ESCUELA POLITECNICA DEL EJÉRCITO

SEDE LATACUNGA

FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA

DESARROLLO DE UNA HERRAMIENTA DE GESTION DE RIESGOS DE PROYECTOS SOFTWARE

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS E INFORMATICA

SANDRA SORAYDA RUBIO RUBIO

Latacunga-Ecuador-2005

CERTIFICACION

Se certifica que el presente trabajo fue desarrollado por Sandra Sorayda Rubio Rubio, bajo nuestra supervisión

_____

Ing. Santiago Jácome

DIRECTOR DE PROYECTO

_____

Ing. José Luis Carrillo

CODIRECTOR DE PROYECTO

DEDICATORIA

De manera especial a mi madre que siempre me supo a dar su apoyo incondcional, demostrándome su afecto y comprensión dándome lo mejor de ella; a mi Padre y Hermano que supieron incentivarme a seguir adelante para alcanzar mis metas.

Sandra Sorayda Rubio Rubio

AGRADECIMIENTO

Mi agradecimiento sincero a Dios, a mi madre por haberme dado la vida por entregarme su amor, sacrificio y entrega incondicional en todos los momentos importantes como este, la culminación de un sueño que ahora gracias a ella es una realidad; a mi Padre y Hermano por su paciencia y apoyo en mi carrera estudiantil.

A mis profesores por su labor de educación brindada y a la ESPE-L que me acogió durante mis estudios brindándome los conocimientos necesarios.

Sandra Sorayda Rubio Rubio

INDICE

CAPITULO I.- PROYECTO SOFTWARE

CAPITULO II.- TEORIA DE GESTIÓN DE RIESGOS

CAPITULO IV.- DESARROLLO DE LA HERRAMIENTA DE GESTIÓN DE RIESGOS

CAPITULO V.- CONCLUSIONES Y RECOMENDACIONES

CAPITULO I

El presente capítulo trata sobre lo que es un proyecto software, el proceso de construcción de software, el proceso software frente al ciclo de vida, estados por los que va pasando un producto software, procesos del ciclo de vida; modelos de ciclos de vida aquí se tratan los modelos de ciclo de vida tradicionales como son: cascada o clásico, refinamiento sucesivo o mejora iterativa, modelos de ciclo de vida con emisión gradual, estándares militares y dentro de este las normas MIL-STD-2167 y ESA PSS-05-0, modelo de ciclo de vida por prototipos (modelo de amplificación del modelo y uso adecuado de prototipos), modelo de ciclo de vida por prototipado rápido, modelo incremental. Modelos de ciclo de vida alternativos aquí se estudian los modelos de proceso de producción de software dentro de este los modelos operativos (especificaciones operativas para prototipado rápido, automatización de la programación y del proceso software, automatización del software basado en conocimientos) y no operativos (modelo en espiral y modelos de transformación continua). Problemas comunes en el desarrollo del software, estimación de un proyecto software, modelo de estimación, herramientas automáticas de estimación y lo que son sistemas de información.

También se trata los objetivos y las constantes que persigue la creación de un proyecto software, las características del software dentro de este se estudia la característica más importante como es la calidad (concepto, calidad en los productos software, calidad por etapas y control de calidad) y, finalmente el ámbito de un proyecto software.

1. - PROYECTO SOFTWARE

1.1 .- QUÉ ES UN PROYECTO SOFTWARE

Software es un conjunto de instrucciones responsables de que el Hardware realice su tarea. Como concepto general el Software puede dividirse en varias categorías basadas en el tipo de trabajo realizado. Las dos categorías primarias del Software son los Sistemas Operativos llamado también Software de Sistema que controlan los trabajos del ordenador o computadora, y el Software de Aplicación, que dirige las distintas tareas para las que se utilizan las computadoras. Por lo tanto, el Software del Sistema procesa tareas tan esenciales, aunque a menudo invisibles, como el mantenimiento de los archivos de disco y la administración de la pantalla mientras que el Software de Aplicación lleva a cabo las tareas de tratamiento de textos, gestión de bases de datos y similares. Constituyen dos categorías separadas el software de red, que permite comunicarse a grupos de usuarios, y el software de lenguaje utilizado para escribir programas

Partiendo de este concepto se puede deducir que un proyecto software es el proceso de gestión para la creación de un software, la cual encierra un conjunto de actividades como son: Especificación de Requisitos, Análisis, Diseño, Implementación, Pruebas, Implantación, Mantenimiento etc.

