la Amenaza es de tipo N/A se deberá registrar en la sección de Amenazas, incluida en el anexo I de este trabajo.

Informe al Responsable

Informar sobre la ocurrencia de los incidentes a las personas o sectores correctos, es esencial para fomentar la gestión del conocimiento dentro de empresa, por lo cual se debe 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.

Formulario de Informe al responsable

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Incidencia: Dato Único y definido por el usuario dato incluido en el Formulario Denuncia de Incidencias.
- Responsable: Persona responsable de la ejecución del plan de contingencia.
- Informe: Identificar uno o varios tipos de informes como ser
 - sincro: si el informe se realizó de forma sincrónica, como ser reunión presencial, llamado telefónico, tele asistencia.
 - email: Si el informe se realizó por vía de correo electrónico, se sugiere que se configure el email con acuse recibo y confirmación de recepción.
 - ws: Si el informe se envió por el software whatsapp
 - Sms: Si el informe se envió por vía mensaje de texto.
- Fecha: Fecha realizado el informe.
- Hora: Realizado el informe.

Responsable: Personal afectado a la gestión de activos, y los agentes que intervengan en la solución del problema, deberán por cada riesgo o problema ejecutado en un activo, cargar el formulario.

Código de Incidencia	Responsable	Informe	Fecha
I01	[Nombre y Apellido]	[sincro],[email],[ws],[sms]	[DD/MM/AAAA]
[...]	[...]	[...]	[...]

Tabla 35 -Formulario de Informe al Responsable

Salida: Como salida se obtiene un listado de comunicación de incidentes a responsables, observando los distintos métodos y tecnologías en las cuales se realizó la comunicación.

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.

Formulario Finalización del Incidente

Entradas: Como entrada de datos del formulario se incluirán:

- Código de Incidencia: Dato Único y definido por el usuario dato incluido en el Formulario Denuncia de Incidencias.
- Acciones realizadas: Texto en lenguaje natural que resuma las tareas que realizaron sobre la incidencia.
- Dictamen de Finalización: Texto en lenguaje natural de un dictamen u observación de finalización de la incidencia.
- Tipo Final: Tipo de finalización posee dos tipos B = bien, M= Mal.
- Fecha: Fecha de finalización del incidente.
- Cont. AGR: Informar si se ejecutó el plan de contingencia identificado en el formulario de Gestión de Riesgos tabla 26.
- Eficacia: Porcentaje de la eficacia del plan de contingencia establecido.

Responsable: Personal afectado a la gestión de activos, y los agentes que intervengan en la solución del problema, deberán por cada riesgo o problema ejecutado en un activo, cargar el formulario.

Código de Incidencia	Acciones realizadas	Dictamen de finalización	Tipo Final	Fecha	Cont. AGR	Eficacia
I01	[Acciones]	[dictamen lenguaje natural]	[B/M]	[DD/MM/AAAA]	[S/N]	[%]
[...]	[...]	[...]	[...]	[...]	[...]	[...]

Tabla 36 - Formulario finalización de Incidente

Salida: Se obtiene un documento, en el cual se puede analizar la finalización de las incidencias y el porcentaje de efectividad, además de ver si el riesgo cuenta con gestión.

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.

En este trabajo se presentan los formularios de informes, tres formularios diferentes, se sugiere de ser necesario simplificar dichos formularios, generando un solo formulario con el contenido de todos y utilizar un software para la gestión como planillas de cálculo.

4.4 Capítulo C – Comunicación

“Comunicar es el proceso mediante el cual, se transmite información de un entidad a otra”¹⁷, por qué es imperante comunicar la información procesada de los seguimiento realizados en el AGR y de los incidentes ocurridos en la organizaciones[79], esta etapa, es exclusiva de este método, el objetivo de la misma es que el conocimiento obtenido en el proceso del AGR y de la gestión de incidentes, quede como conocimiento documentado e informado en la organización, para que el este conocimiento no se exclusivo del personal participante de la gestión de riesgos y sea parte del conocimiento de la organización completa.

¹⁷ <http://es.wikipedia.org/wiki/Comunicaci%C3%B3n>

El método conjuga conocimiento explícito y tácito dentro de los formularios, debido a que además de poseer una estructura cuantitativa, también soporta en muchos formularios texto en lenguaje natural, para poder incorporar información tácita al sistema de conocimiento.

Posee dos tipos de grupos de conocimiento, el conocimiento explícito en el cual se informan, todos los informes que poseen estructura cualitativa y conocimiento tácito donde se generan informes en los cuales, no se posee parámetros estructurados y la información solicitada es de texto libre.

4.4.1 Etapa Conocimiento Explícito

Consta de dos procedimientos como muestra la figura 38, informe del seguimiento y estadísticas.

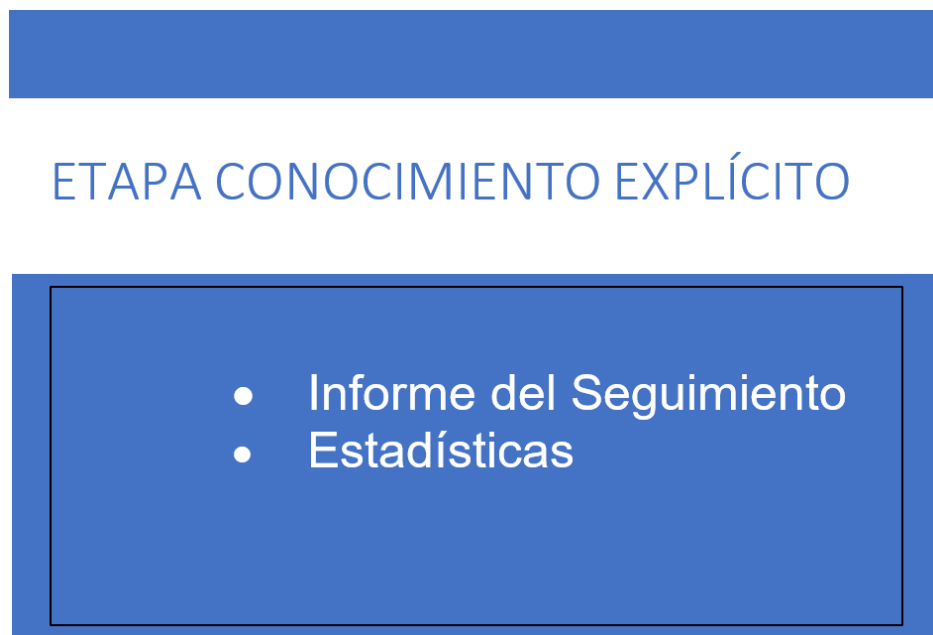


Figura 38 - Etapa Conocimiento Explícito

Informe de seguimiento

Se debe generar informes referidos al estado del seguimiento de acciones del plan de acción, estos reportes deben ser:

- a) Informe de actividad de seguimiento por fecha.
- b) Informe de seguimiento finalizado correctamente.

Estructura Sugerida

Código de Proyecto	Nombre proyecto	Salvaguarda	% Realizado	Fecha	Riesgo	Responsable
101	[Texto lenguaje natural]	[Texto lenguaje natural]	[%]	[DD/MM/AAAA]	[Texto lenguaje natural]	[Nombre Responsable]
[...]	[...]	[...]	[...]	[...]	[...]	[...]

Tabla 37 - Informe de seguimiento

En el caso del informe finalizado, solo se expondrán los datos que cuyo porcentaje sea igual a 100%

Estadística

Informe de estadístico de Activos Gestionados por incidentes.

Estructura Sugerida

Fecha Desde	[DD/MM/AAAA]
Fecha Hasta	[DD/MM/AAAA]
<u>Activo Evaluado</u>	<u>Cantidad</u>
N/A (Sin Evaluación)	[N]
AG (Evaluado y No gestionado)	[N]
AGR (Gestionado)	[N]

Tabla 38 - Estadística

4.4.2 Conocimiento Tácito

Etapa que cuenta con dos procesos, como muestra la figura 39, informe del incidente e informe de experiencia propia de riesgo.

ETAPA CONOCIMIENTO TÁCITO

- Informe del Incidente
- Informe de experiencia propia de Riesgos

Figura 39 - Etapa Conocimiento Tácito

Informe de incidente

Se debe generar informes de los incidentes ocurridos, los reportes a generar deben ser:

- Informe de total de incidentes ocurridos.
- Informe de incidentes finalizados correctamente.
- Informe de incidentes finalizados con problemas.
- Informe de incidentes con activos que no estuvieron analizados en el proyecto.
- Informe de incidentes con activos que estuvieron analizados en el proyecto, pero no gestionados.
- Informe de incidentes con activos que tuvieron analizados y gestionados.

Estructura Sugerida

Código de Incidencia	Riesgo	Responsable	Fecha	Plan de Contingencia	Finalizado
I01	[Texto lenguaje natural]	[Nombre y Apellido]	[DD/MM /AAAA]	Disparador1: ☐ • Tareas 1 • Tarea 1..X Disparador N: ☐ • Tareas N Tarea N..X	[S N]
[...]	[...]	[...]	[...]	[...]	[...]

Tabla 39 - Informe del Incidente

Informe de Experiencia Propia de Riesgos

Informe de cualitativo donde tanto el personal describe en formato de texto natural la experiencia utilizada y los pasos seguidos para gestionar una incidencia, se proporcionará un plan de acción sugerido y un plan de contingencia.

Estructura Sugerida

Código de Riesgo	[R01]
Descripción Riesgo	[Texto Lenguaje Natural]
Riesgo Nuevo	[S N] *Si es nuevo el código de riesgo es = N*
Mejora en Plan de Acción	[Texto Lenguaje Natural]
Mejora en Plan de contingencia	[Texto Lenguaje Natural]
Autor	[Nombre Persona]
Fecha	[DD/MM/AAAA]

Tabla 40 - Informe de Experiencia Propia de Riesgos

A modo de conclusión del capítulo, queda establecido el modelo RIC, en donde se definen los capítulos etapas y procesos, para lograr generar un análisis y gestión de riesgo, que se destaca por las siguientes cualidades:

- Manejable, debido a que posee 3 capítulos y 6 etapas, en la cual en el cual la etapa de Control y Seguimiento del capítulo R, 12 procesos, y los capítulos I y C son exclusivamente utilizadas por este método contiene 9 procesos que son utilizados de ser necesarios, da un total de 21 procesos.
- Amigable, por incorporar 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.
- Confiable, dado que está derivado de las 3 metodologías que se consideran completas y abarcativa en torno al análisis y gestión de

riesgos en la actualidad, SEI –CRM, Magerit V3 y OCTAVE-S, se consideran confiables ya que son utilizadas en proyectos de TI y desarrollo de software; en el proceso de investigación de este trabajo, que permite acceder a documentación de implementación de estas metodologías en proyectos tecnológicos.

- Adaptable: debido que la taxonomía creada es aplicable a las pequeñas y medianas empresas.

Capítulo 5 -La Herramienta SCRisk

5.1 Introducción

En este capítulo se desarrollan los componentes utilizados para la elaboración de la herramienta construida dar soporte del método RIC, se exponen los objetivos del sistema, metodología de análisis, diseño y características del sistema, dejando en claro que al momento de la presentación del TFM la herramienta está en etapa de construcción debido a la metodología utilizada. -

5.2 Objetivos Generales del prototipo herramienta

Desarrollar una herramienta software para validar el modelo RIC, como objetivo principal la cual permitirá la gestión de activos, amenazas o riesgos, salvaguardas, proyectos, personas, taxonomías, gestión de riesgos, plan de contingencias y generación automática de plan de acción por proyecto, seguimiento, incidencias e informes, generar información estadística y proponer mejoramiento de los planes antes mencionados y deberá poseer seguridad de acceso y control del sistema, auditoría de sistema y de procesos.

5.3 Metodología elegida

5.3.1 AgEnD- Metodología Ágil y evolutiva

Para la elaboración del software “SCRisk”, se seleccionó la metodología AgEnD, desarrollada por el Ing. Marcelo Hernán Schenone [80], 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 adaptabilidad de sus elementos, estos pueden ser utilizados según

la necesidad del proyecto software, brindando flexibilidad en sus etapas y artefactos.

Especificaciones del desarrollo utilizando ADgnD

Background del Proyecto

Para el desarrollo de SCRisk se decidió utilizar un equipo de desarrollo de una persona. El proyecto utiliza algunas prácticas de la metodología AgEnD como proceso, estas son seleccionadas por un coordinador (en este caso es el maestrando y desarrollador) 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.

Roles y Recursos

Los trabajos de AgEnD son llevados a cabo por una sola persona, el cual cumple distintos “roles” dentro del proyecto de análisis y desarrollo del software. A continuación, mencionamos a los trabajadores:

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

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

Reseña: El Analista es una persona con mucha habilidad y experiencia en relevamientos en grandes proyectos. Está especializado 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 ayuda al equipo de desarrollo en la implementación de las prácticas de AgEnD y en la creación de los artefactos propuestos. También actúa 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 encarga de diseñar y ejecutar los casos de prueba de la aplicación

Reseña: El tester, es 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.

5.3.2 Justificación de la Elección metodológica

I. Construcción de prototipos evolutivos: El sistema de software a desarrollar será una herramienta de ayuda, basada en un nuevo modelo en el que no hay experiencia, por lo tanto, una de las mejores prácticas recomendadas por la ingeniería de software es generar prototipos y que evolucionen y mejoren con la ayuda del usuario y los casos prácticos.

II. Método de construcción ágil: Debido a que es un Trabajo Final de Maestría, el desarrollo debe ser realizado por una sola persona y los tiempos de construcción son escasos, por lo que el paradigma debe tener la particularidad de generar software de manera ágil sin perder la formalidad en el análisis y desarrollo, esto permitirá la persona se concentren en la tarea de construir software promoviendo prácticas fáciles de adoptar y a través de un ambiente ordenado que ayude le ayude trabajar mejor y permita que los proyectos terminen con éxito y en plazos mínimos.

5.3.3 Tecnologías

Al momento de formular la propuesta económica se realizó la selección basada en herramientas RAD¹⁸ 4GL¹⁹ para el desarrollo de la aplicación, debido a que las mismas comprenden 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 herramienta), de programación y aumentando la calidad del trabajo, basándose principalmente en el diseño del sistema.

La WEB como plataforma, en virtud a que las nuevas tecnologías se basan en aplicaciones cuya plataforma principal es el navegador, al ser generada por una herramienta 4GL la misma herramienta de programación y lenguaje, cuenta con una plataforma WEB para la ejecución de sus productos, la empresa donde se realiza el caso de estudio es propietaria del lenguaje de programación de la herramienta desarrollada y posee licencia para ello.

Como herramientas de análisis y diseño se priorizó por herramientas CASE²⁰.

Arquitectura de la Aplicación

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

Plataforma Base y Herramientas

- Microsoft Windows: SO de desarrollo
- CVS Clarion EE: Sistema de Administración de la Configuración.

¹⁸ Desarrollo rápido de aplicaciones.

¹⁹ Lenguajes de cuarta generación, cuya característica principal es que basado en un modelo de datos posee generación automática de código fuente.

²⁰ Computer Aided Software Engineering, Ingeniería de Software Asistida por Computadora, son diversas aplicaciones informáticas o programas informáticos destinadas a aumentar el balance en el desarrollo de software reduciendo el costo

- Clarion 11: IDE de Desarrollo
- NetPort: Servidor Web.
- Enterprise Architect: Herramienta de modelado para realizar el modelo de casos de uso, diagrama de requerimientos y de secuencia.
- Gantt Project: Herramienta para realizar proyectos.

Framework de Aplicación y Reportes

Clarion 11 es el Framework utilizado para la capa de presentación de la aplicación y para el diseño de los reportes, esta herramienta es utilizada en la organización donde se realiza el caso de estudio, propietaria de la licencia.

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.

5.3.4 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 UML²¹. Luego se definió los límites del sistema y el alcance del mismo.

²¹ Lenguaje unificado de modelado.

Se observó que al ser un software herramienta, fue necesario tomar un rol de arquitecto de software para tener una idea clara de los requerimientos no funcionales del sistema, abordando primeramente los mismos.

Tomando el concepto del Scrum Daily Meeting sugerido [81], se decidió agregar dentro de la disciplina de Administración de Proyecto de AgEnD. La reunión diaria de quince minutos a primera hora de la mañana. Al no contar con un equipo de personas, que es lo usual en las reuniones diarias, se simuló esta práctica generando igualmente las actividades diarias, para los distintos roles. En un principio esta práctica fue dificultosa de entender, debido a que una sola persona debe asumir distintos roles; pero con el paso del tiempo, no solo desapareció esa dificultad, sino que, se incrementó la productividad en todos los roles definidos.

Como técnica de documentación, se utilizó el software trello, donde se generó una tarea por cada actividad, que contaba con: roles de usuario, las actividades realizadas el día anterior y las tareas planificadas para el día, aclarando los obstáculos posibles de presentarse en las actividades. Esta práctica permitió ir obteniendo un control y monitoreo constante sobre el progreso y los riesgos que se iban presentando.

Administración de la Configuración

Se utilizó como repositorio el mismo lenguaje de programación, ya que el Clarion 11 posee herramientas de control de versiones (CSV), se debe aclarar que fue usado 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, dado que no se contaba con el cliente, como especifica la metodología. Pero, de todas maneras, se utilizó al personal de la obra social de la Universidad Nacional de Misiones en el rol de cliente, para llevar a cabo esta práctica.

Enfoque en la Arquitectura

Una vez que comenzada 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, fue construir un sistema flexible y de simple mantenimiento, el cual pudiera incorporar cambios con facilidad y ser parametrizable.

Tomando como input²² 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 en una sola iteración, 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 III), 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 fomentará la integración continua. Con el rol de desarrollador, se trabajó en la implementación de los casos de uso y diariamente se incorporaba el trabajo realizado al repositorio, en este caso el CVS.

Una vez que estaba finalizado el release²³, se realizó pruebas de forma unitaria y de funcionalidad para verificar que el sistema cumplía con los requisitos relevados. Al fin de cada etapa, en el rol de tester, se registró la totalidad de lo construido y guiándose con los casos de prueba, se llevó a cabo el testing funcional. En el proyecto SCRisk no existieron problemas relacionados con la integración.

²² Entradas

²³ Versión de software entregable

Requerimientos funcionales

Los requerimientos funcionales se incluyen detalladamente dentro del modelo en forma de artefactos. A continuación se definen de manera general:

- Etapa de Análisis
 - Inventario de Activos: El sistema gestionara los activos, los usuarios podrán ingresar activos, sus elementos, la dependencia entre activos y sus relaciones entre ellos.
 - Propósitos y Objetivos: Se debe gestionar los proyectos, marcando los límites de ellos y se le asigna activos al mismo.
 - Equipo de Trabajo: Se asignarán recursos humanos al proyecto, para lo cual se debe gestionar, la persona, el rol que cumple y el equipo al cual pertenece.
 - Identificar Vulnerabilidades: se deberá cargar los activos críticos, identificando tipo de acceso al mismo y tipo de relación, además de generar la dependencia entre activos críticos y su tipo de dependencia.
 - Taxonomía: Por cada proyecto es necesario generar automáticamente la taxonomía de riesgos.
 - Declaración: Por cada riesgo se definen la condición que debe existir para que el riesgo se transforme en problema, la consecuencia que recibirá la organización si el riesgo se transforma en problema y el efecto que tendrá el problema en la organización.
 - Estimación de Probabilidad e impacto: Por cada riesgo se define probabilidad de ocurrencia del riesgo y se define el impacto que tendrá si el riesgo se ejecuta.
 - Exposición: Se calcula la exposición al riesgo por cada riesgo.
- Etapa de Gestión
 - Gestión: Se gestionan los riesgos. Es necesario describir la:
 - Información necesaria para manejar el riesgo
 - Responsable del control de riesgo y recursos necesarios
 - Generar un plan de acción dependiente de las salvaguardas

- Generar un plan de contingencias.
- Etapa de Control y Seguimiento
 - Generación del Plan: 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.
 - Gestión del Seguimiento: 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.
- Etapa de Incidencias
 - Carga del Incidente: El sistema deberá poseer un módulo para cargar los incidentes ocurridos. El mismo permitir el ingreso de cualquier usuario del sistema, en el cual se podrá cargar:
 - El Activo que tuvo el incidente
 - La Amenaza que se ejecutó.
 - El responsable inmediato de tomar el caso.
 - La fecha y hora del incidente
 - Breve observación de acción a tomar
 - Final del Incidente: 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.
- Informes
 - Informes de Incidentes: 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.

- Estadísticas de Incidentes: 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 y AGR - SE analizaron y gestionaron.
- Seguimiento: Se deberá prever un informe sobre los seguimientos terminados y los activos en actualmente. También se deberá prever la posibilidad de exportar el informe procesado.
- Parámetros del sistema
 - Activos: se deberán gestionar los datos de los tipos de activos, dimensiones, elementos y valoración.
 - Amenazas: se deberá parametrizar las amenazas, tipos de amenazas, amenazas por tipo de activo, amenazas por dimensión.
 - Salvaguardas: Las salvaguardas se gestionarán utilizando como base las salvaguardas descritas en la metodología Magerit V3 adaptando únicamente a las que se utilizan en una pequeña y mediana empresa.
 - Medida de Tiempo: Medida de tiempo a ser utilizada por el plan de acción en la cuales es necesario poseer características de unidad de tiempo y distancia entre días.
 - Fuente de Información: Es necesario gestionar las distintas dependencias de la organización en donde se tomará como fuente de información sobre los activos analizado.
 - Gestión de Usuarios del sistema: Se necesita gestionar los usuarios del sistema, con descripción, acceso por niveles y contraseña encriptada.
- Interfaz de usuario y Reglas de Negocio se explayan en detalle en el anexo III.

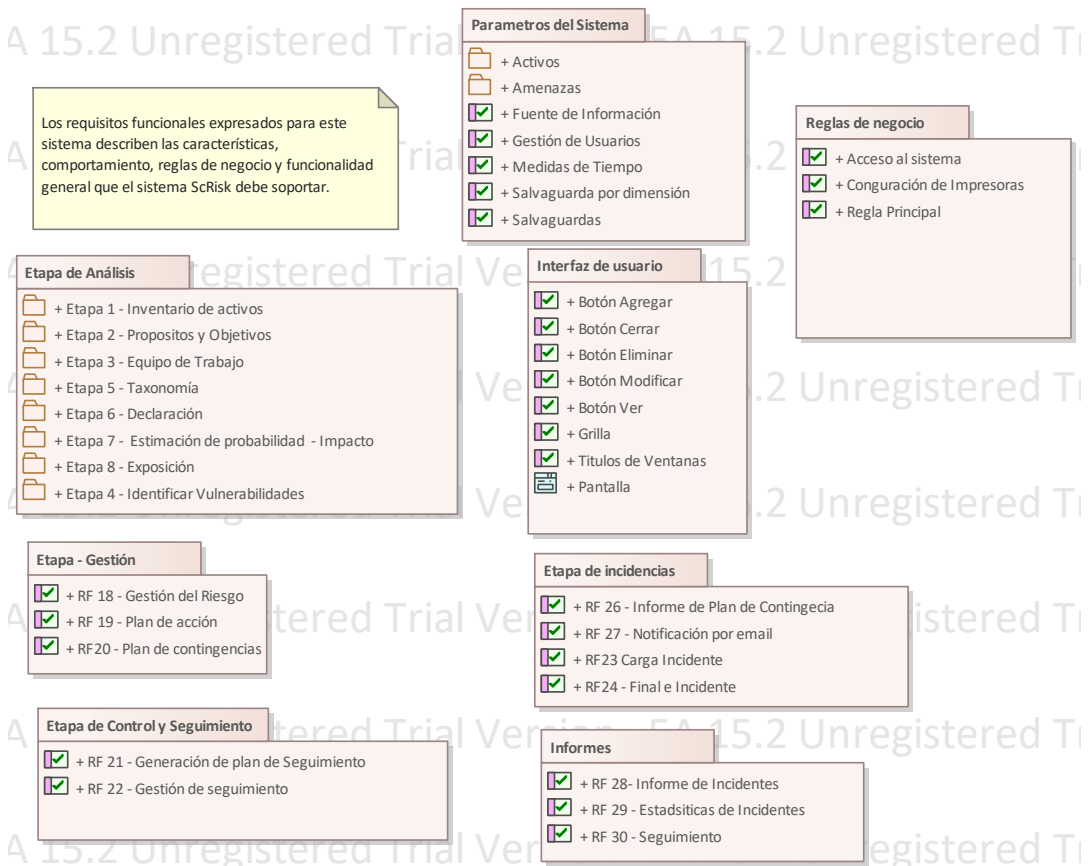


Figura 40 - Requisitos Funcionales

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 irán 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 III.

5.4 Resultados del Proyecto

Después de 3 meses de desarrollo, llega el hito de entrega del primer release V1.0, se implementó y se realizó ajustes solicitados por la organización, comprendido en mejorar la transferencia de conocimiento sobre los incidentes ocurridos, la misma concluye, con la puesta en práctica de las características AgEnD.

El producto final, al ser una herramienta asistente para la implementación del método RIC, se decidió generar un “estudio de caso” del método y la herramienta, en el Servicio Médicos Asistencial de la Universidad Nacional de Misiones (S.M.A.U.Na.N.), en donde se realizaron tres proyectos de AGR: Sala de Servidores, Recursos Humanos y Desarrollo Sistema SOL. Se testeó el sistema utilizando el

proyecto Desarrollo SOL 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 pondrá hincapié en este capítulo 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.

Como conclusión de este capítulo 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 caso para la prueba del método y la herramienta, artefactos para el análisis y desarrollo del mismo y encuesta realizada en la investigación).

Nota: El desarrollo está propuesto como prototipo, debido a que, por cuestiones de tiempo, únicamente se realizaron los proyectos de AGR antes descriptos como prueba de la herramienta.

Capítulo 6 - Experimentación

En este capítulo se desarrolla la experimentación del método RIC junto con la herramienta SCRisk abordando el total de sus etapas y analizando el comportamiento del mismo en un caso real, se realizaron 3 proyectos de análisis y gestión de riesgos, se relevaron los activos correspondientes a los proyectos y se ejecutó el método, logrando evidenciar sus resultados, y realizar una validación de expertos del método; en el anexo II se presentan en detalle la ejecución del proyecto “Desarrollo Sistema SOL” utilizando la herramienta SCRisk, como también la parametrización y configuración de la herramienta.

6.1 Lugar

Para lograr evaluar el sistema, y al no poseer un usuario final que solicitó el desarrollo del mismo, acorde a lo aprobado por el comité de trabajo final de la maestría, se autorizó realizar el caso de estudio y probar el método RIC y la herramienta SCRisk en el Servicio Médico Asistencial de la Universidad Nacional de Misiones.

6.2 Estado Actual de la Organización

El Servicio Médico Asistencial de la Universidad Nacional de Misiones (S.M.A.U.Na.M.), es la prestadora de salud de la Universidad Nacional de Misiones cuya función es gerenciar las prestaciones de salud del personal activo de la universidad. Cuenta con una casa central y 3 regionales distribuidas en la provincia de Misiones, la casa central ubicada en la calle Tucumán 2452 de la ciudad de Posadas y regionales en las ciudades de Oberá, Eldorado y Apóstoles, en la cual en su conjunto trabajan alrededor de 35 personas.

6.3 Entorno

Tecnológico

- Software: La empresa cuenta con desarrollo de software propio, conformados por 17 sistemas desarrollados en plataformas escritorio y

web, que gestionan todos los recursos de salud, en su mayoría los sistemas se encuentran centralizados en la casa central; utilizan un software enlatado para la gestión contable, y además utilizan software herramientas de uso de oficina (procesador de texto, planilla de cálculos),

- Equipamiento: En la sede central, posee una sala de servidores donde están instalados 4 servidores de datos para el uso de los sistemas, además cuenta con 40 computadores personales, para el total de su personal y servicios de auto gestión.
- Comunicación y Redes: En la sede central se cuenta con 2 servicios de internet de alta velocidad y cada sede cuenta con su propio servicio de conexión a internet; con respecto a las redes de datos, cada espacio de trabajo cuenta con una red LAN y la casa central y las sedes se comunican entre sí mediante una red VPN punto a punto dedicada.

6.4 Recursos Humanos

La empresa cuenta con dos personas en el planten informático de planta permanente, ambos poseen titulación académica habilitante siendo los dos analistas en sistemas de información graduados de la Universidad Nacional de Misiones, y cuenta con un profesional informático con título de Licenciado en Sistemas de Información que realiza el rol de encargado de IT que posee un contrato anual.

Caso de estudio

Para llevar a cabo la validación del método RIC se utilizó la herramienta prototipo en su versión beta, funcional, y es la versión que se muestra en esta unidad.

Proyectos

Se generaron tres proyectos sala de servidores, personal y desarrollo del sistema sol.

- Sala de Servidores: Proyecto que trata de resguardar los activos que están ubicados en la sala de servidores de la casa central, para asegurar la continuidad de las tareas que realizan.

- Personal: Trata sobre el personal informático de la organización, debido a que este, es el eje principal para el soporte, mantenimiento del equipamiento y desarrollo de software.
- Desarrollo Sistema SOL: El sistema SOL es un sistema de gestión de prácticas de salud automatizada, el cual provee de servicios de prácticas médicas y odontológicas en una plataforma online, mediante servicios web; la misma hoy día es el sistema con mayor importancia de servicio al afiliado que posee la obra social, el mismo está en constante desarrollo, implementando mejoras en formato de release.

Basando nuestro estudio de caso para validar el modelo, se utilizó el proyecto “Desarrollo SOL”, en donde se generó un análisis y gestión de riesgos utilizando en el personal informático de dicha organización, se simularon incidencias bajo la amenaza “Errores del Administrador” del activo “Cloud server principal” e informes que se detallan a continuación.

6.5 Capítulo R – Análisis, Gestión y seguimiento del riesgo

6.5.1 Etapa de Análisis

Para iniciar con el análisis del riesgo, como primer paso, se relevó la totalidad de los activos correspondientes al IT que posee la organización, y se cargaron al sistema, esta tarea, es valiosa debido a que la empresa cuenta con un catálogo relevado de todos sus activos tecnológicos. El catálogo de activos está 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 si el activo es crítico, para identificar la importancia que posee el activo en la organización.

Este proceso también abarca la identificación por activo, el tipo de activo, los elementos que posee, las dimensiones que abarca, fuente de información y dependencias.

La tarea fue realizada por el personal informático, y estableció una visión más concreta de la importancia de los activos, y que los mismos, por más que sean de la misma clase (Ej. Servidores) según su tipo, dimensión y elementos difieren en el valor que posee cada uno para la gestión de riesgos.

Se generaron los proyectos 3 y a cada uno se:

- Identificaron el propósito, objetivo y límites: Identificar el propósito de los proyectos, llevo a la discusión de la importancia del mismo, primeramente, se plantearon otros proyectos, pero a la hora de fijar su importancia y sus objetivos, los mismos no fueron preponderantes, lo cual se apreció que identificar el propósito y objetivo de cada proyecto, muestra la relevancia de cada uno.
- Activos por proyecto: al tener todos los activos relevados, la actividad no tuvo factores de dificultad.

En la fase Equipo de Trabajo, primeramente, se cargaron los parámetros de personas, rol y equipo de trabajo, luego se designaron el equipo de trabajo por cada proyecto, donde se definieron para cada persona, a que equipo de trabajo pertenecía en el proyecto y que rol ocupa en el proyecto.

Dentro de la fase de taxonomía, el sistema automáticamente, toma los activos de los proyectos, evalúa el tipo de activo al cual pertenece y busca en la base de conocimiento de amenazas, los registros coincidentes con estos tipos, y genera un informe clasificado y ordenado con la totalidad de amenazas o riesgos que posee cada activo.

Generar el informe de taxonomía duró unos pocos segundos, como muestra la figura 41, y como resultado presentó 60 amenazas registradas o riesgos encontrados para ese proyecto y sus activos, se observó la importancia del proceso, según el volumen de registros que muestra como resultante, en el caso de hacerlo de manera manual, tomaría mucho tiempo de trabajo.

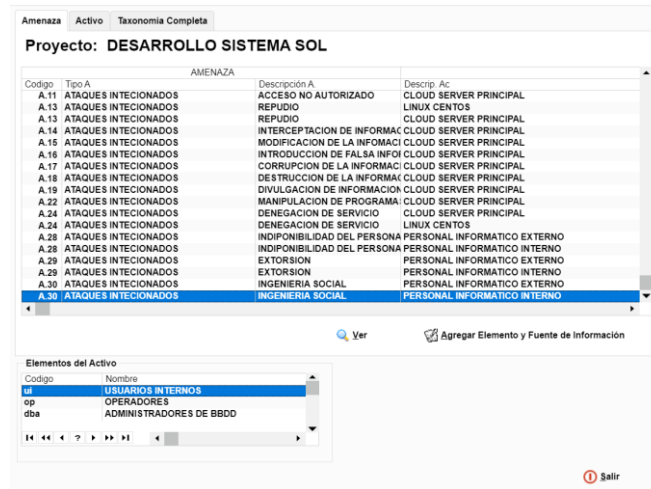


Figura 41 - Generación de Taxonomía

Luego se inició la fase de validación de vulnerabilidades, donde se pudo observar un informe de los activos críticos, se definió la ruta de acceso a los activos críticos, y se cargaron la información de las dependencias críticas.

Para la fase de declaración del riesgo, se unifican las amenazas por proyecto, en la cual se expresan la condición, la consecuencia y el efecto, en esta fase, pudimos observar la falta de claridad del personal al diferenciar la característica de consecuencia de efecto.

Para la fase de probabilidad e impacto se debieron cargar las tablas comparativas tanto de probabilidad de ocurrencia como de impacto para cada proyecto, se observó que se diferencian manejo de impacto por proyecto, pero no se observó diferencia en la probabilidad de ocurrencia por proyecto, utilizando la totalidad de los proyectos cargados la misma tabla comparativa.

Al finalizar la definición de las tablas comparativas se ejecutó el proceso denominado “Cálculo de probabilidad e impacto”, donde se registra el porcentaje de probabilidad y el valor del impacto por cada riesgo, como se puede apreciar en la figura 42.

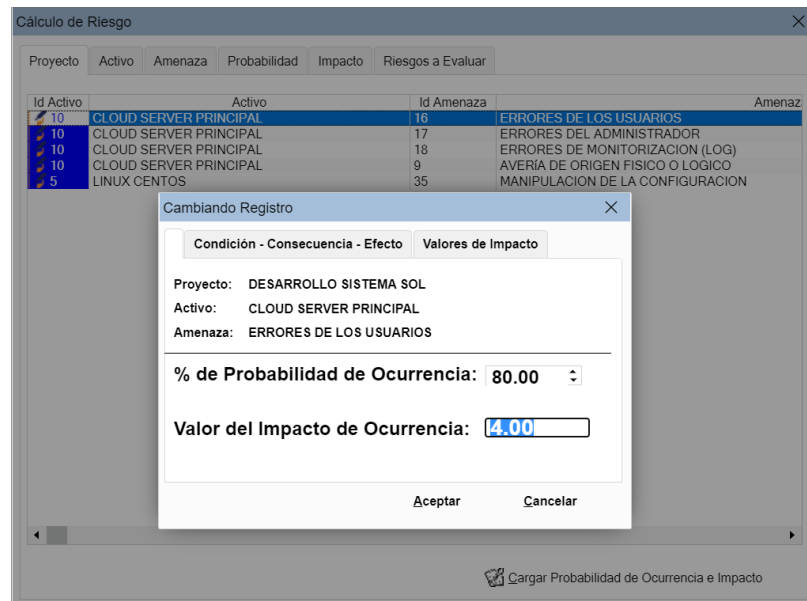


Figura 42 - Asignación de % Probabilidad e Impacto

Se incorpora el valor de la probabilidad real y el sistema calcula en base a la tabla comparativa de probabilidades para el proyecto calcula la probabilidad promedio.

Fase de Exposición, se ejecuta el proceso de exposición al riesgo, proceso que dura unos segundos y muestra los riesgos que deben ser gestionados.

6.5.2 Etapa de Gestión

La gestión de riesgos comienza con los riesgos que, como resultado del proceso de la fase de exposición, obtuvieron un valor positivo mayor a cero.

Por cada riesgo afectado a los proyectos se cargaron:

- Información necesaria para su gestión, la cual, el sistema presenta un listado de información de la base de conocimiento, y la opción de cargar una nueva fuente de información de ser necesaria.
- Responsable: personas responsables de la gestión del riesgo, listado de personas alojadas en la base de conocimiento.
- Recursos: Recursos necesarios para gestionar el riesgo, cada recurso puede ser utilizado por otros riesgos, se definió una observación específica a tener en cuenta por parte del recurso en el riesgo establecido.

Por cada riesgo expuesto, se cargaron las actividades del plan de acción, la herramienta ofrece un módulo de carga automática del plan de acción, la cual procesa el plan de acción provisto por Magerit, calculando, el riesgo y la dimensión del activo obteniendo como resultante un informe del plan de acción a realizar por cada riesgo.

Por el contrario, el plan de contingencia se tuvo que cargar por cada riesgo, el disparador, el responsable de la tarea y el plan de tareas, donde se divisó información relevante de cada uno de los pasos a seguir, como muestra la figura 43.

El formulario 'Insertando Registro' tiene un título con un botón de cerrar (X). Los campos incluyen: 'Id Contingencia:' con el valor 8; 'Paso:' con un menú desplegable en 1; 'Codigo' con un campo de texto y 'Nombre' con un campo de texto; 'Descripcion' con un área de texto grande; dos opciones de control con casillas de verificación: 'Realizar Control sobre la Contingencia' y 'Realizar Seguimiento sobre la Contingencia'; y 'Observacion' con un área de texto grande. En la parte inferior derecha hay botones 'Aceptar' y 'Cancelar'.

Figura 43 - Carga de incidencia

Finaliza la carga de los datos solicitados se da por finalizada la etapa de Gestión.

6.5.3 Etapa de Control y Seguimiento

En esta etapa se generó el plan de seguimiento, que consiste, en un proceso automático, que genera el plan de tareas a realizar por cada personal responsable del plan de acción y las tareas correspondientes. Luego del proceso se generó la agenda del personal, que muestra un plan de trabajo por fecha, en forma de listado en el que se carga por cada tarea el porcentaje de avance y observaciones si las tuviera.

6.6 Capítulo I – Gestión de Incidencias

6.6.1 Etapa de Incidencia

Para el caso de estudio del método y la herramienta, se simularon casos de problemas con los activos, sin identificar, si estos, estuvieron afectados en los proyectos de AGR definidos en este caso de estudio.

Para lo cual, se ejecutó el módulo de carga de incidencia, en la cual, se incluyó datos como ser, el activo, el responsable del activo, la amenaza, la fecha y hora del incidente y las acciones que se tomaron para resolver el problema. El módulo no presento problema en la gestión de los datos asignados, solo se observó, que la persona que carga la incidencia, debe tener conocimiento de la amenaza que generó la misma.

Una vez aceptada la carga, el sistema genera un informe donde muestra, si el activo en cuestión está incluido en un proyecto de AGR, y es gestionado o no; además muestra el plan de contingencias asignado a este riesgo.

Se observó en el panel principal del registro de incidencia, información que ayuda a la visualización del informe, como ser la posibilidad de filtrar la información por distintas características y exportar a distintos formatos de documentos.

Una vez finalizada la incidencia se ejecutó el módulo de “Finalización de incidencia” (figura 44), donde se muestra únicamente las incidencias activas; en las que se cargaron los datos solicitados; como ser una observación, si el plan de acción propuesto fue correcto, la fecha de corrección y si se actualizó el plan de ARG.

The screenshot shows a window titled 'Cambiar Registro (56)' with the following fields:

- Id Incidente:** 56
- Activo:** 5
- LINUX CENTOS**
- Amenaza:** 29
- DIVULGACION DE INFORMACION**
- Responsable:** 1
- SERGIO CABALLERO**
- Observacion:** (Empty text area)
- ☒ **El incidente se Solucionó Correctamente**
- FECHA FIN:** (Empty date field)
- ☐ **Actualizó el AGR?**
- Aceptar** and **Cancelar** buttons.

Figura 44 - Finalización de Incidencia

6.7 Capítulo C – Gestión del Conocimiento

6.7.1 Etapas Conocimiento Explícito y Tácito

La base de conocimiento está distribuida por todo el sistema, tanto el conocimiento explícito, que incluyen los informes de seguimiento de incidencias, como también los informes de estadísticas, ver la figura 45:

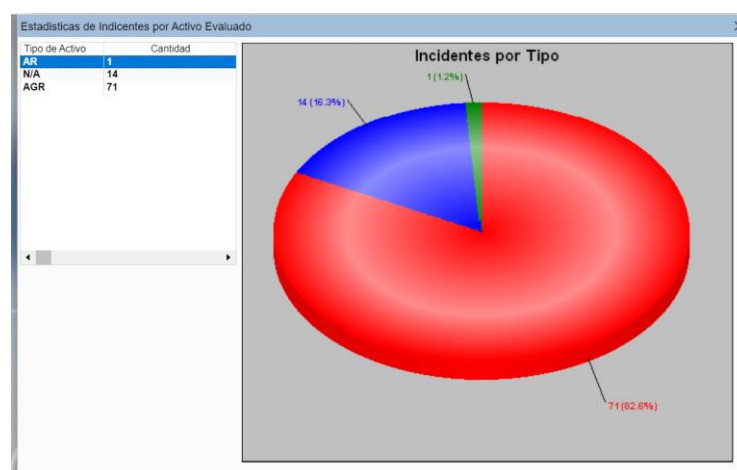


Figura 45 - Informe estadístico de incidencia por activo gestionado

Y por otro lado el conocimiento tácito, que se visualiza en todos los formularios e informes, como ser, planes de acción, plan de contingencias y resolución de incidencias, en las que el usuario tiene la opción de cargar información

en texto libre, el cual cumple con lo definido como conocimiento tácito[59]. La herramienta no cuenta, con el manejo e identificación de este tipo de conocimiento.

6.8 Enseñanza

Al experimentar el método y la herramienta, se pudo observar algunas características de las cuales no se esperaban, como ser:

Característica	Descripción	Efecto
POSITIVO	Relevamiento de Activos e identificación de tipos y dimensiones	Se notó una valoración de los activos, y mayor conocimiento en base a su tipo y dimensión. Se utilizó la experimentación para generar un listado de activos tecnológicos.
POSITIVO	Definición de proyectos	Se observó la importancia de definir el propósito y objetivo del proyecto. Esto llevó al personal a reunirse con la gerencia e informar la importancia del AGR.
POSITIVO	Generación automática de Taxonomía	La herramienta genera automáticamente la taxonomía de los riesgos por proyecto, ahorrando tiempo de trabajo del personal.
NEGATIVO	Definición de consecuencia y efecto en la descripción del riesgo.	La definición de la consecuencia y el efecto, trajo muchas dudas al personal, por no tener una clara visión de la diferencia de los conceptos.
NEGATIVO	Tablas de comparación de probabilidad por proyecto	Se observó que diferenciar las tablas comparativas de probabilidad de ocurrencia por proyecto es innecesaria, debido a que dicha tabla se puede utilizar como referencia para cualquier proyecto.

POSITIVO	Fuente de información de la gestión de Riesgo	Establecer un listado de fuentes de información que se puedan utilizar en la declaración de cualquier riesgo, esto minimiza la repetición del dato.
POSITIVO	Generación de plan de acción automático	Generar un plan de acción automático, brinda ahorro de trabajo al personal y minimiza la posibilidad de saltar algún paso en la confección del mismo.
NEGATIVO	Identificar la amenaza en la incidencia	En la gestión de incidencia, se solicita identificar la amenaza por la cual se generó la misma, y el personal actuante puede no tener conocimiento de las amenazas que pueden afectar a los activos.

Tabla 41 - Enseñanzas de la experimentación

En la experimentación hemos observado algunas falencias por parte del método que se deberán discutir en futuras versiones, pero, observamos características positivas que generan tanto el método como la herramienta que proveen de valor a la organización, ahorra trabajo del personal, y visualizan la importancia de los activos y del proceso de gestión de riesgos.

6.9 Validación del modelo

Para la validación del modelo, se utilizó el método basado en juicios de expertos, utilizando como base la escala de tipo likert²⁴ en el cual se generó una encuesta basada preguntas.[82]

A partir de la selección de cuatro expertos, se entregó un email con la invitación personalizada, explicando los objetivos de la prueba, el propósito de la validación y demás especificaciones para contextualizar a los jueces; así como se adjuntaron las 4

²⁴ Escala psicométrica comúnmente utilizada en las investigaciones de ciencias sociales que emplean cuestionarios.

preguntas y la unidad del método RIC, el tiempo límite de respuesta fue un lapso de una semana[83].

Se realizó el método denominado “agregación individual”[84], en la que se obtiene la información de cada uno de los expertos, de manera individual, sin que éstos se encuentren en contacto, de forma anónima y confidencial, por lo cual, los mismo fueron seleccionados de distintas industrias de las tecnologías informáticas.

Las preguntas a contestar poseían las mismas posibles respuestas

1. No cumple con el criterio
2. Bajo Nivel
3. Medio Nivel
4. Alto Nivel

Y los parámetros a evaluar al estudio del método fueron:

- Coherencia
- Relevancia
- Claridad
- Suficiencia

Los resultados obtenidos fueron los siguientes:

<u>Coherencia</u>	<u>Respuesta</u>
No cumple con el criterio	0
Bajo Nivel	0
Medio Nivel	3
Alto Nivel	1

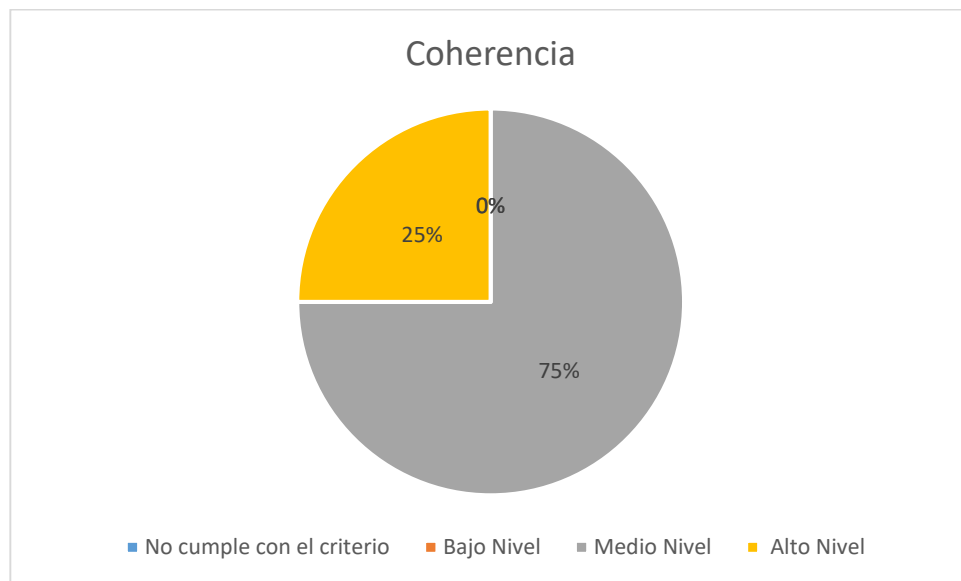


Figura 46 - Respuesta de coherencia

<u>Relevancia</u>	<u>Respuesta</u>
No cumple con el criterio	0
Bajo Nivel	0
Medio Nivel	2
Alto Nivel	2

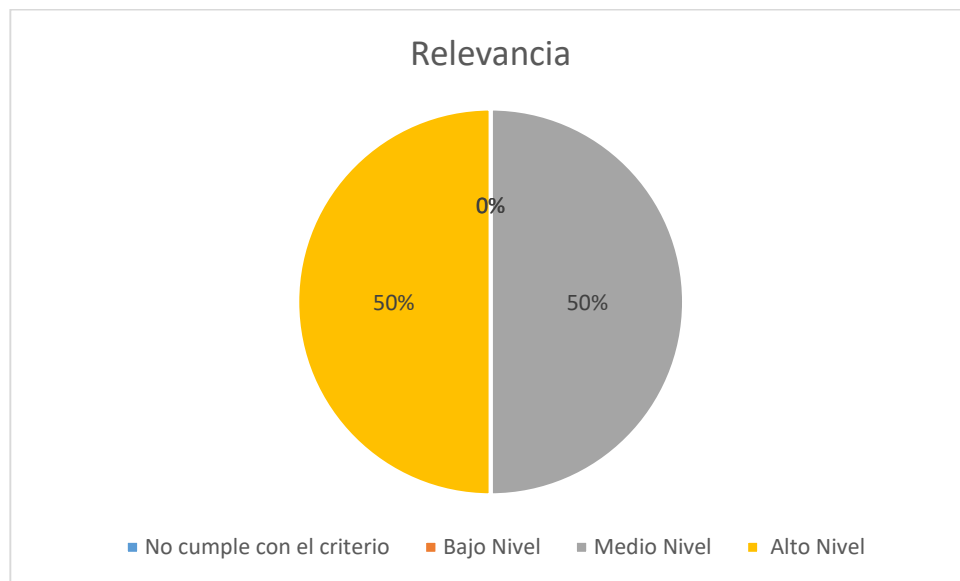


Figura 47 - Respuesta de relevancia

<u>Claridad</u>	<u>Respuesta</u>
No cumple con el criterio	0
Bajo Nivel	0
Medio Nivel	3
Alto Nivel	1

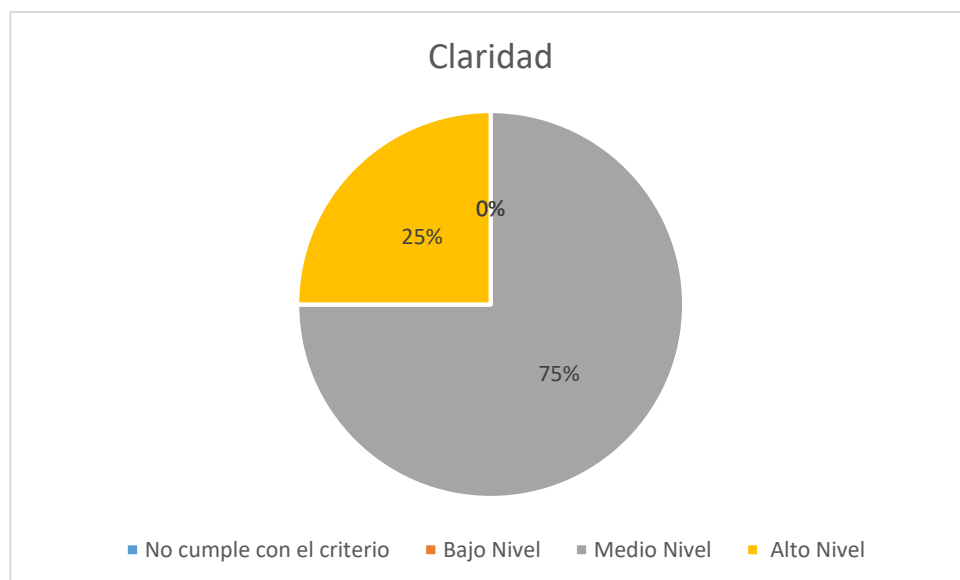


Figura 48 - Respuesta de claridad

<u>Suficiencia</u>	<u>Respuesta</u>
No cumple con el criterio	0
Bajo Nivel	0
Medio Nivel	1
Alto Nivel	3

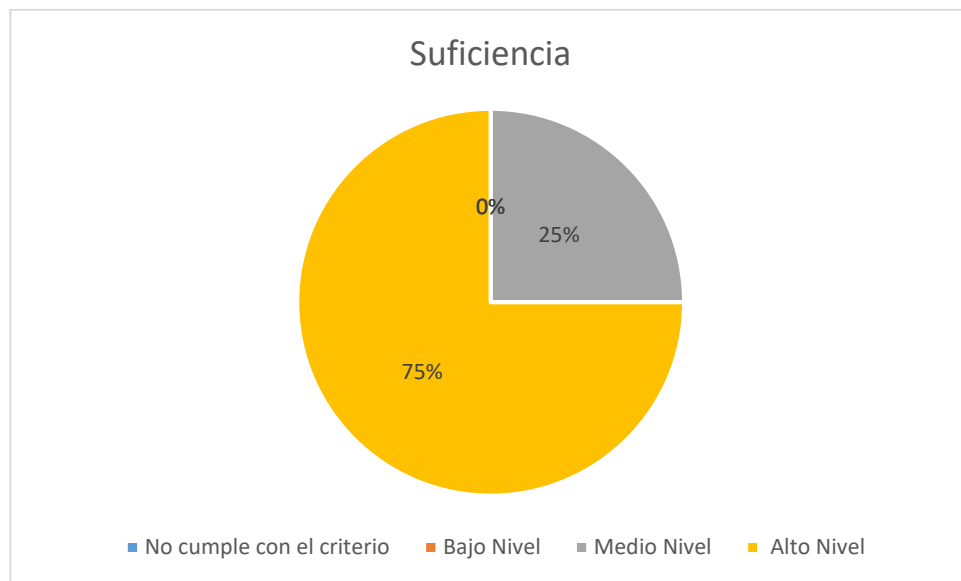


Figura 49 - Respuesta de suficiencia

Podemos concluir que el método fue validado por expertos.

6.10 Conclusión

Una vez probada la herramienta en su totalidad y su constatación de cumplimiento del método propuesto y de la validación del modelo, utilizando método de juicio de expertos, se llega a la siguiente conclusión: El método RIC y la herramienta, cumple con los requerimientos de la organización en la cual se generó la experimentación. El caso de estudio del proyecto de análisis y gestión de riesgos fue generado, controlado y seguido en forma satisfactoria, la gestión de incidentes e informes requeridos cumplieron con las descriptas por el método.

El proyecto de AGR e incidencias fue ejecutado en su totalidad por el personal informático de la institución, el cual no posee una profunda experiencia en gestión de riesgos.

Capítulo 7 - Conclusión del trabajo Futuras líneas de investigación

7.1 Conclusión

Se pudo observar en la bibliografía relevada y en otros trabajos de investigación, que una gran parte de 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 método, es decir, integrar características de diferentes metodologías, y lo más destacado es la posibilidad de ser utilizada por cualquier tipo organización pyme.

Métodos de AGR hay muchos, pero a diferencia de los relevados, este método busca la agilidad y adaptabilidad de las actividades. Presenta por cada proceso y subproceso un conjunto de formularios guía para su implementación, e 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.

No es suficiente, para gestionar la TI de la organización, solo la implementación de un método de AGR formal, por ello, se propone una instancia de generación de tareas de control de los riesgos a gestionar, sumando a ello una agenda de actividades de control.

Por otro lado, la realidad nos demuestra que ocurren incidentes en los activos de TI, pero no todos son gestionados, por ese motivo se creó la fase de incidencias, que permite una gestión de la totalidad de los incidentes de los activos, resolviendo e informando ese incidente; teniendo en cuenta que alguno de ellos forman parte de un proyecto de AGR, otros fueron analizados pero no gestionados y existen activos que no se incluyen en proyecto alguno, el método clasifica los activos y riesgos que participaron en el incidente.

El método clasifica los activos y riesgos que participaron en el incidente, cuando un activo tiene un incidente y el riesgo ejecutado es gestionado, el módulo propone un análisis del plan de contingencia, para constatar que es correcto, y de no serlo, propone ajustar dicho plan. Cuando No es gestionado, aumenta la probabilidad

de ocurrencia del riesgo ejecutado. Además, se suma a la base de conocimiento, el plan de contingencia o tareas ejecutadas para solucionar la incidencia, que puede ser utilizada en proyectos de análisis y gestión de riesgos futuros, restando carga de trabajo al recurso humano.

Comunicar los riesgos que contemplan los activos de TI mejora el conocimiento de valor de estos; que la comunicación sea gestionada y que la información se establezca como activo de la organización, es un valor que busca hoy toda pyme.

A fin de cumplir con la totalidad de los objetivos propuestos e independizar el método de la herramienta, facilitando el trabajo de los auditores informáticas, el método incluye formularios.

El desarrollo de SCRisk, herramienta prototipo que abre paso a la automatización de procesos, genera una base de conocimientos y un proceso de aprendizaje, que se podrá ampliar en futuras líneas de investigación.

Generar un caso de estudio real, ayudó a validar el modelo, poniendo a prueba RIC y SCRisk, el método y la herramienta, en instancias tempranas sugieren aspectos de formalidad, practicidad, facilidad, automatización e información para la optimización del modelo.

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

7.2 Futuras líneas de investigación

Inicialmente el método y la herramienta creados para este Trabajo Final de Maestría, se enmarcan en un trabajo de investigación aplicada.

Además, está pensado, utilizar la herramienta en el Servicio Médico Asistencial de la Universidad Nacional de Misiones, que brindará una retro

alimentación del uso del método y de la herramienta en entornos y situaciones reales, probablemente se dará origen a nuevas propuestas de ampliación de ambos.

Antes de esto, se expone 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 identifica el método, se deberá generar un procedimiento para que el mismo adquiera la capacidad de aprender de dicha información. Esto permitiría incorporar al plan de riesgos, el conocimiento de nuevos incidentes y su plan de contingencia, además de la información sobre la ocurrencia y la importancia de los activos que tuvieron dichos incidentes.
- Adaptar la herramienta utilizando un lenguaje de programación y motor de base de datos con licencia GNU²⁵.
- Mejorar 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, y avisos por sms.

²⁵ Licencia pública de distribución de software libre.

Capítulo 8 - Referencia Bibliográfica

8.1 Bibliografía

En este capítulo se detallan la bibliografía en formato IEEE empleadas durante el desarrollo del presente trabajo.

8.2 Referencias Bibliográficas

- [1] H. Tipton, M. Nozaki, B. Pilewski, and C. Pilewski, "CERT Resilience Management Model," *Inf. Secur. Manag. Handbook, Sixth Ed. Vol. 6*, no. February, pp. 135–152, 2012, doi: 10.1201/b11802-17.
- [2] R. P. Higuera and Y. Y. Haimes, "Software Risk Management," 1996, Accessed: Mar. 17, 2018. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/1996_005_001_41753.pdf.
- [3] R. N. Charette, K. M. G. Adams, and M. B. White, "Managing risk in software maintenance," *IEEE Softw.*, vol. 14, no. 3, pp. 43–50, 1997, doi: 10.1109/52.589232.
- [4] Secretaría General de Administración Digital, "PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información." https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wq0hoLOvG01 (accessed Mar. 17, 2018).
- [5] Jessica García Hanson and Paola Salazar Escobar, "Métodos de Administración y Evaluación de Riesgos," Accessed: Sep. 27, 2019. [Online]. Available: http://repositorio.uchile.cl/tesis/uchile/2005/garcia_j2/sources/garcia_j2.pdf.
- [6] S. D. Maniasi, "Identificación de Riesgos de Proyectos de Software en Base a Taxonomías," Instituto Tecnológico de Buenos Aires, 2005.
- [7] S. Maniasi, P. Britos, and R. García-Martínez Global, "A Taxonomy-Based Model for Identifying Risks," *Proc. V Ibero-American Symp. Softw. Eng.*, no. March, pp. 13–18, 2006.
- [8] T. F. Hammer and L. Rosenberg, "Continuous Risk Management at NASA," Feb. 1999, Accessed: Sep. 06, 2019. [Online]. Available: <https://ntrs.nasa.gov/search.jsp?R=19990064616>.
- [9] B. W. Boehm, "Software Risk Management : Principles and Practices," no. January, 1991.

- [10] B. P. Gallagher, T. Note, S. Engineering, and P. Management, "Interpreting Capability Maturity Model ® Integration (CMMI)," *Integr. Vlsi J.*, no. April, 2002.
- [11] M. J. Carr and S. L. Konda, "Taxonomy-Based Risk Identification," no. June, 1993.
- [12] J. J. Cebula and L. R. Young, "A Taxonomy of Operational Cyber Security Risks," *Carnegie-Mellon Univ Pittsburgh Pa Softw. Eng. Inst.*, no. December, pp. 1–47, 2010.
- [13] SEI Administrative Agent, "CMMI® for Development, Version 1.3," Accessed: Sep. 27, 2019. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf.
- [14] R. Bertone, P. Thomas, D. Taquias, and S. Pardo, "Herramienta para la Gestión de Riesgos en Proyectos de Software," Accessed: Mar. 17, 2018. [Online]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/19289/Documento_completo.pdf?sequence=1.
- [15] Microsoft, "Microsoft Solutions Framework MSF Risk Management Discipline v.1.1," no. May, 2004, [Online]. Available: <http://www.microsoft.com/en-us/download/details.aspx?id=721>.
- [16] E. Australiano, "Adminstracion De Riesgos," 1999.
- [17] P. Con, S. D. E. Tecnología, and D. E. L. A. Información, "Aplicación del risk management en la dirección y gestión de proyectos con soporte de tecnología de la información," pp. 1446–1455.
- [18] F. J. oro López, *Administración de proyectos de informática*. 2013.
- [19] P. P. M. Institute, *La guía de los fundamentos para la dirección de proyectos (Guía del PMBOK)*. 2017.
- [20] R. T. Futrell, D. F. Shafer, and L. I. Safer, *Quality Software Project Management*. 2002.
- [21] N. A. Hashim, Z. Z. Abidin, N. A. Zakaria, R. Ahmad, and A. P. Puvanasvaran, "Risk assessment method for insider threats in cyber security: A review," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 126–130, 2018, doi: 10.14569/ijacsa.2018.091119.
- [22] R. J. Chapman, "The effectiveness of working group risk identification and assessment techniques," *Int. J. Proj. Manag.*, 1998, doi: 10.1016/S0263-7863(98)00015-5.

- [23] J. Ropponen and K. Lyytinen, “Components of software development risk: how to address them? A project manager survey,” *IEEE Trans. Softw. Eng.*, vol. 26, no. 2, pp. 98–112, 2000, doi: 10.1109/32.841112.
- [24] “Taxonomía de riesgo SEI. | Descargar diagrama científico.” https://www.researchgate.net/figure/SEI-risk-taxonomy_fig3_288557968 (accessed Dec. 01, 2020).
- [25] P. Hantos, “A Practical Approach to Quantifying Risk Evaluation Results,” no. February, pp. 15–19, 2009.
- [26] M. A. Amutio Gómez, *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*. 2012.
- [27] G. M. A. Amutio, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de Elementos*. 2012.
- [28] Consejo Superior de Administración Electrónica, *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas*. 2012.
- [29] O. Páez Obando, “Aplicación de la norama OCTAVE-S en la Empresa Pirámide Digital CIA. LTDA,” PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, 2013.
- [30] J. B. Lara, “Análisis de las metodologías de gestión de riesgos para garantizar la continuidad del negocio en el departamento de tecnologías de la información en la Corporación,” 2016.
- [31] J. C. G. Porras, S. C. H. Pastor, and M. De, “Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú,” UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS, 2019.
- [32] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, “OCTAVE-S Implementation Guide,” *Softw. Eng. Inst.*, vol. 1, no. V 1.0, pp. 1–63, 2005.
- [33] D. Lock and D. Lock, “Managing project risk,” *Proj. Manag.*, pp. 573–591, 2018, doi: 10.4324/9781315199764-24.
- [34] “La ingeniería del Software.” Accessed: Jul. 29, 2019. [Online]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/4055/3_-_La_ingenieria_de_software.pdf?sequence=7&isAllowed=y.
- [35] Project Management Institute., *A guide to the project management body of knowledge (PMBOK guide)*. Project Management Institute, 2004.
- [36] J. R. Rodriguez, *Gestión de proyectos informáticos: métodos, herramientas y casos*. UOC, 2005.

- [37] S. M. Artiles Visbal and M. Pumar Hernández, “Gestión del Conocimiento: Elementos para Mejorar el Proceso de Identificación en las Organizaciones,” *Knowl. Manag. Elem. Improv. Identif. Process Organ.*, vol. 1, no. 2, pp. 32–52, 2013, [Online]. Available: http://www.upo.es/revistas/index.php/gecontec/article/download/744/pdf_3dDoc.csic.es:8080s/revistas/index.php/gecontec/article/download/744/pdf_3.
- [38] C. Lochmüller, “Información, Conocimiento y Desarrollo Económico,” Accessed: Mar. 18, 2019. [Online]. Available: <http://es.wikipedia.org/wiki/Conocimiento>.
- [39] I. Nonaka, “La empresa creadora de conocimiento,” 2007. Accessed: Jun. 08, 2019. [Online]. Available: https://s3.amazonaws.com/academia.edu.documents/35652193/Nonaka.pdf?response-content-disposition=inline%3Bfilename%3DLaempresacreadorade_conocimiento.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190608%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20190608T143703Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=85a8ba00ec272ded9fde7fe848536bae1f81a43d95cae95ea57ad1198dff1432.
- [40] M. Yadira, N. Lahaba, L. Yasneidy, D. Río López, D. Maria, and D. C. Villardefranco, “Elementos para la identificación del conocimiento en especialidades Universitarias Cubanas.” Accessed: Jun. 08, 2019. [Online]. Available: [http://eprints.rclis.org/19762/2/Identificacion del conocimiento.pdf](http://eprints.rclis.org/19762/2/Identificacion%20del%20conocimiento.pdf).
- [41] M. León Santos, C. G. Ponjuán Dante, and M. Rodríguez Calvo, “Procesos estratégicos de la gestión del conocimiento,” *Acimed*, vol. 14, no. 2, 2006.
- [42] Ph. D. en Educacion Miguel Angel Soto Vidal, “Modelos de Gestión del Conocimiento (Dirigir en la complejidad).” <https://es.calameo.com/read/0002321121f60193015cb> (accessed Mar. 16, 2019).
- [43] E. M. Morales Morgado, *Gestión del conocimiento en sistemas "e-learning"; basado en objetos de aprendizaje, cualitativa y pedagógicamente definidos*. Ediciones Universidad de Salamanca, 2010.
- [44] M. Monagas-Docasal, *Ingeniería Industrial.*, vol. 33, no. 2. Instituto Superior Politcnico Jose Antonio Echeverria (Cujae), 2010.
- [45] A. Kok, “Intellectual Capital Management as Part of Knowledge Management Initiatives at Institutions of Higher Learning,” *Electron. J. Knowl. Manag.*, vol. 5, no. 2, pp. 181–192, 2007, doi: 10.1016/j.expneurol.2007.11.025.
- [46] A. S. Thomas, *La nueva riqueza de las organizaciones, el Capital Int.*

Granica, 1998.

- [47] A. Barragán Ocaña, “An approach to taxonomy of knowledge management models,” *Intang. Cap.*, vol. 5, no. 1, pp. 65–101, 2009, doi: 10.3926/ic.2009.v5n1.p65-101.
- [48] J. Ventura Victoria, *Análisis estratégico de la empresa*. Paraninfo Cengage Learning, 2008.
- [49] C. W. Choo, *The Knowing Organization: How Organizations Use Information to Construct Meaning, Create Knowledge, and Make Decisions*. 2007.
- [50] N. L. Pons, Y. P. Pérez, E. R. Stiven, and L. P. Quintero, “Diseño de un modelo de gestión del conocimiento para mejorar el desarrollo de equipos de proyectos informáticos,” *Rev. Esp. Doc. Cient.*, vol. 37, no. 2, pp. 1–14, 2014, doi: 10.3989/redc.2014.2.1036.
- [51] “Modelo de Gestión del Conocimiento de KPMG CONSULTING – Liderazgo y Gestion de Personas.”
<https://luisbringas.wordpress.com/2011/08/30/modelo-de-gestion-del-conocimiento-de-kpmg-consulting/> (accessed Oct. 03, 2019).
- [52] V. G. A. G. Gerardo Gabriel Alfaro Calderón, “Modelo de gestión del conocimiento para la pequeña y mediana empresa,” *Sotavento MBA*, vol. unknown, no. 20, pp. 8–21, 2012.
- [53] T. M. S. ARIAS, “Propuesta de un Modelo De Gestión De Conocimiento para una ips Pública De I Nivel de atención establecida en el Municipio De Togüí (Boyacá),” 2018. doi: 10.1017/CBO9781107415324.004.
- [54] C. Estrat, “La Gestión del Conocimiento : Modelos de comprensión y definiciones,” vol. 2, no. 2, 2015.
- [55] F. J. R. P. C. Tomer, *Intangible capital.*, vol. 9, no. 1. Universitat Politècnica de Catalunya, 2013.
- [56] A. Katia; Herrera Lemus, Katy; Losada Trabada, *Revista de investigaciones políticas y sociológicas : RIPS.*, vol. 12, no. 1. Servicio de Publicacions da Universidade de Santiago de Compostela, 2000.
- [57] OECD, “Resumen Medición de la gestión de conocimientos en las empresas: primeros resultados Overview Measuring Knowledge Management in the Business Sector: First Steps Spanish translation,” p. 2, 2004.
- [58] M. Henao-cala, A. C. Diez, A. Cecilia, and D. Gaviria, “Beatriz Uribe Ochoa 2,” no. August 2016, 2017.
- [59] F. Peris, M. Lloria, and M. Méndez, “Creación de conocimiento y diseño de organizaciones : equidad , confianza y objetivos compartidos , como reto de la

- gestión del conocimiento.,” *Cuad. CC. EE. y EE*, vol. 43, pp. 41–56, 2002.
- [60] K. M. Wiig, “Integrating intellectual capital and knowledge management,” *Long Range Plann.*, vol. 30, no. 3, pp. 399–405, 2003, doi: 10.1016/s0024-6301(97)90256-9.
- [61] P. . P. F. J. Ordóñez de Pablos, *Investigaciones Europeas de Dirección y Economía de la Empresa.*, vol. 11, no. 1. Academia Europea de Dirección y Economía de la Empresa, 2005.
- [62] A. J. Pérez de Miguel, “Hacia el Índice de Conocimiento Roto: Introducción a los coeficientes de rotura de conocimiento,” 2006, Accessed: Jun. 01, 2019. [Online]. Available: <http://hdl.handle.net/10366/75207>.
- [63] R. J. Castello, *Auditoría en entornos informáticos*. 2006.
- [64] E. Sweet, “Information systems auditing: tools and techniques,” *ISACA J.*, 2016, [Online]. Available: https://www.isaca.org/COBIT/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.pdf.
- [65] Isaca, *COBIT 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. 2011.
- [66] “Un vistazo general de COBIT 5 for Risk,” 2013.
- [67] “COBIT 5[1] ‘COBIT 5 for Risk—A Powerful Tool for Risk Management.’ [Online]. Available: <http://www.isaca.org/COBIT/focus/Pages/cobit-5-for-risk-a-powerful-tool-for-risk-management.aspx>. [Accessed: 15-Jan-2020]. for Risk—A Powerful Tool for Risk Management.” <http://www.isaca.org/COBIT/focus/Pages/cobit-5-for-risk-a-powerful-tool-for-risk-management.aspx> (accessed Jan. 15, 2020).
- [68] “Cloud Risk—10 Principles and a Framework for Assessment.” <https://www.isaca.org/Journal/archives/2012/Volume-5/Pages/Cloud-Risk-10-Principles-and-a-Framework-for-Assessment.aspx> (accessed Jan. 15, 2020).
- [69] O. Akinrolabu, S. New, and A. Martin, “Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study,” *Proc. - 6th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2019 5th IEEE Int. Conf. Edge Comput. Scalable Cloud, EdgeCom 2019*, pp. 81–88, 2019, doi: 10.1109/CSCloud/EdgeCom.2019.00-14.
- [70] E. Pineda Marín, “Diseño de un sistema de costos para pymes,” *Panorama*, vol. 2, no. 4, pp. 18–35, 2013, doi: 10.15765/pnrm.v2i4.261.
- [71] P. Kulik and C. Weber, “Software Risk Management Practices - 2001 Software Risk Management Practices – 2001 Software Risk Management Practices - 2001,” vol. 0484, no. August, pp. 1–7, 2001.
-

- [72] J. Kontio, “Konemiehentie 2 at the Helsinki University of Technology on the 28 th of,” 2001.
- [73] A. Syalim, Y. Hori, and K. Sakurai, “Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft’s security management guide,” *Proc. - Int. Conf. Availability, Reliab. Secur. ARES 2009*, pp. 726–731, 2009, doi: 10.1109/ARES.2009.75.
- [74] N. H. Alemán and C. Rodríguez Barrera, “Vista de Metodologías para el análisis de riesgos en los sgsi | Publicaciones e Investigación.” <https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874> (accessed Apr. 15, 2021).
- [75] D. Boundy, “A taxonomy of programmers.,” *ACM SIGSOFT Softw. Eng. Notes*, vol. 16, no. 4, pp. 23–30, 1991, doi: 10.1145/122552.122553.
- [76] S. D. Caballero, “Un nuevo método integrando la metodología SEI y Magerit2,” Universidad Nacional de Misiones, 2010. Accessed: May. 19, 2021. [Online]. Available: https://www.fceqyn.unam.edu.ar/siteapos/wp-content/uploads/2020/03/AGR-Sergio_Caballero.pdf.
- [77] H. D. Kuna, S. Caballero, S. E. Jaroszczuk, and M. J. Miranda, “Plan de riesgos para la implementación, desarrollo y mantenimiento de componentes de web 2.0 en bibliotecas, caso de estudio en una biblioteca especializada,” 2008, Accessed: Mar. 17, 2018. [Online]. Available: <http://sedici.unlp.edu.ar/handle/10915/48365>.
- [78] Consejo Superior de Administración Electrónica - Magerit Libro II, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II - Catálogo de Elementos,” pp. 1–75, 2012, [Online]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY.
- [79] M. C. Fenema, C. V. Flores, M. V. Poliche, J. P. Moreno, M. S. Molina, and E. Lobo, “La gestión del conocimientos en las organizaciones,” Jun. 2013, Accessed: Sep. 27, 2018. [Online]. Available: <http://sedici.unlp.edu.ar/handle/10915/27375>.
- [80] S. M. Hernán, “Diseño de una Metodología Ágil de Desarrollo de Software .,” 2004.
- [81] M. A. Korimbocus, T. Singh Towokul, and S. D. Nagowah, “Scrum Meeting Tool for Knowledge Capture and Sharing,” *2nd Int. Conf. Next Gener. Comput. Appl. 2019, NextComp 2019 - Proc.*, pp. 19–24, 2019, doi: 10.1109/NEXTCOMP.2019.8883672.
- [82] I. Pedrosa, J. Suárez-Álvarez, and E. García-Cueto, “Evidencias sobre la

validez de contenido: Avances Teóricos y Métodos para su estimación.”
<http://dx.doi.org/10.5944/ap.10.2.11820> (accessed Nov. 25, 2020).

- [83] L. Aidé, G. Alarcón, J. Arturo, B. Trápaga, and R. E. Navarro, “Validez de contenido por juicio de expertos: propuesta de una herramienta virtual Content validity by experts judgment: Proposal for a virtual tool,” 2017, doi: 10.32870/Ap.v9n2.993.
- [84] J. Cabero and M. del C. Llorente, “Aplicación de juicio de experto como técnica de evaluación de las TIC,” *Rev. Tecnol. Inf. y Comun. en Educ.*, vol. 7, no. 2, pp. 11–22, 2013, [Online]. Available: <http://www.mriuc.bc.uc.edu.ve/bitstream/123456789/1175/1/art01.pdf>.
- [85] “ISOWin: Los Activos de Información en la norma ISO 27001 2017.” <https://isowin.org/blog/activos-ISO-27001/> (accessed May 11, 2021).

Anexo I - Aspectos Particulares del Software y Estudio de Caso Software SCRisk

Aspectos particulares del sistema RIC

- I. Ingreso al sistema: El sistema contiene un panel de ingreso, en el cual se deberá ingresar el usuario y contraseña asignados. Únicamente ingresarán los usuarios autorizados.
- II. Parámetros Iniciales: Trata sobre los parámetros generales. Estos deben estar cargados previamente para lograr 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 dimensiones que posee un activo, y son las características principales en donde se ejecutan las salvaguardas o planes de contingencias.
 - d. Valoración: Trata sobre el valor de importancia que se le asigna al activo. Dicho valor dimensiona al activo, y se utiliza en la evaluación cuando el riesgo se transforma en una pérdida para la empresa o que su funcionamiento no sea el esperado.
 - e. Tipo de Amenazas: Trata sobre los grupos en donde se enmarcan las amenazas o riesgos.
 - f. Amenazas: Riesgos que corren los activos, a cada amenaza se agrupará dentro de un tipo de amenaza.

- g. Salvaguardas: Trata sobre las tareas detectivas que deben poseer los activos para tratar que los riesgos no se trasformen en un problema. Se asignará a las salvaguardas las etapas del ciclo de vida en donde es importante; si posee seguimiento y control agregado, se parametriza el tiempo seguimiento de la tarea.
- 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 fases I del método RIC. Está distribuido en etapas y algunas de ellas en sub-etapas.

- a. Etapas - 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. Etapas - 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. Etapas - 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. Etapas - Taxonomía: Módulo 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 de 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 establece la información necesaria para el abordaje del riesgo, el responsable del control y seguimiento, como así también 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. Presenta el listado resultante de este proceso, donde se pueden añadir las salvaguardas que sean necesarias.
- iii. **Plan de Contingencias:** en este módulo se incorpora 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 segunda etapa 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 de 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 ellas, 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 RIC.

- a. Carga de la Incidencia: Módulo en donde se cargan las incidencias, 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, 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 procesar la 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 de fechas, 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.

Lanzamiento del Estudio de caso

Etapas 1 – Instalación y parametrización del sistema.

Utilizando el instalador del sistema SCRisk, se instaló el mismo en equipo tipo Servidor, con sistema operativo Windows Server 2008 SR2, que es utilizada como servidor de pruebas, 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 50).

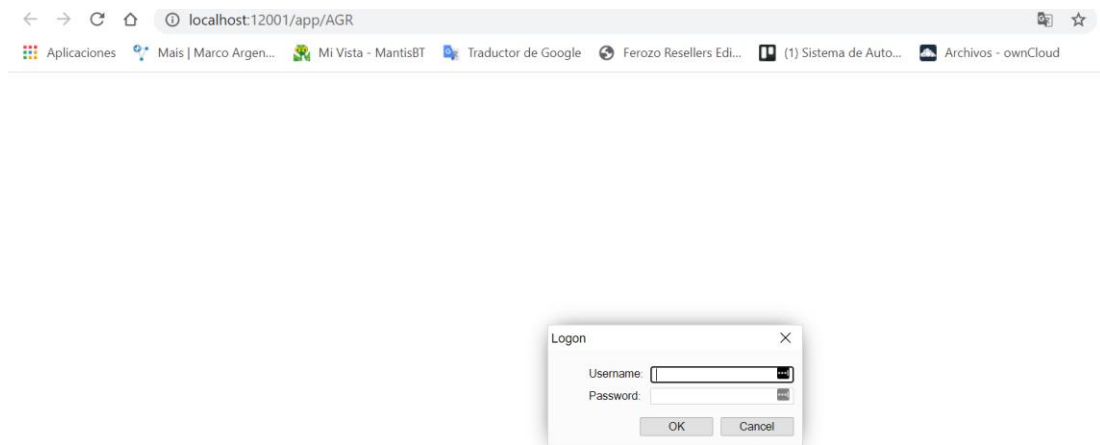


Figura 50 -Login de acceso al sistema

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

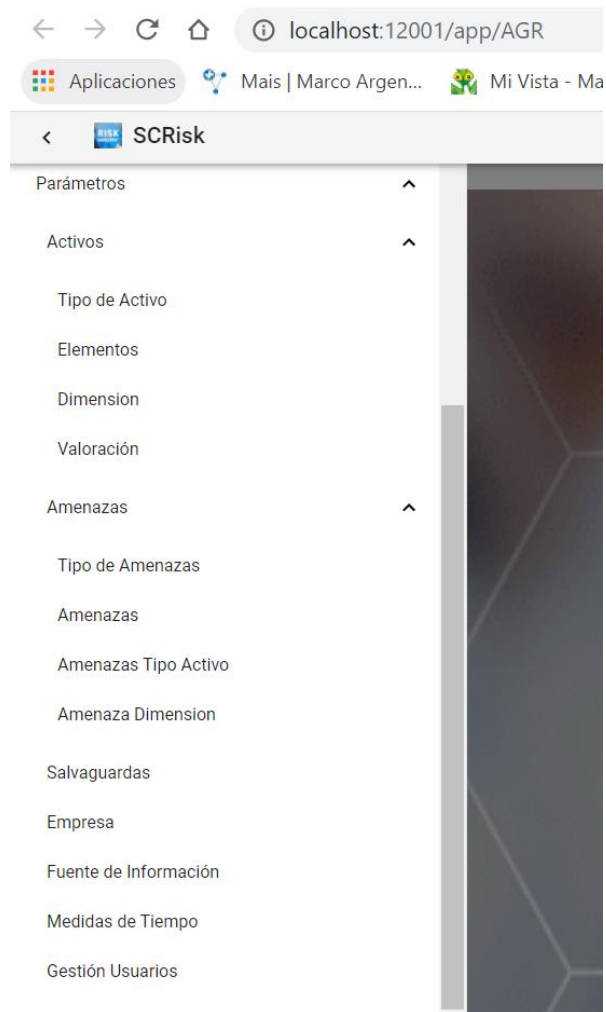


Figura 51 -Menú Parámetros

Tipos de Activos

Como parámetro inicial se cargaron los tipos de activos (sugeridos por MageritV3) con sus descripciones en el módulo de gestión de tipos de activos (ver figura 52).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

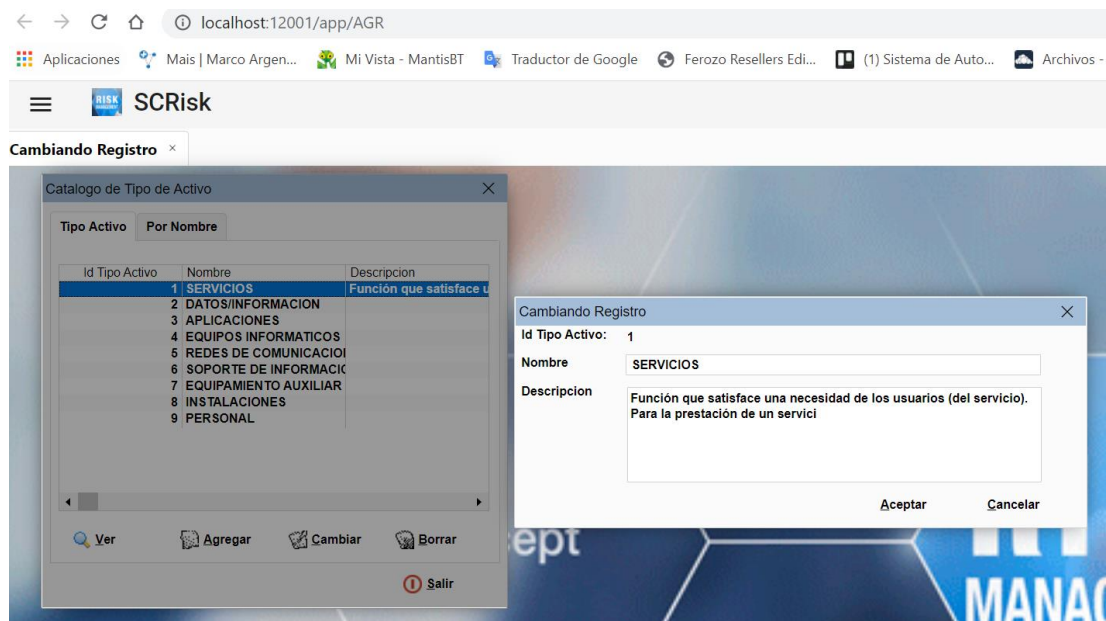


Figura 52 -Gestión de Tipo de Activos

Elementos

Se cargaron los elementos que posee cada tipo de activo, los mismos son sugeridos por Magerit V3, en donde se expresan el código propio del elemento, el nombre y el tipo de activo al cual pertenece (ver figura 53).

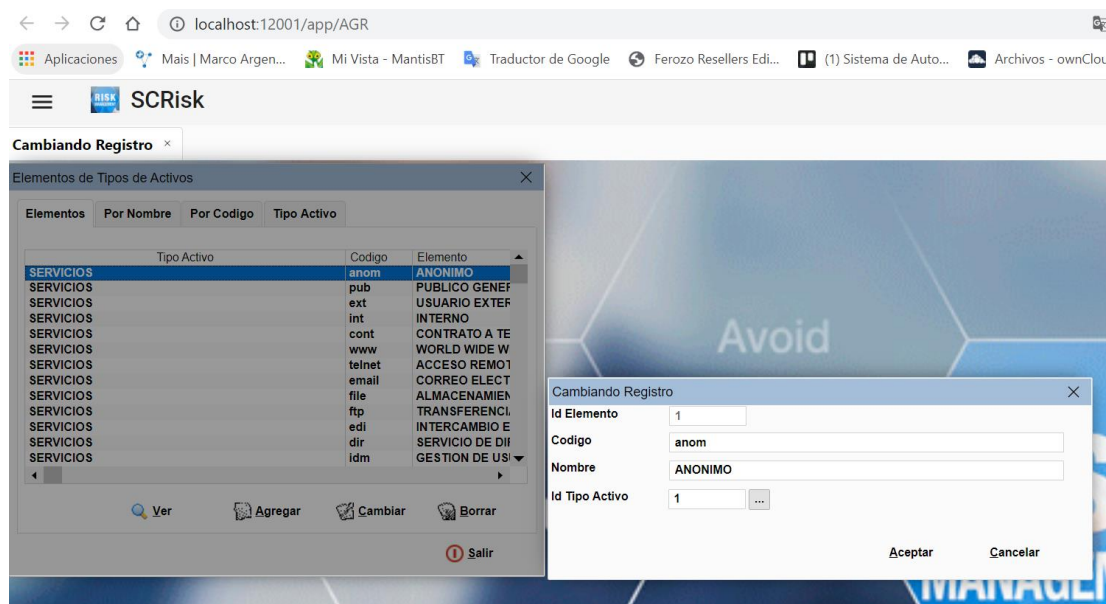


Figura 53 -Gestión de Elementos

Dimensión

Se cargaron las diferentes dimensiones que poseen los activos.

Para la carga inicial del sistema se tomó como base las dimensiones del Magerit V3, 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 detallada de la dimensión (ver figura 54).

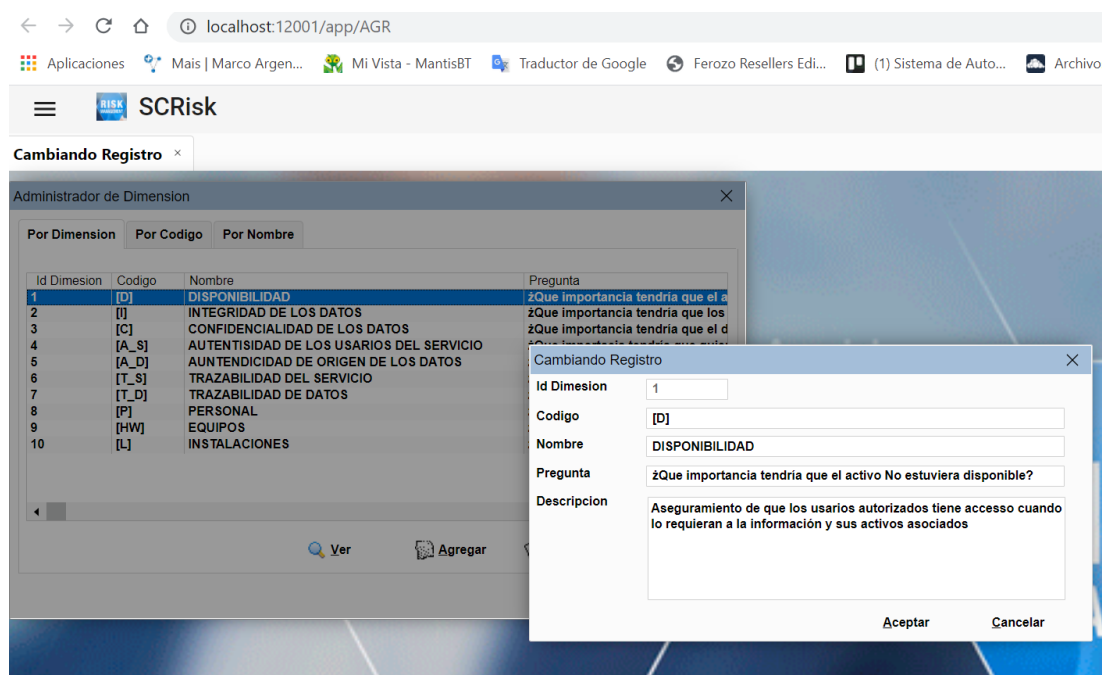


Figura 54 -Gestión de Dimensión

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 55 se puede apreciar la grilla de valoración y el formulario cargado por cada uno de los ítems.

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.

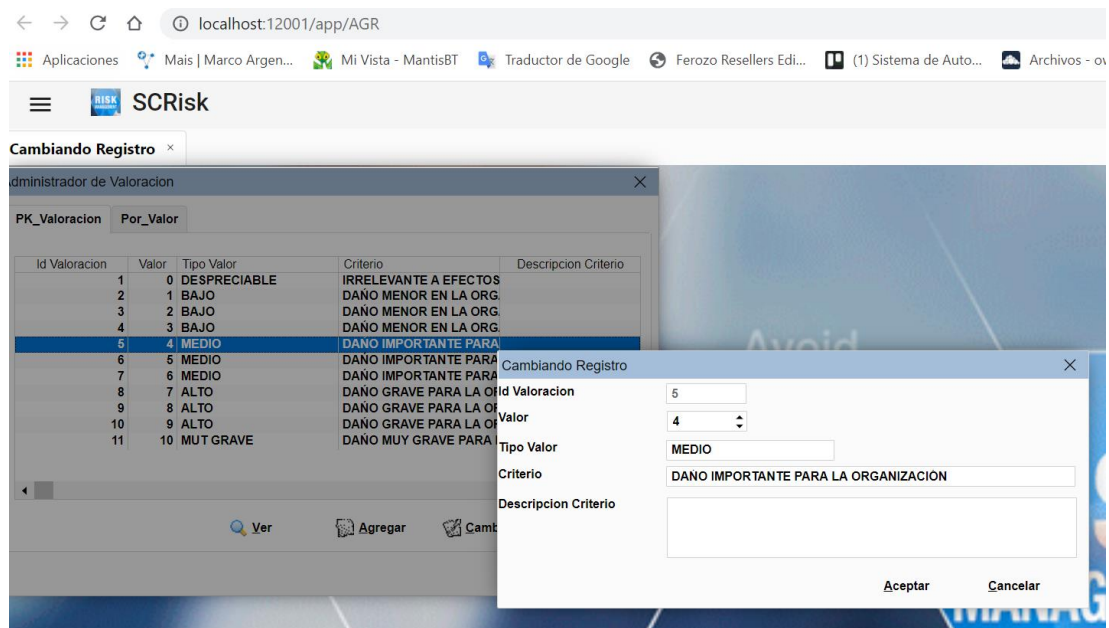


Figura 55 -Gestión de Valoración

Tipos de Amenazas

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

Como muestra la figura 56, 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 V3.