1.1.1 PROCESO DE CONSTRUCCIÓN DE SOFTWARE

El proceso de construir un producto software es una **actividad de resolución de problemas.** En realidad, la construcción de software tiene dos objetivos. Por un lado, dada una necesidad, pretende satisfacerla mediante una solución tratable o Software (figura 1.1). Por otro lado, el subsecuente mantenimiento de software hasta el final de su vida útil.

Considerando el primer objetivo, el proceso software es la transformación de una necesidad (problema) en un software (solución automatizada) que satisface esa necesidad. Así, dicho proceso puede entenderse como la actividad de resolución de un problema.

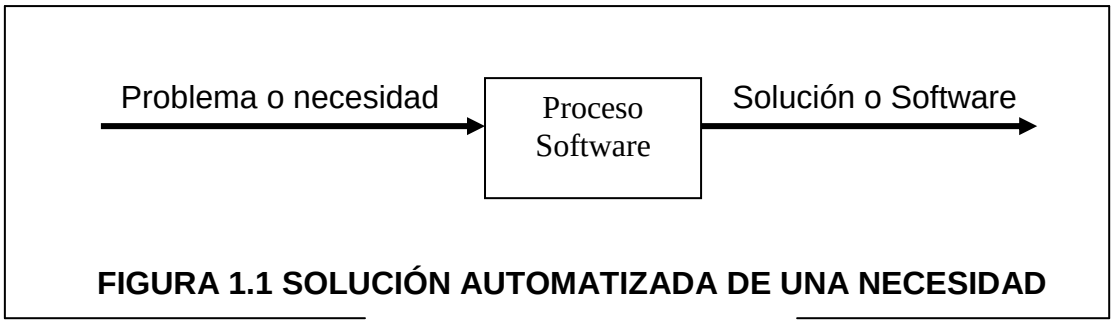
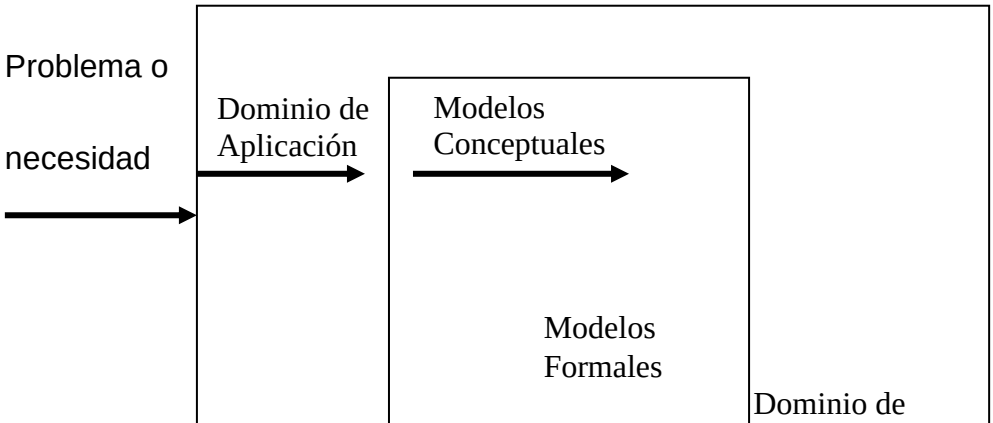


FIGURA 1.1 SOLUCIÓN AUTOMATIZADA DE UNA NECESIDAD

La solución de un problema mediante ingeniería de software es una actividad de **modelización** que comienza con el desarrollo de **modelos conceptuales** (no formales) y los convierte en **modelos formales**, que son productos implementados (figura 1.2). Estas dos actividades de modelización trabajan a niveles distintos: el **nivel del problema** o necesidad (nivel conceptual o dominio de aplicación), y el **nivel de la solución** implementada en computadora (o nivel formal). En análisis de sistemas software, el modelo conceptual se corresponde con el punto de vista que las personas tienen del problema, en tanto que el modelo formal concierne a la perspectiva de que ese mismo problema tiene la computadora.