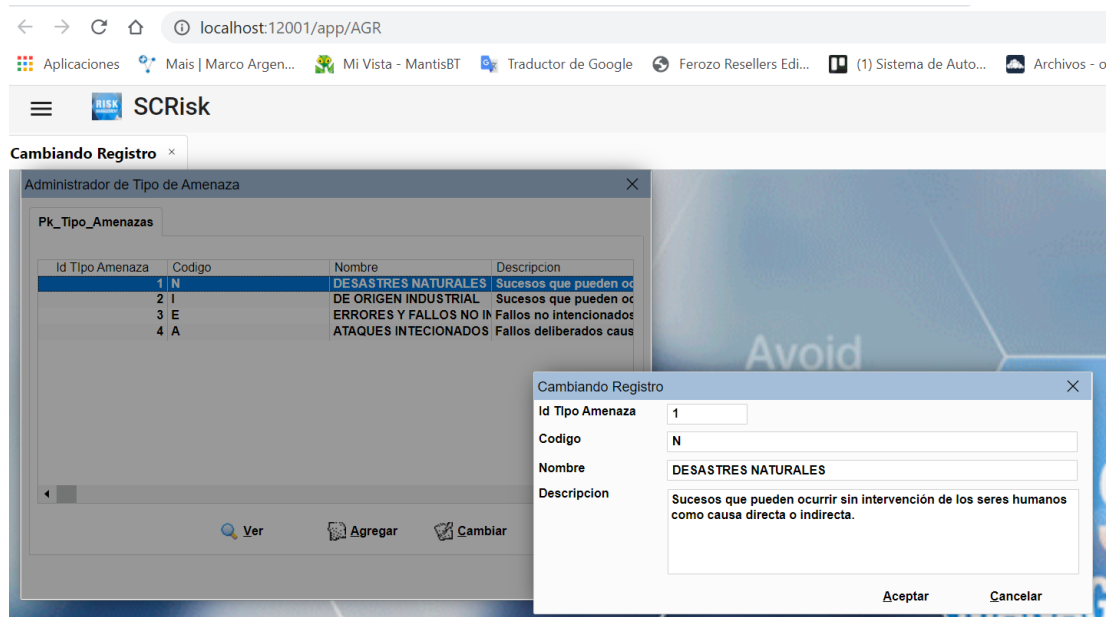


Figura 56 -Tipo de Amenazas

Amenazas

Se cargaron las 41 amenazas de las 58 propuestas por Magerit V3, adecuando las amenazas a las utilizadas por una organización tipo pyme, 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 57).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

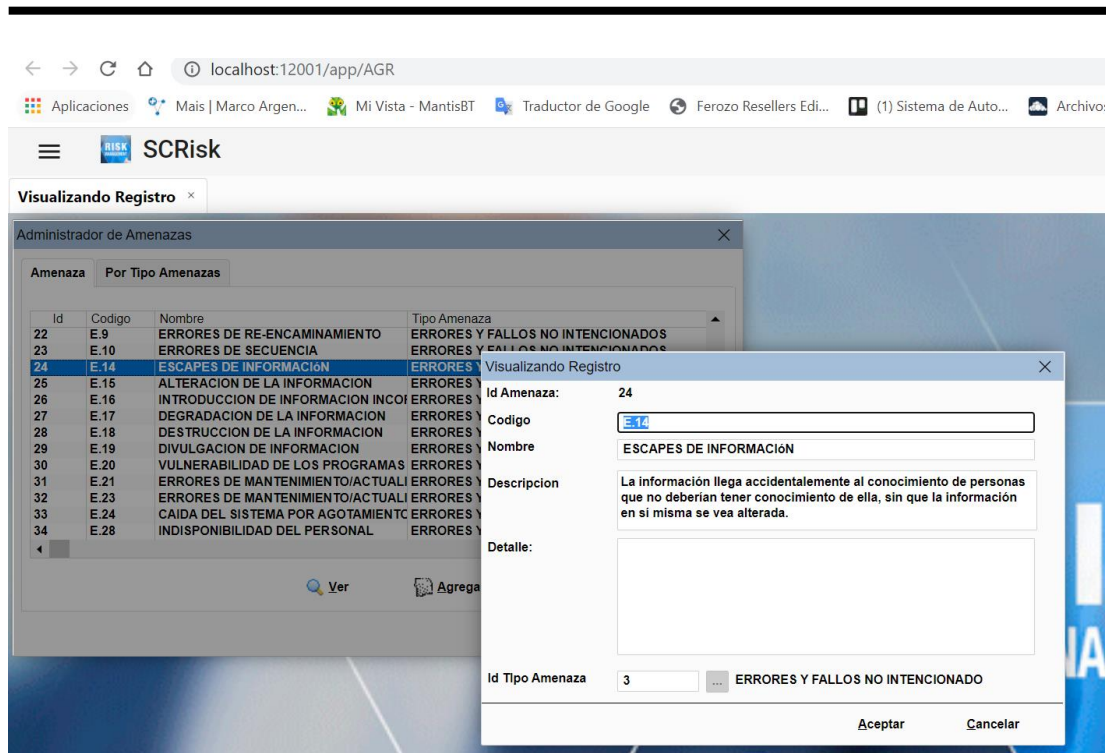


Figura 57 - Gestión de Amenazas

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 58, y en segundo término se asignaron dimensiones a las amenazas como muestra la figura 59.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

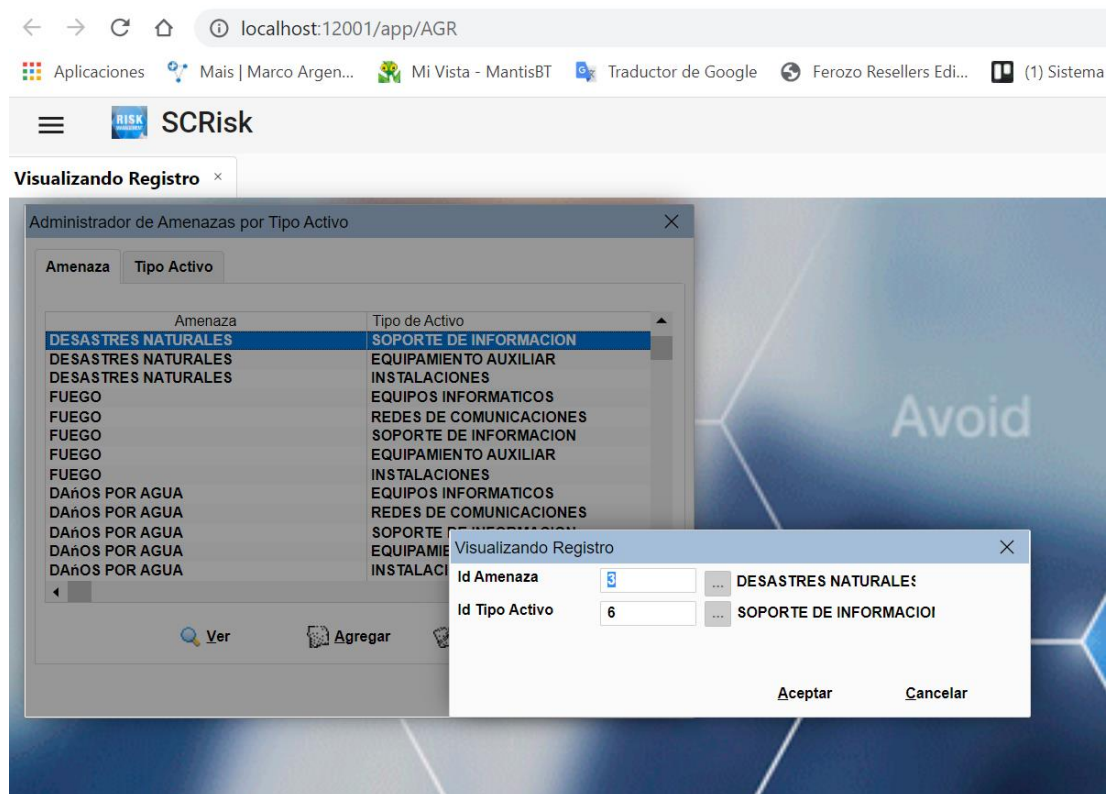


Figura 58 - Amenazas por tipo de Activo

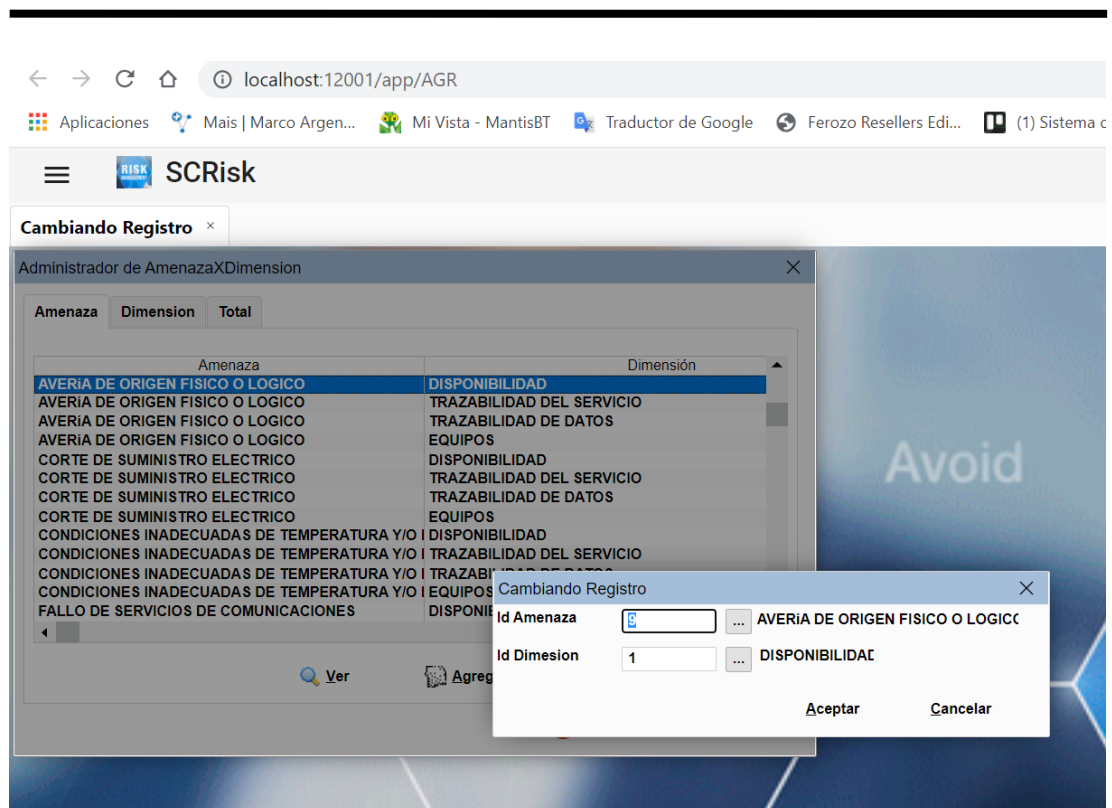


Figura 59 - Amenazas por Dimensión

Salvaguardas

Se procedió a cargar las salvaguardas que serán utilizadas en el plan de acción en la etapa Análisis del capítulo R, como datos propios de la misma, se cargó, la descripción, si posee control, si es afirmativo en que unidad de tiempo, si posee seguimiento, si es así, la unidad de tiempo del seguimiento, y una descripción detallada de la salvaguarda.

Se adoptaron las salvaguardas se tomaron de las sugeridas por Magerit V3 y se incorporaron salvaguardas propias que surge como necesarias del estudio de caso (ver figura 60).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

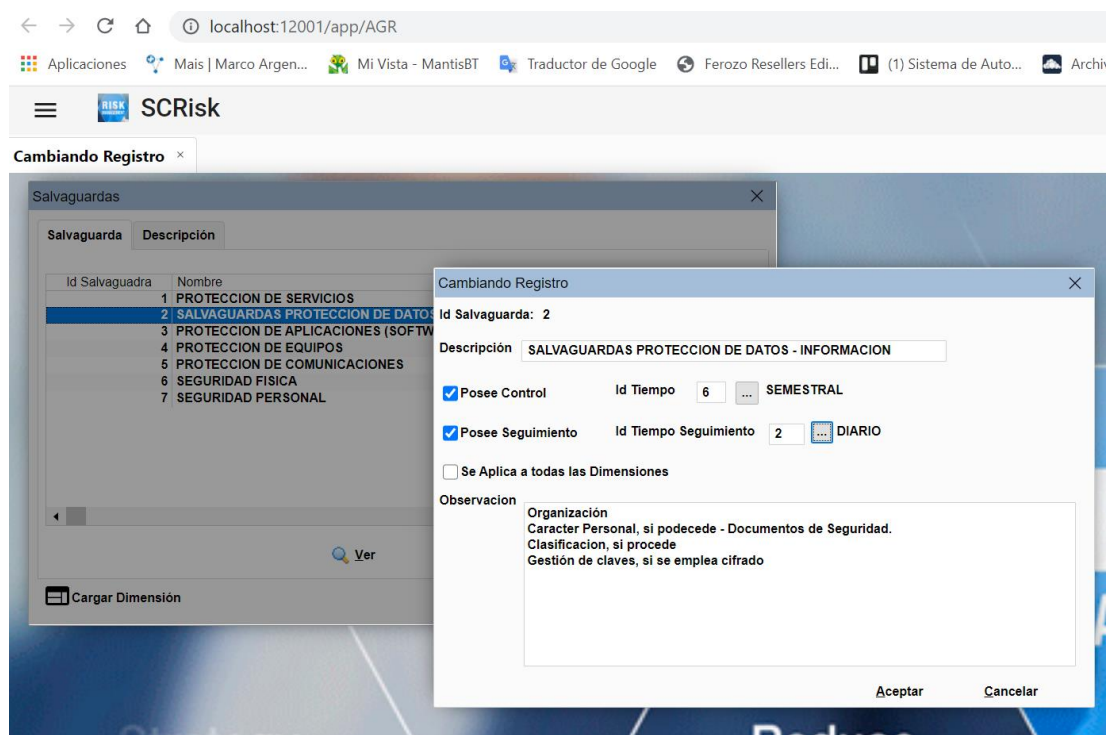


Figura 60 - Gestión de Salvaguardas

Una vez terminada la carga de las salvaguardas, se realizó la asignación de las dimensiones que posee cada de ellas. (ver figura 61).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

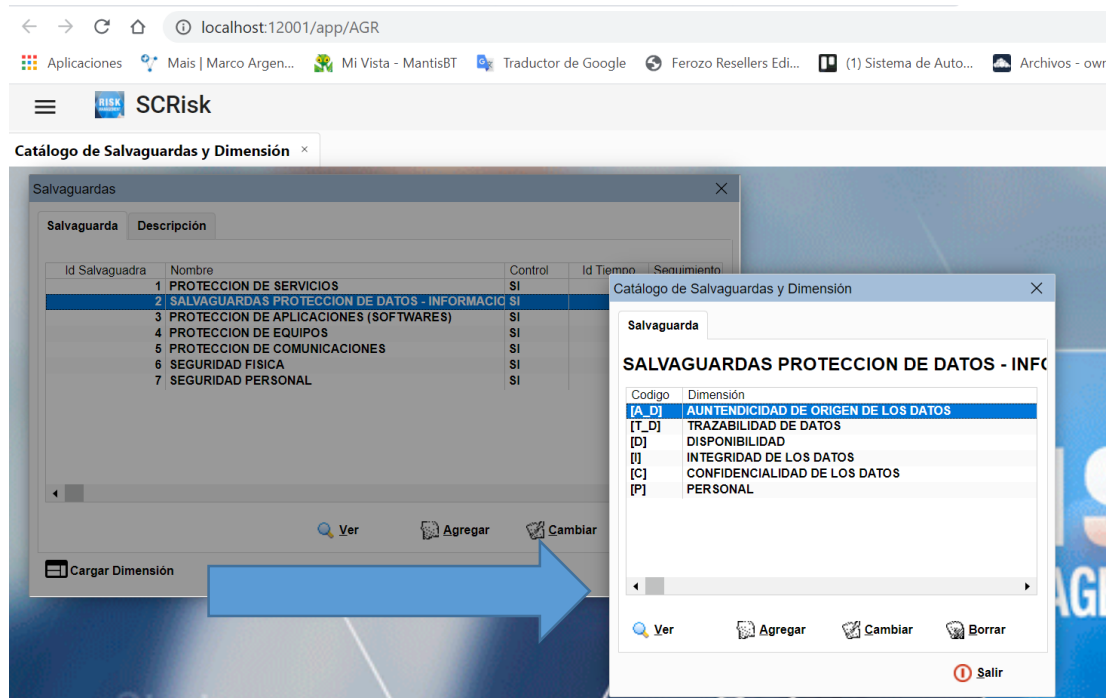


Figura 61 - Asignación de Dimensiones a la Salvaguarda

Catálogo de la Organización

Para lograr adaptar el sistema a distintas organizaciones se generó el módulo de gestión de empresas, cargando los datos mínimos de la organización de prueba (ver figura 62).

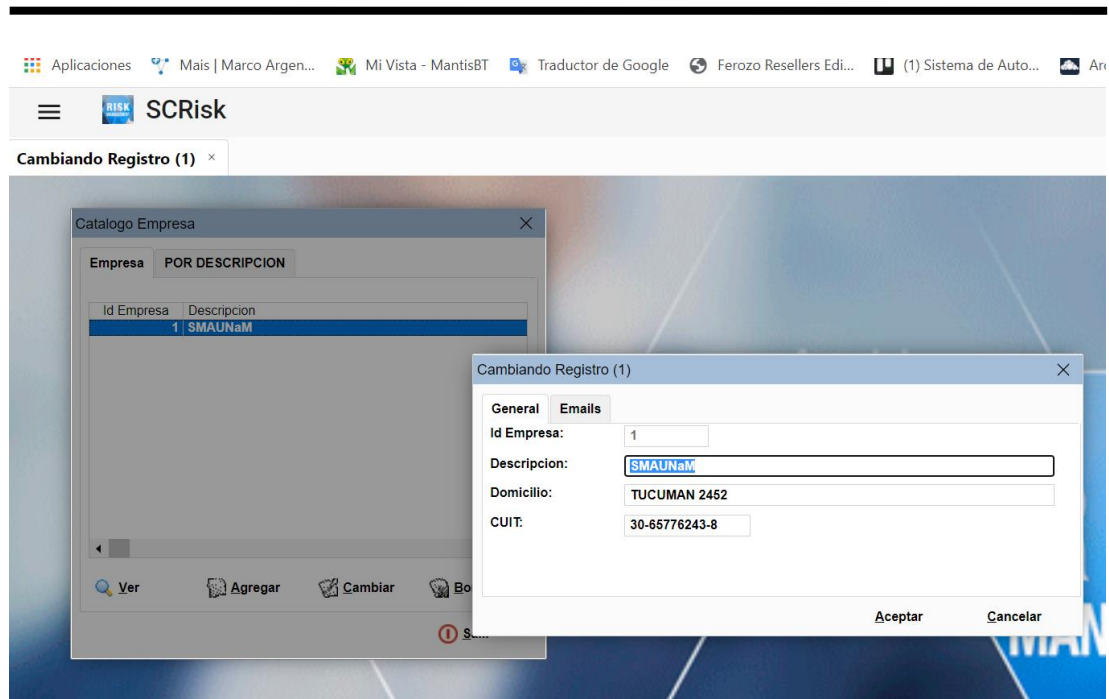


Figura 62 - Gestión de la Organización

Fuente de Información

Se relevaron las distintas áreas que utilizaban activos de IT, y los datos obtenidos fueron cargados al sistema en el módulo “Fuentes de información” (ver figura 63), se asignó un nombre al área o departamento investigado y una descripción de las tareas que realiza.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

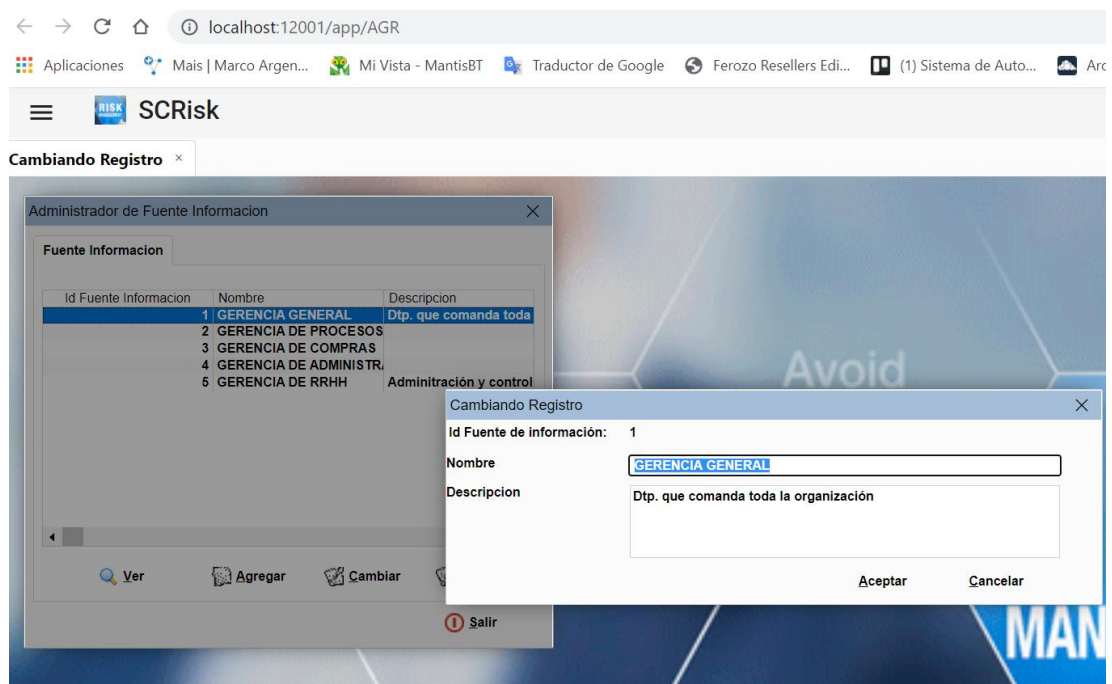


Figura 63 - Gestión de fuentes de información

Medidas de tiempo

Se parametrizaron las medidas de tiempo, que van a ser utilizadas en el proceso de generación del seguimiento de los planes de acción. La carga posee la descripción de la unidad de tiempo, la cantidad de ejecuciones por año y la distancia entre días de 24 Hs. (ver figura 64).

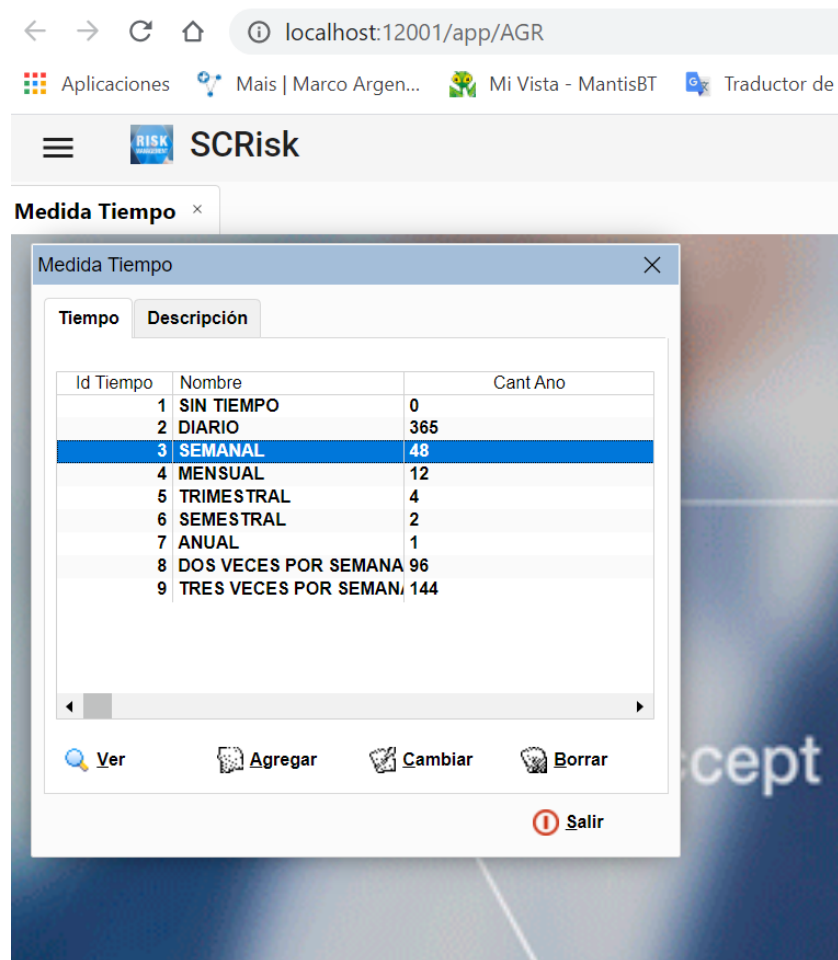


Figura 64 - Gestión de medidas de tiempo

Con todos los datos de parámetros principales cargados, se procedió a iniciar la Etapa de Gestión del Capitulo R del modelo RIC.

Capítulo R – Análisis Gestión y Seguimiento del riesgo

Etapas de Análisis

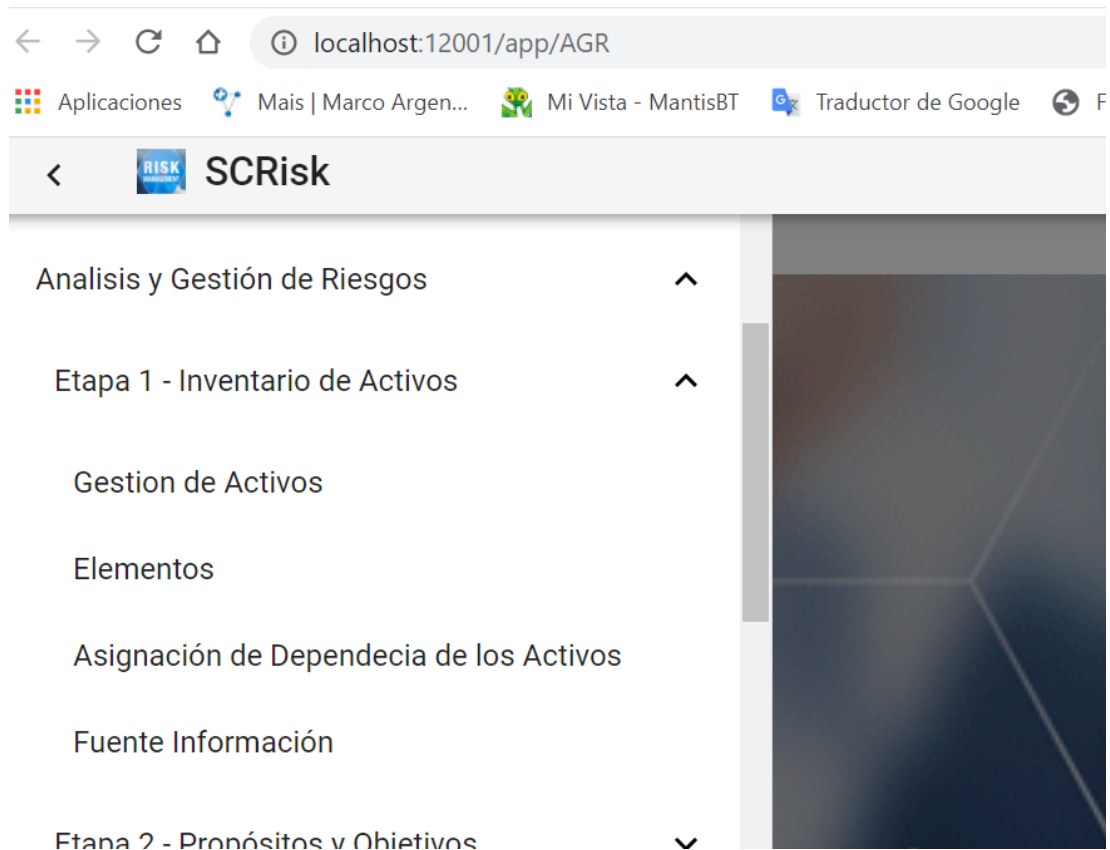


Figura 65 - Menú Etapa 1

Etapas de Análisis – Inventario de Activos

Gestión de Activos

Para iniciar 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 66. El catálogo de activos está 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.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

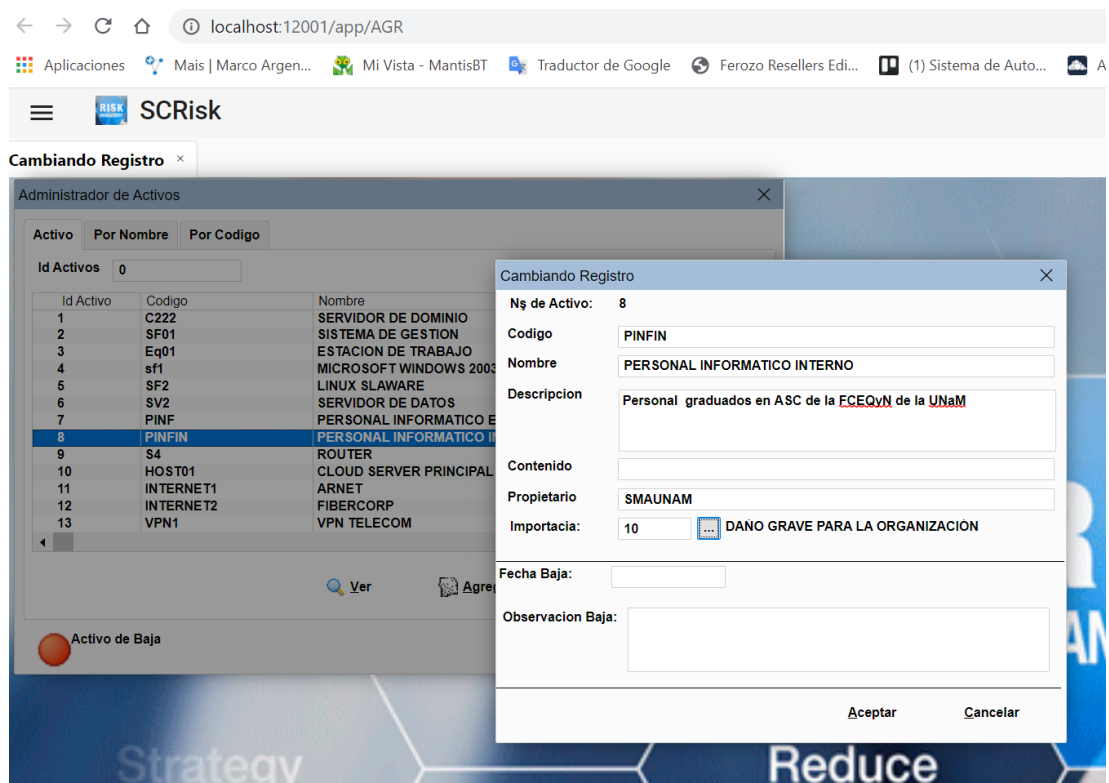


Figura 66 - Gestión de Activos

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 67).

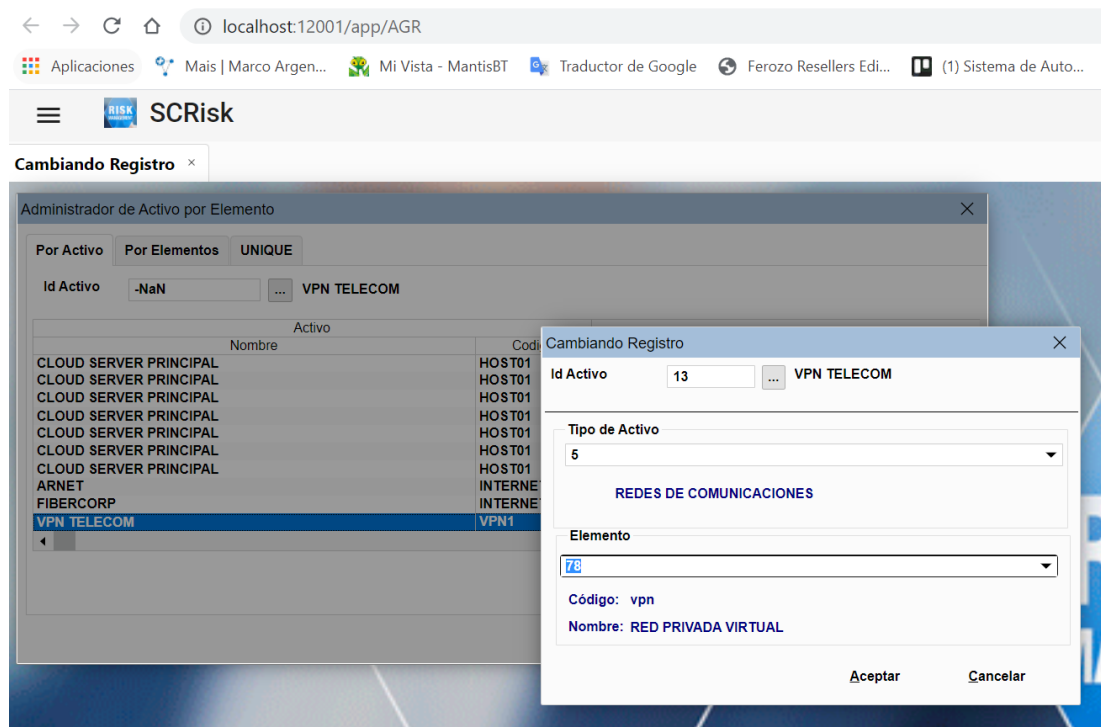


Figura 67 - Asignación de elementos a un activo

Asignación de dependencia

Se asignaron los activos de bajo nivel a los de alto nivel. Como la organización no posee activos de alto nivel, está práctica no tuvo mayores inconvenientes (ver figura 68).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

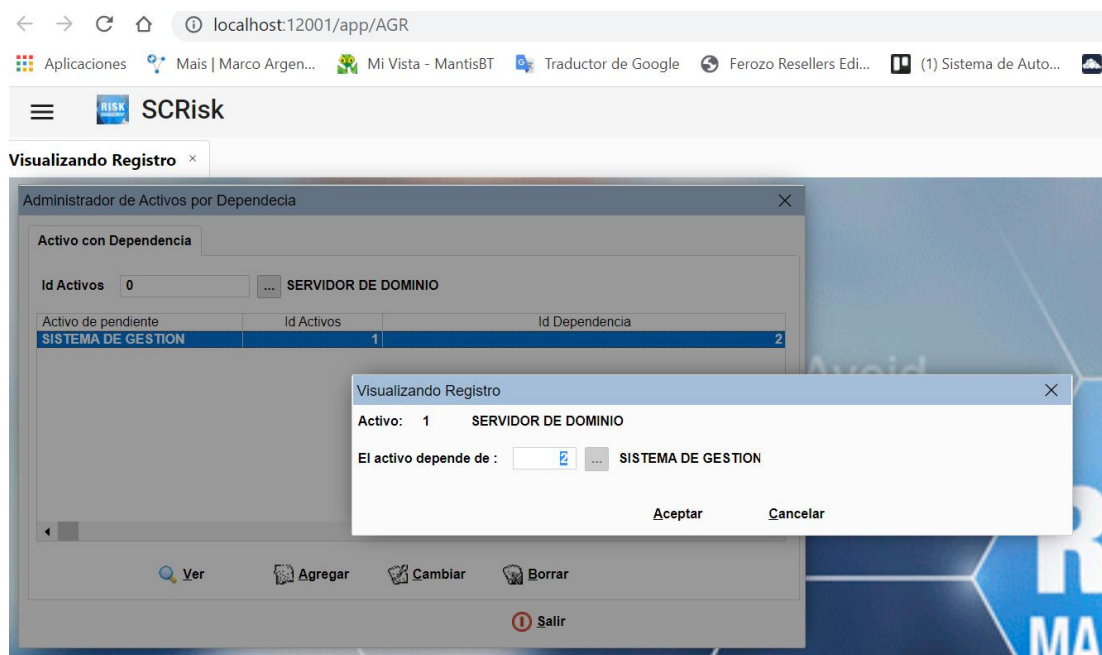


Figura 68 - Dependencia de activos

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 69).

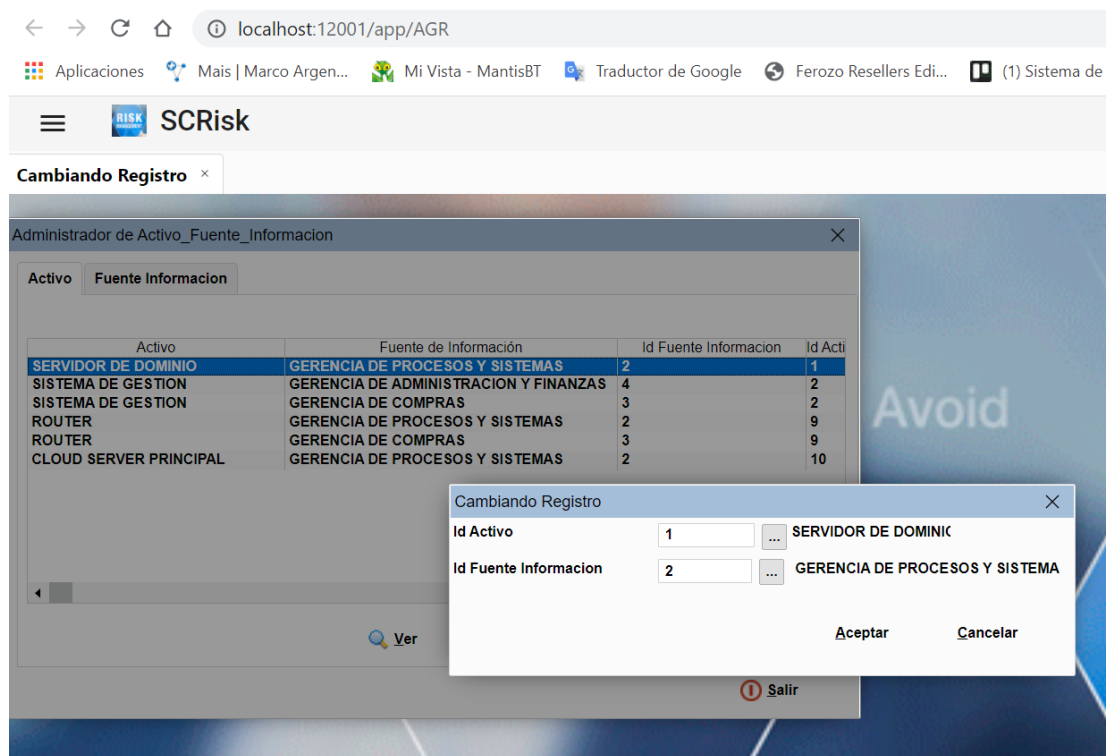


Figura 69 - Asignación de fuente de información

Gestión de propósitos y Objetivos

Gestión del proyecto

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

Como muestra la figura 70 los datos propios del proyecto son: el Propietario, se describe el propietario de la organización o el propietario del proyecto, ya que él 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.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

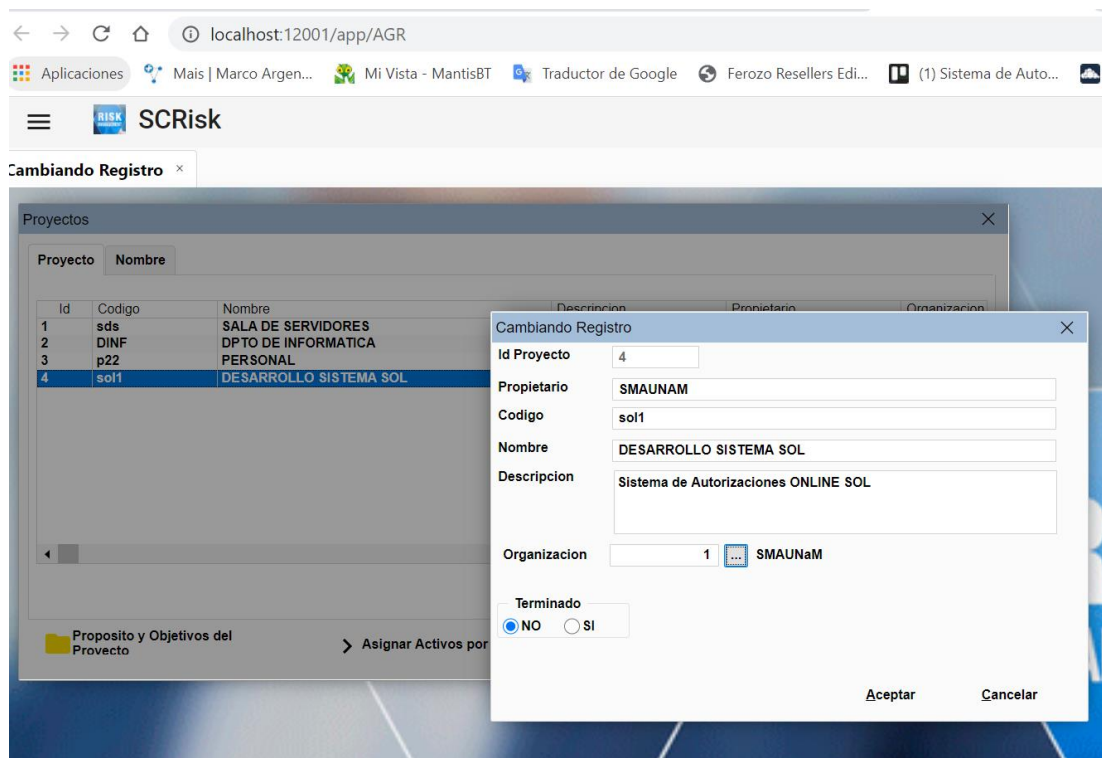


Figura 70 - Gestión de proyectos

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 71.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

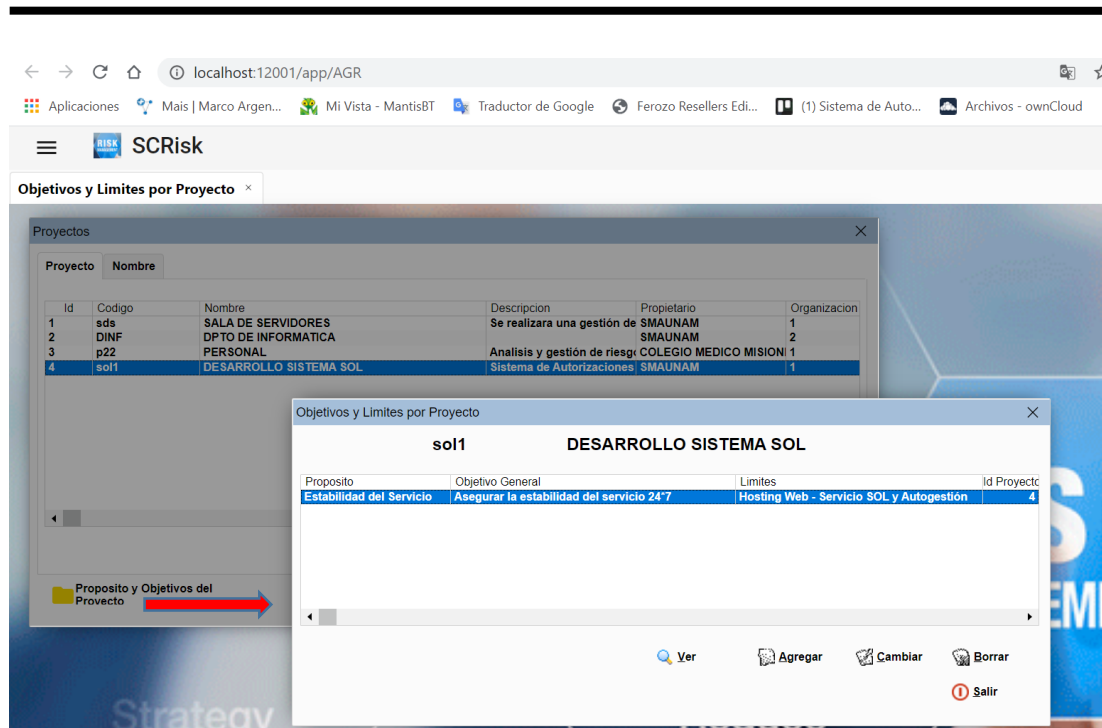


Figura 71 - Asignación de propósitos y objetivos al proyecto

También se asignó activos al proyecto como muestra la figura 72.

En el estudio de caso, al proyecto “Desarrollo Sistema SOL” se le asignaron tres activos, personal informático externo y personal informático interno.

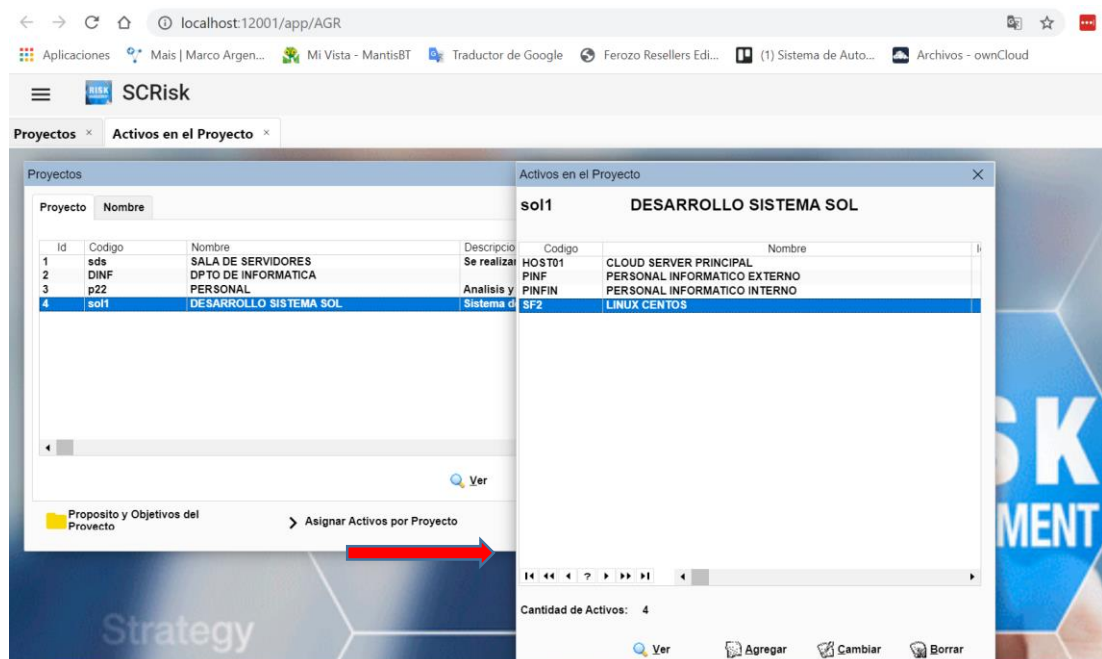


Figura 72 - Asignación de activos al proyecto

Equipo de Trabajo

Gestión de Equipos

En esta etapa se designó el equipo de trabajo para el proyecto “Desarrollo Sistema SOL”, para lo cual previamente, se gestionó 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 73. Por cada persona asignada se debió parametrizar a que equipo pertenece, y que rol cumple en el proyecto.

La flexibilidad del sistema permite asignar a una persona distintos roles y equipos dentro del proyecto, como es plasmado en la realidad de una organización pequeña.

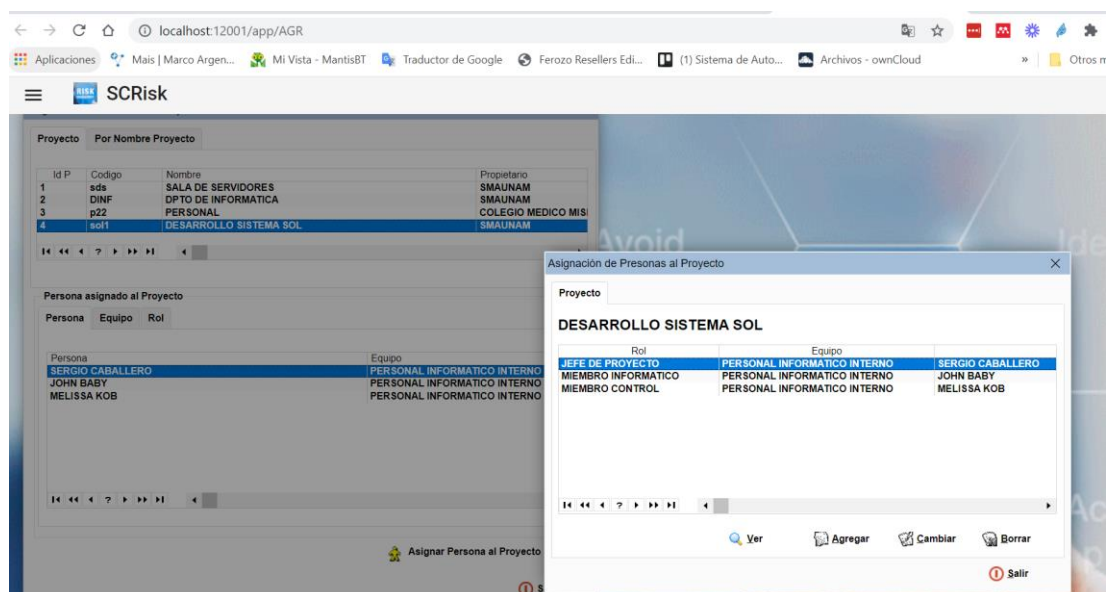


Figura 73 - Gestión de equipos

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 74) y luego procesa lo antes explicado.

Al finalizar 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 75.

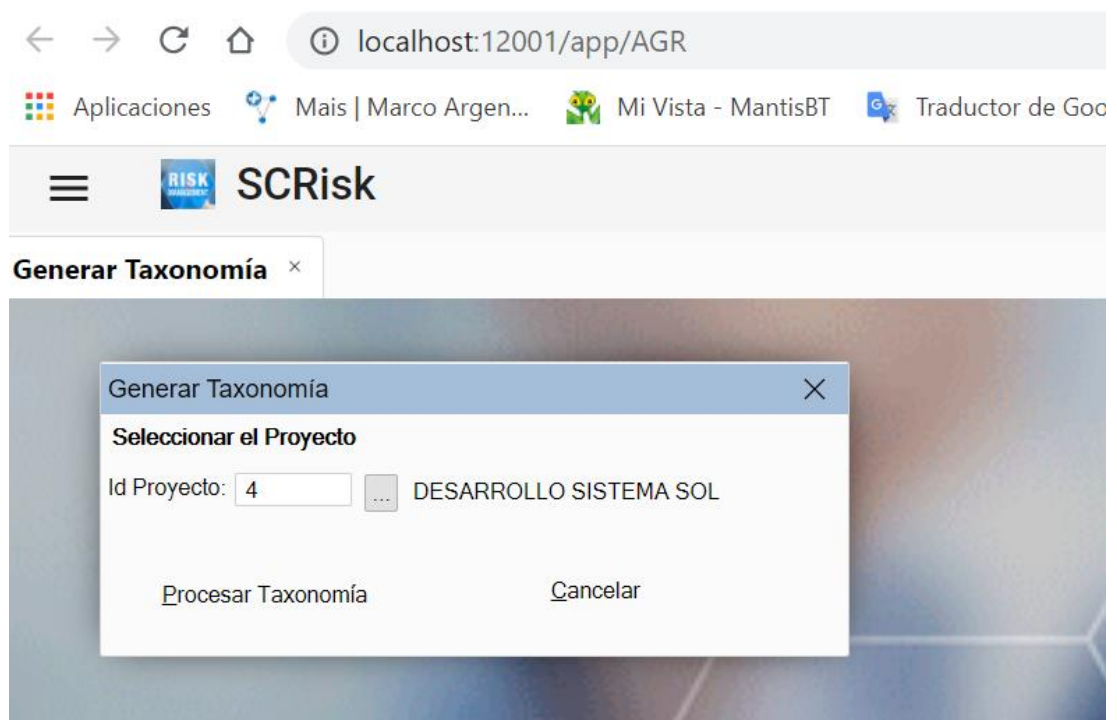


Figura 74 -Selección de proyecto para generar la taxonomía

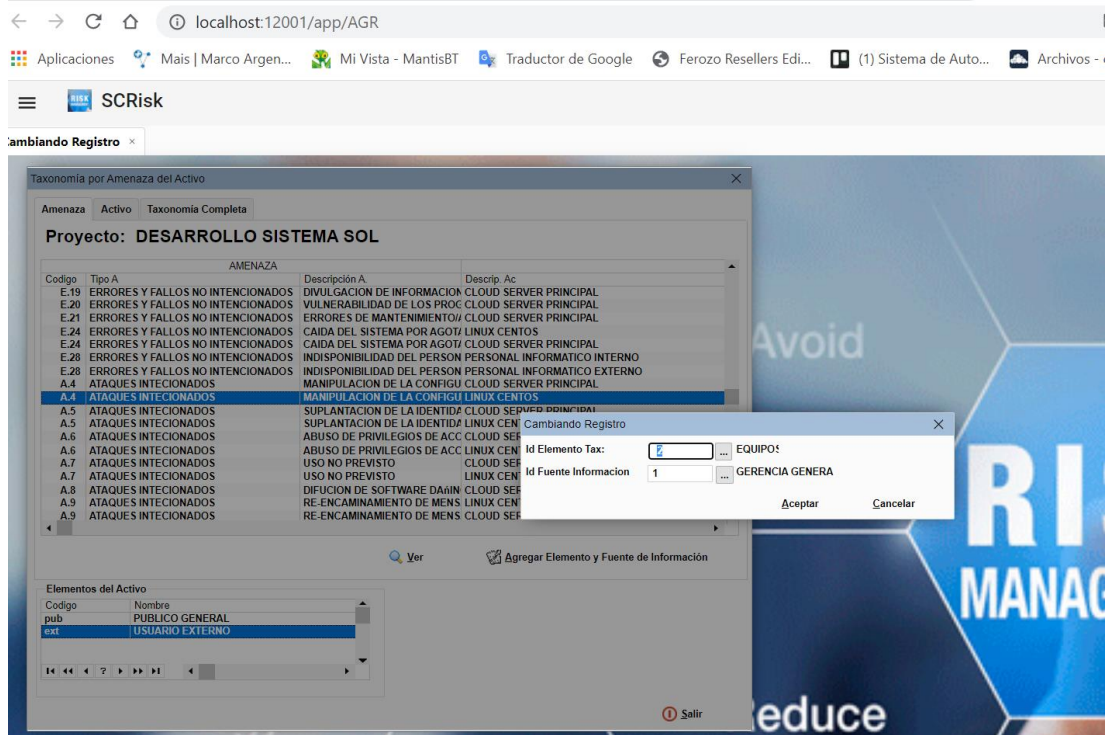


Figura 75 - Gestión de elementos y fuentes de información

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

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 otorga agilidad a la carga del sistema, y la automatización de muchas de las variables, además, posibilita al operador modificar los valores por defecto, como muestra la figura 76.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

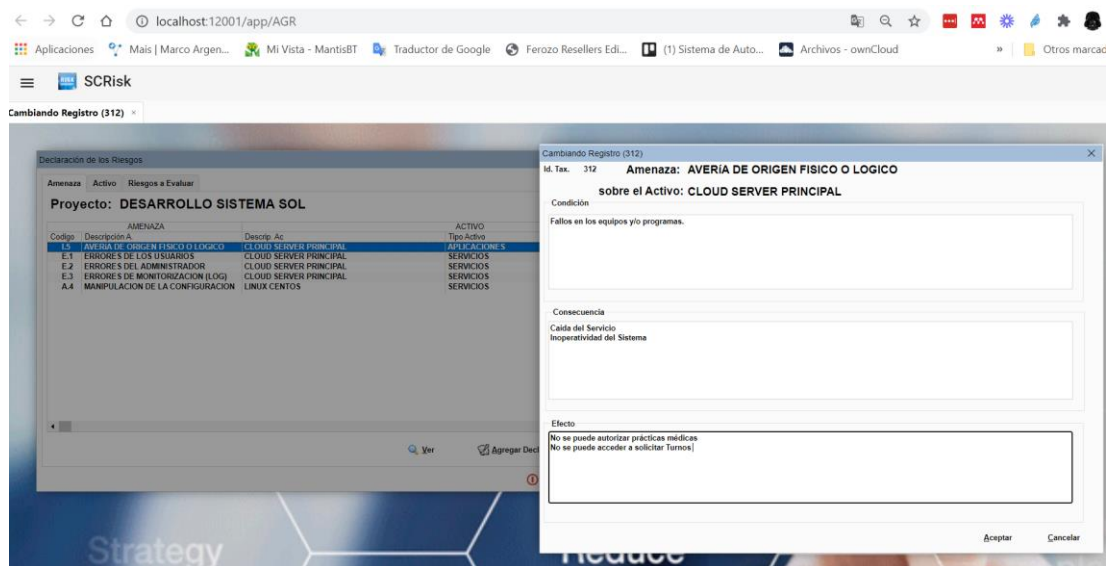


Figura 76 - Gestión de declaración

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

Estimación de probabilidad

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 77.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

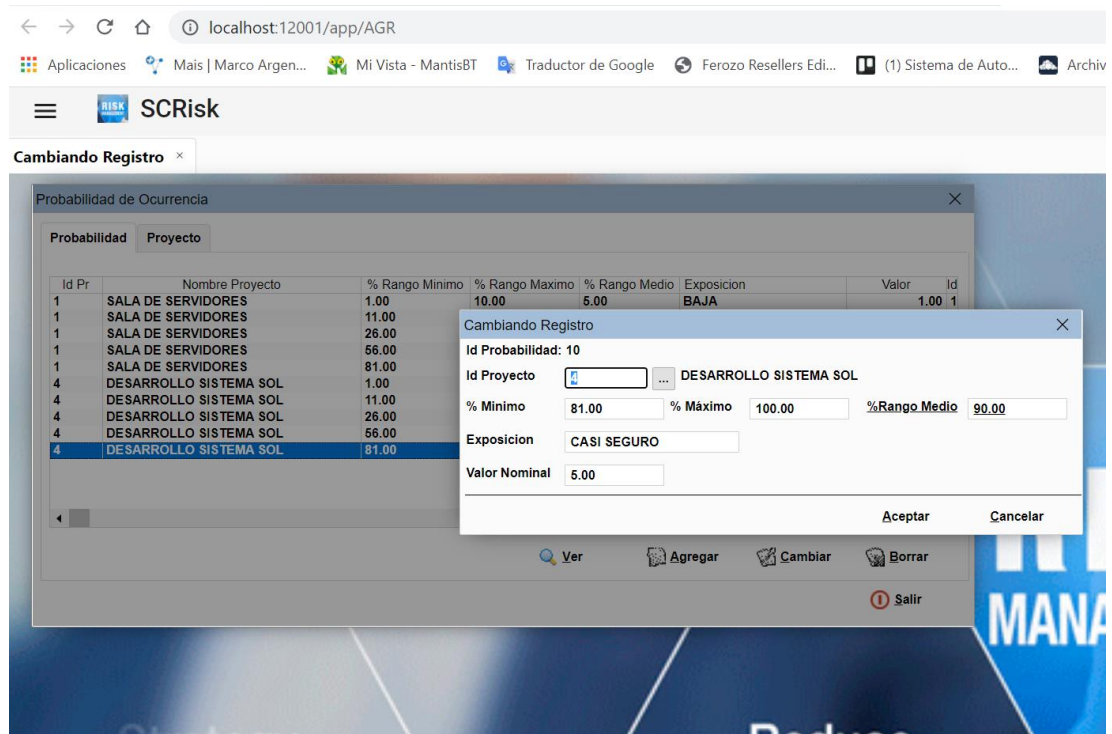


Figura 77 - Tabla de probabilidad de ocurrencia por riesgo

Estimación de Impacto

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 78, 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.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

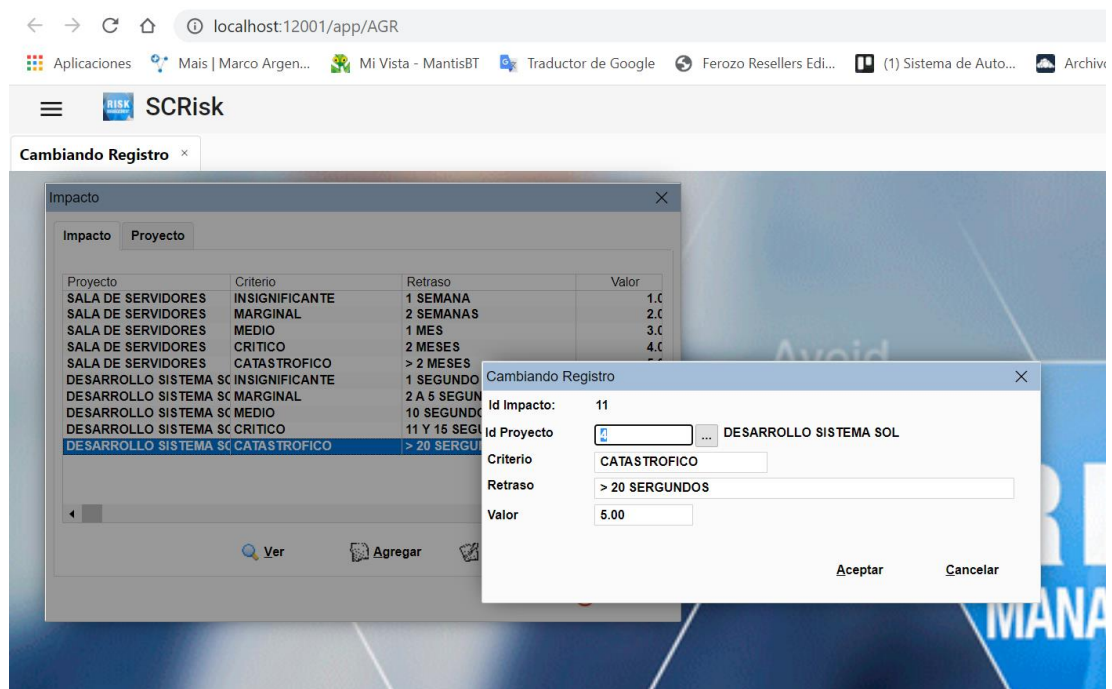


Figura 78 - Impacto de ocurrencia por proyecto

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 79).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

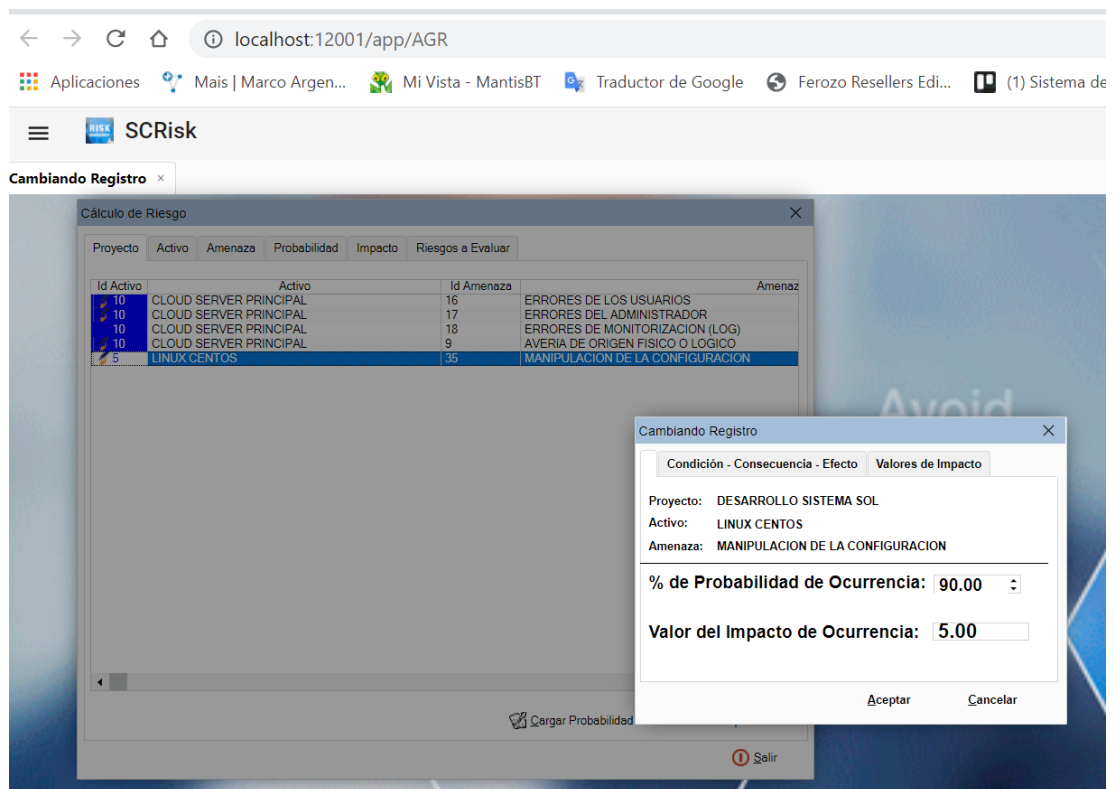


Figura 79 - Asignación de probabilidad e impacto

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 divide en la figura 80.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

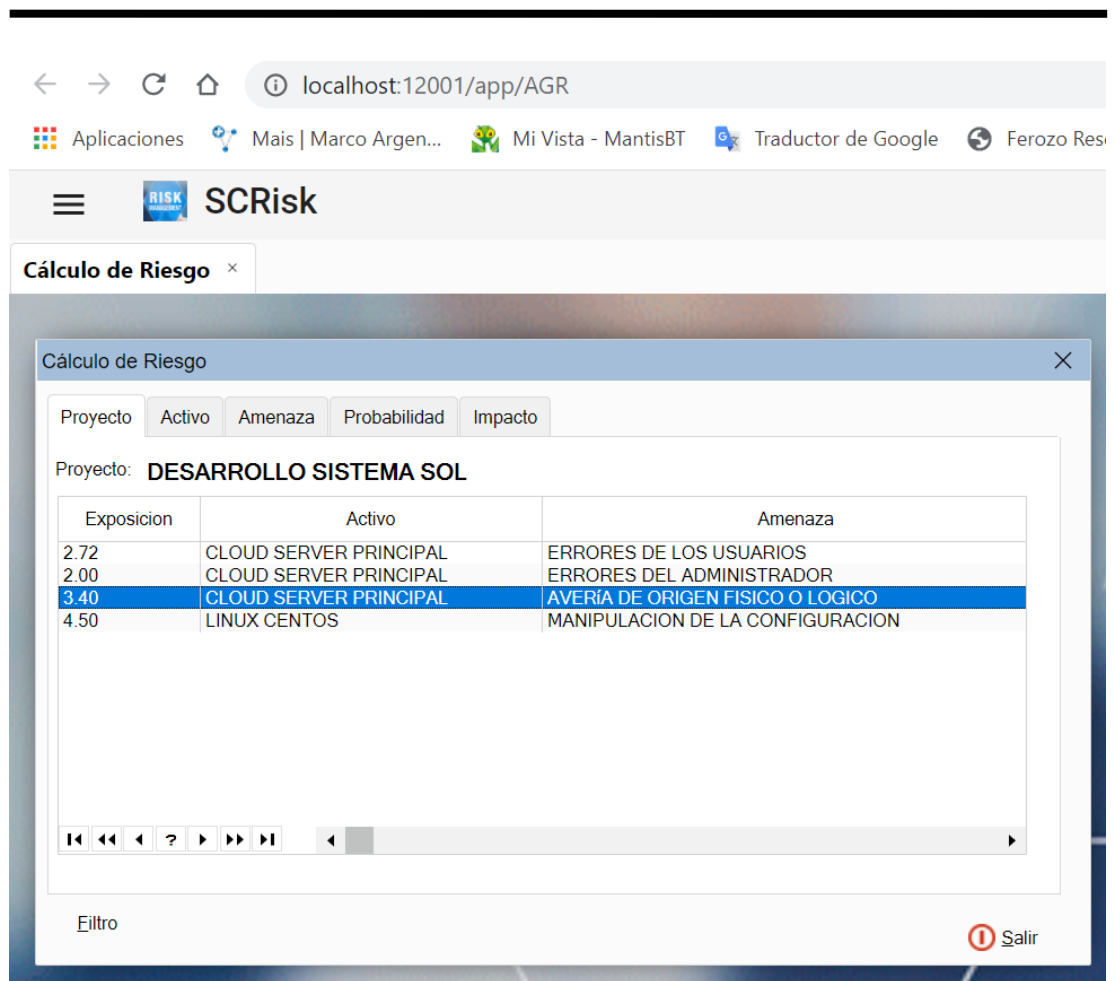


Figura 80 - Exposición al riesgo

Etapas Gestión de los riesgos

Información

En este módulo se cargaron las fuentes de información que se utilizaron en la gestión de riesgos (ver figura 81).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

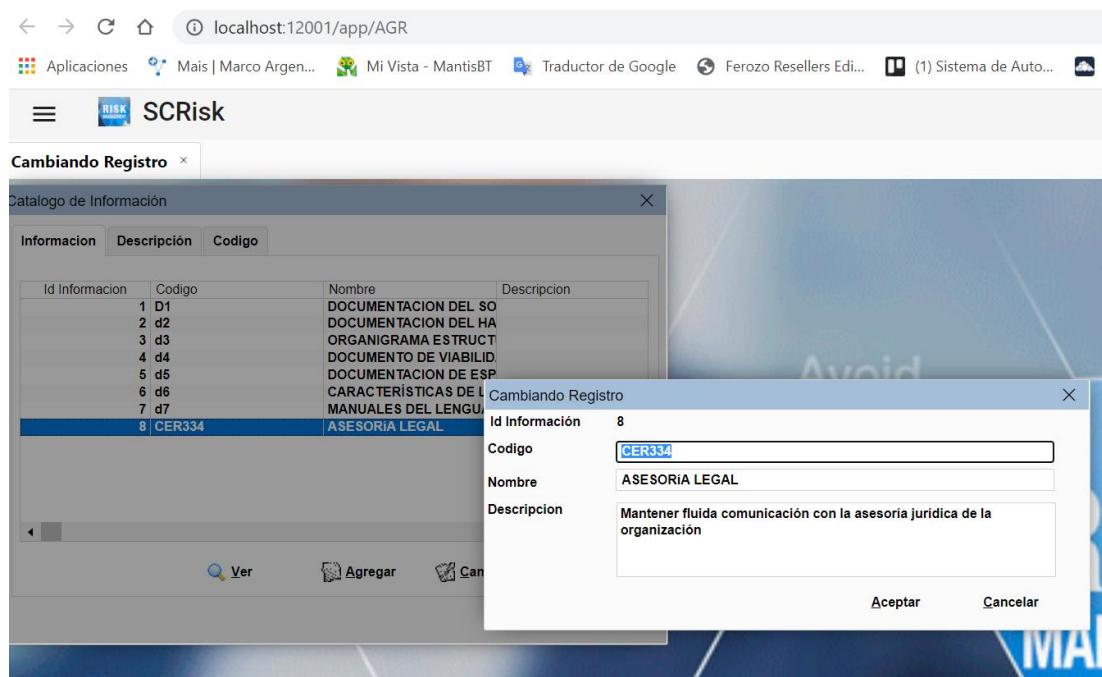


Figura 81 - Información de riesgos

Recursos

Gestiona los recursos necesarios para tratar los riesgos, estos recursos pueden ser asignados a distintos proyectos del sistema (ver figura 82).

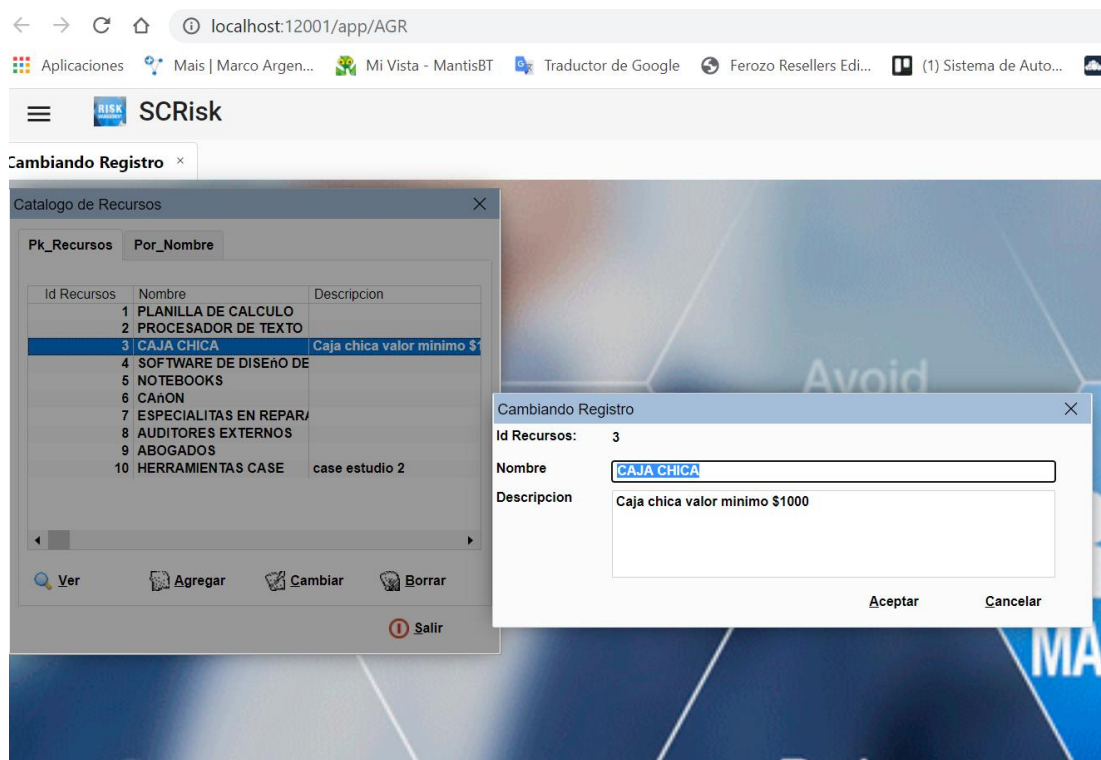


Figura 82 - Recursos

Gestión

Este es el módulo más importante de las etapas de la fase I, debido que, en él, 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 83. Además de la generación automática, se le agregó al riesgo al proyecto “problemas legales” una salvaguarda propia del proyecto.
2. Se parametrizaron manualmente el plan de contingencia por cada uno de los riesgos expuestos, asignando las siguientes variables (ver figura 84):
 - 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 85).
 4. Se estableció el/los responsables del control y seguimiento del riesgo, y los encargados de solucionar el problema si este ocurriera (ver figura 86).
 5. Se cargaron los recursos necesarios para la gestión del riesgo (ver figura 87).

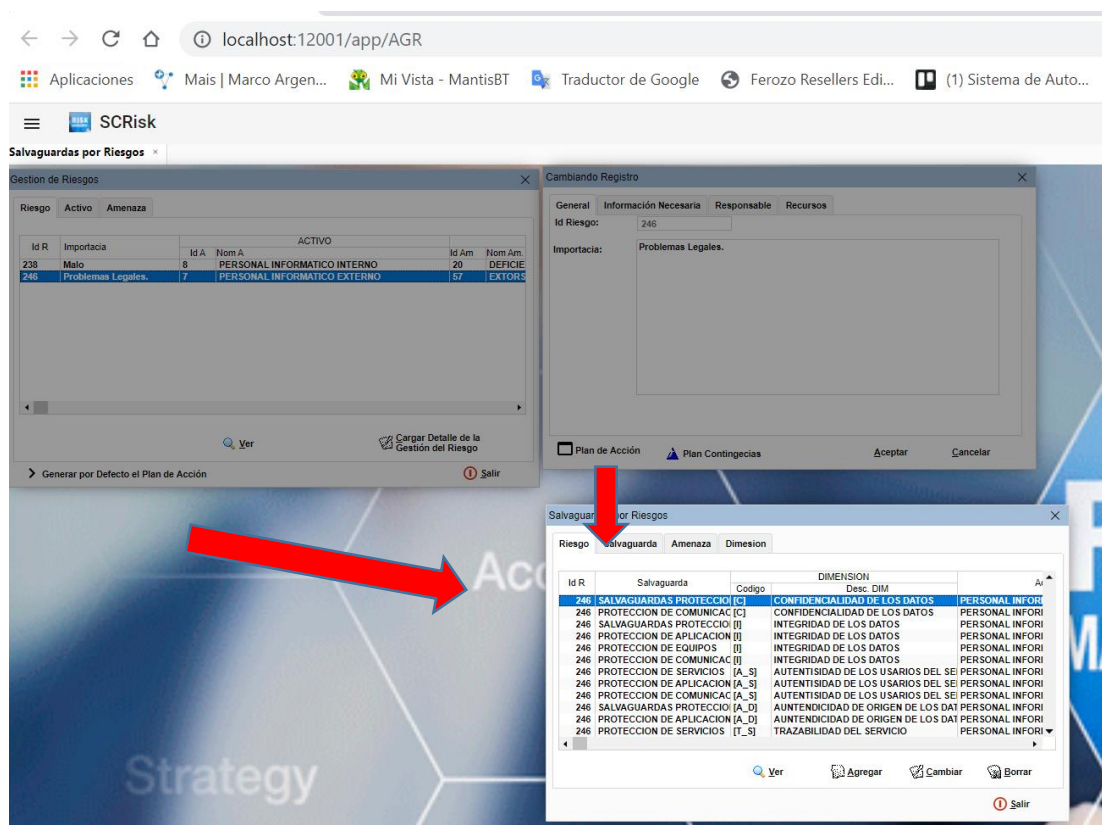


Figura 83 - Asignación de plan de acción

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

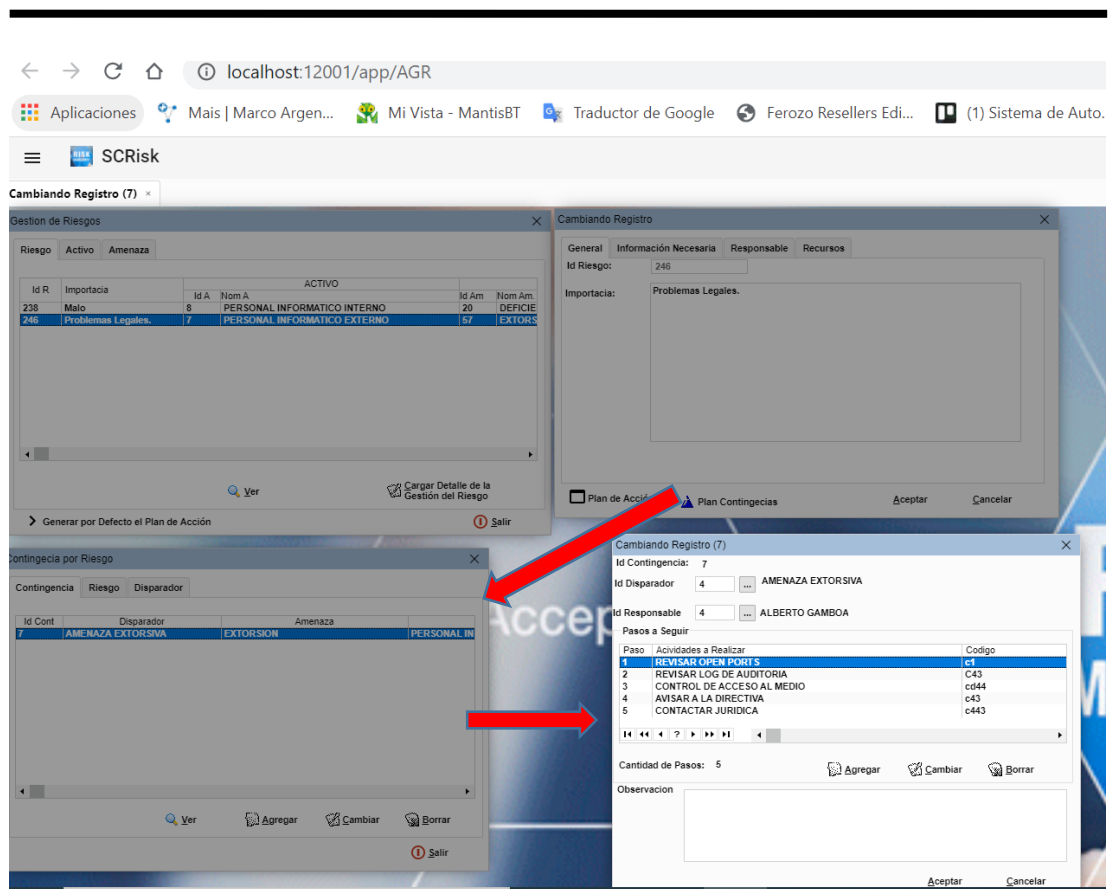


Figura 84 - Plan de contingencia

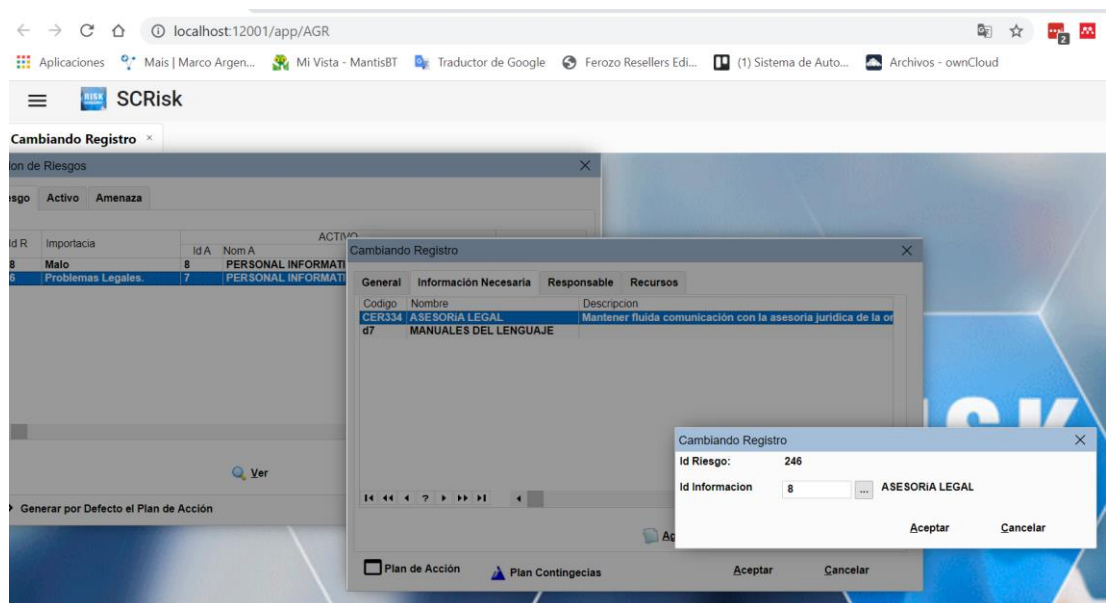


Figura 85 - Información necesaria

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

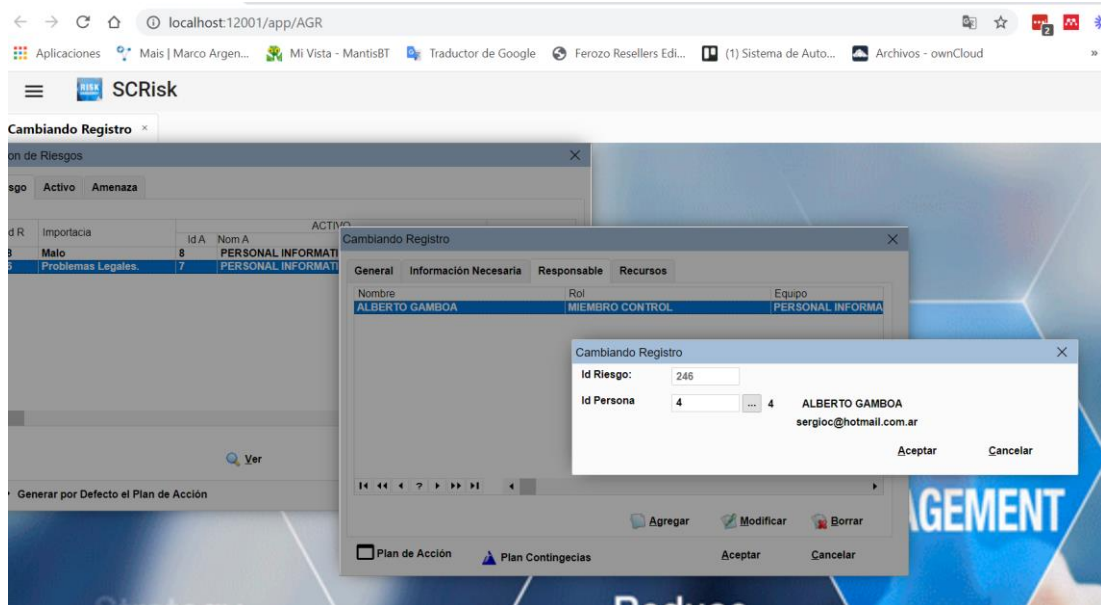


Figura 86 - Responsable

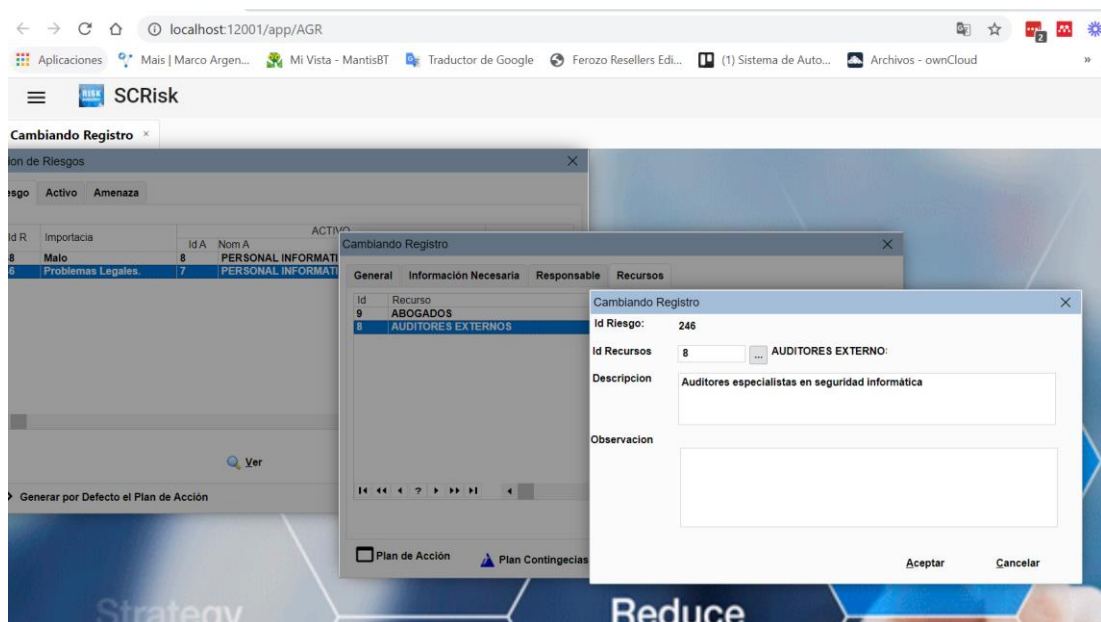


Figura 87 - Recursos

Etapa - Seguimiento

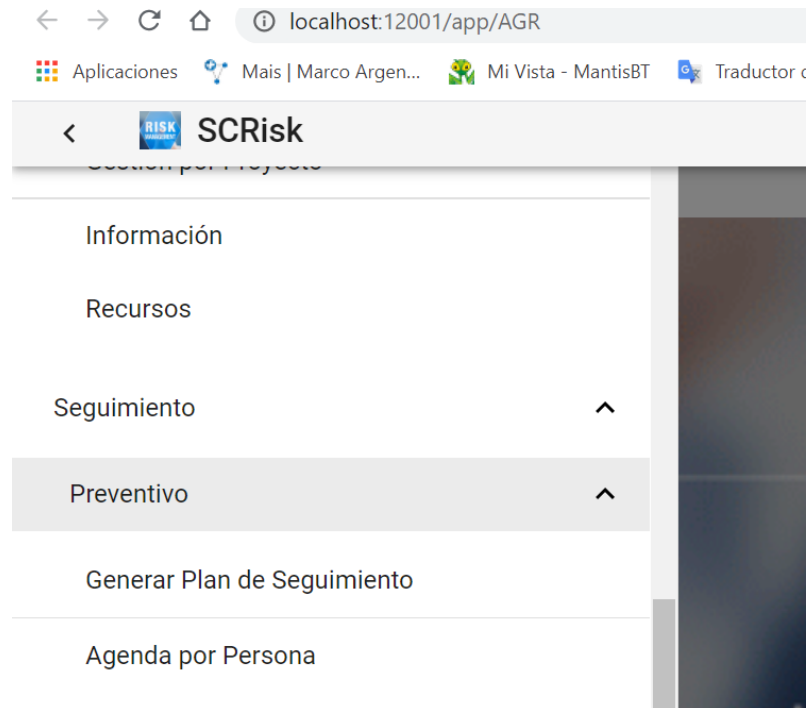


Figura 88 - Menú Seguimiento

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 agregan nuevos riesgos. Figura 89.

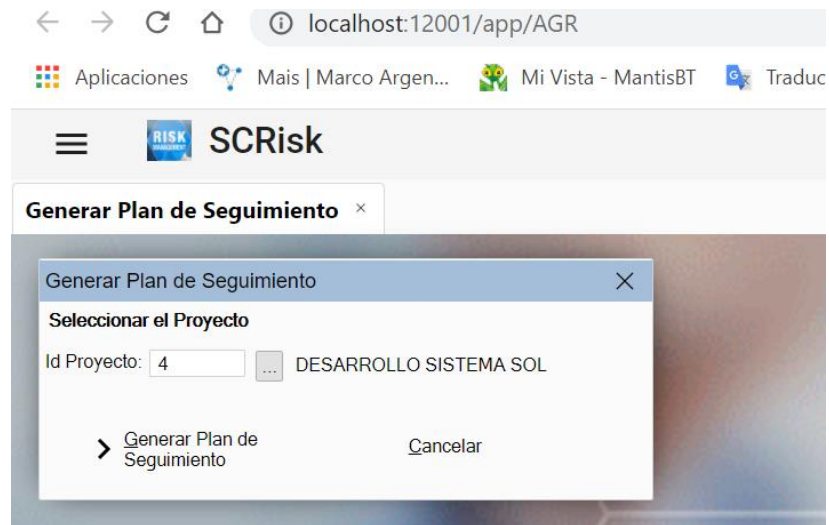


Figura 89 - Plan de seguimiento

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 90.

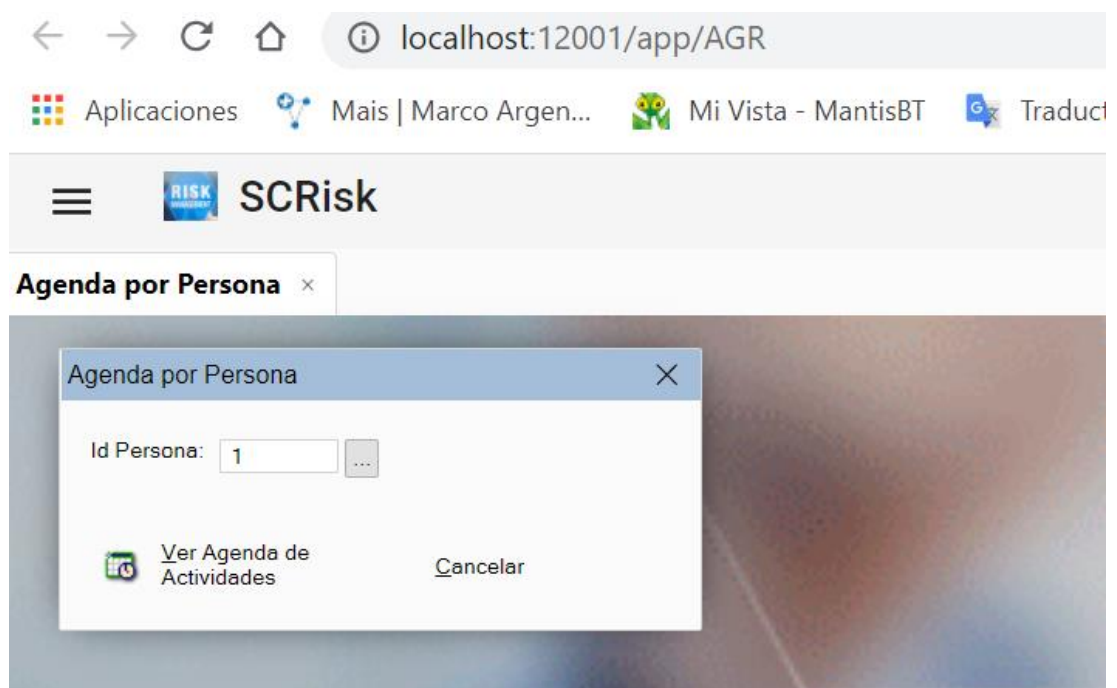


Figura 90 - Agenda de actividades

Una vez identificada la persona en el proyecto indicado, el sistema muestra el panel de control del seguimiento (ver figura 91).

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.

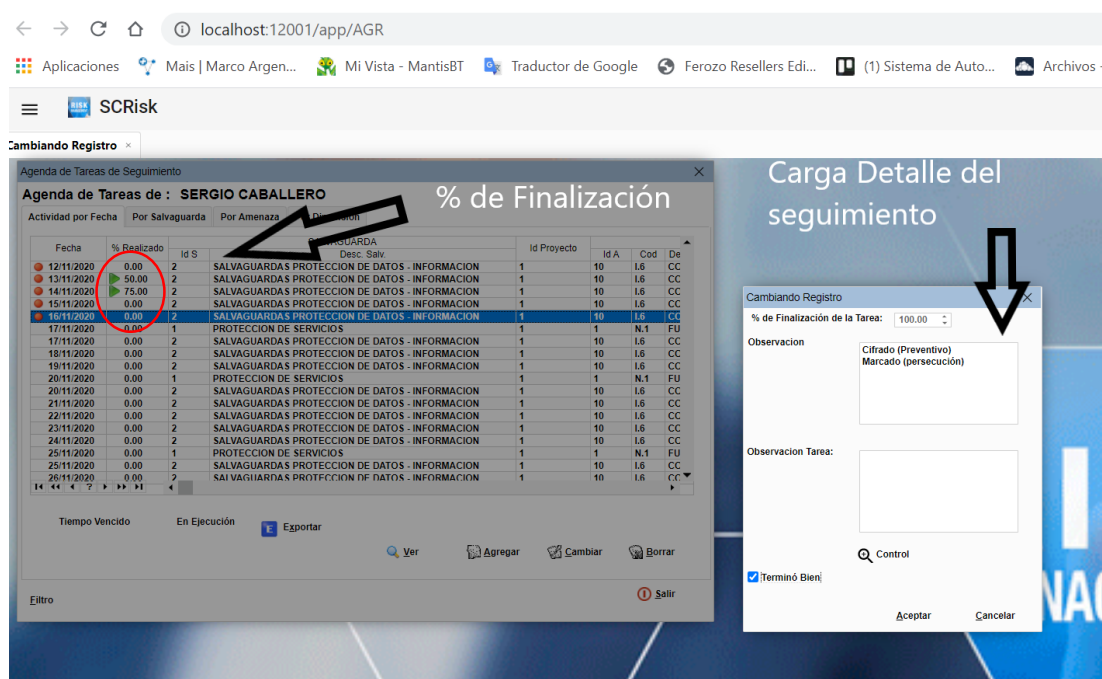


Figura 91 - Gestión de control de Seguimiento

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.

Capítulo I – Gestión de Incidencias

Etapa - Incidencias

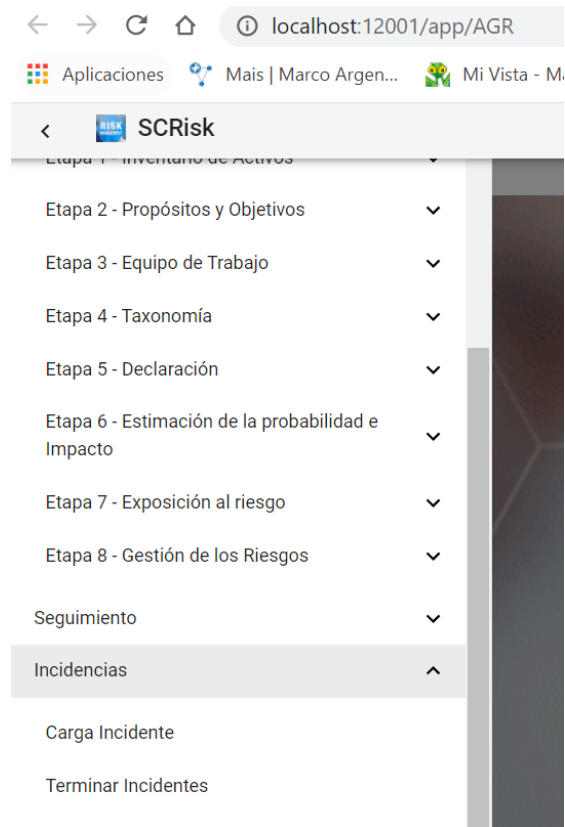


Figura 92 - Menú de seguimiento

Carga Incidente

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

En este estudio de caso, simulamos el siguiente incidente:

- El modelo VPN de la empresa de telecom, está sin energía.
- El profesional encendió el equipo, llamó a la empresa proveedora del servicio y avisó a los integrantes de un grupo vía un software de mensajería.

En la figura 93 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.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

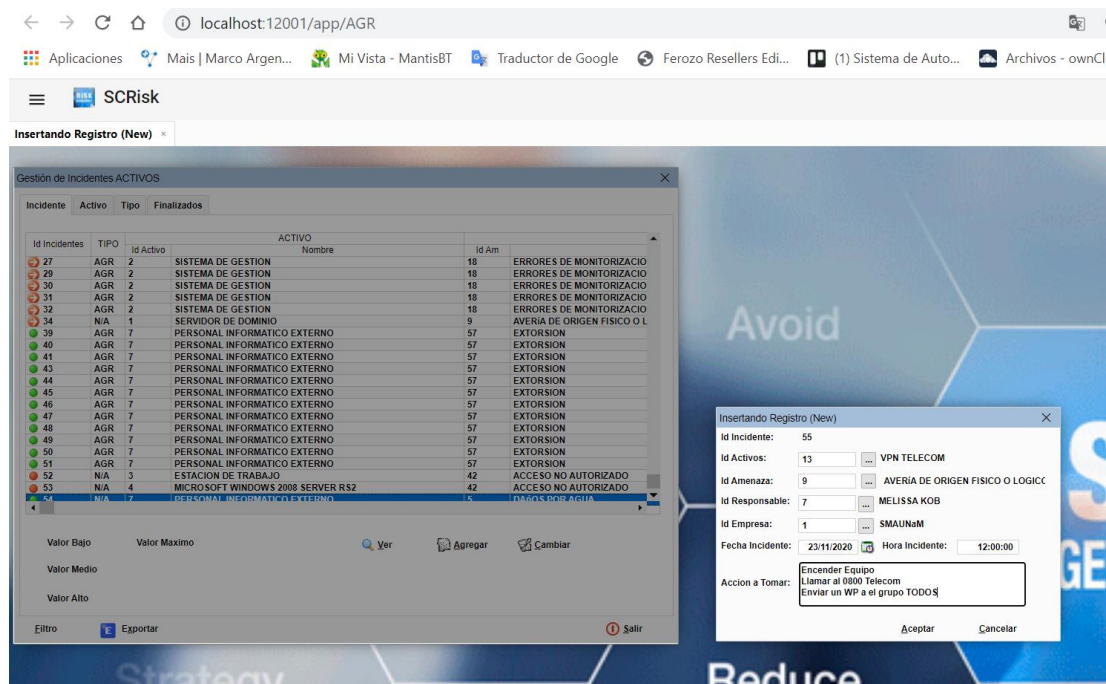


Figura 93 - Carga de incidente

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 94).