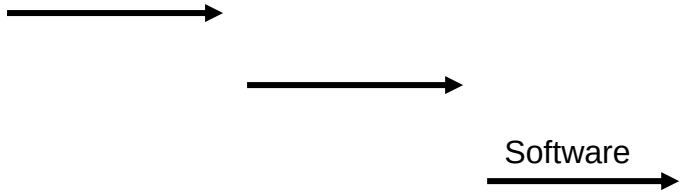


FIGURA 1.2 PROCESO ESENCIAL DE CONSTRUCCIÓN DE SOFTWARE

La figura 1.2 ilustra varios aspectos importantes del proceso de construcción software. Lo fundamental que puede apreciarse en la figura 1.2 es que los modelos conceptuales y formales son distintos y no pueden derivarse lógicamente el modelo formal a partir del modelo conceptual. El modelo conceptual determina la validez (¿es válido el modelo obtenido para la necesidad que tenía?), en tanto que el formal determina el funcionamiento correcto (¿funciona correctamente el modelo?). De hecho, es imposible establecer la corrección de un modelo conceptual pero, usando modelos formales del dominio, es posible descubrir errores que invaliden el modelo conceptual. En el dominio de la aplicación, los modelos son conceptuales en el sentido de que modelizan como el software debería responder a una necesidad. Aunque pueden emplearse formalismos para representar estos modelos, desde la perspectiva de la computadora son, hasta el momento, modelos meramente declarados o descriptivos, no operativos. La actividad de modelización formal comienza sólo después de que existe un modelo conceptual, o sea, un modelo descriptivo de cómo el software responde a la necesidad. El modelo formal generado es un modelo prescriptivo o procedimental y computable por la máquina.

Además, la figura 1.2 muestra que el proceso software siempre culmina con la creación de un modelo formal. Pero, aunque la actividad de modelización formal es esencial y los métodos formales que preservan la corrección son importantes, esto no asegura el éxito de un proyecto. Cuando los sistemas son abiertos, las necesidades cambian y entonces la validez del modelo conceptual

es un factor de riesgo. En efecto, la corrección del producto con respecto al modelo formal es, naturalmente, condición necesaria pero difícilmente suficiente.

Por último, el modelo conceptual muestra por que la construcción del software puede ser tan difícil. Existen muchas respuestas potenciales a una necesidad, y el modelo conceptual limita la elección a una. Raramente, hay una mejor elección; habitualmente, sólo hay malas elecciones a evitar. Además, para cada clase de modelo conceptual, se definen muchos modelos formales que pueden producir una respuesta satisfactoria, y muchas posibles programaciones correctas por cada modelo formal. De este modo, hay que trabajar en dos dominios, con dos tipos de modelos y gestionando elecciones que, necesariamente, están basadas en el juicio y la experiencia.

En el proceso de construcción de los modelos existen riesgos que se debe tomar en cuenta por ejemplo: al realizar el modelo conceptual se debe validarlo con la información que se obtuvo del usuario sobre la necesidad que este tiene empleando diferentes técnicas de recolección de datos para llegar a un modelo formal completo y detallado de que es lo que se quiere realizar para satisfacer de manera correcta y eficiente la necesidad del usuario.