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

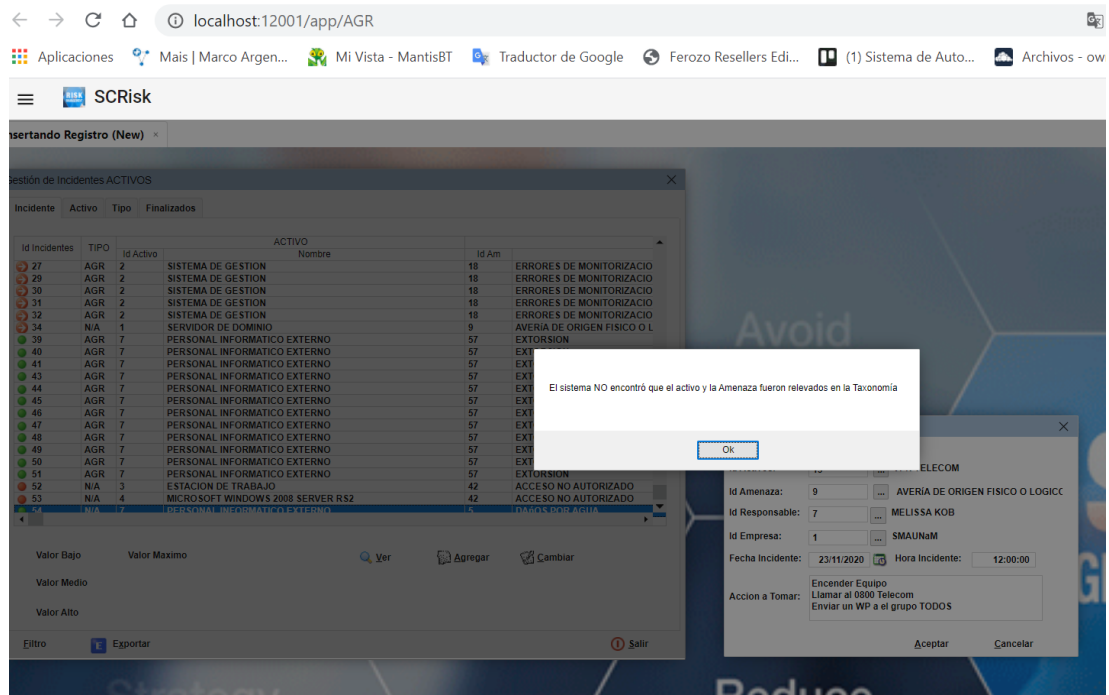


Figura 94 - Control de tipo de riesgo

Punto 2 – Si el activo seleccionado posee un riesgo asociado, y este, está gestionado, el sistema muestra al operador, el/los riesgos que posee este activo, mostrando información detallada sobre la gestión del riesgo al usuario, como muestra la figura 95. El usuario deberá seleccionar el riesgo correspondiente.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

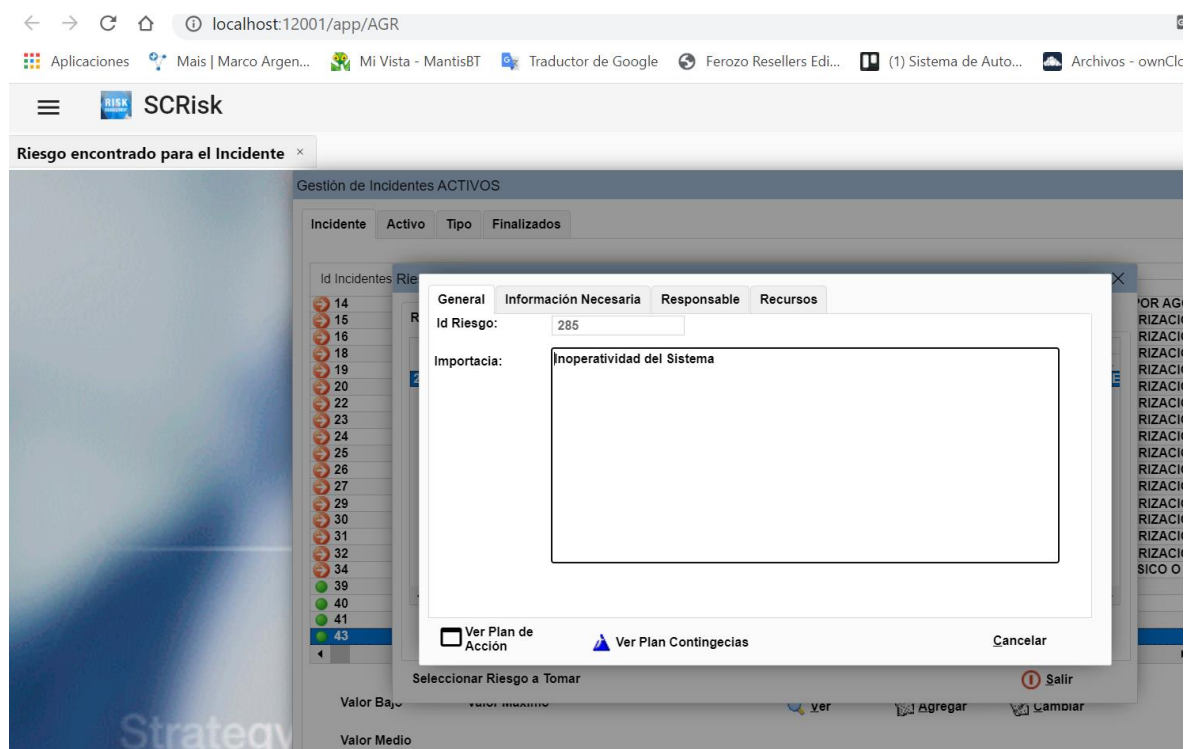


Figura 95 - Detalle de riesgos encontrado

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 96), 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 96 - 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 97).

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:

- Si el incidente se solucionó correctamente
- Si el plan de contingencias utilizado resultó adecuado (esta opción se activa si el riesgo está gestionado y posee plan de contingencias).
- 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.

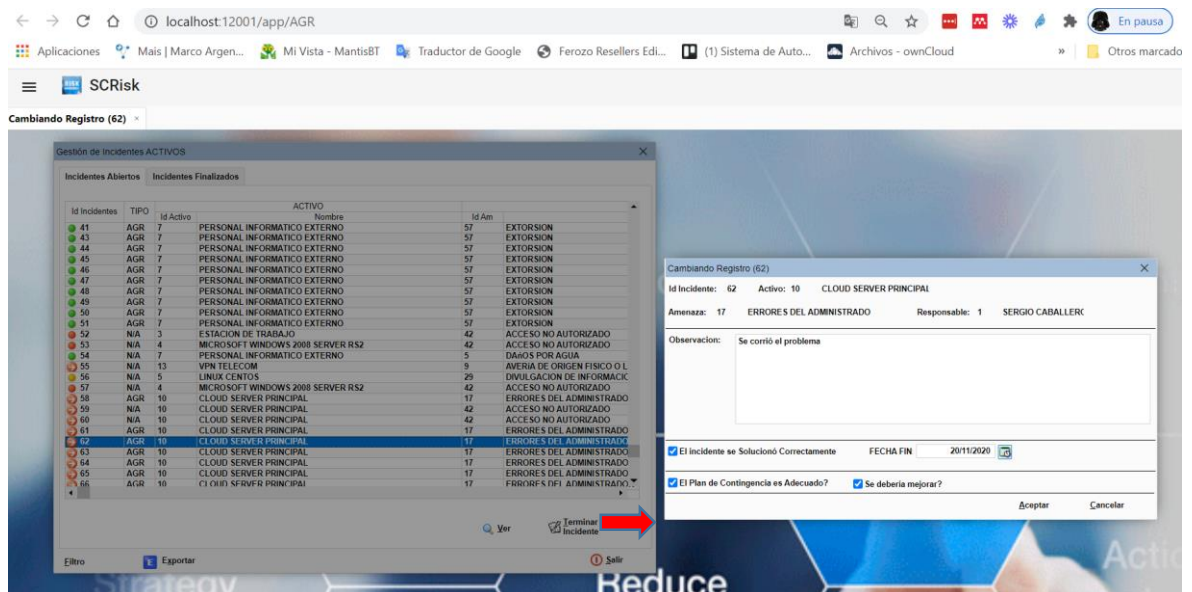


Figura 97 - Finalización de un incidente

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

Capítulo C – Gestión de Conocimiento

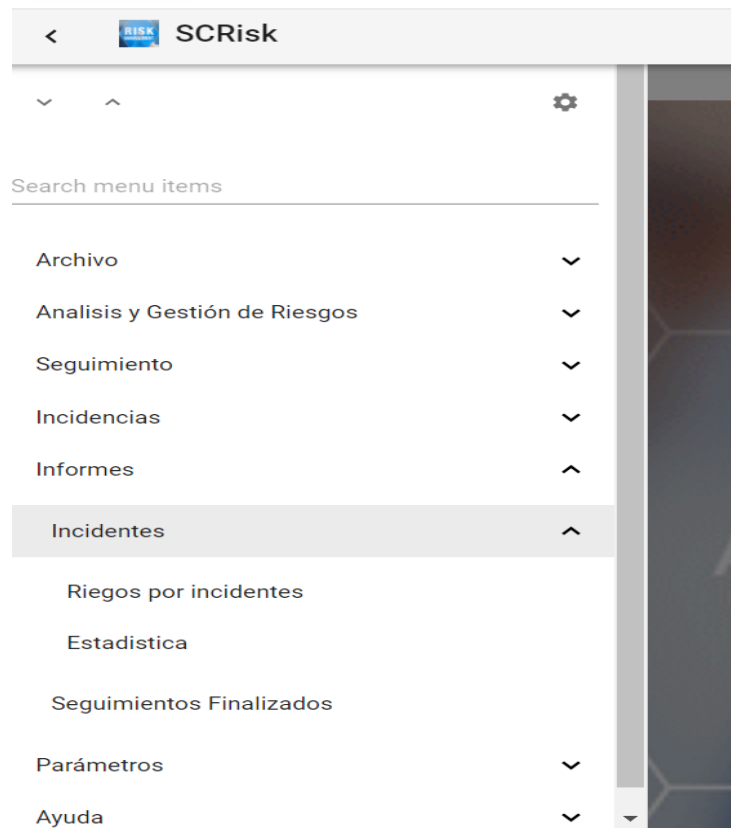


Figura 98 - Menú de Informes

Etapa Conocimiento Explícito

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 99 se muestra en el informe, solamente los incidentes que terminaron correctamente y utilizando el filtro avanzado que posee este módulo,

The screenshot shows the SCRisk application interface. The main window is titled 'Informe de Incidentes por Riesgo'. It features a tabbed interface with options: 'Totales', 'Terminados Bien', 'Terminados Mal', 'Pendientes', 'Activos sin AGR', 'Activos AR', and 'Activos AGR'. The 'Terminados Bien' tab is selected. The table below shows a list of incidents with the following columns: Id In, Fecha Inci, Hora Inci, Accion a Tomar, Id R, Importacia, Riesgos, and Nombre. The table is filtered to show incidents that have been resolved correctly. The 'Consultas' section at the bottom allows for advanced filtering.

Id In	Fecha Inci	Hora Inci	Accion a Tomar	Id R	Importacia	Riesgos	Nombre
48	18/12/2010	09:00:00		246	Problemas Legales.	A.29	EXTORSION
49	18/12/2010	08:00:00	ii	246	Problemas Legales.	A.29	EXTORSION
50	18/12/2010	09:00:00	kk	246	Problemas Legales.	A.29	EXTORSION
51	18/12/2010	09:00:00		246	Problemas Legales.	A.29	EXTORSION
52	18/08/2020	12:00:00	reportar	0		A.11	ACCESO NO AUTORIZADC
53	18/08/2020	12:00:00	prueba	0		A.11	ACCESO NO AUTORIZADC
54	29/08/2020	19:00:00	Falto	0		I.2	DAÑOS POR AGUA
55	23/11/2020	12:00:00	Encender Equipo	0	Llamar al 0800 Te	I.5	AVERIA DE ORIGEN FISIC
56	17/11/2020	12:00:00	Se realizó una copia de seguridad	0		E.19	DIVULGACION DE INFORM
57	10/11/2020	12:00:00		0		A.11	ACCESO NO AUTORIZADC
58	11/11/2020	12:00:00		0		E.2	ERRORES DEL ADMINISTF
59	12/11/2020	09:00:00		0		A.11	ACCESO NO AUTORIZADC
60	12/11/2020	12:00:00		0		A.11	ACCESO NO AUTORIZADC
61	12/11/2020	12:00:00	12	0		E.2	ERRORES DEL ADMINISTF
62	23/11/2020	12:00:00		285	Inoperatividad del Sistema	E.2	ERRORES DEL ADMINISTF
63	23/11/2020	01:00:00		285	Inoperatividad del Sistema	E.2	ERRORES DEL ADMINISTF
64	18/11/2020	12:00:00		285	Inoperatividad del Sistema	E.2	ERRORES DEL ADMINISTF
65	17/11/2020	01:00:00		285	Inoperatividad del Sistema	E.2	ERRORES DEL ADMINISTF
66	12/11/2020	00:00:00		285	Inoperatividad del Sistema	E.2	ERRORES DEL ADMINISTF

The 'Consultas' section at the bottom allows for advanced filtering with the following fields: Columna, Operador, Valor/Expresión, and Operador de Conexión. There are also buttons for 'Exportar', 'Limpiar', 'Grabar Filtro', 'Grabar Como', 'Cargar Filtro', and 'Aplicar'.

Figura 99 - Menú de Informes

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 100).

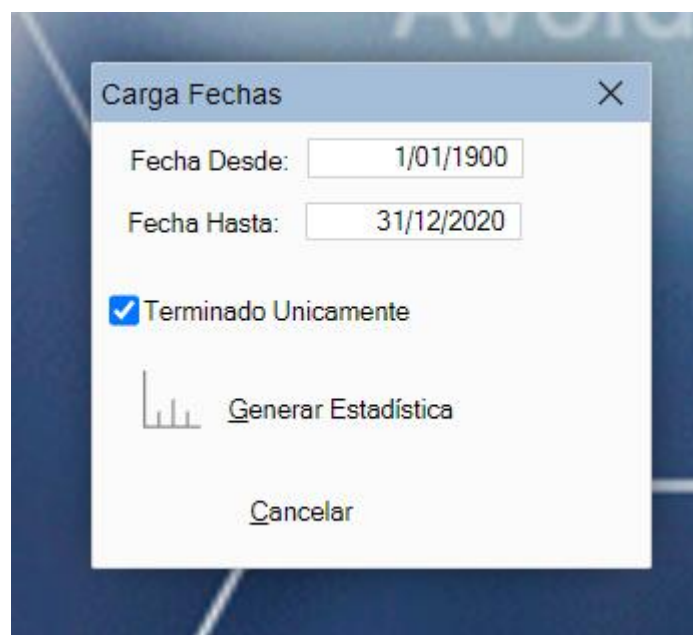


Figura 100 - Parámetros de estadística

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 101).

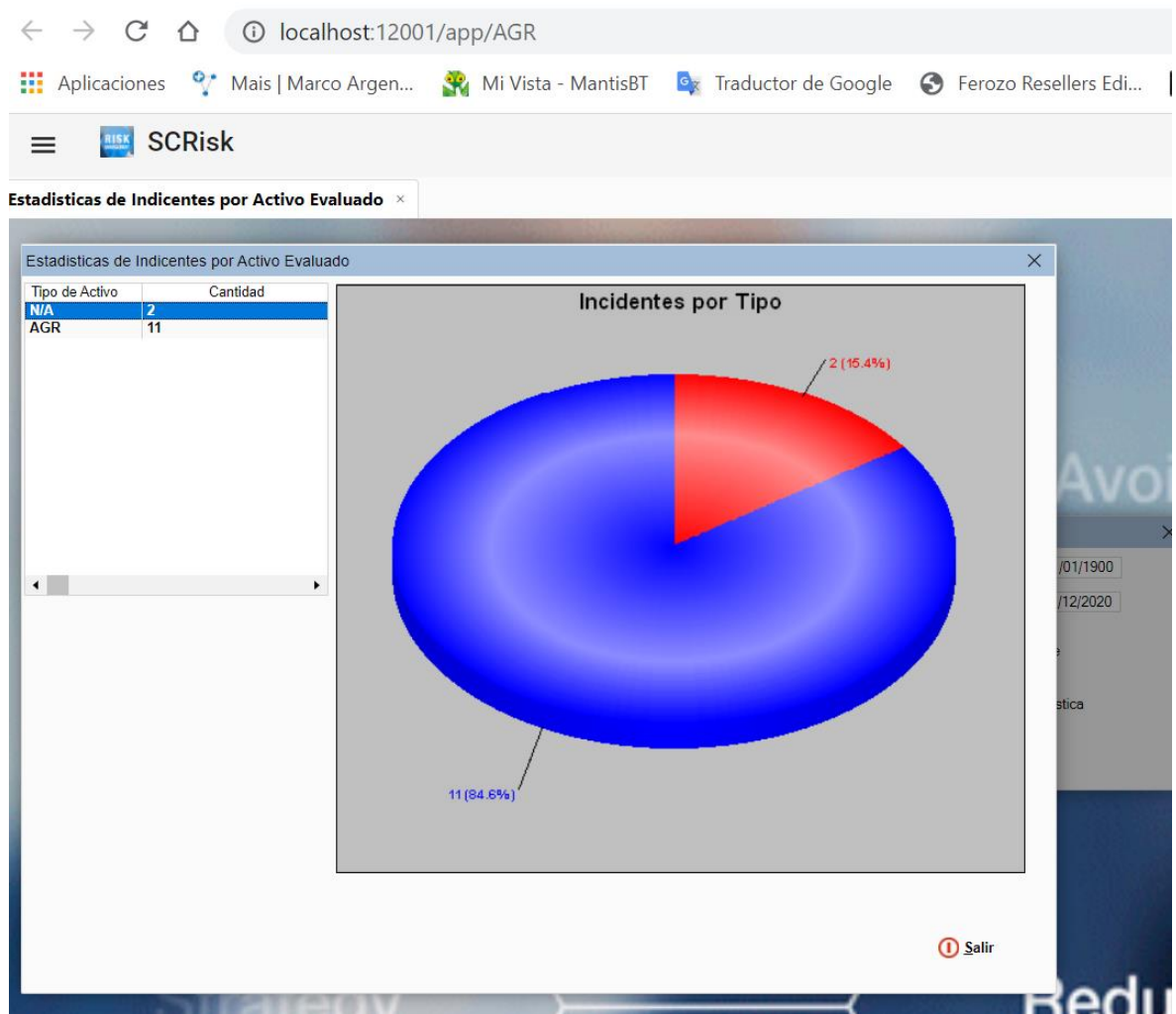


Figura 101 - Estadística de incidentes por activo evaluado

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: muestra 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 102, el módulo cuenta con un componente de filtrado de datos.

Sección de Seguimientos Realizados en SCRISK:

Actividad por Fecha	Por Salvaguarda	Por Amenaza	Por Dimension	Terminado Bien	Terminado Mal
RIESGO					
Id Riesgo	Importancia	Fecha	% Realizado	Id S	SALVAGUARDA Desc. Salv.
1	Lentitud de Conexión, de Procesos.	23/08/2010	100.00	5	PROTECCION DE COMUNICACIONES
1	Lentitud de Conexión, de Procesos.	23/08/2010	100.00	5	PROTECCION DE COMUNICACIONES
1	Lentitud de Conexión, de Procesos.	4/09/2010	100.00	5	PROTECCION DE COMUNICACIONES
1	Lentitud de Conexión, de Procesos.	29/08/2020	100.00	5	PROTECCION DE COMUNICACIONES
1	Lentitud de Conexión, de Procesos.	12/11/2020	100.00	5	PROTECCION DE COMUNICACIONES
134	RR	16/11/2020	100.00	2	SALVAGUARDAS PROTECCION DE DATOS - INFOR
134	RR	25/08/2021	100.00	2	SALVAGUARDAS PROTECCION DE DATOS - INFOR

Consultas:

Columna	Operador	Valor/Expresión	Operador conexión
---------	----------	-----------------	-------------------

Botones: ☐ Respetar Mayusculas, Limpiar, Guardar, Guardar Como, Cargar, Aplicar, Exportar, Salir

Figura 102 - Seguimientos realizados

Anexo II - Tablas de Elementos y Amenazas

Estructura de desarrollo de 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, evaluar 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

Elementos de un Activo

Código	Descripción	Tipo Activo
anom	ANONIMO	SR
pub	PUBLICO GENERAL	SR
ext	USUARIO EXTERNO	SR
int	INTERNO	SR
cont	CONTRATO A TERCEROS	SR
www	WORLD WIDE WEB	SR

telnet	ACCESO REMOTO A CUENTAS LOCALES	SR
email	CORREO ELECTRONICO	SR
file	ALMACENAMIENTO DE FICHEROS	SR
ftp	TRANSFERENCIA DE ARCHIVOS	SR
edi	INTERCAMBIO ELECTRONICO DE DATOS	SR
dir	SERVICIO DE DIRECCIONES	SR
idm	GESTION DE USUARIOS	SR
ipm	GESTION DE PRIVILEGIOS	SR
pki	INFRAESTRUCTURA DE CLAVE PUBLICA	SR
vr	DATOS VITALES	DI
com	DATOS DE INTERES COMERCIAL	DI
adm	DATOS DE INTERES PARA LA ADMINISTRACION PUB	DI
int	DATOS DE GESTION INTERNA	DI
voice	VOX	DI
multimedia	MULTIMEDIA	DI
source	CODIGO FUENTE	DI
exe	CODIGO EJECUTABLE	DI
conf	DATOS DE CONFIGURACION	DI
log	REGISTRO DE ACTIVIDAD	DI
test	DATOS DE PRUEBA	DI
per A	DATOS DE CARACTER PERSONAL ALTO	DI
per M	DATOS DE CARACTER PERSONAL MEDIO	DI
per B	DATOS DE CARACTER PERSONAL BAJO	DI
label S	DATOS SECRETOS	DI
label R	DATOS RESERVADOS	DI
label C	DATOS CONFIDENCIALES	DI
label DL	DATOS CON DIFUSION LIMITADA	DI
label SC	DATOS SIN CLASIFICAR	DI
prp	DESARROLLO PROPIO	AP
sub	DESARROLLO A MEDIDA	AP
std	ESTANDAR	AP
browser	NAVEGADOR WEB	AP
www	SERVIDOR DE PRESENTACIÓN	AP
app	SERVIDOR DE APLICACIONES	AP
email_client	CLIENTE DE CORREO ELECTRONICO	AP
file	SERVIDOR DE FICHEROS	AP
dbms	SISTEMA DE GESTION DE BASE DE DATOS	AP
tm	MONITO TRANSACCIONAL	AP
office	OFIMATICA	AP
av	ANTI VIRUS	AP
os	SISTEMA OPERATIVO	AP
ts	SERVIDOR DE TERMINALES	AP

backup	SISTEMA DE COPIAS DE SEGURIDAD	AP
host	GRANDES EQUIPOS	EI
mid	EQUIPOS MEDIANOS	EI
pc	COMPUTADOR PERSONAL	EI
mobile	INFORMATICA MOVIL	EI
pda	AGENDAS ELECTRONICAS	EI
easy	FACILMENTE REEMPLAZABLE	EI
data	ALMACENA DATOS	EI
print	MEDIOS DE IMPRESION	EI
scan	SCANNER	EI
crypto	DISPOSITIVOS CRIPTOGRAFICOS	EI
modem	MODEM	EI
hub	CONCENTRADORES	EI
switch	CONMUTADORES	EI
router	ENCAMINADORES	EI
bridge	PASARELAS	EI
firewall	CORTA FUEJOS	EI
wap	PUNTO DE ACCESO WIRELESS	EI
pabx	CENTRAL TELEFONICA	EI
PSTN	RED TELEFONICA	RC
ISDN	RDSI RED DIGITAL	RC
x25	X25 RED DE DATOS	RC
adsl	ADSL	RC
pp	PUNTO A PUNTO	RC
radio	RED INALAMBRICA	RC
sat	SATELITE	RC
lan	RED DE AREA LOCAL	RC
man	RED METROPOLITANA	RC
internet	INTERNET	RC
vpn	RED PRIVADA VIRTUAL	RC
disk	DISCOS	SI
san	ALMACENAMIENTO EN RED	SI
diskettes	DISKETTES	SI
cd	CD ROM	SI
usb	DISPOSITIVO USB	SI
dvd	DVD	SI
tape	CINTA MAGNETICA	SI
mc	TARGETAS DE MEMORIA	SI
ic	TARGETAS INTELIGENTES	SI
printed	MATERIAL IMPRESO	SI
ctape	CINTA DE PAPEL	SI
film	MICRO FILM	SI
cards	TARGETAS PERFORADAS	SI

power	FUENTA DE ALIMENTACION	EA
ups	SISTEMA DE ALIMENTACION ININTERRUMPIDA	EA
ups	SISTEMA DE ALIMENTACION ININTERRUMPIDA	EA
gen	GENERADORES ELECTRICOS	EA
ac	EQUIPOS DE CLIMATIZACION	EA
cabling	CABLEADO	EA
rtape	ROBOT DE CINTA	EA
rdisk	ROBOT DE DISCO	EA
supply	SUMINISTROS ESENCIALES	EA
destroy	EQUIPOS DE DESTRUCCION	EA
furniture	MOBLILIARIO	EA
safe	CAJAS FUERTES	EA
site	EMPLAZAMIENTO	IN
building	EDIFICIO	IN
local	LOCAL	IN
car	VEHICULO TERRESTRE	IN
plane	VEHICULO AEREO	IN
ship	VEHICULO MARITIMO	IN
shelter	CONTENEDORES	IN
channel	CANALIZACION	IN
ue	USUARIOS EXTERNOS	PR
ui	USUARIOS INTERNOS	PR
op	OPERADORES	PR
adm	ADMINISTRADORES DE SISTEMAS	PR
con	ADMINISTRADORES DE COMUNICACIONES	PR
dba	ADMINISTRADORES DE BBDD	PR
des	DESARROLLADORES	PR
sub	SUBCONTRATISTAS	PR
prov	PROVEEDORES	PR

Tabla 42 - Amenazas Magerit V3[26]

Amenazas

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

Nota: se describe textualmente las amenazas del catálogo de elementos [78], para no generar malos entendidos o interpretaciones erróneas, se han quitado 19 amenazas que no se consideran esenciales para una pyme.

Las amenazas se agrupan por tipos y pueden ser[4]:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: que se pueden ver afectados por este tipo de amenazas	Dimensiones: 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

[N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[N.*] Desastres naturales	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	

[I] De origen industrial

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Esta amenaza puede darse de forma accidental o deliberada.

[I.1] Fuego	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	Dimensiones: 1. [D] disponibilidad

Descripción:

incendio: posibilidad de que el fuego acabe con los recursos del sistema.

Origen:

Entorno (accidental)

Humano (accidental o deliberado)

[I.2] Daños por agua

Tipos de activos:

[HW] equipos informáticos (hardware)

[Media] soportes de información

[AUX] equipamiento auxiliar

[L] instalaciones

Dimensiones:

1. [D] disponibilidad

Descripción:

escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.

Origen:

Entorno (accidental)

Humano (accidental o deliberado)

[I.3] Contaminación mecánica

Tipos de activos:

[HW] equipos informáticos (hardware)

[Media] soportes de información

[AUX] equipamiento auxiliar

Dimensiones:

1. [D] disponibilidad

Descripción: vibraciones, polvo, suciedad.

[I.5] Avería de origen físico o lógico

Tipos de activos:

[SW] aplicaciones (software)

[HW] equipos informáticos (hardware)

[Media] soportes de información

[AUX] equipamiento auxiliar

Dimensiones:

1. [D] disponibilidad

Descripción: 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.

[I.6] Corte del suministro eléctrico	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información (electrónicos) [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: cese de la alimentación de potencia	

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.	

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos: [COM] redes de comunicaciones	Dimensiones: 1. [D] disponibilidad
Descripción: 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.	

[E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas.

La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

[E.1] Errores de los usuarios

Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información	Dimensiones: [I] integridad [C] confidencialidad [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc.	

[E.3] Errores de monitorización (log)	
Tipos de activos: [D.log] registros de actividad	Dimensiones: 1. [I] integridad (trazabilidad)
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos.	

[E.4] Errores de configuración	
Tipos de activos: [D.conf] datos de configuración	Dimensiones: 1. [I] integridad
Descripción: 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.	

[E.8] Difusión de software dañino	
Tipos de activos: [SW] aplicaciones (software)	Dimensiones: [D] disponibilidad [I] integridad [C] confidencialidad
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

[E.15] Alteración accidental de la información

Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones	Dimensiones: 1. [I] integridad
Descripción: 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.	

[E.18] Destrucción de información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: 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.	

[E.19] Fugas de información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones [P] personal (revelación)	Dimensiones: 1. [C] confidencialidad
Descripción: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc. En Argentina Ley 25.326	

[E.20] Vulnerabilidades de los programas (software)	
--	--

Tipos de activos: [SW] aplicaciones (software)	Dimensiones: [I] integridad [D] disponibilidad [C] confidencialidad
Descripción: 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.	

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: [SW] aplicaciones (software)	Dimensiones: [I] integridad [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes electrónicos [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	

[E.25] Robo	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar	Dimensiones: [D] disponibilidad [C] confidencialidad
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	

[E.28] Indisponibilidad del personal	
Tipos de activos: [P] personal interno	Dimensiones: 1. [D] disponibilidad
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica.	

[A] Ataques intencionados

Fallos deliberados causados por las personas.

[A.4] Manipulación de los registros de actividad (log)	
Tipos de activos: [D.log] registros de actividad	Dimensiones: 1. [I] integridad (trazabilidad)

[A.4] Manipulación de la configuración	
Tipos de activos: [D.log] registros de actividad	Dimensiones: [I] integridad [C] confidencialidad [A] disponibilidad
Descripción: 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.	

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones	Dimensiones: [C] confidencialidad [A] autenticidad [I] integridad
Descripción: 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.	

[A.7] Uso no previsto	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	Dimensiones: [D] disponibilidad [C] confidencialidad [I] integridad
Descripción: 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.	

[A.8] Difusión de software dañino	
Tipos de activos: [SW] aplicaciones (software)	Dimensiones: [D] disponibilidad [I] integridad [C] confidencialidad
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

[A.11] Acceso no autorizado	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	Dimensiones: 1. [C] confidencialidad 2. [I] integridad

Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.15] Modificación deliberada de la información

Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones	Dimensiones: 1. [I] integridad
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	

[A.18] Destrucción de información

Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [Media] soportes de información [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	

[A.19] Revelación de información

Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones	Dimensiones: 1. [C] confidencialidad
Descripción: revelación de información.	

[A.22] Manipulación de programas

Tipos de activos: [SW] aplicaciones (software)	Dimensiones: [C] confidencialidad [I] integridad [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

[A.22] Manipulación de los equipos	
Tipos de activos: [HW] equipos [Media] soportes de información [AUX] equipamiento auxiliar	Dimensiones: [C] confidencialidad [D] disponibilidad
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

[A.24] Denegación de servicio	
Tipos de activos: [S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones	Dimensiones: 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	

[A.25] Robo	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar	Dimensiones: [D] disponibilidad [C] confidencialidad
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. 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.	

[A.26] Ataque destructivo	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	Dimensiones: 1. [D] disponibilidad
Descripción: 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.	

[A.28] Indisponibilidad del personal	
Tipos de activos: [P] personal interno	Dimensiones: 1. [D] disponibilidad
Descripción: ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.	

[A.30] Ingeniería social (picaresca)	
Tipos de activos: [P] personal interno	Dimensiones: [C] confidencialidad [I] integridad [D] disponibilidad
Descripción: abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

Anexo III - Artefactos utilizados en el Análisis y Diseño

Planificación del Proyecto

SCRisk

21-nov-2020

Servicio Médico Asistencial Universidad Nacional de Misiones

Encargado del proyecto	Sergio Daniel Caballero
Fechas de inicio y fin del proyecto	03-ago-2020 - 10-oct-2020
Progreso	0%
Tarea	8
Recursos	2

Desarrollar un Sistema Software para realizar el análisis y gestión de riesgos basados en el método SCRiskMethod, 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.

SCRisk

21-nov-2020

Tarea

2

Nombre	Fecha de inicio	Fecha de fin
Objetivos Generales	3/08/20	3/08/20
Límites del Sistema	5/08/20	5/08/20
Casos de Requisitos	7/08/20	13/08/20
Caso de Uso	15/08/20	17/09/20
Diagramas de Secuencia	15/08/20	17/09/20
Diseño de Base de Datos	19/09/20	23/09/20
Codificación	25/09/20	9/10/20
Pruebas	25/09/20	9/10/20

SCRisk

Recursos

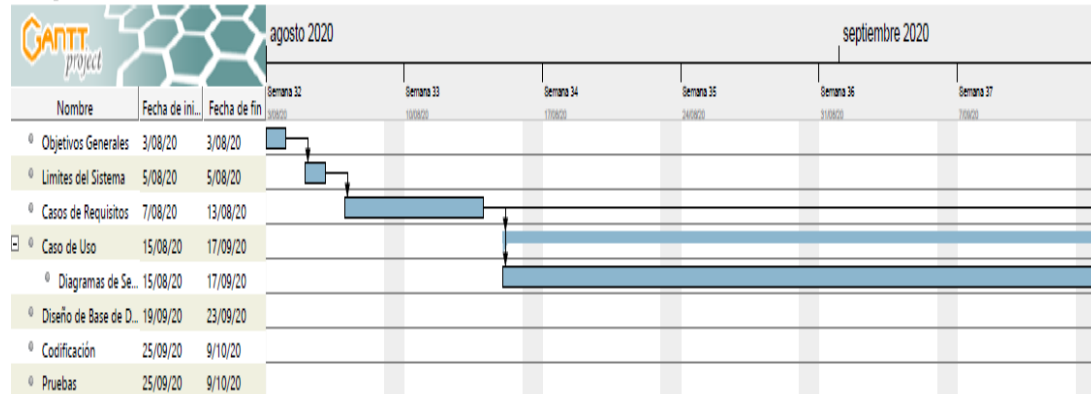
Nombre	Función
Sergio Daniel Caballero	Encargado del proyecto
Horacio Daniel Kuna	Encargado de pruebas

SCRisk

21-nov-2020

Diagrama de Gantt

4



Modelo de Requisitos

Requisitos no funcionales

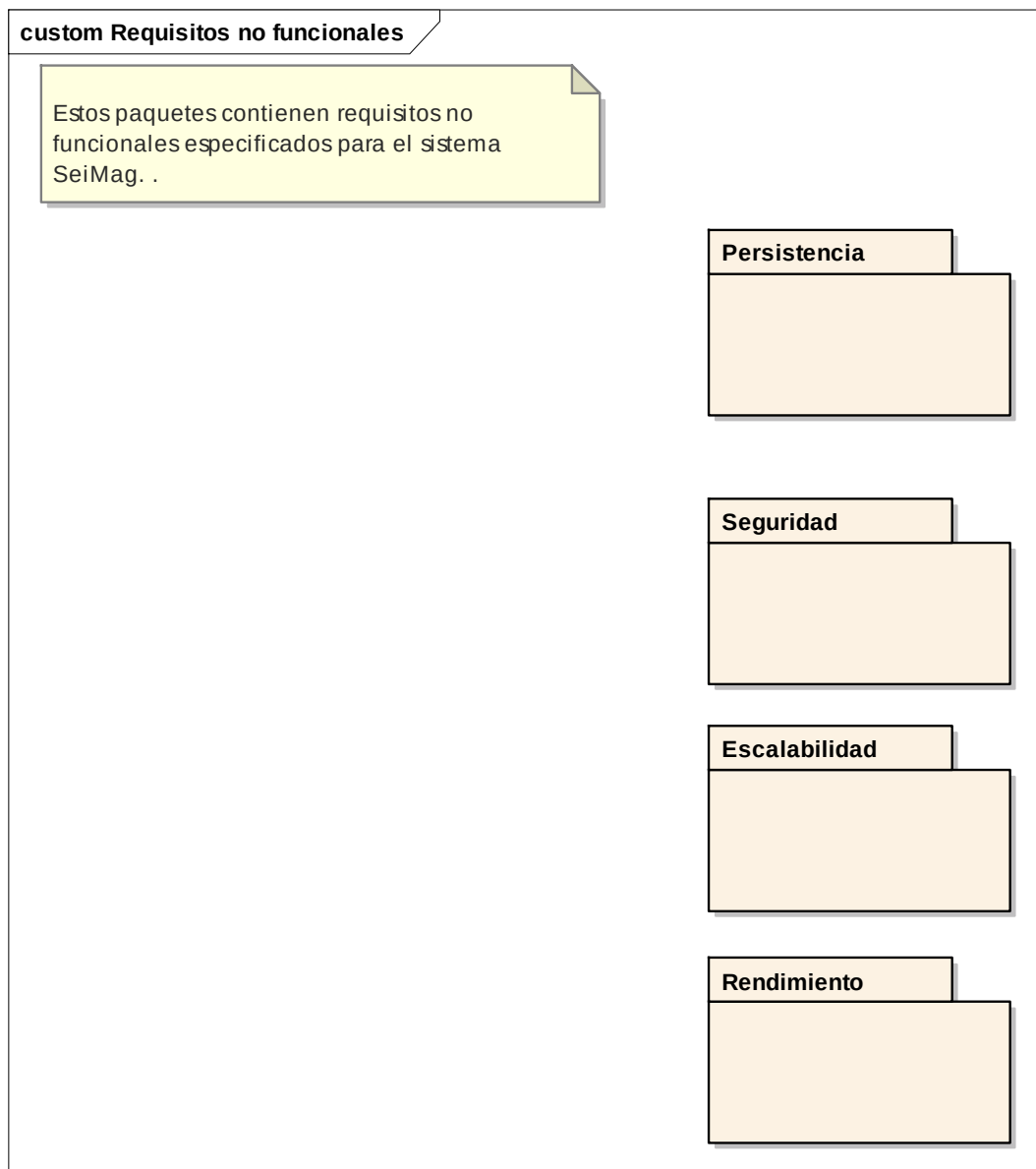


Imagen: Requisitos no funcionales

Nota

Estado: Proposed

Prioridad:

Dificultad:

Fase: 1.0

Versión: 1.0

Estos paquetes contienen requisitos no funcionales especificados para el sistema SCRisk. .

Escalabilidad

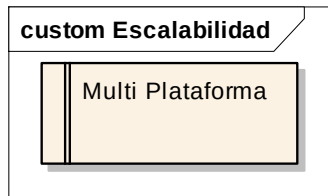


Imagen: Escalabilidad

Multi Plataforma

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

Rendimiento

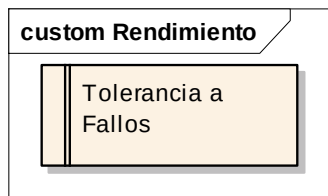


Imagen: Rendimiento

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

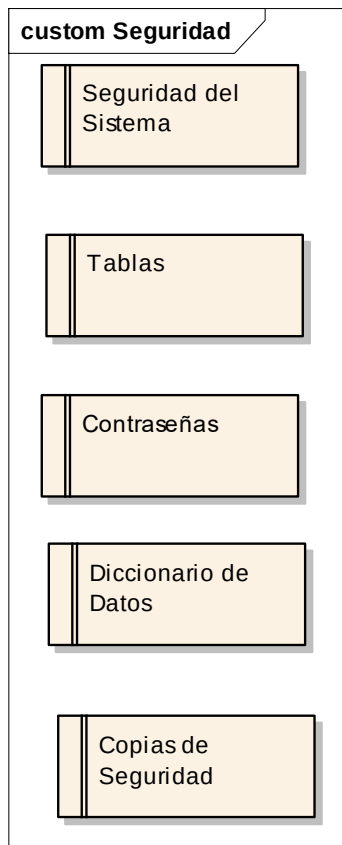


Imagen: Seguridad

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

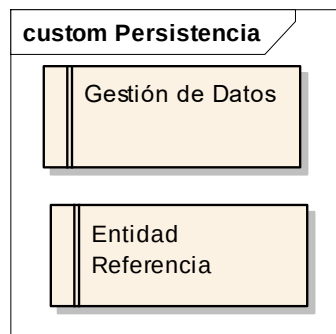


Imagen: Persistencia

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

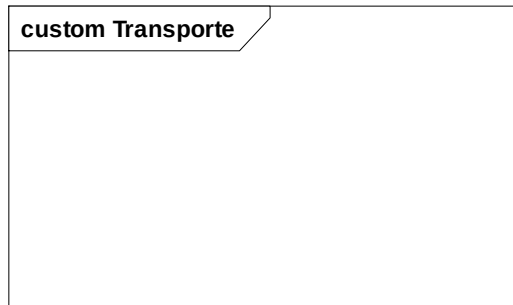


Imagen: Transporte

Requisitos Funcionales

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: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {1AA2EE6C-6BD0-48f8-A179-688E208DF3A7}

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

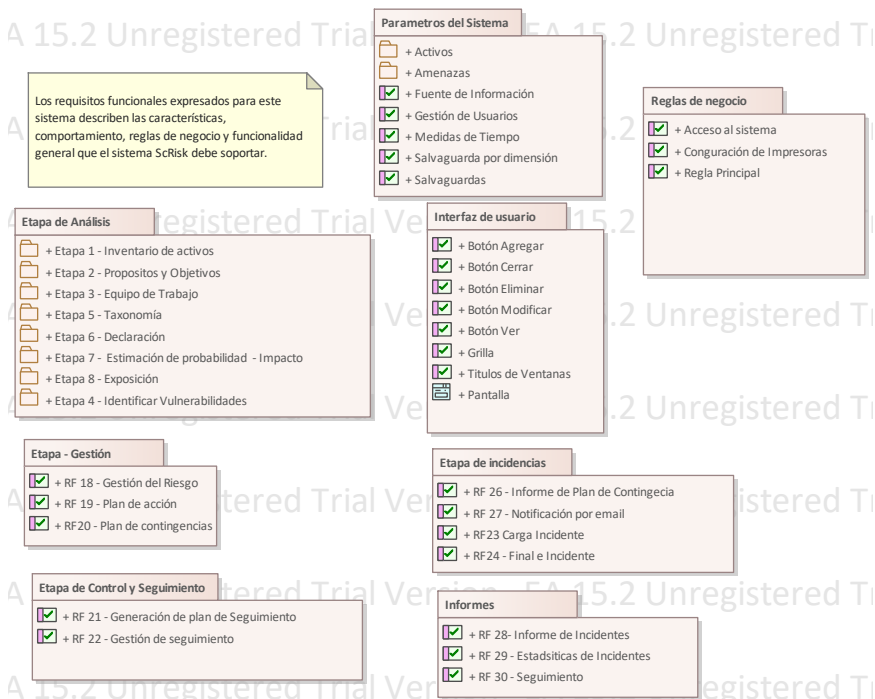


Imagen: 1

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 14/10/2020.

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 RIC debe soportar.

Fase I

Tipo: Paquete

Estado: Proposed. Versión 1.0. Fase 1.0.

Paquete: Requisitos funcionales

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020

GUID: {44CE00F4-0838-40f7-8469-D579509002B6}

Fase 1 del método Sei - Mag

Fase I - (diagrama Requirements)

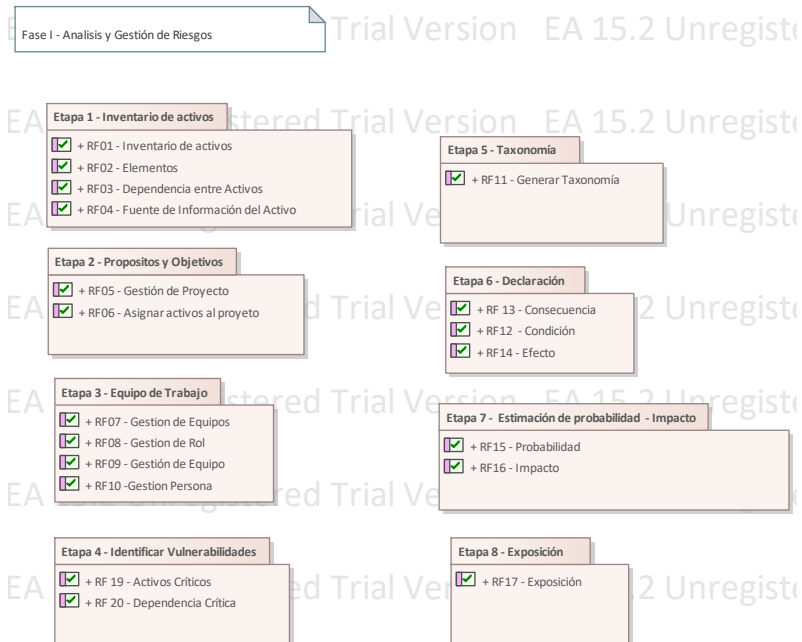
Creado por: caballerosd el 13/10/2020

Última modificación: 14/10/2020

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Versión: 1.0. Bloqueado: Falso
GUID: {F1F38762-D31A-4171-9A10-13935C346FDE}



<Anónimo>

Tipo: Nota
Estado: Propuesto. Versión 1.0. Fase 1.0.
Paquete: Fase I Palabras claves:
Detalle: Creado el 14/10/2020. Última modificación el 14/10/2020.
GUID: {23DBA207-5B8E-4850-8FD1-B223D20B0701}

Fase I - Análisis y Gestión de Riesgos

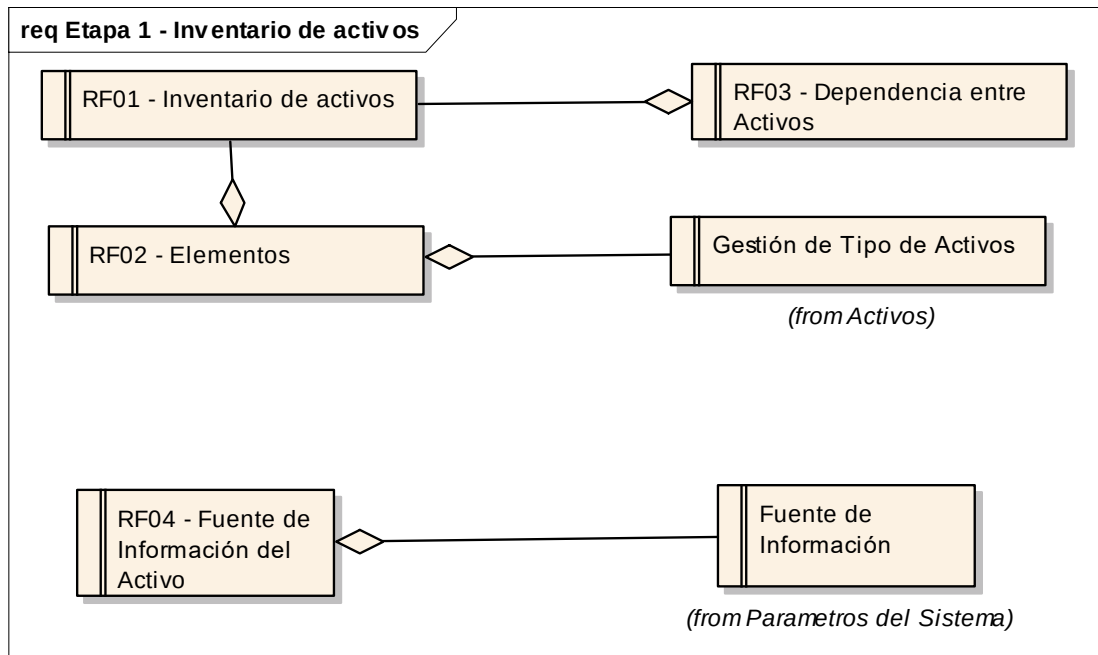
E1 - Inventario de activos

Tipo: Paquete
Estado: Proposed. Versión 1.0. Fase 1.0.
Paquete: Fase I
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020
GUID: {40EB49F3-CF03-4871-B094-DFA8E45B12AD}

E1 - Inventario de activos - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020
Última modificación: 13/10/2020
Versión: 1.0. Bloqueado: Falso

GUID: {F1306217-1B7D-436f-8A0E-C1FC74888F1A}



RF01 - Inventario de activos

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Etapa 1 - Inventario de activos Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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	

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Connector	Origen	Destino	Notas
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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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	

Connector	Origen	Destino	Notas
		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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020

GUID: {F7C57FC0-BFCD-44d1-805B-8DA1757A8D3F}

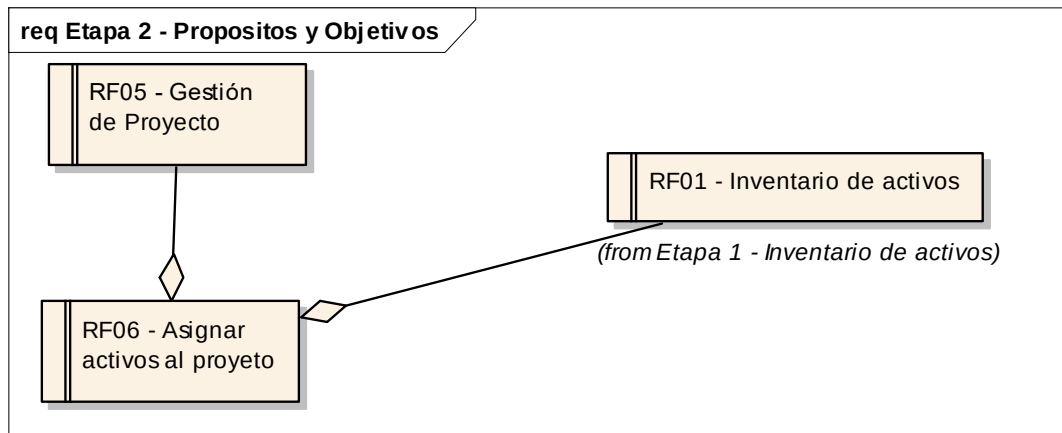
Etapa 2 - Propósitos y Objetivos - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {734C9DEE-F26F-49d0-8876-9D76BCEAE495}



RF05 - Gestión de Proyecto

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Etapa 2 - Propósitos y Objetivos Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

GUID: {D4A8DC29-D2A6-4f4f-AD3B-72CFE658C339}

Es necesario asigna activos a los proyectos.

Conexiones

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Connector	Origen	Destino	Notas
Aggregation Origen -> Destino	Public RF05 - Gestión de Proyecto	Public RF06 - Asignar activos al proyecto	
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 13/10/2020. Última modificación el 13/10/2020

GUID: {D0AC9C8D-2344-4b10-ACAB-71924AEC313E}

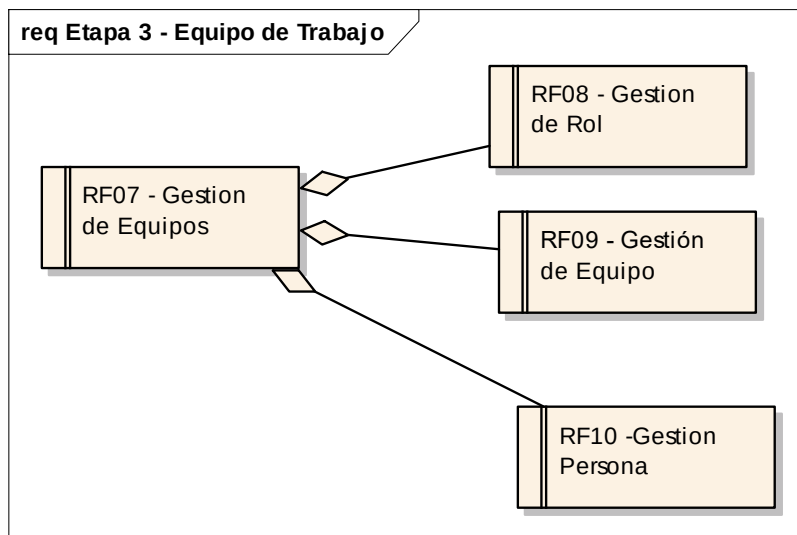
Etapa 3 - Equipo de Trabajo - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {03CCFFE1-1631-48cb-88A6-64C4A04F2402}



RF07 - Gestión de Equipos

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Etapa 3 - Equipo de Trabajo Palabras claves:

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
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.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Paquete: Etapa 3 - Equipo de Trabajo Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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	

RF10 -Gestion Persona

Tipo: Requisito
Estado: . Versión 1.0. Fase 1.0.
Paquete: Etapa 3 - Equipo de Trabajo Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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	

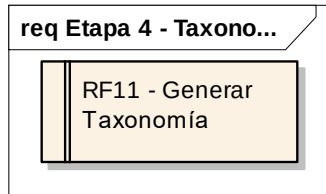
Etapa 4 - Taxonomía

Tipo: Paquete
Estado: Proposed. Versión 1.0. Fase 1.0.
Paquete: Fase I
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020
GUID: {1855F438-B4D0-4b78-9B11-D6FC5EF84918}

Etapa 4 - Taxonomía - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020
Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso
GUID: {1C8A215D-2E7B-463d-AE4F-AC61CC36394B}



RF11 - Generar Taxonomía

Tipo: Requisito
Estado: . Versión 1.0. Fase 1.0.
Paquete: Etapa 4 - Taxonomía Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
GUID: {1834A5E2-D23E-4222-ABE0-DC8F19A8E5A8}

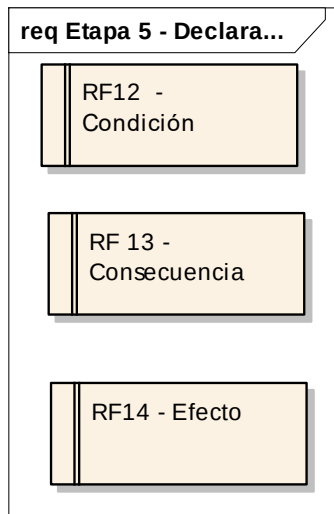
Por cada proyecto es necesario generar automáticamente la taxonomía de los riesgos.

Etapa 5 - Declaración

Tipo: Paquete
Estado: Proposed. Versión 1.0. Fase 1.0.
Paquete: Fase I
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020
GUID: {F9140C3C-732B-45ea-86EC-F9DB6142CFE8}

Etapa 5 - Declaración - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020
Última modificación: 13/10/2020
Versión: 1.0. Bloqueado: Falso
GUID: {0CBCAC52-1B97-4b04-B851-D8F8880E86EE}



RF 13 - Consecuencia

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Etapa 5 - Declaración Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

GUID: {2CA55FB8-0B8B-4d68-A40A-303625019BCD}

Por cada riesgo se define la condición que debe existir para que el 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 13/10/2020. Última modificación el 13/10/2020.

GUID: {DAC775F3-5968-4713-B074-77CE8B4921B5}

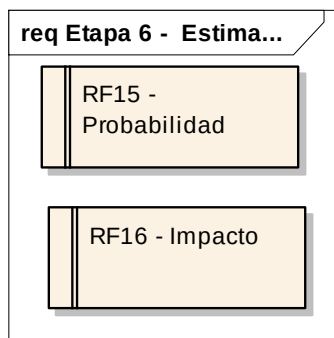
Por cada riesgo se define el efecto que tendrá el problema en la organización.

Etapa 6 - Estimación de probabilidad - Impacto

Tipo: Paquete
Estado: Proposd. Versión 1.0. Fase 1.0.
Paquete: Fase I
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020
GUID: {5D7E1339-35C9-4a88-BD94-AF45FAF9F96C}

Etapa 6 - Estimación de probabilidad - Impacto - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020
Última modificación: 13/10/2020
Versión: 1.0. Bloqueado: Falso
GUID: {273E3A00-C966-438c-8BB6-ECD5A5C9C508}



RF15 - Probabilidad

Tipo: Requisito
Estado: . Versión 1.0. Fase 1.0.
Paquete: Etapa 6 - Estimación de probabilidad - Impacto Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020

GUID: {87F630B4-1CD2-47f5-8F0F-5BF6A4A9F774}

Etapa 7 - Exposición - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {69983725-4DC4-4ed6-BFCD-EB5F14BABCE8}



RF17 - Exposición

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Etapa 7 - Exposición Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020

GUID: {0282B77E-528E-4caf-A680-FBFBC49D7B25}

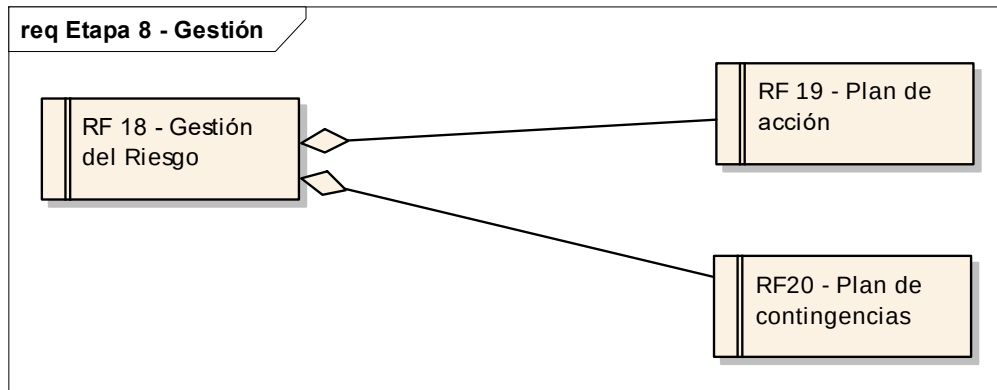
Etapa 8 - Gestión - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {A3496FD9-3D9C-45ee-90DC-88A6D44A8630}



RF 18 - Gestión del Riesgo

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Etapa 8 - Gestión Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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	

RF 19 - Plan de acción

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Tipo: Requisito
Estado: . Versión 1.0. Fase 1.0.
Paquete: Etapa 8 - Gestión Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020
GUID: {0F175C0B-A4EA-4aa8-AC60-ECF9949689B4}

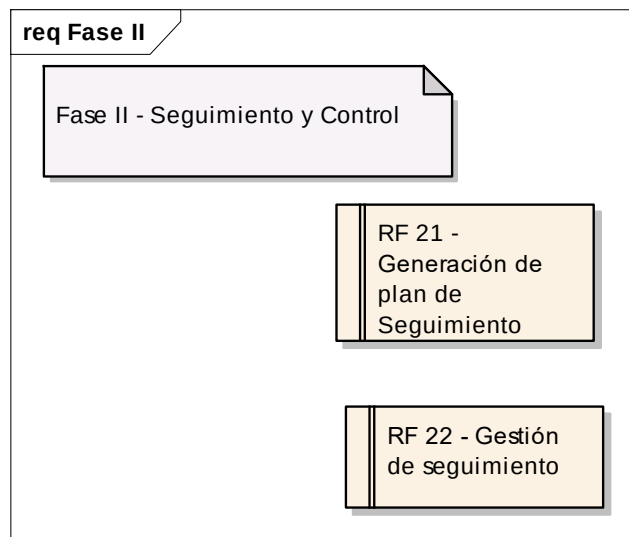
Fase II - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 14/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {874A891A-0BC7-4667-87DB-DEC3FF2E815F}



RF 21 - Generación de plan de Seguimiento

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Fase II Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020

GUID: {C579F58C-F754-4a7b-BCDD-8C454D203C00}

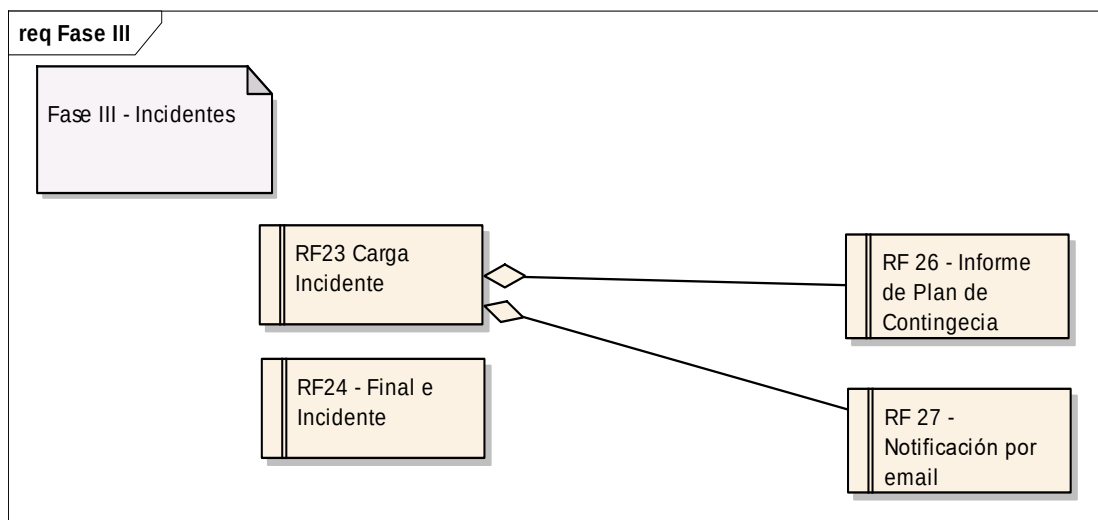
Fase III - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 14/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {EA33E0E5-2CE3-4860-AA9C-19D29E643ECF}



RF 26 - Informe de Plan de Contingencia

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Fase III Palabras claves:

Detalle: Creado el 14/10/2020. Última modificación el 14/10/2020.

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 14/10/2020. Última modificación el 14/10/2020.

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 14/10/2020. Última modificación el 14/10/2020.

GUID: {63CFDC0A-6B12-414c-B20E-9C89D1F28A3F}

El sistema deberá poseer 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 14/10/2020. Última modificación el 14/10/2020.

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 13/10/2020. Última modificación el 13/10/2020

GUID: {844ADD6F-0606-45e1-BDCE-75A6216CD30F}

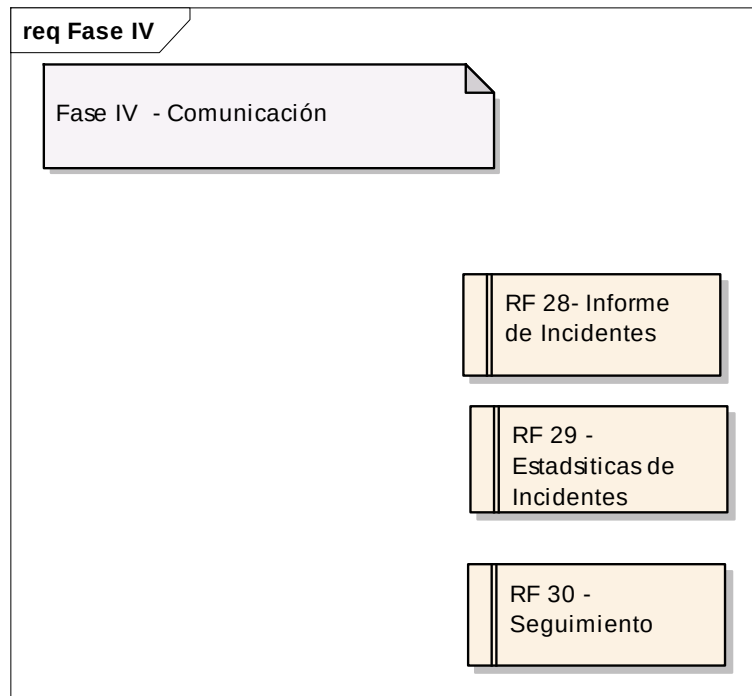
Fase IV - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 14/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {4DFDEBE8-81AB-441a-A60D-D51DF787AADF}



RF 28- Informe de Incidentes

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Fase IV Palabras claves:

Detalle: Creado el 14/10/2020. Última modificación el 14/10/2020.

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 14/10/2020. Última modificación el 14/10/2020.

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 14/10/2020. Última modificación el 14/10/2020.

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 13/10/2020. Última modificación el 13/10/2020

GUID: {97E850D0-CD92-49db-B5CD-B01237D5C940}

Se establecerán los parámetros del sistema antes de comenzar con la Fase I del mismo.

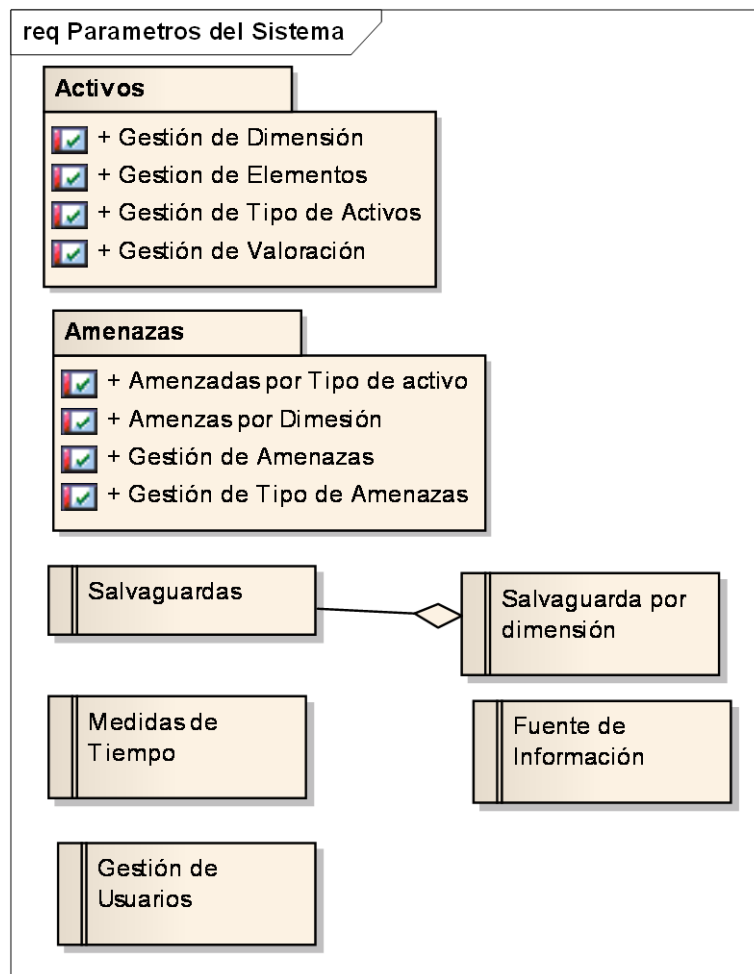
Parametros del Sistema - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {501A0003-444E-4a14-96A1-6B23302F90D1}



Fuente de Información

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Parametros del Sistema Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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.

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Paquete: Parametros del Sistema Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
GUID: {5DD759F7-EF44-40a8-8B71-73320F385F1F}

Las salvaguardas se gestionarán utilizando como base las salvaguardas descriptas en la metodología Magerit V2

Conexiones

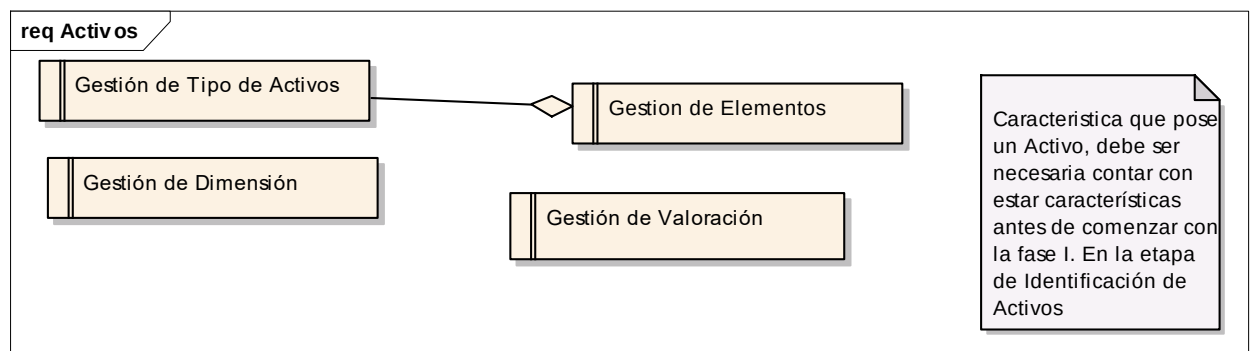
Connector	Origen	Destino	Notas
Aggregation Origen -> Destino	Public Salvaguardas	Public Salvaguarda por dimensión	

Activos

Tipo: Paquete
Estado: Proposed. Versión 1.0. Fase 1.0.
Paquete: Parametros del Sistema
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020
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 13/10/2020
Última modificación: 13/10/2020
Versión: 1.0. Bloqueado: Falso
GUID: {32513E87-D65F-441b-8D55-BB9364663B81}



Gestión de Elementos

Tipo: Requisito
Estado: . Versión 1.0. Fase 1.0.
Paquete: Activos Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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	

Gestión de Dimensión

Tipo: Requisito
Estado: . Versión 1.0. Fase 1.0.
Paquete: Activos Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020

GUID: {1608C238-8F45-4d22-BA06-EB0EA344E7A6}

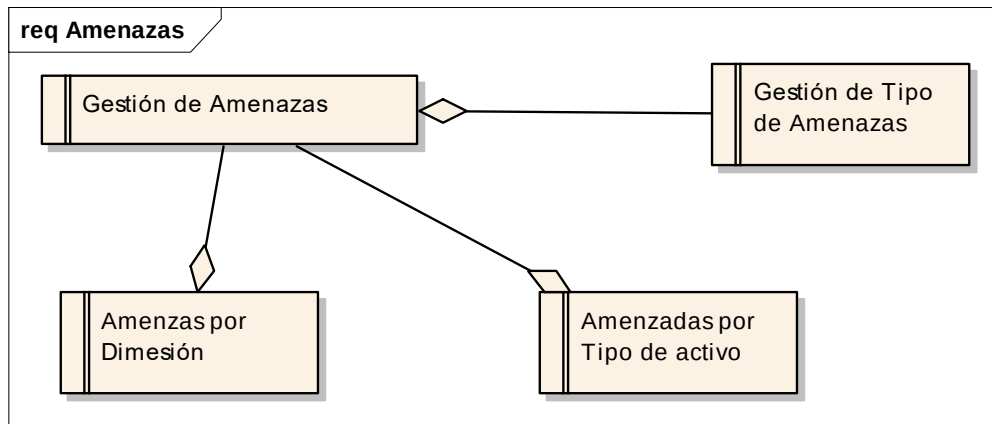
Amenazas - (diagrama Requirements)

Creado por: caballerosd el 13/10/2020

Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {00AC87C1-271E-48b9-BB5A-76C9A794CDC7}



Amenazas por Tipo de activo

Tipo: Requisito

Estado: . Versión 1.0. Fase 1.0.

Paquete: Amenazas Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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}

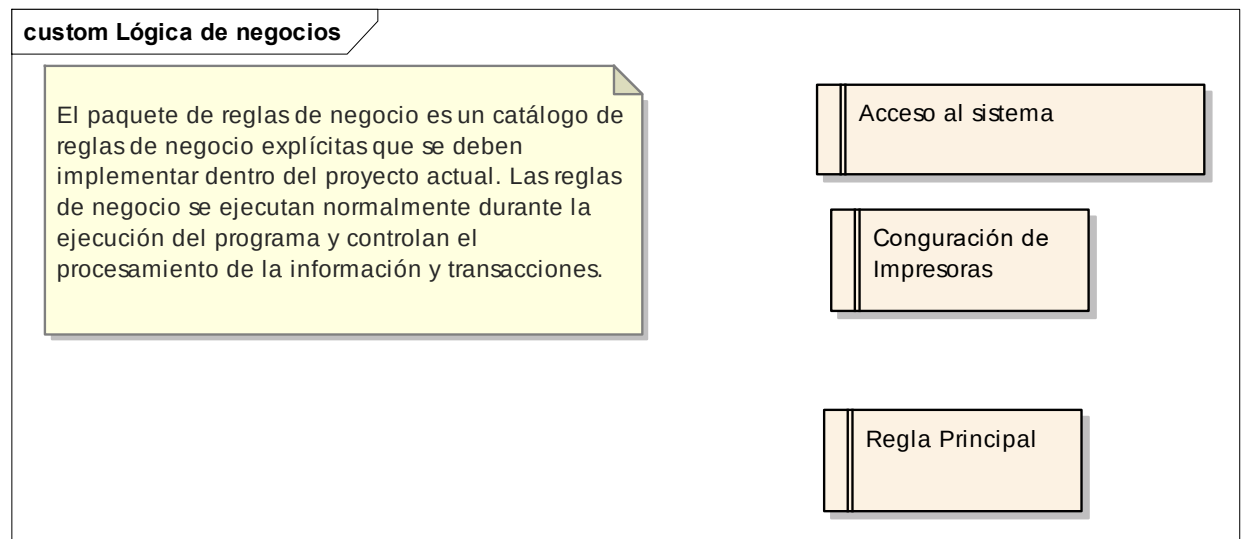
Lógica de negocios - (diagrama Personalizado)

Creado por: caballerosd el 19/11/2005

Última modificación: 13/10/2020

Versión: 1.0. Bloqueado: Falso

GUID: {03E6B261-6C5F-4619-AFB0-A195CB298C50}



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 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
GUID: {393F384C-A5F5-4232-94AC-F66DFEA3283E}

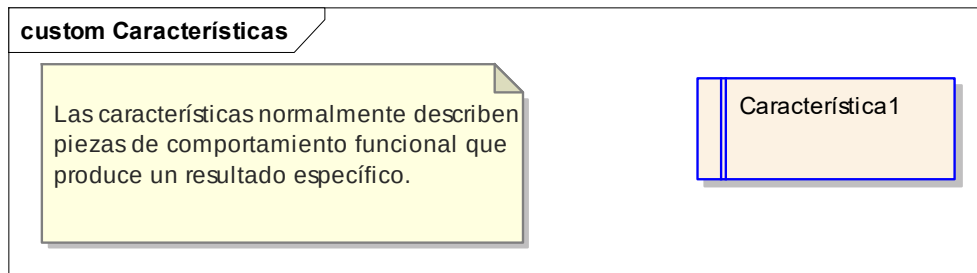
Deberá estar cargadas los parámetros del sistemas antes de comenzar la fase I del AGR.

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}



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

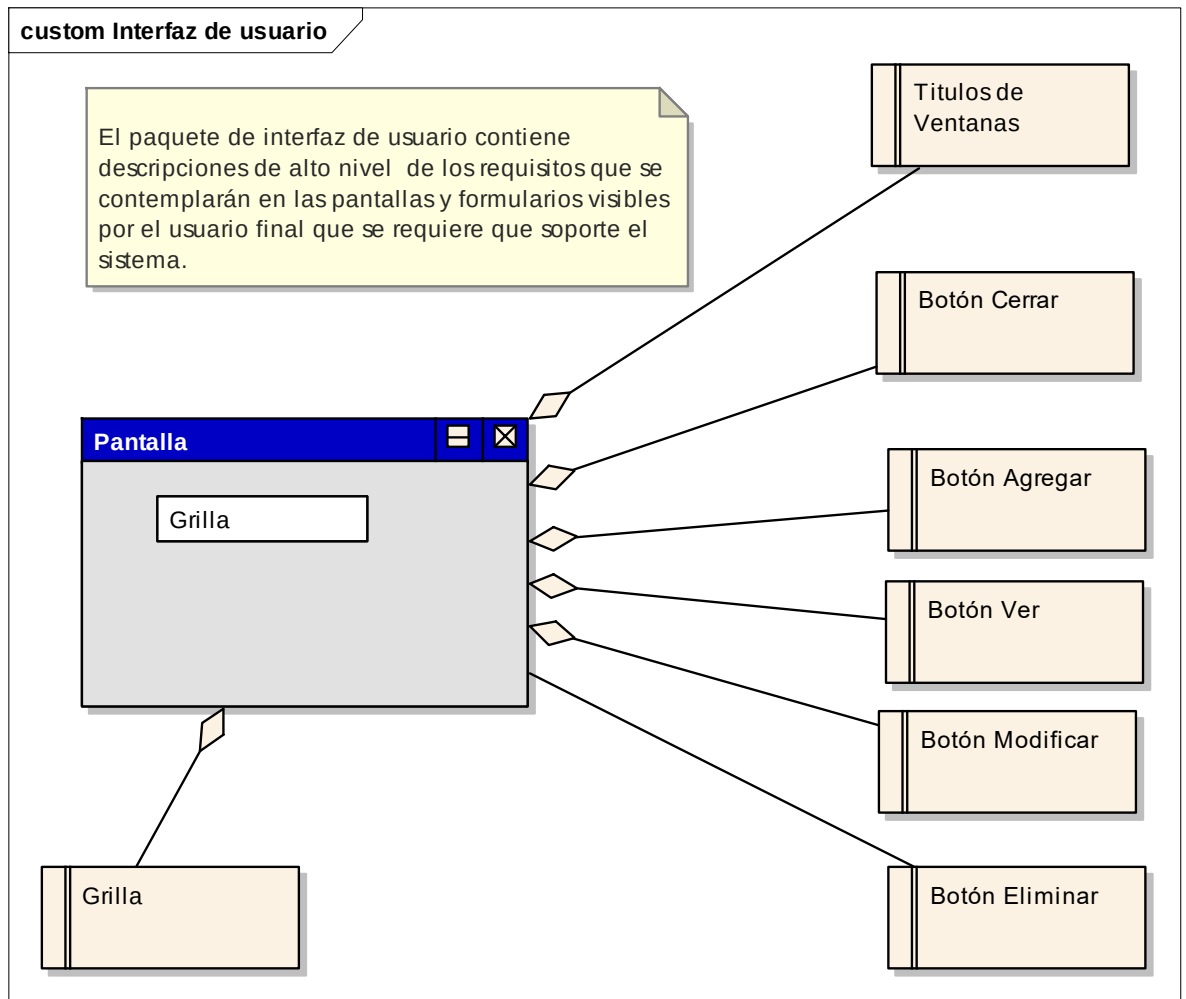
☐ isStatic = Falso

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: 13/10/2020
Versión: 1.0. Bloqueado: Falso
GUID: {76EC4CFE-1E43-4bfe-8855-BE866766A143}



Pantalla

Tipo: Pantalla

Estado: Proposed. Versión 1.0. Fase 1.0.

Paquete: Interfaz de usuario Palabras claves:

Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.

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	

Connector	Origen	Destino	Notas
Aggregation Origen -> Destino	Public Botón Agregar	Public Pantalla	
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 13/10/2020. Última modificación el 13/10/2020.

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 13/10/2020. Última modificación el 13/10/2020.

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

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

Estado: . Versión 1.0. Fase 1.0.
Paquete: Interfaz de usuario Palabras claves:
Detalle: Creado el 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
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

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

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 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.
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 13/10/2020. Última modificación el 13/10/2020.

GUID: {8F51672C-EB3B-4b64-BFAE-2C8E14E24E4A}

Los títulos de las vistas deberán describir acción - descripción de datos . Ej. Alta Personas.

Conexiones

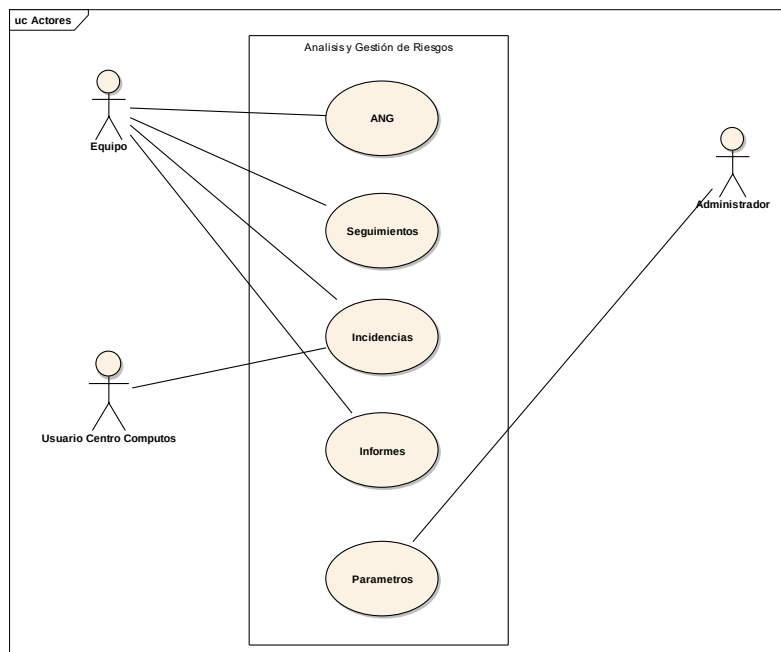
Connector	Origen	Destino	Notas
Aggregation Origen -> Destino	Public Títulos de Ventanas	Public Pantalla	

Modelo de Casos de Uso

Casos de Uso

Modelo de casos de uso

Limites del Sistema



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

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.

Usuario Centro Cómputos

Usuarios de los activos tecnológicos de la organización con conocimientos del modelo de AGR.

Pueden cargar las incidencias.-

ANG

Análisis y Gestión de Riesgos

Inventarios de activos

Propósitos y Objetivos

Equipo de trabajo

Taxonomía

Declaración

Estimación de la Probabilidad

Estimación del Impacto

Exposición al Riesgo

Gestión de Riesgos.

PRE-condición

Estado: Approved

Deben estar cargados todos los parámetros del sistema Previamente

Incidencias

Carga de Incidencias (problemas encontrados sobre un activo)

Gestión de la incidencia por parte del equipo.

Informes
Seguimientos
Terminados
Activos

Incidentes
Riesgos por incidente
Estadísticas.

parámetros
Parámetros del Sistema

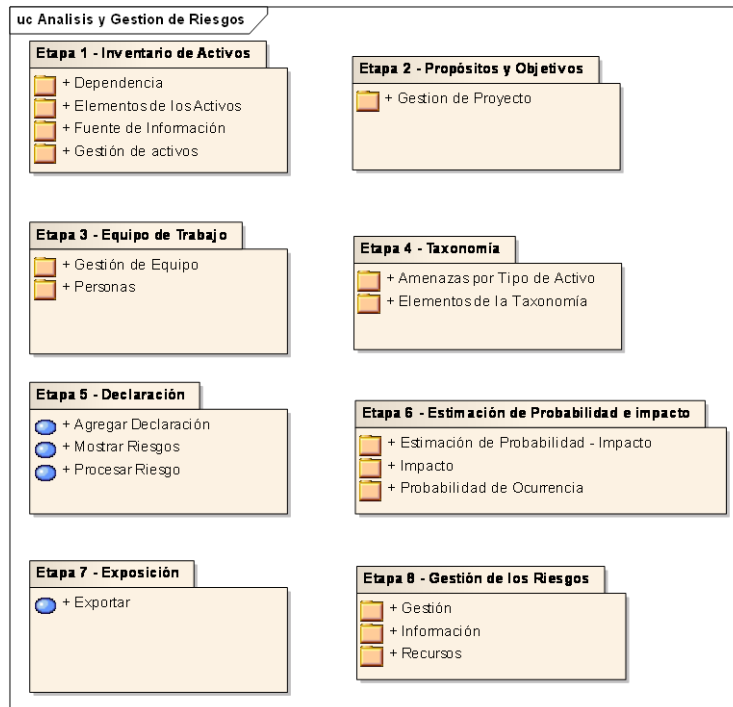
Seguimientos
Seguimiento de los Planes de acción generados en la gestión de los riesgos.
Gestiona las actividades de los usuarios encargados de los seguimientos por amenazas detectadas por activo.

PRE-condición
Estado: Approved
Deben estar cargados la gestión de riesgos y parametrizados las salvaguardas.

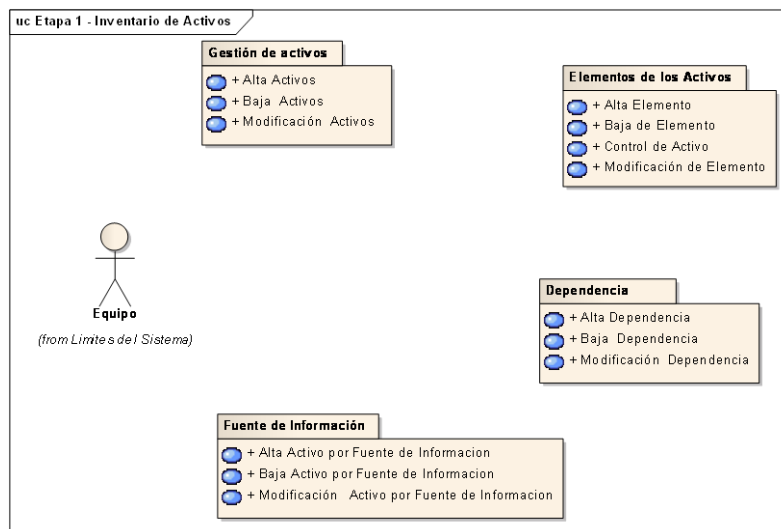
Análisis y Gestión de Riesgos

Análisis de Riesgo en Proyectos Software

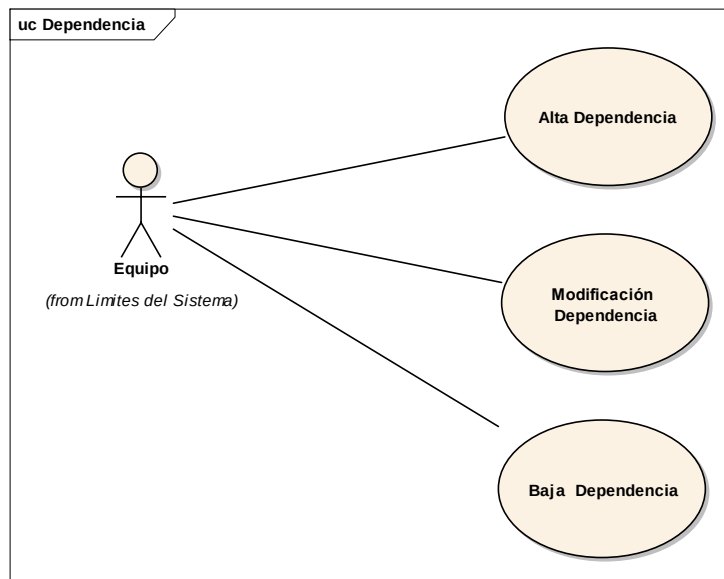
Un nuevo modelo integrando la metodología SEI y Magerit3



Etapa 1 - Inventario de Activos



Dependencia



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 carga 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

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

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

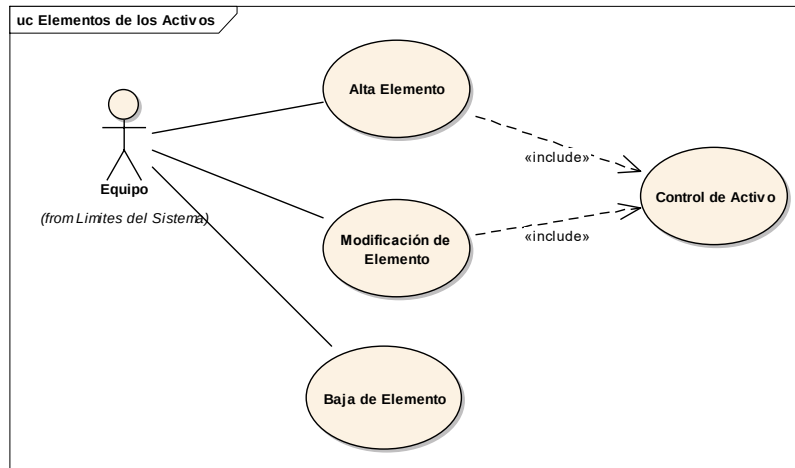
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Elementos de los Activos



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 N° 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

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

Control 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.

Modificación 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

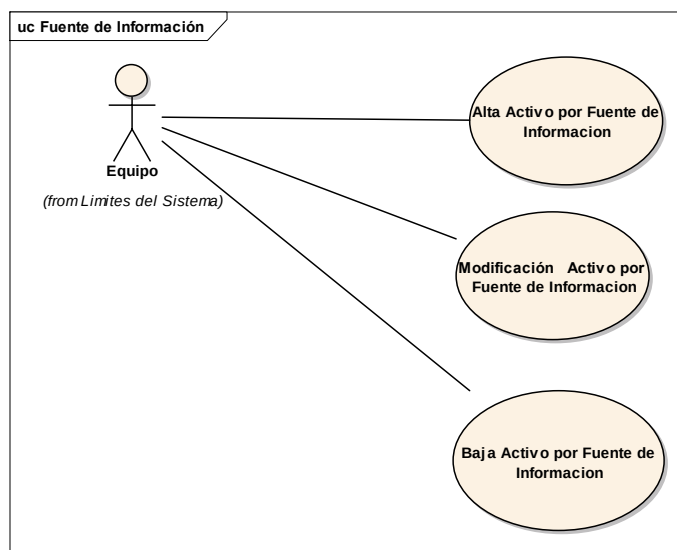
El sistema ejecuta el caso de uso "Control de Activo" y guarda los datos en la base de datos. Y devuelve el control a la grilla.

Invariant

.Se debe seleccionar un registro de la grilla

Estado: Approved

Fuente de Información



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

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

Modificación Activo por Fuente de Información
Gestiona los activos por la fuente de información de donde se recaba los mismos.

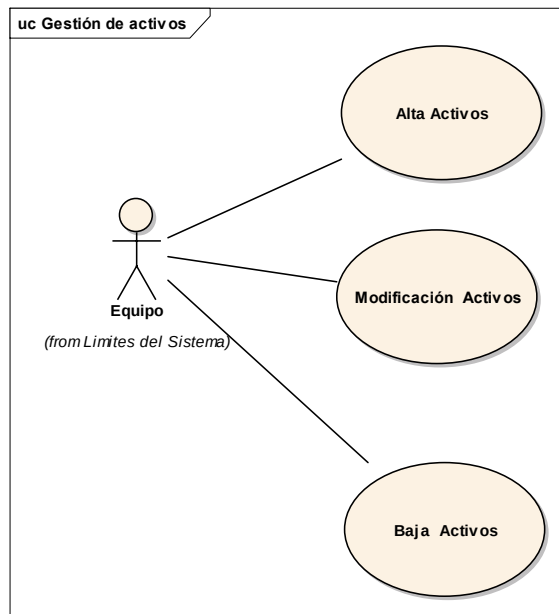
Flujo de Eventos
Basic Path
Paso 1
El caso de uso comienza cuando el Usuario selecciona un registro a modificar y presiona el botón Cambiar
Basic Path
Paso 2
El sistema muestra una ventana en donde el usuario puede modificar los datos.
Basic Path
Paso 3
El usuario modifica los datos y presiona el botón 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
Deben Existir datos Cargados

Estado: Approved

Gestión de activos



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

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

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

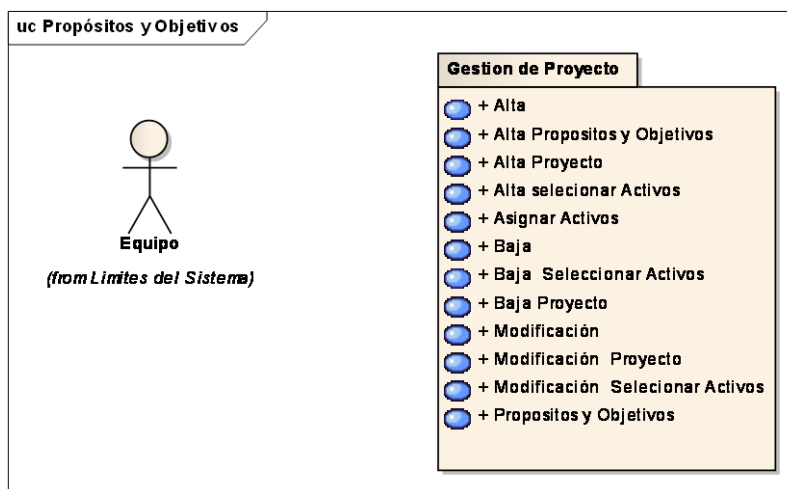
El sistema verifica que posea todos los datos necesarios y guarda los mismos.
Luego devuelve el control a la pantalla grilla.

PRE-condición

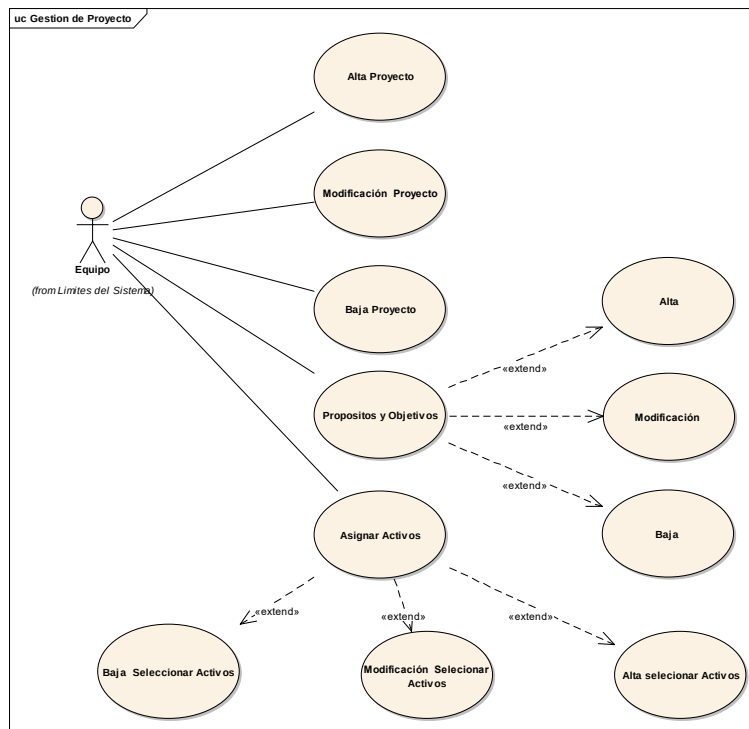
Estado: Approved

Deben Existir datos Cargados

Etapa 2 - Propósitos y Objetivos



Gestión de Proyecto



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

Alta propósitos y Objetivos

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

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.

Asignar 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 .

Baja

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

Baja 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

Baja 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

Modificación

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

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

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

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

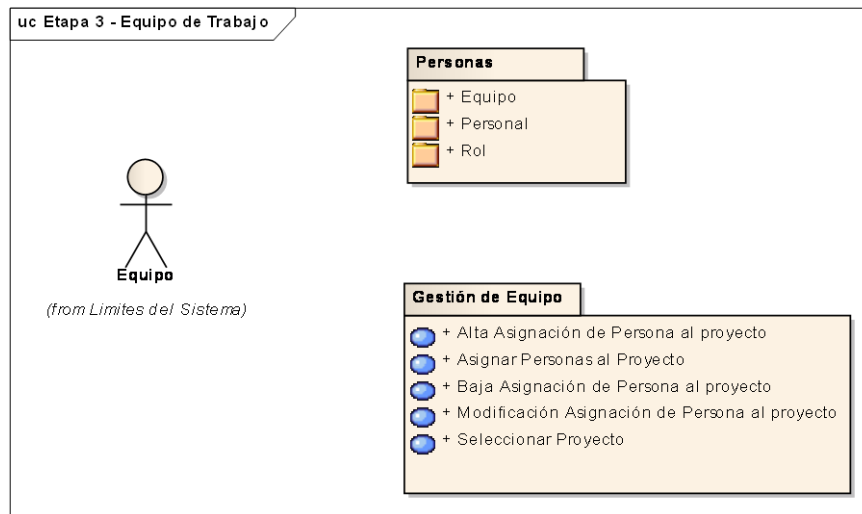
El sistema abre una ventana en donde muestra los propósitos, objetivos y límites cargados para ese Proyecto. Muestra los botones Nuevo, Modificar y Eliminar.

Invariant

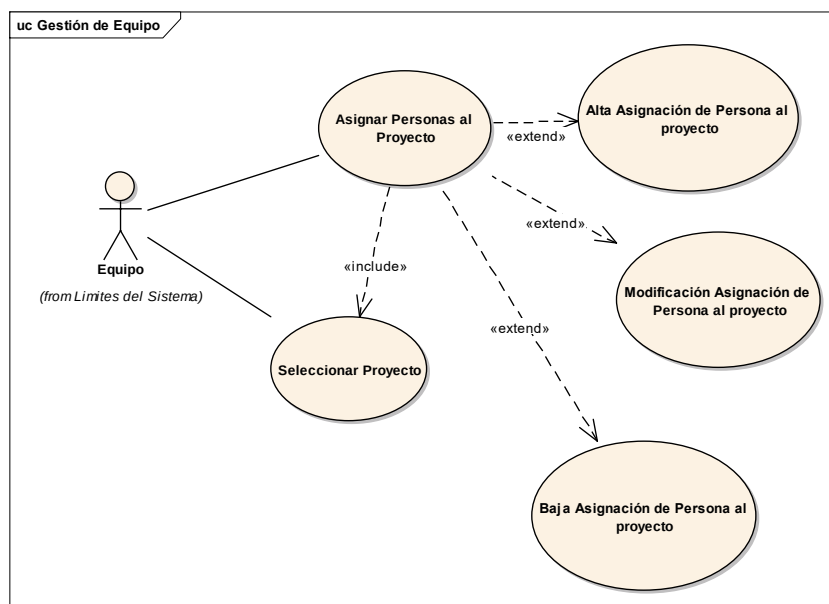
Estado: Approved

.Debe existir el proyecto

Etapa 3 - Equipo de Trabajo



Gestión de Equipo



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"

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.

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
Deben Existir datos Cargados

Estado: Approved

PRE-condición
"Debe haber seleccionado un Proyecto. Caso de Uso "Seleccionar Proyecto

Estado: Approved

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
"Debe haber seleccionado un Proyecto. Caso de Uso "Seleccionar Proyecto

Estado: Approved

PRE-condición
Deben Existir datos Cargados

Estado: Approved

Seleccionar Proyecto
Selecciona un Proyecto

Flujo de Eventos

Basic Path

Paso 1

El caso de uso comienza cuando el usuario carga el N° de proyecto .

Basic Path

Paso 2

El sistema corrobora que el ID ingresado exista y muestra el nombre del proyecto .

Alternate

Sistema

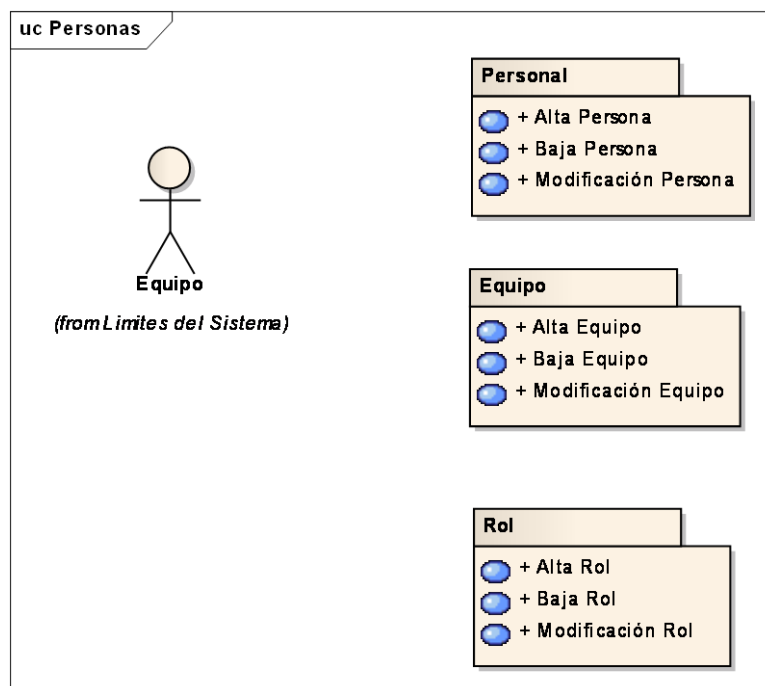
Si el Id No existe el sistema muestra una lista de los datos del almacén proyectos para que el usuario elija una opción

PRE-condición

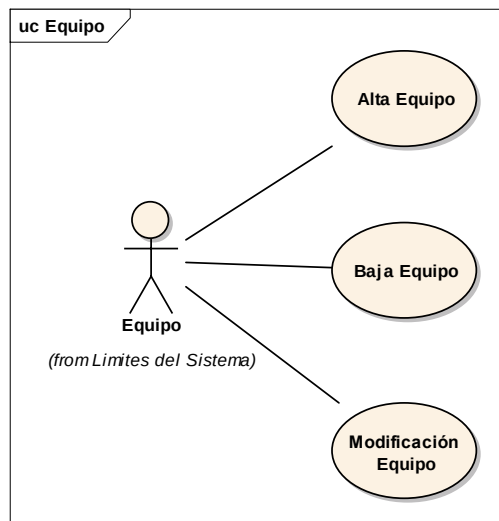
Estado: Approved

.Deben existir proyectos

Personas



Equipo



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.

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

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

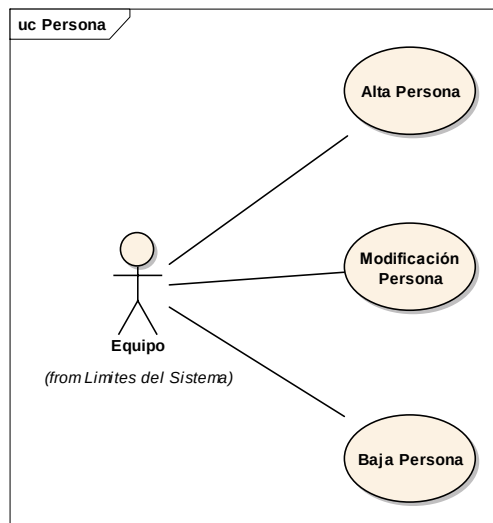
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Personal



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.

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

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.

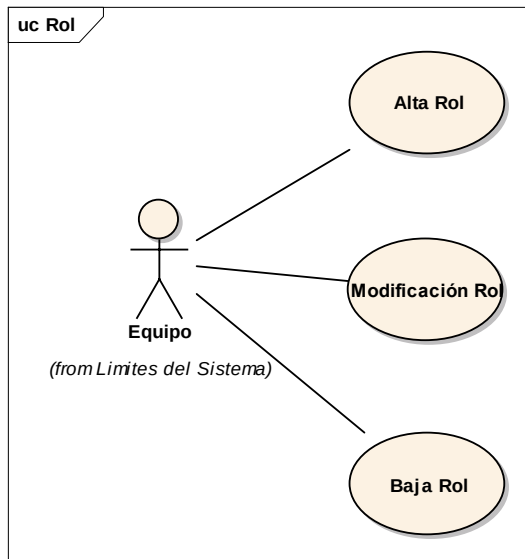
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Rol



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.

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

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

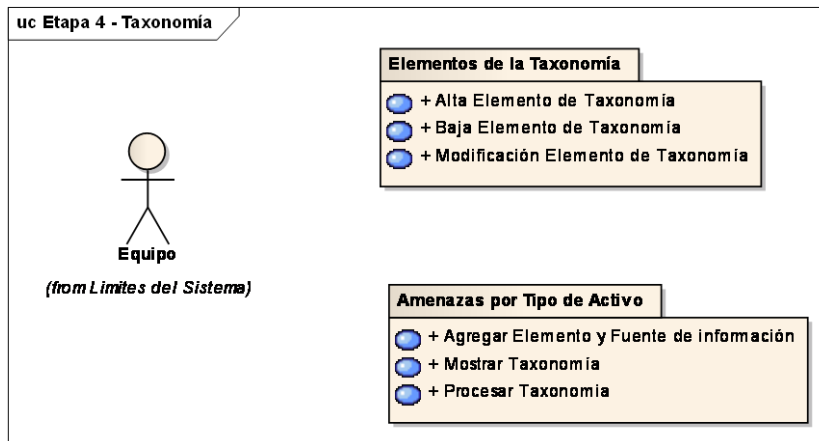
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

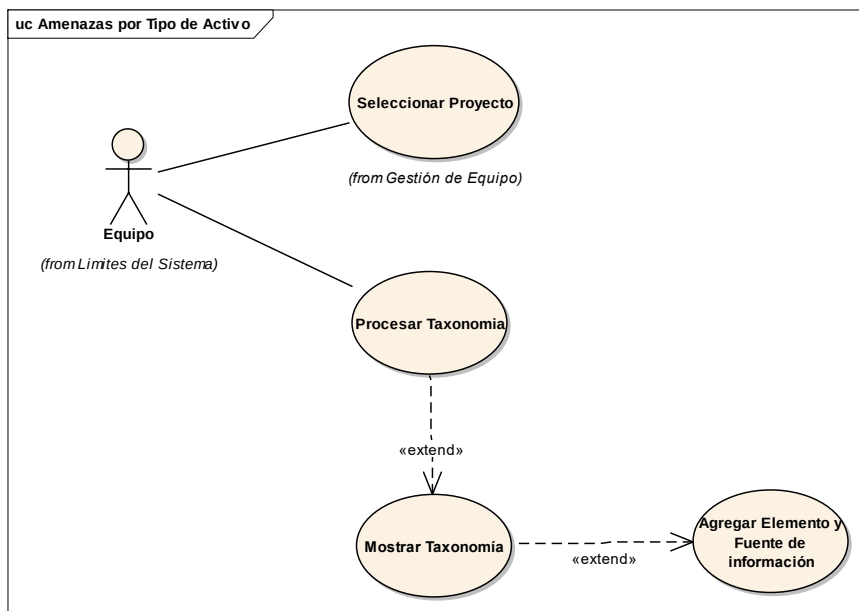
Estado: Approved

Deben Existir datos Cargados

Etapa 4 - Taxonomía



Amenazas por Tipo de Activo



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

Mostrar Taxonomía

1º Muestra los resultados del proceso de taxonomía

Posee etiquetas de Orden:

Amenaza

Activo

Y Filtro muestra solo los Ítems "Completo"

2º Muestra una grilla relacionando los elementos del activo a cada ítem de taxonomía

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

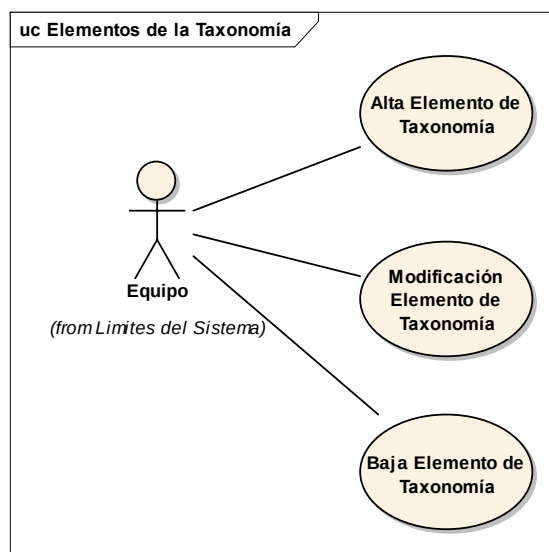
Paso 2

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
Debe seleccionarse un proyecto

Estado: Approved

Elementos de la Taxonomía



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.

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

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

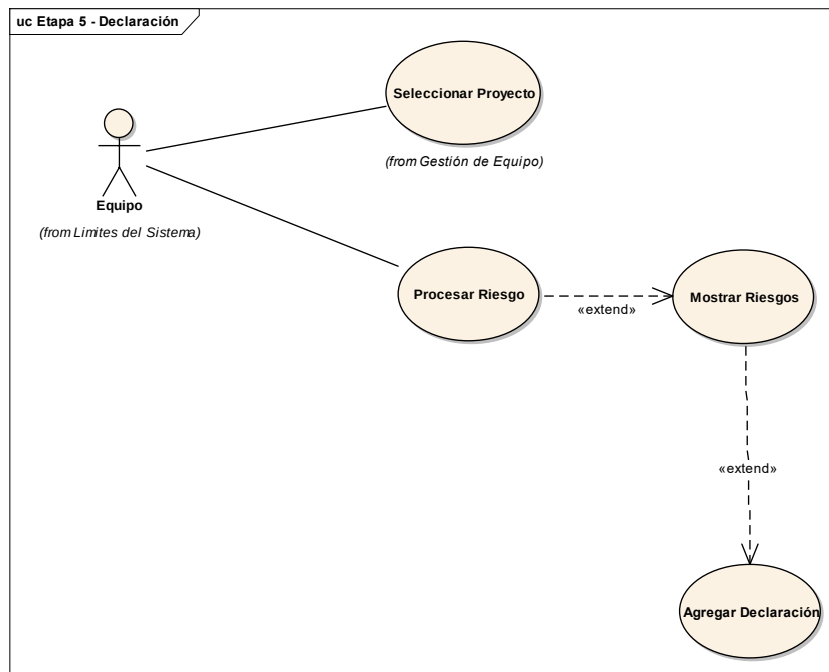
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Etapa 5 - Declaración



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
Deben Existir elementos en la grilla

Estado: Approved

Mostrar Riesgos
Muestra los resultados del proceso de taxonomía
Posee etiquetas de Orden:
Amenaza
Activo

Y Filtro muestra solo los Ítems "Riesgos a Evaluar"

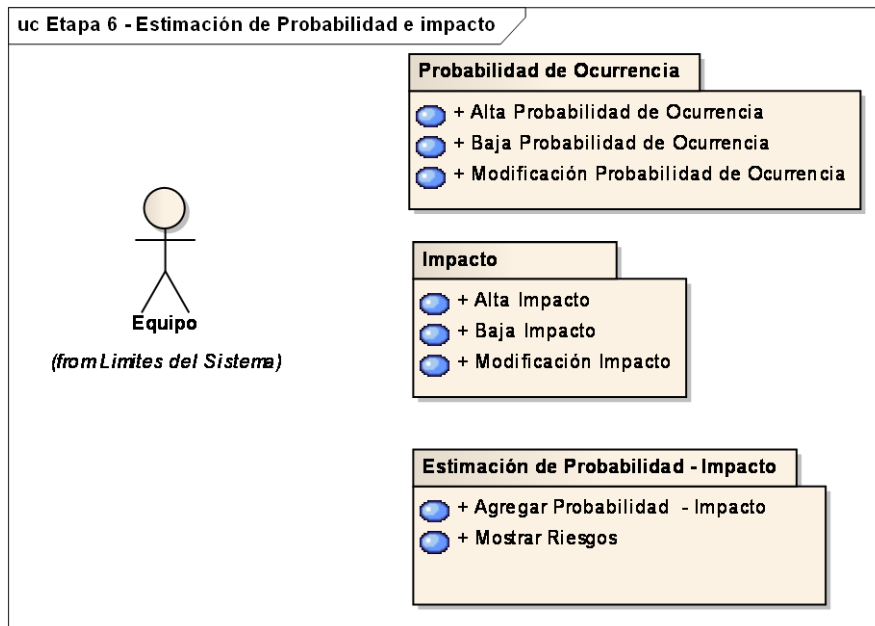
Procesar Riesgo
El caso de uso procesa los riesgos según el proyecto elegido.
Recorre el almacén de taxonomías completas y lo carga al almacén de riesgos. Al finalizar Muestra una grilla con los datos cargados en el almacén taxonomía.
SI el Riesgo existe lo actualiza.

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

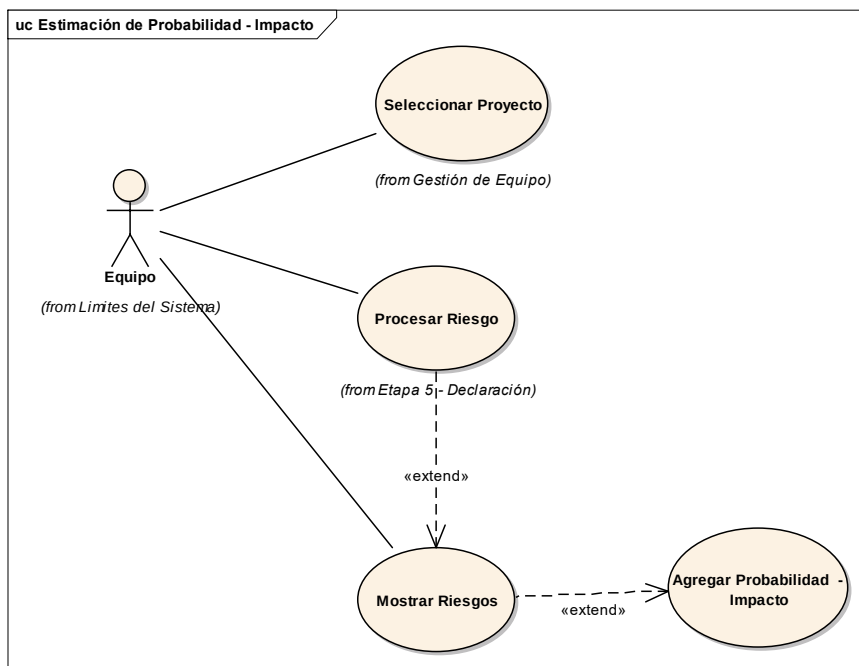
PRE-condición
Debe seleccionarse un proyecto

Estado: Approved

Etapa 6 - Estimación de Probabilidad e impacto



Estimación de Probabilidad - Impacto



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

Mostrar Riesgos

Muestra los resultados del CU "Procesar Riesgos"

Posee etiquetas de Orden:

Amenaza

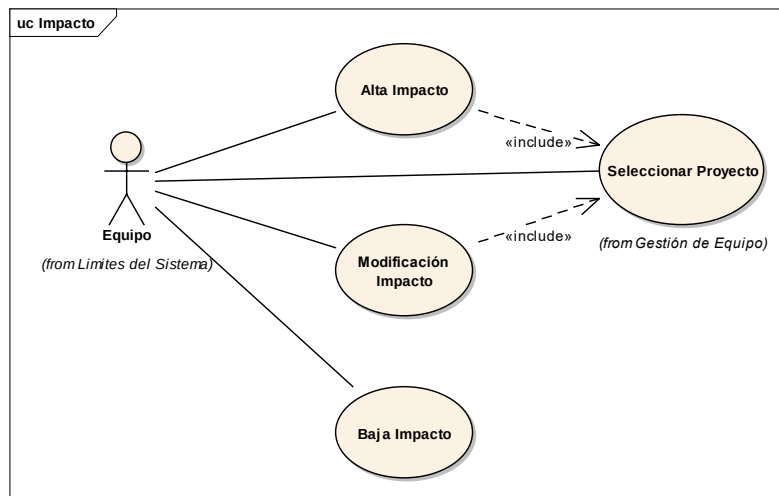
Activo

Probabilidad

Impacto

Y Filtro muestra solo los Ítems "Riesgos a Evaluar"

Impacto



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

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

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

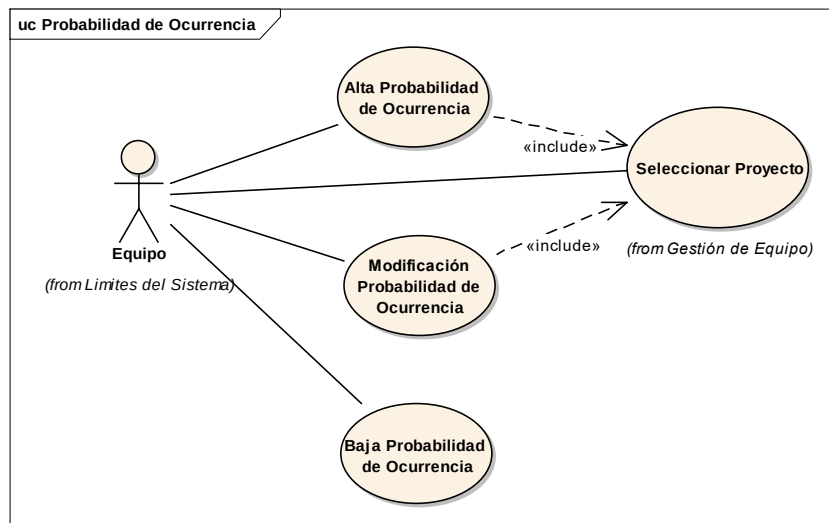
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Probabilidad de Ocurrencia



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

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

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

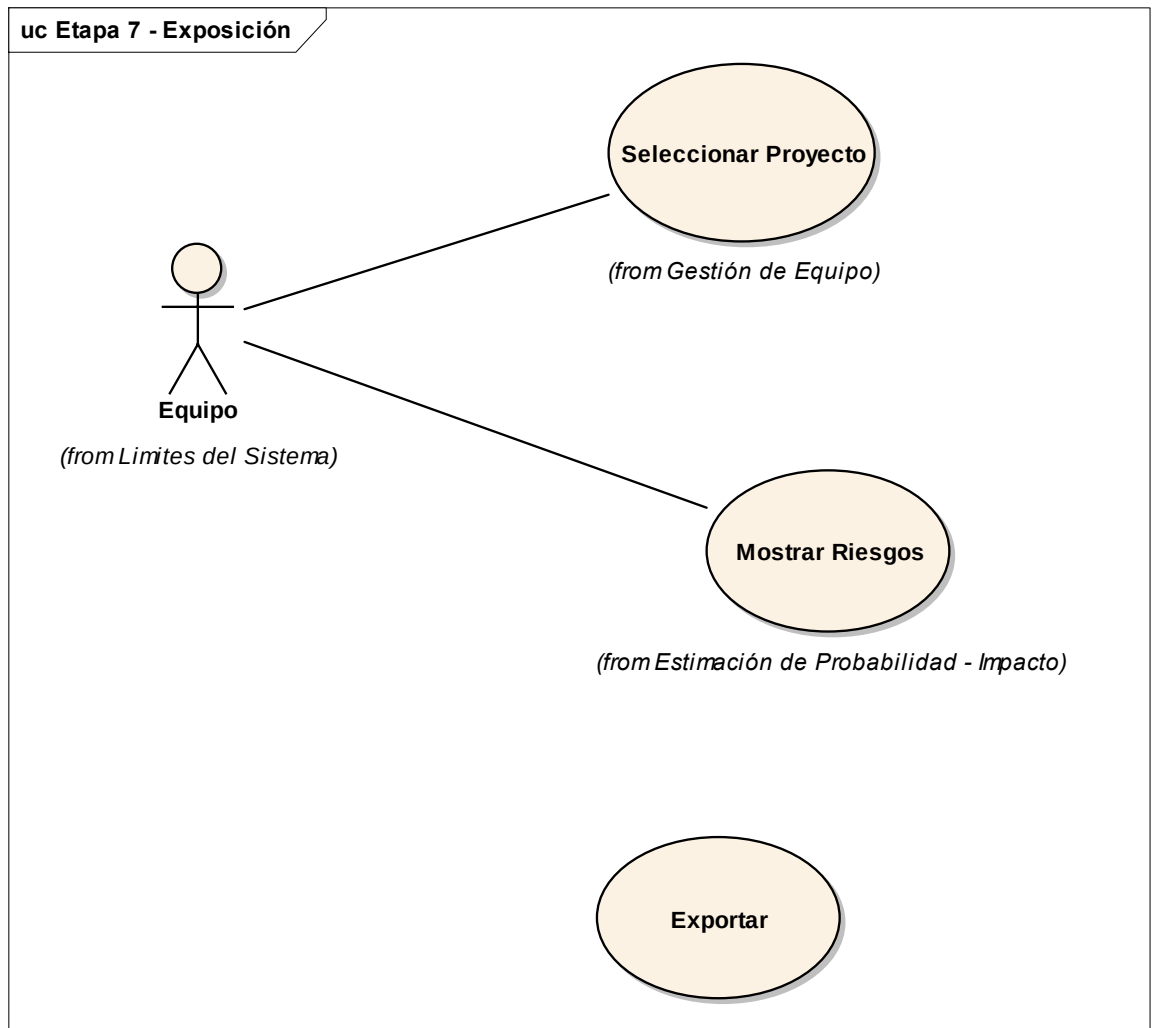
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Etapa 7 - Exposición

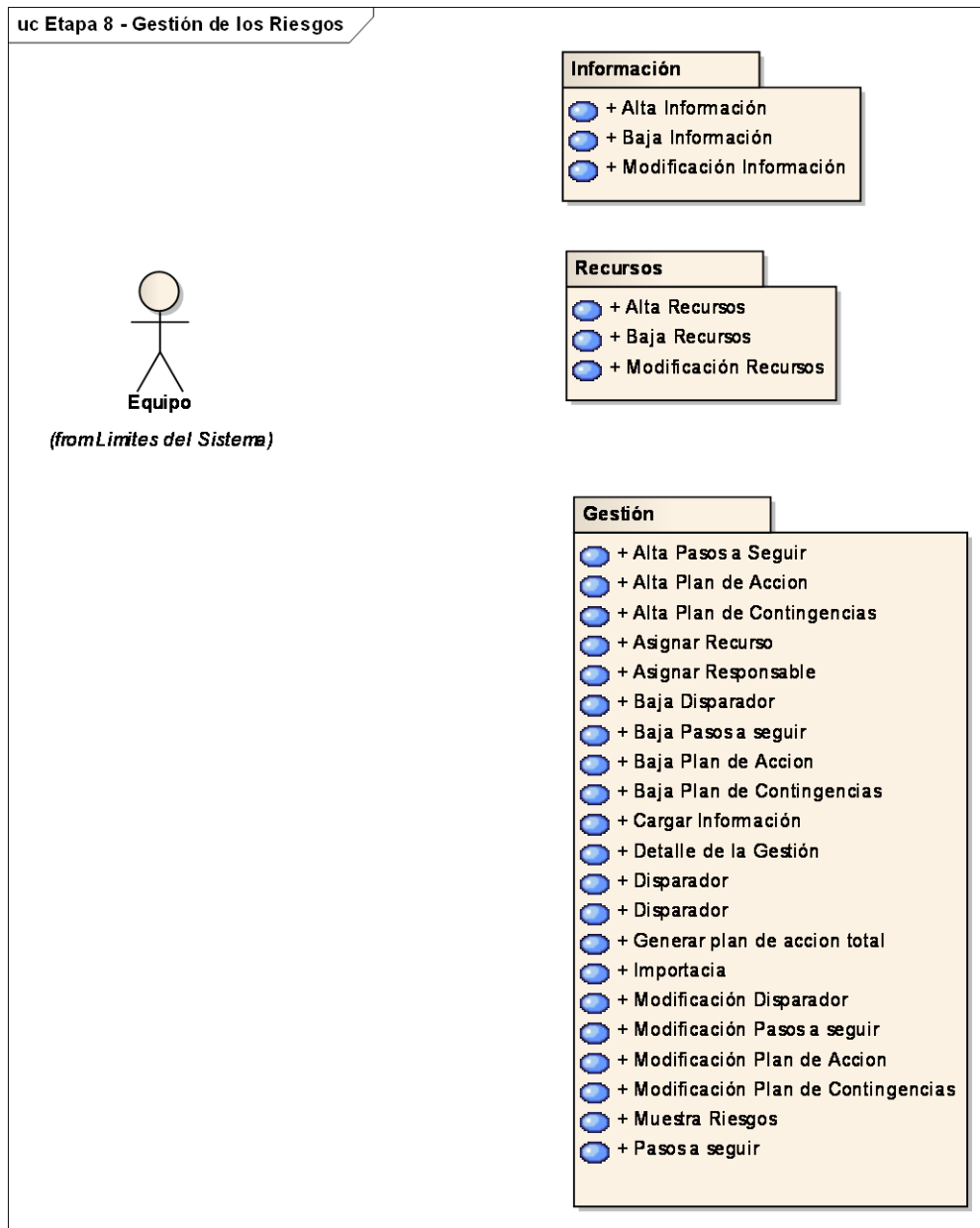


Exportar

Modulo para exportar datos de una grilla a distintos formatos digitales.

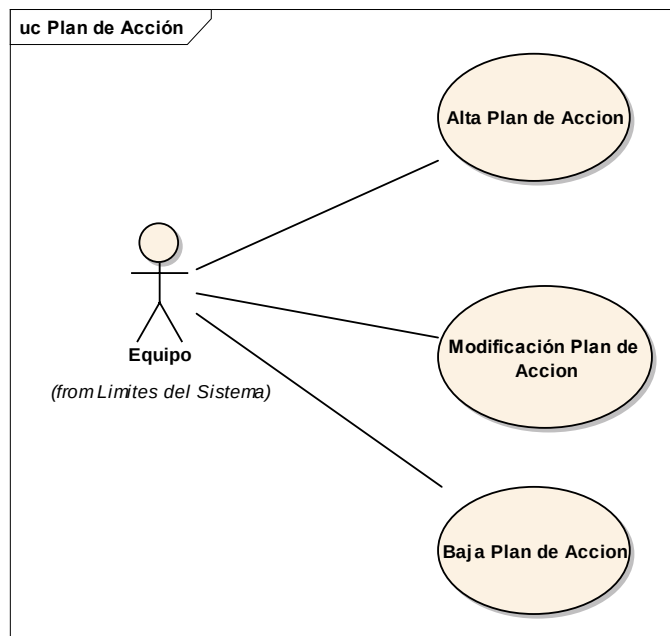
XLS
XML
TXT
HTML

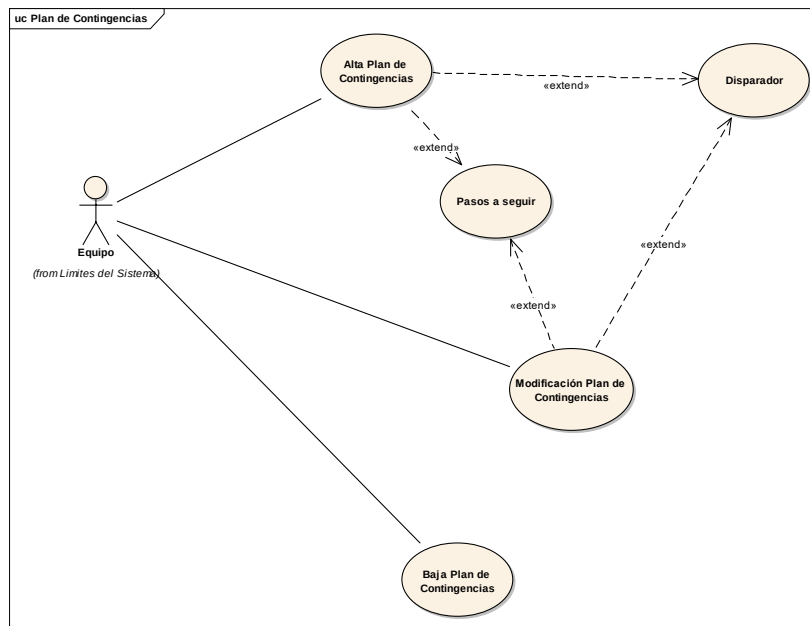
Etapa 8 - Gestión de los Riesgos



Gestión

Un nuevo modelo integrando la metodología SEI y Magerit3





Alta Pasos a Seguir

Se establecen los pasos secuenciales a seguir para poder minimizar o eliminar el problema

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

.Debe existir cargado los proyectos

Estado: Approved

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

Asignar 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

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

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

Baja Pasos a seguir

Pasos secuenciales 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
Deben Existir datos Cargados

Estado: Approved

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
Deben Existir datos Cargados

Estado: Approved

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 informe al usuario.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

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

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.

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

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

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

importancia

Se carga la importancia de que el riesgo se transforme 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.

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

Modificación Pasos a seguir

Pasos secuenciales 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

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

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

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.

Pasos a seguir

Gestión de Pasos a seguir.

Pasos secuenciales 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: N° 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

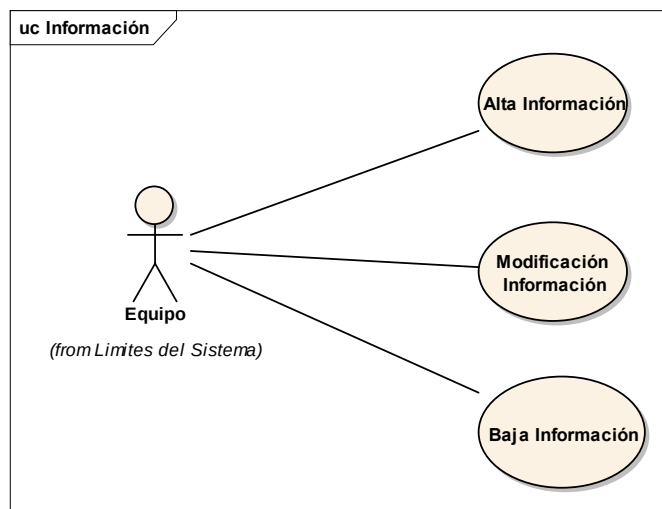
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

.Debe existir cargado los proyectos

Información



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.

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

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.

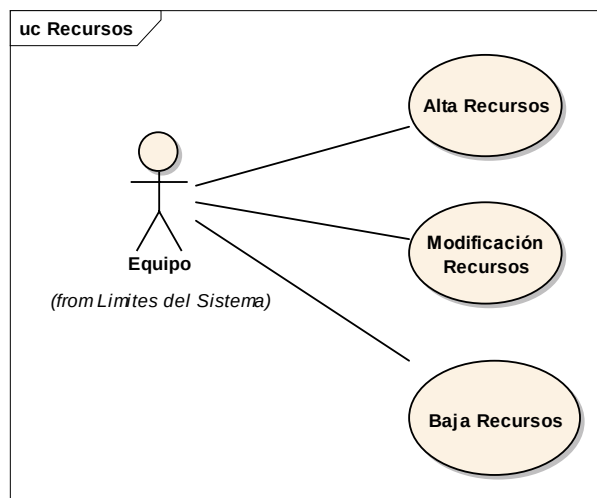
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Recursos



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.

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

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.

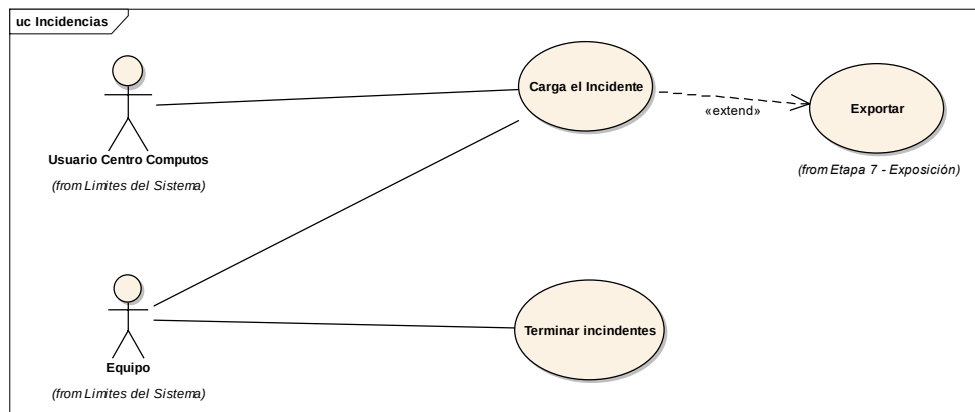
El sistema verifica que posea todos los datos necesarios y guarda los mismos.
Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Incidencias



Carga el Incidente

Se cargan los incidentes.

El sistema controla si el activo con incidente:

Está analizado y gestionado

Está analizado

No está 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.

Incidentes Activos

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.

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.

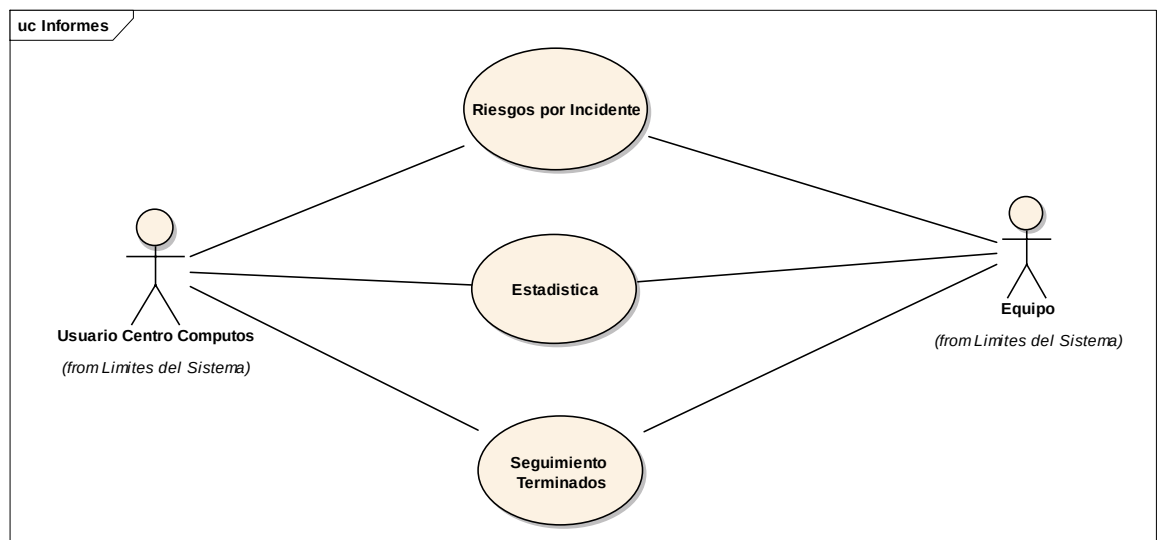
Luego imprime un reporte y vuelve a la pantalla anterior.

PRE-condición

Estado: Approved

El incidente debe estar cargado y No finalizado.

Informes



Estadística

Informe de Ranking estadístico por tipo de incidente y fecha con gráfico de torta.

Características

Incidentes Terminados

Total de Incidentes.

Riesgos por Incidente

Informe de Incidentes con las siguientes características

Terminados Bien

Terminados Mal

Pendientes

Activos con AGR

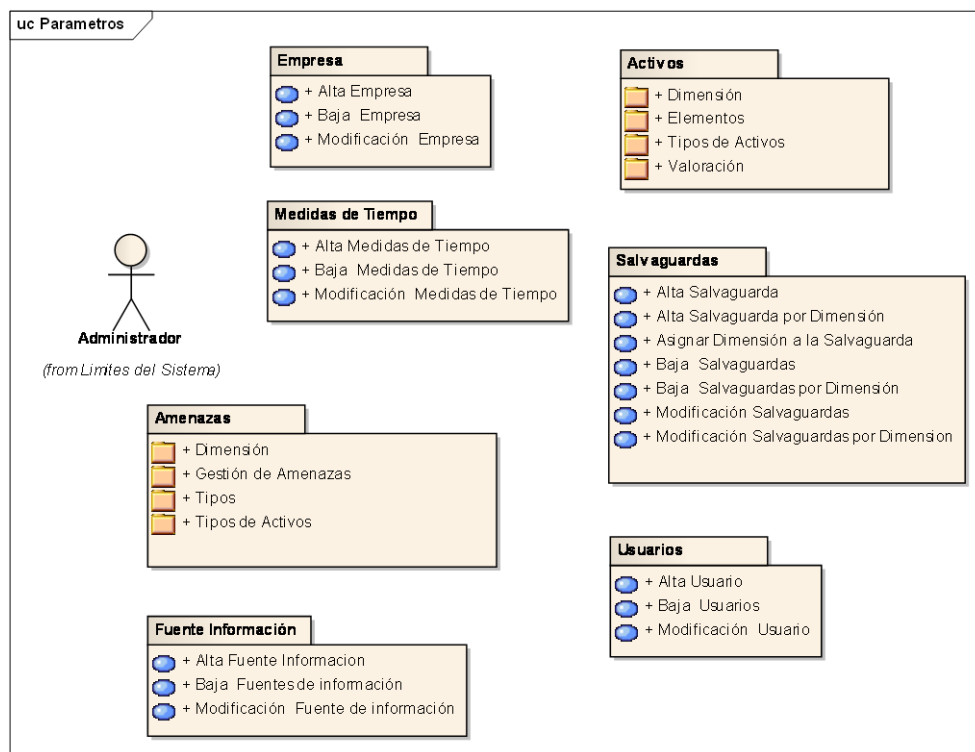
Activos con Análisis

Activos sin análisis

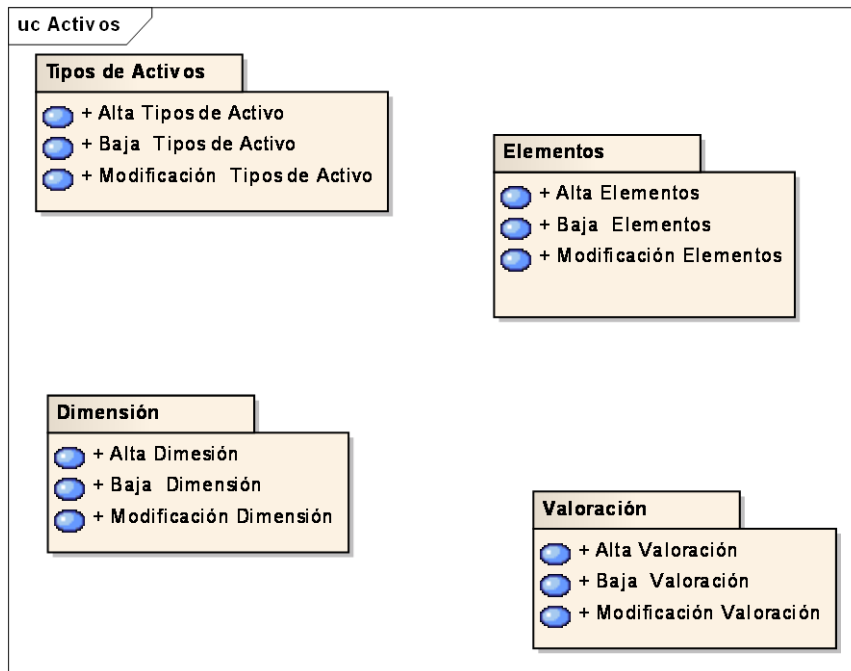
Seguimiento Terminados
Informe de Seguimientos terminados.
Características:

- Ordenado por Fecha
- Por Amenaza
- Por Salvaguarda
- Por Dimensión
- Terminado Bien
- Terminado Mal.

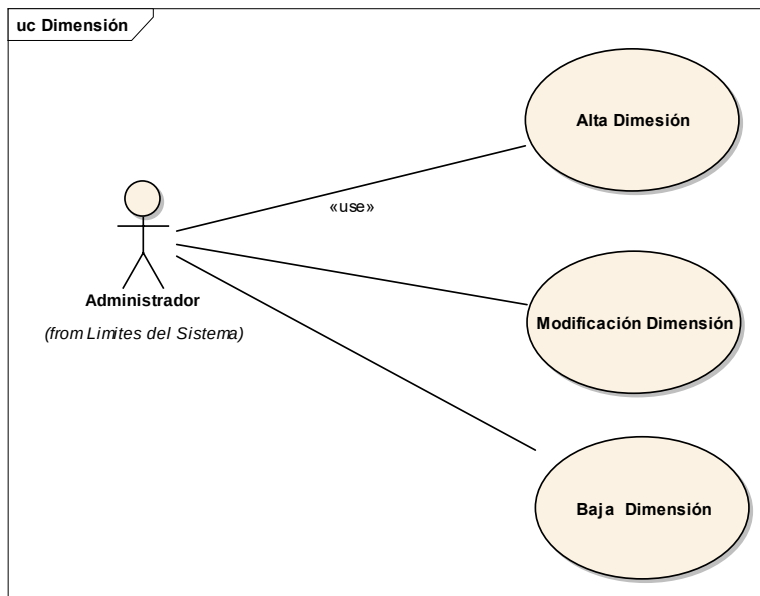
parámetros



Activos



Dimensión



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.

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

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

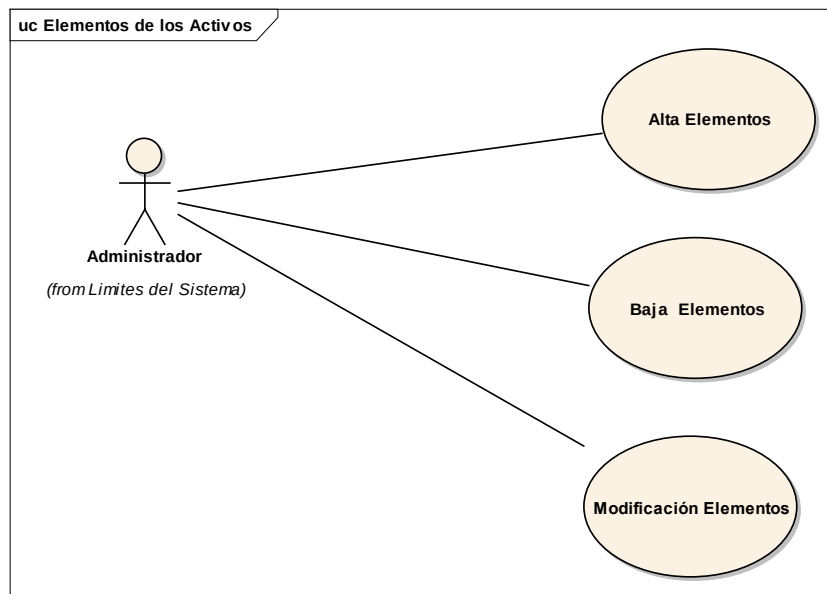
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Elementos



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 carga 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

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

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

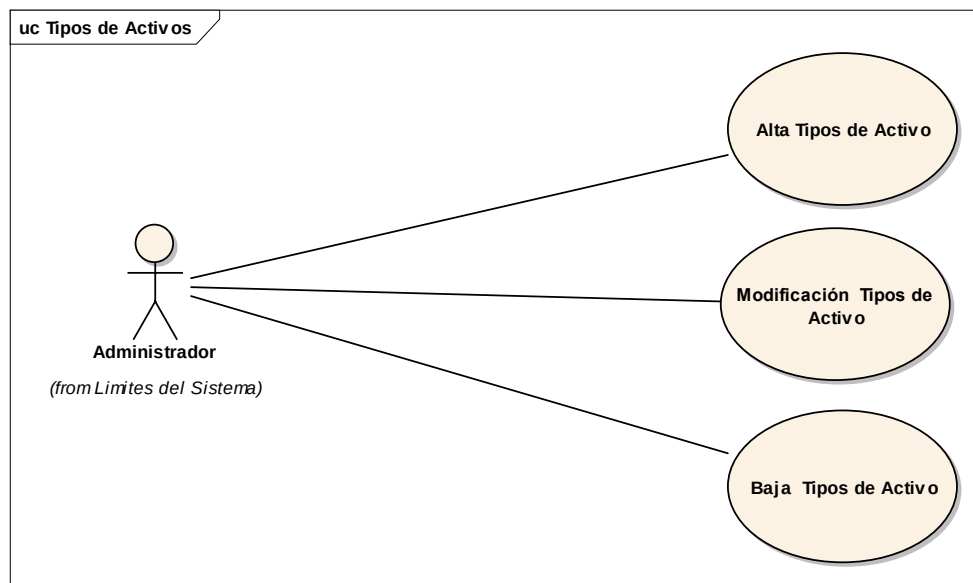
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Deben Existir datos Cargados

Estado: Approved

Tipos de Activos



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.

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

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

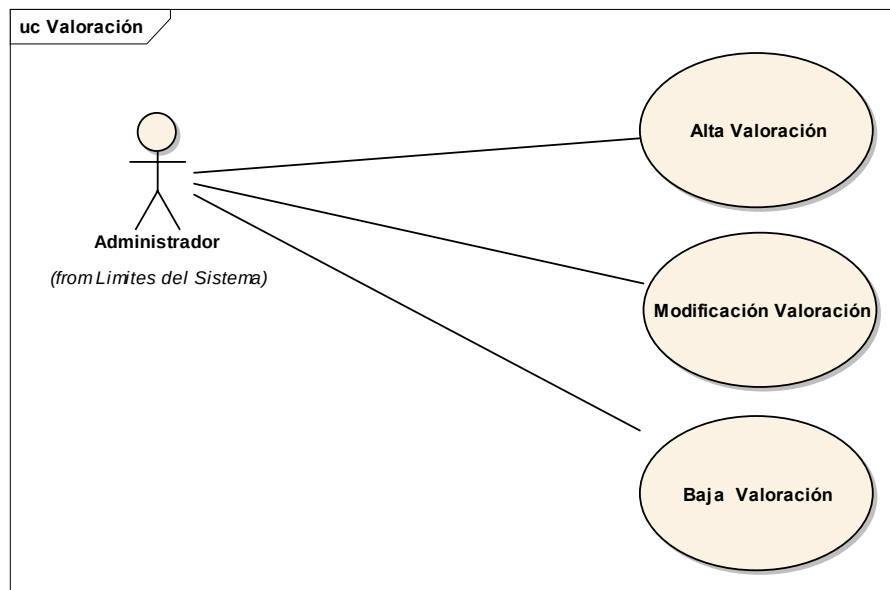
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Valoración



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.

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

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

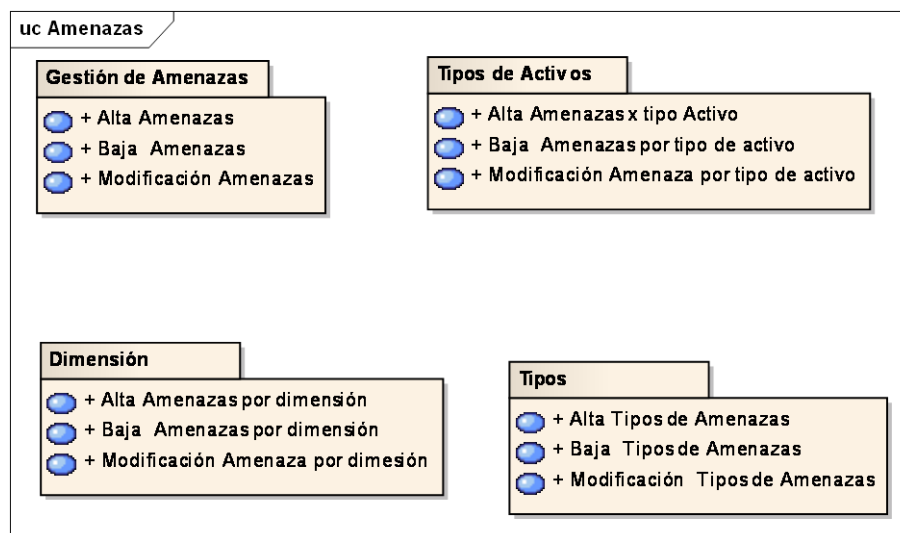
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

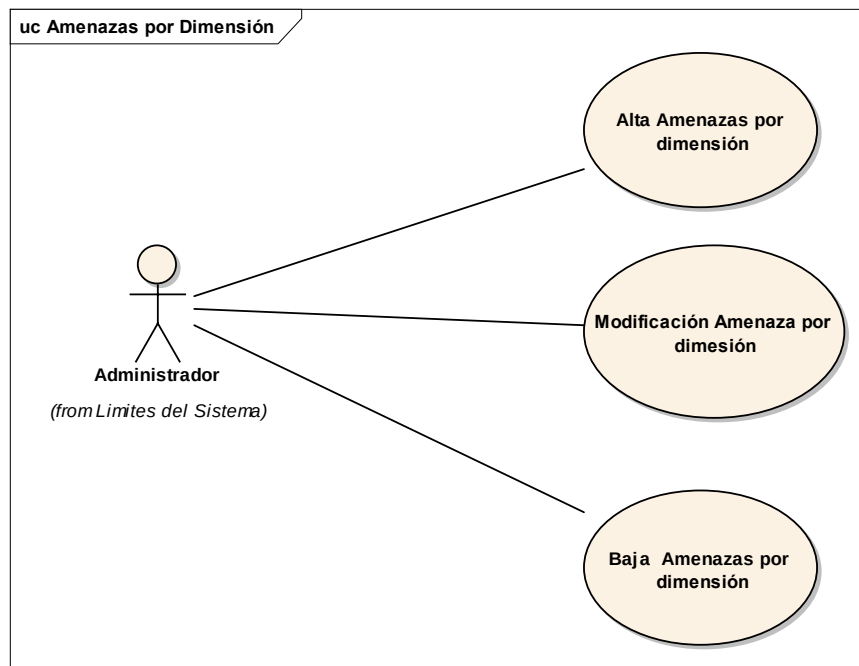
Estado: Approved

Deben Existir datos Cargados

Amenazas



Dimensión



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

Baja 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

Modificación 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

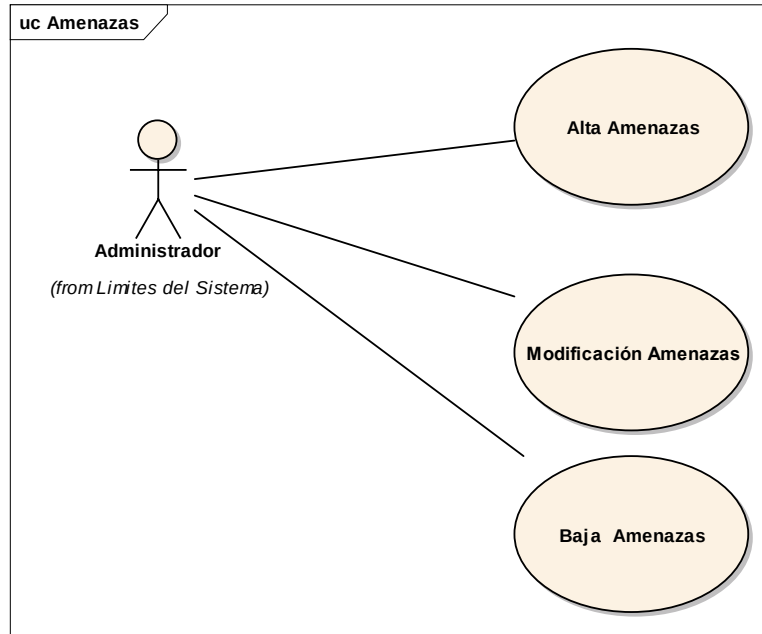
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Gestión de Amenazas



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 carga 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

Baja 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

Modificación 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

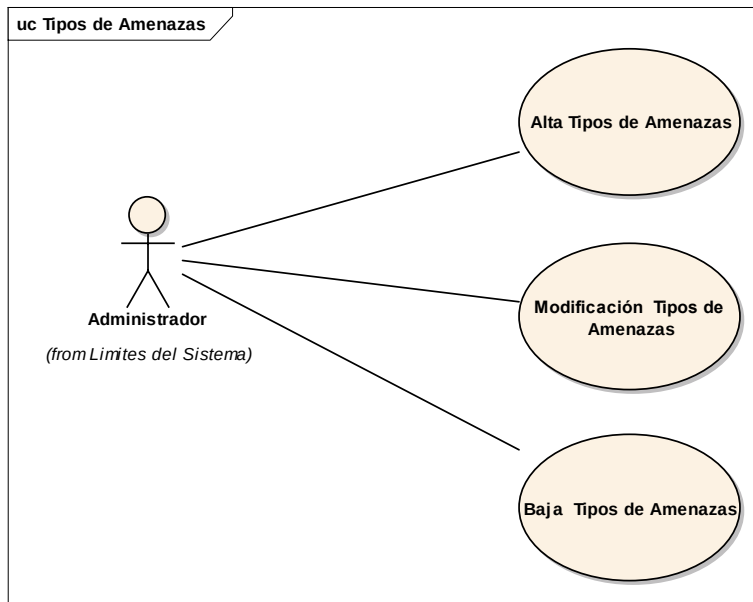
Paso 4

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Tipos



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.

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

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

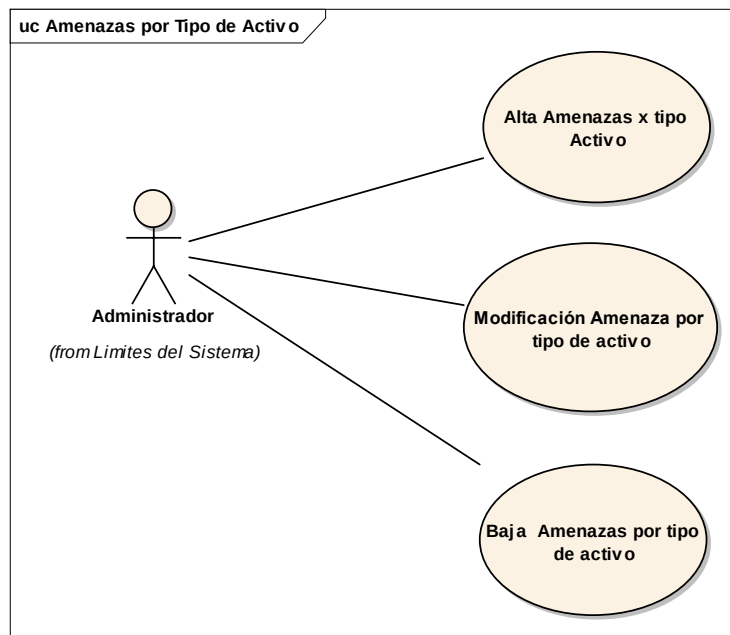
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Tipos de Activos



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

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

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

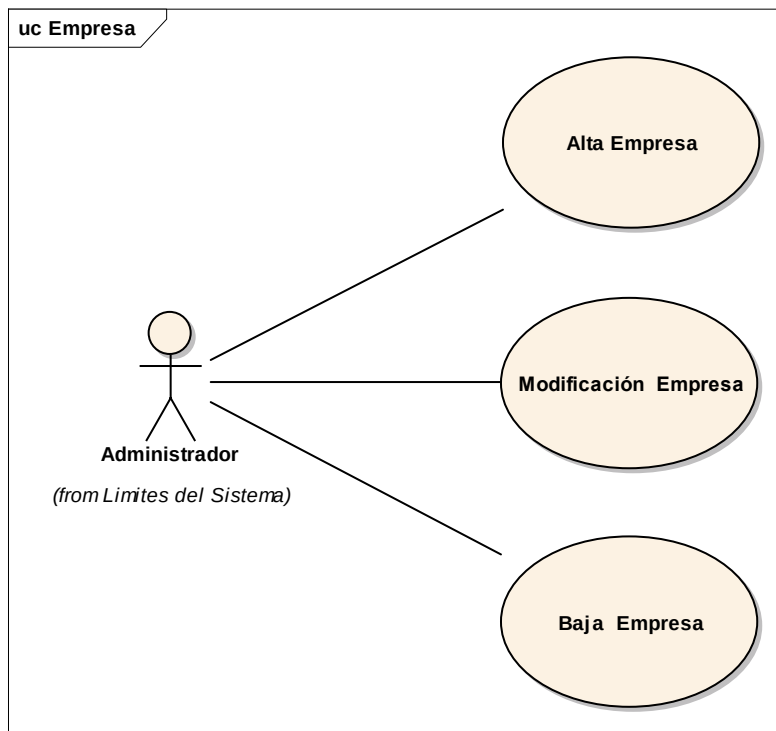
Paso 4

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Empresa



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.

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

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

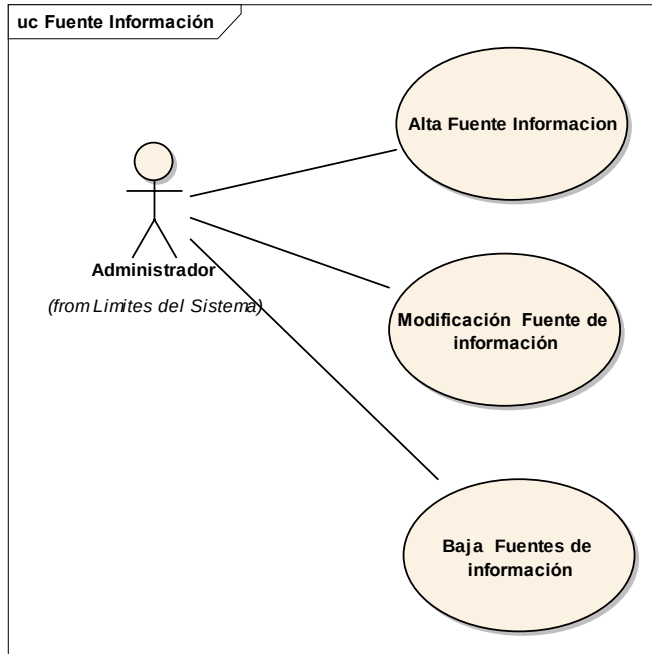
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Fuente Información



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.

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

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

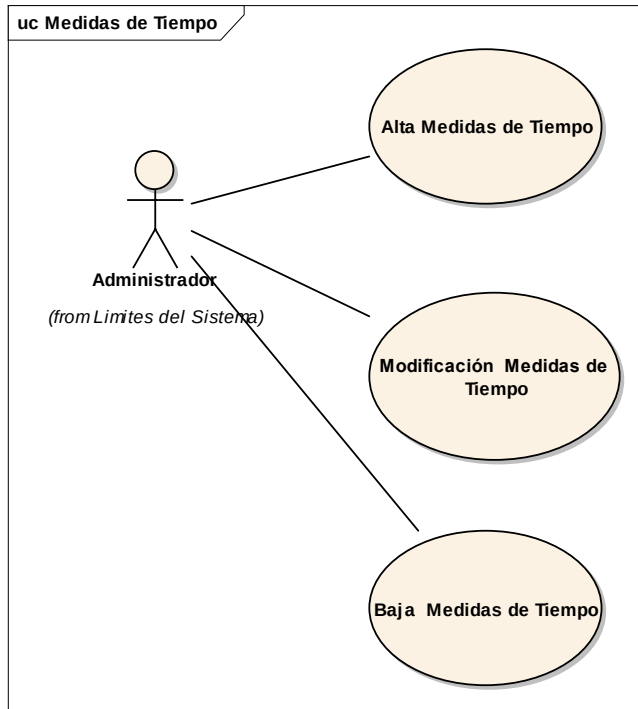
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Medidas de Tiempo



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.

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

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

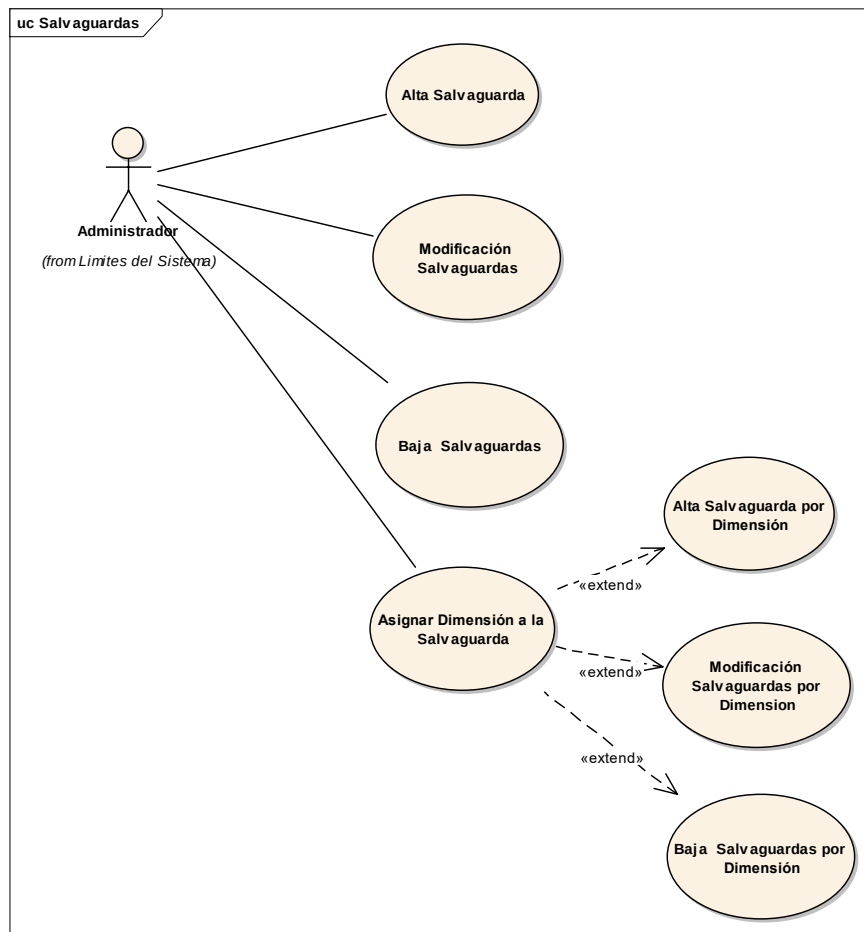
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Salvaguardas



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.

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

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
Deben Existir las dimensiones

Estado: Approved

PRE-condición
Deben existir las salvaguardas

Estado: Approved

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
Deben Existir datos Cargados

Estado: Approved

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

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

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

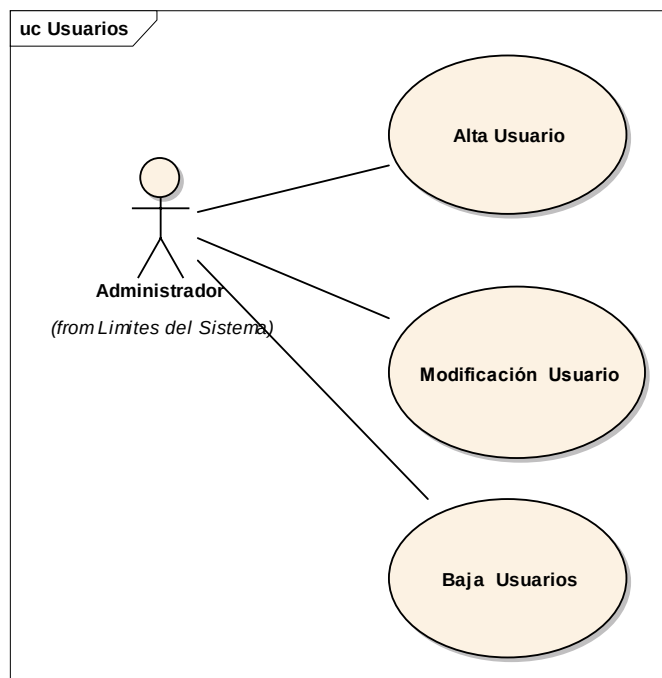
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control al Caso de Uso "Asignar Dimensión a la Salvaguarda"

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Usuarios



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.

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

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

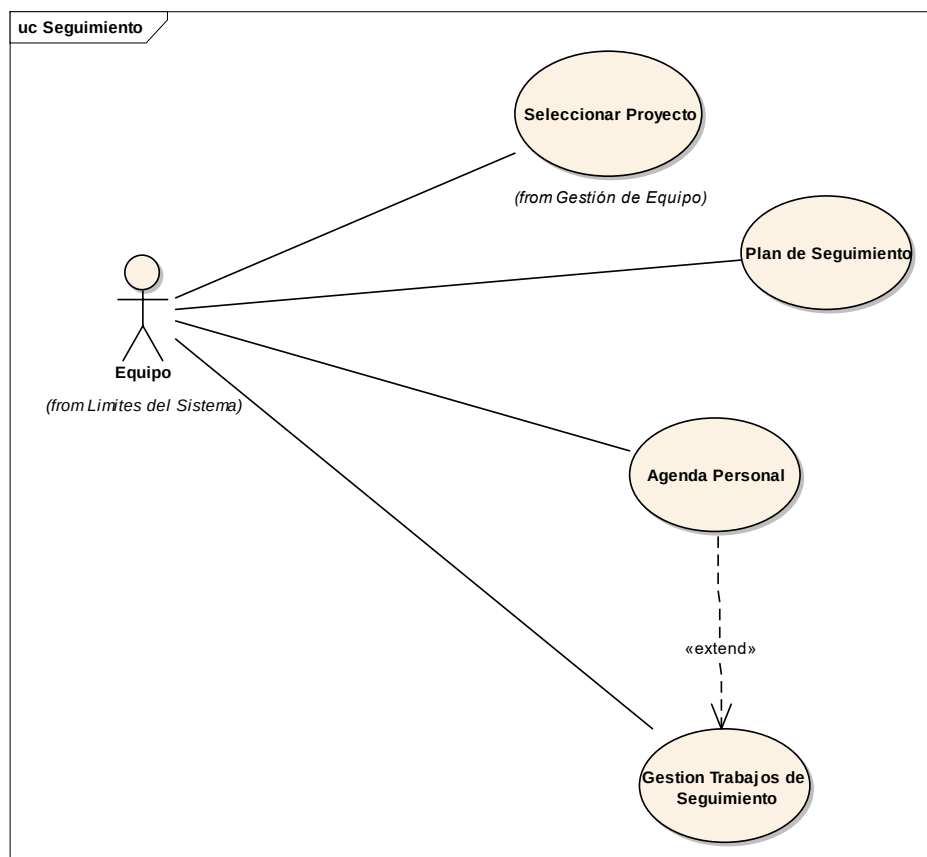
El sistema verifica que posea todos los datos necesarios y guarda los mismos. Luego devuelve el control a la pantalla grilla.

PRE-condición

Estado: Approved

Deben Existir datos Cargados

Seguimiento



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"

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%.

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.

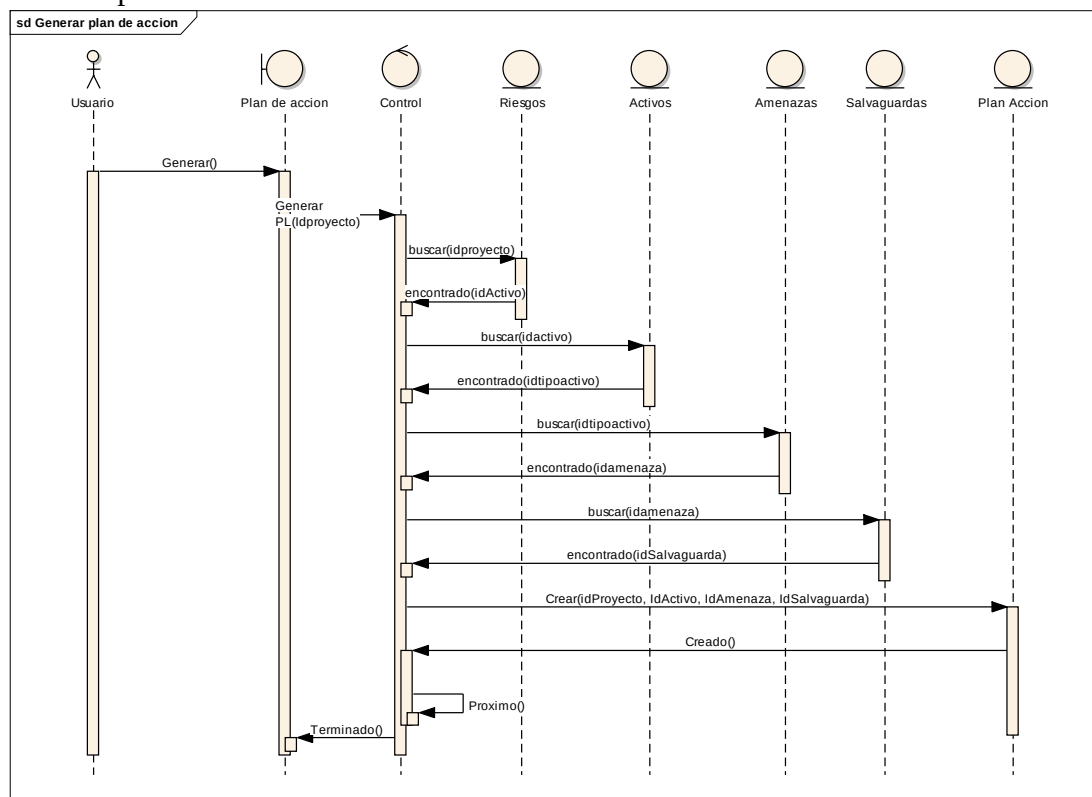
PRE-condición

Estado: Approved

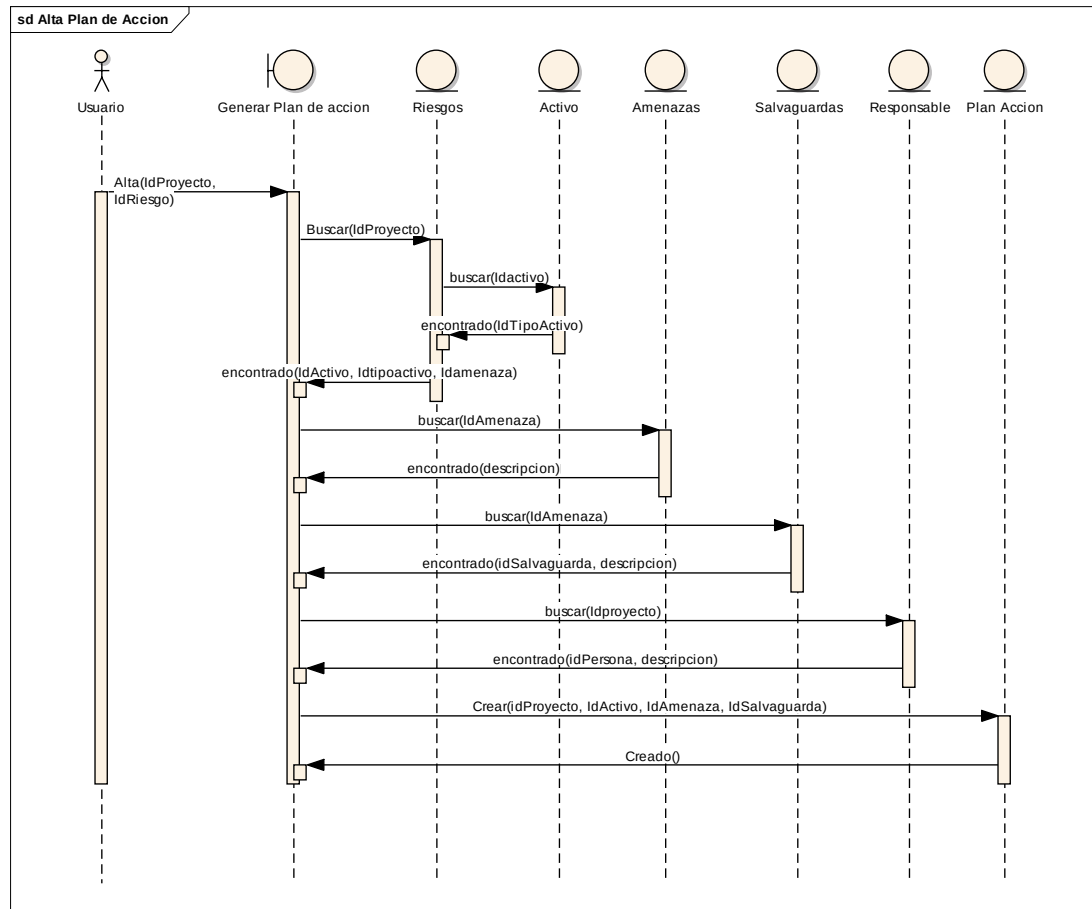
Es necesario que estén cargadas las salvaguardas.

Diagramas de secuencia

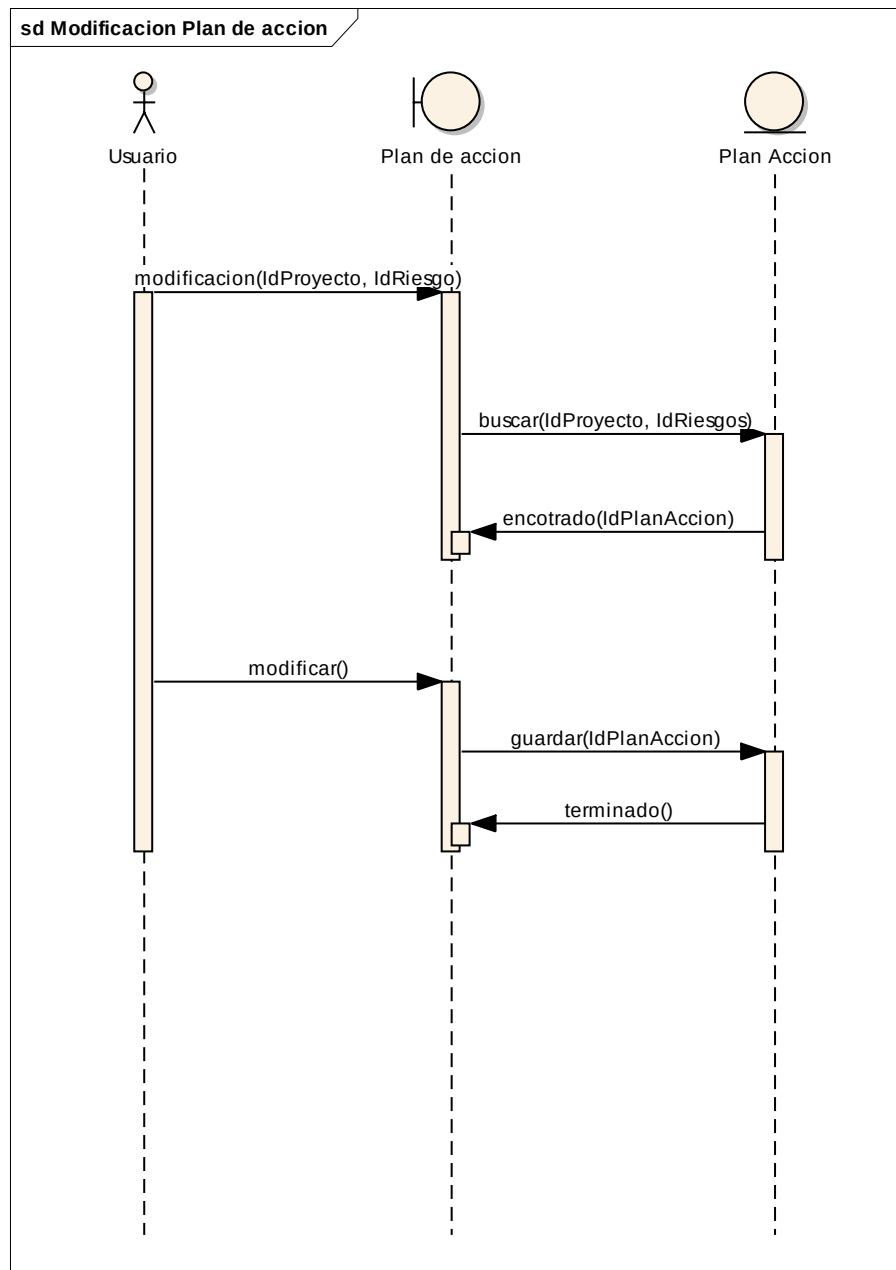
Generar plan de acción



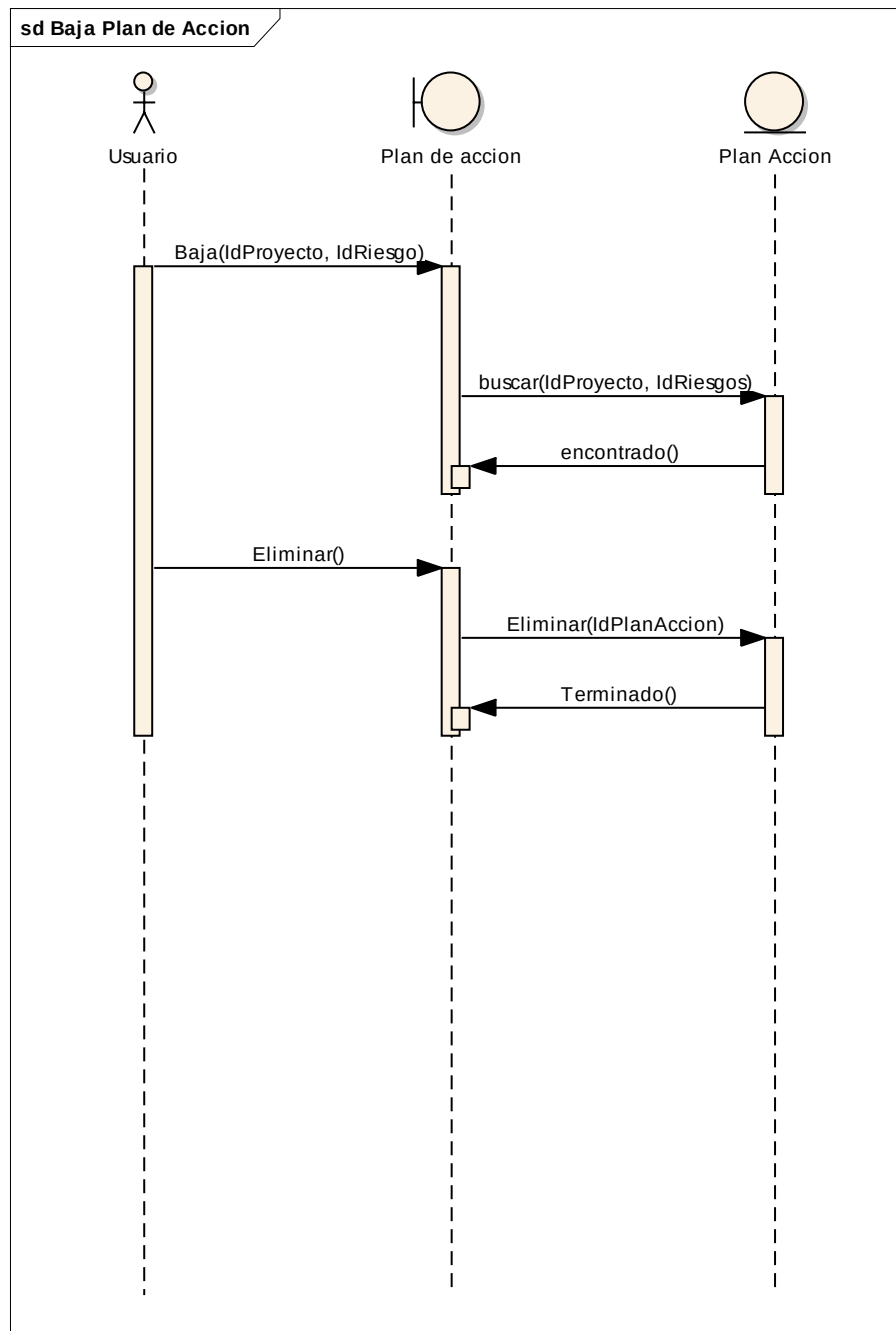
Alta plan de Acción



Modificación plan de acción



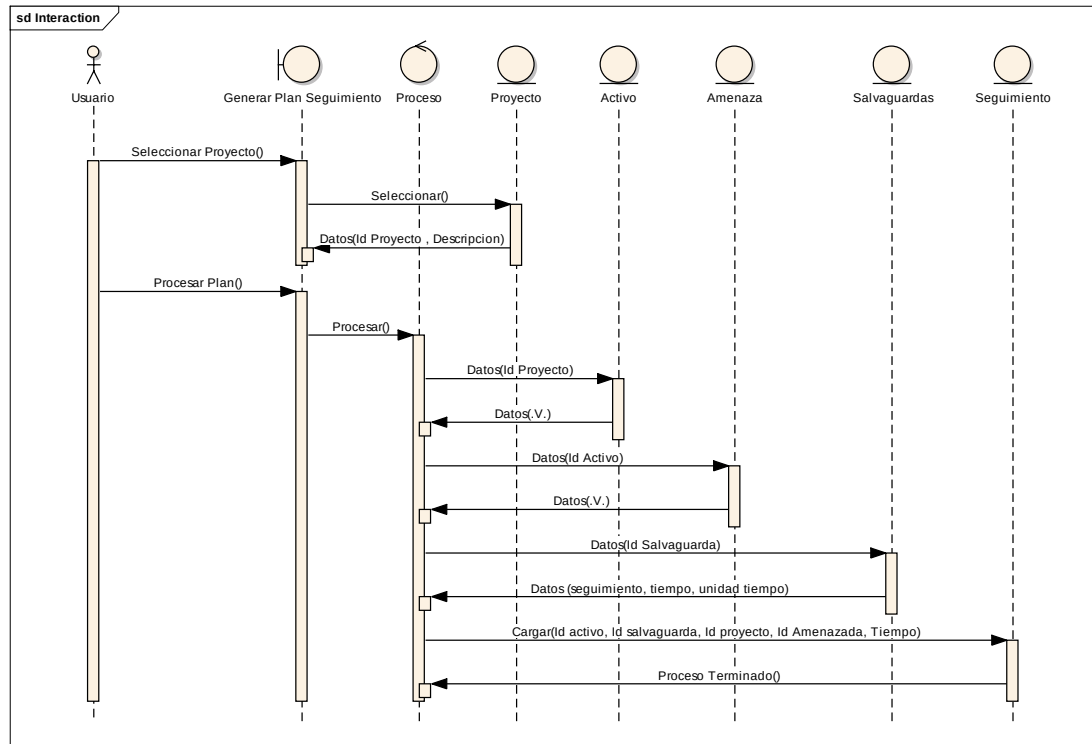
Baja Plan de acción



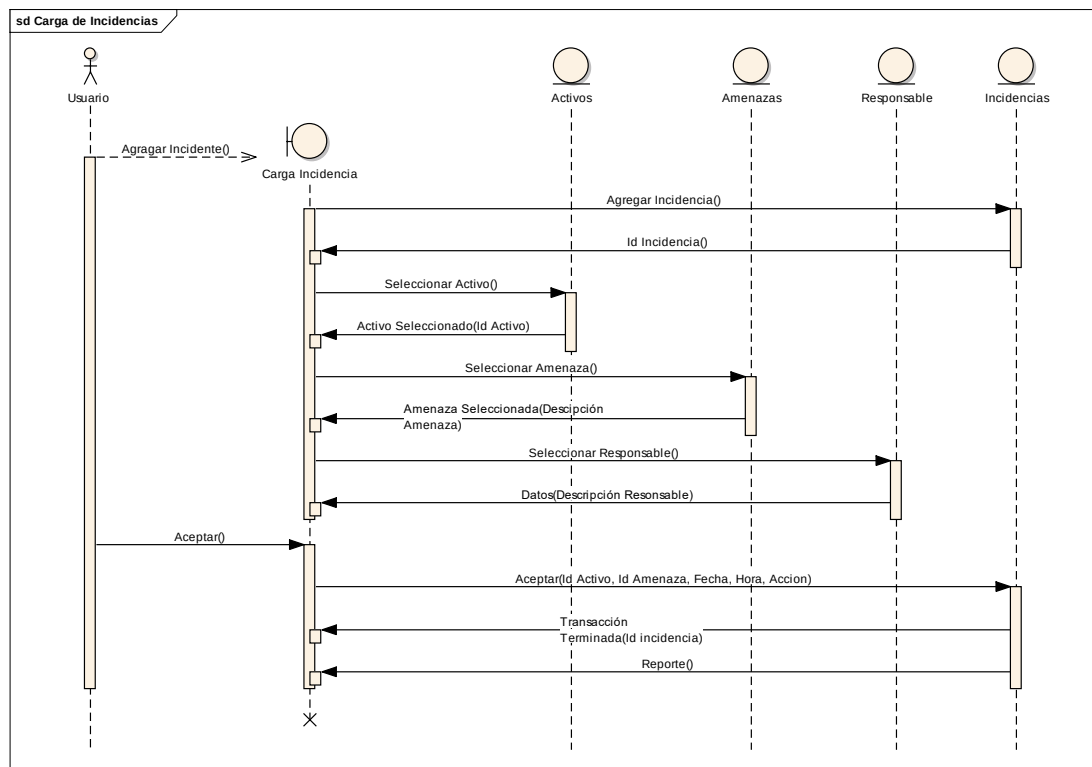
Plan de seguimiento

Análisis de Riesgo en Proyectos Software

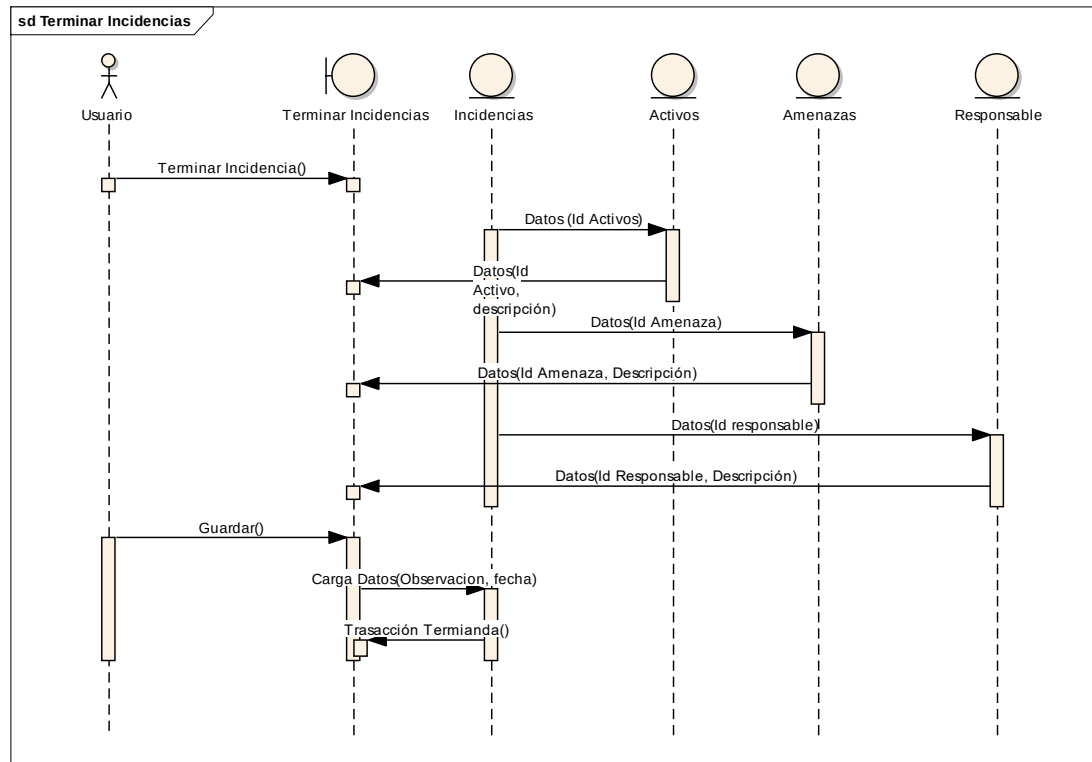
Un nuevo modelo integrando la metodología SEI y Magerit3



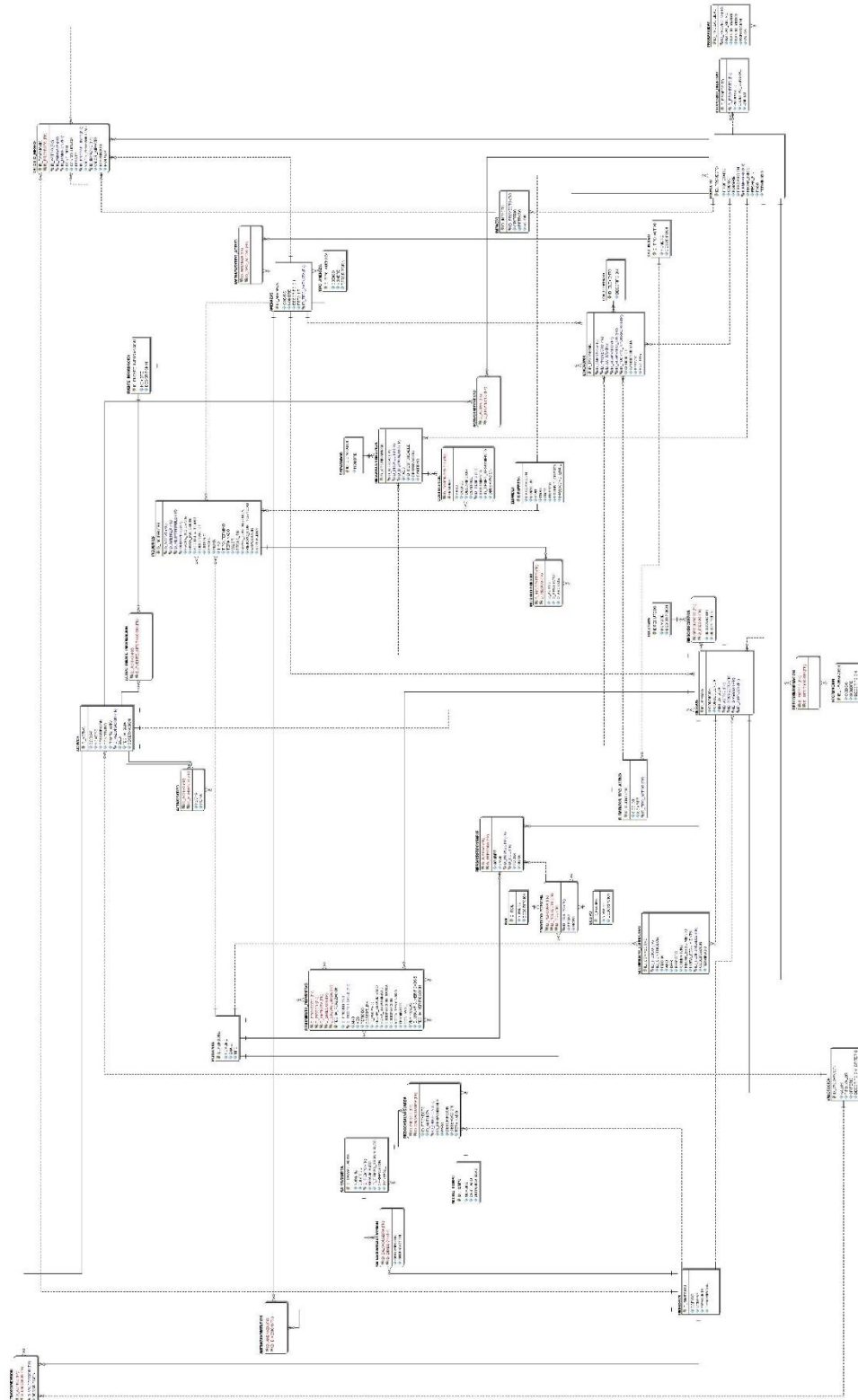
Carga de incidencias



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 actividad	Criterio: Resultado: El sistema debe mostrar un icono en el browse y cambiar el % de actividad por el nuevo.	Estado: Pasó Fecha de Ejecución: 09/10/2020 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 Ejecución: 06/10/2020 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 encontró ningún tipo de riesgo	Estado: Falló Fecha de Ejecución: 15/09/2020 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 Ejecución: 22/09/2020 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.idr riesgo = Riesgo.idriesgo Resultado: Reporte del plan de contingencias	Estado: Pasó Fecha de Ejecución: 20/10/2020 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 estadístico 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 Ejecución: 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	Criterio: cargar unicamente las salvaguardas para	Estado: Pasó Fecha de Ejecución: 19/10/2020 Ejecutado por: Sergio Daniel Caballero

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

	el riesgo seleccionado Entrada: Id de Riesgo	aquellos casos que cumplan con El riesgo indicado Amenaza del riesgo tipo de activo dimensión salvaguarda Resultado: Solo muestra lo indicado	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 Ejecución: 20/10/2020 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 Ejecución: 08/10/2020 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
--------	---------------	-------------------------	---------------------

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

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. dar de baja el ultimo usuario cargado	Criterio: Resultado: Funcionó ok	Estado: Pasó Fecha de Ejecución: 18/10/2020 Ejecutado por: Sergio Daniel Caballero Controlado: Sergio Daniel Caballero
--	---	--	---

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 Ejecución: 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 Ejecución: 18/10/2020 Ejecutado por: Controlado:

Taxonomía

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

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 Ejecución: 04/10/2020 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 Ejecución: 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: Cambio de estado a Estado = 'FIN'	Estado: Pasó Fecha de Ejecución: 19/10/2020 Ejecutado por: Sergio Daniel Caballero Controlado: Sergio Daniel Caballero

Anexo IV -Encuesta realizada

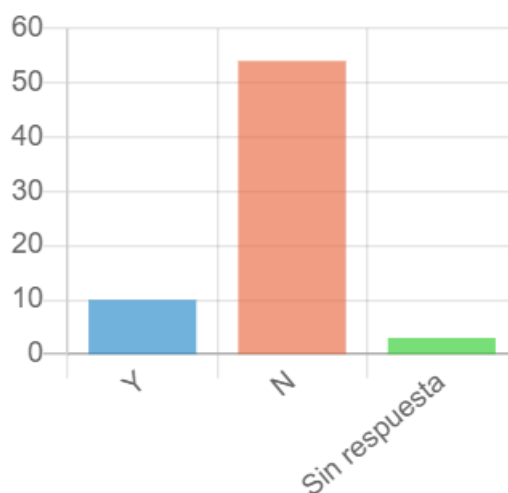
Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3

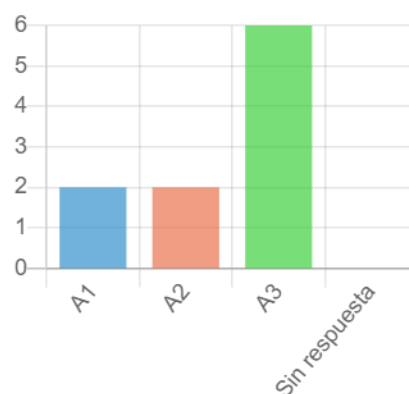
En la Unidad N° 3 se realizó el estudio del cuestionario realizado en este TFM, en este anexo, se incorporan datos que no se muestran dicha unidad.

Número de registros en esta consulta:	77
Total de registros en esta encuesta:	77

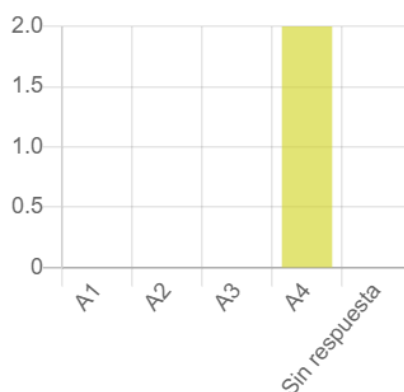
En la organización/empresa que Ud trabaja, utilizan análisis y gestión de riesgos en TI ?		
Opción	Cuenta	Porcentaje
Sí (Y)	10	14,93%
No (N)	54	80,60%
Sin respuesta	3	4,48%



La Metodología utilizada es:		
Opción	Cuenta	Porcentaje
Utiliza un método FORMAL (A1)	2	20,00%
Utiliza un método INFORMAL (A2)	2	20,00%
Utiliza un método MIXTO (A3)	6	60,00%
<u>Observación:</u> Esta pregunta se responde si la opción de la pregunta N° 1 fue SI.		



Que metodología Formal Utiliza?		
Opción	Cuenta	Porcentaje
Magerit (A1)	0	0,00%
SEI - Basado en taxonomías (A2)	0	0,00%
PMBok (A3)	0	0,00%
Otras (A4)	2	100,00%
Sin respuesta	0	0,00%
Observación: Esta pregunta se responde si la opción de la pregunta N° 2 fue FORMAL (A1).		



Cual cree que es la causa por la cual No realiza Análisis y Gestión de Riesgos en TI?		
Opción	Cuenta	Porcentaje
Falta de Recursos (Presupuesto/RRHH/Tiempo) (A1)	13	27,66%
Desconocimiento de Metodologías (A2)	13	27,66%
Falta de Interés Organizacional (A3)	21	44,68%
Otro	0	0,00%
Sin respuesta	0	0,00%

Análisis de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit3



En que rama de TI utilizía AGR			
Opción	Cuenta	Porcentaje	
Desarrollo de Software (SQ001)	2	40,00%	
Proyectos TI (SQ002)	3	60,00%	
Equipamientos e Infraestructura (SQ003)	5	100,00%	
Telecomunicaciones (SQ004)	2	40,00%	
Datos (SQ005)	4	80,00%	
Otros (SQ006)	0	0,00%	