Planteada la construcción del software como una resolución de problemas, debe existir un proceso de resolución que corresponda con el proceso básico de resolución de problemas expuesto anteriormente. En efecto, al primer paso, o definición de *qué*, se le denomina **análisis y especificación de requisitos.** A la decisión de *cómo* hacerlo se la conoce en ingeniería de software, como **diseño del sistema software.** A la realización de ese *cómo* se le llama **codificación.** Posteriormente, el sistema debe ser sometido a **pruebas.** Y finalmente, la solución debe ser usada, o, en el caso de software **instalado.**

Además, cuando las soluciones a los problemas no son puntuales, sino que permanecen en el tiempo, al proceso de resolución debe añadirse una última etapa de **mantenimiento.** Por tanto, el **proceso** mínimo necesario para resolver el problema de la construcción de un sistema software es:

1. Obtención de requisitos software

Incluye el análisis del problema y concluye con una especificación completa del comportamiento externo que debería tener el sistema a construir. El riesgo que se puede presentar en esta etapa es que los requisitos no estén bien claros y por lo tanto no se este realizando lo requerido por el usuario para satisfacer la necesidad del mismo.

2. Diseñar

El diseño del sistema debe realizarse a dos niveles: alto nivel o diseño preliminar, y bajo nivel o diseño detallado. En el **diseño preliminar** se descompone el sistema software en sus componentes principales, estos componentes se subdividen a su vez en componentes más pequeños. Este proceso iterativo continua hasta un nivel adecuado en el que los componentes pueden ser tratados en el diseño de bajo nivel. Generalmente, estos módulos realizan una única función bien detallada y pueden venir descritos por su entrada, su salida y la función que realizan. En el **diseño detallado** se definen y documentan los algoritmos que llevarán a cabo la función a realizar por cada módulo. El riesgo en esta etapa se puede encontrar al momento de descomponer el sistema en componentes más pequeños ya que se puede perder información y por lo tanto el sistema no va a funcionar de la manera que se requiere.

3. Implementar

Consiste en transformar los algoritmos definidos durante el diseño de bajo nivel en un lenguaje compresible para una computadora. La codificación suele llevarse a cabo en dos niveles: la conversión del algoritmo en un lenguaje de alto nivel; y la transformación del lenguaje de alto nivel en lenguaje máquina. Generalmente, el primer nivel es realizado por personas para este caso un Programador y el segundo nivel se realiza automáticamente por un Compilador. Al momento de la implementación se puede presentar el riesgo de que el sistema no cumpla con todos los requisitos especificados para su correcto funcionamiento.

4. Realizar pruebas

Si los humanos fueran perfectos en el desarrollo del software, el proceso podría finalizar en el punto anterior. Desafortunadamente, éste no es el caso. Por tanto, se necesita un proceso de comprobación o pruebas para eliminar los errores. La comprobación se divide en tres niveles.

- Pruebas **unitarias** comprueban cada módulo implementado en busca de errores. En esta comprobación se quiere asegurar que cada módulo se comporta de acuerdo con lo especificado durante el diseño de bajo nivel

- Pruebas de **integración** que interconectan conjuntos de módulos, previamente probados, asegurándose de que el conjunto se comporta tan bien como lo hacían independientemente. Lo ideal es que cada conjunto de módulos integrados se correspondiera con un componente del diseño de alto nivel.

- Pruebas del **sistema,** pretenden asegurar que la totalidad del sistema software (totalmente integrado en su entorno) se comporte de acuerdo con la especificación inicial

5. Instalar

Tras las pruebas, el sistema software y su entorno hardware pasan a la fase operativa (instalación y utilización del software).

6. Mantener y ampliar

El mantenimiento consiste en la detección continuada de errores y su reparación. La ampliación, por su parte, se corresponde con la adición al sistema de nuevas capacidades. Estos dos procesos siguen, de hecho, un proceso completo como el visto hasta aquí.

1.1.2 PROCESO SOFTWARE FRENTE AL CICLO DE VIDA

De todo lo visto hasta aquí puede deducirse que el nombre **proceso software** se corresponde con la colección de actividades que comienza con la identificación de una necesidad y concluye con el retiro del software que satisface dicha necesidad. El proceso software más básico debe estar formado por las seis etapas anteriores. Sin embargo, en un proceso software, las actividades que constituyen deben estar interrelacionadas. Puede existir más de una manera de interrelacionar las actividades. Las distintas maneras representan distintas estrategias para cumplimentar la construcción del software.

1.1.3 ESTADOS POR LOS QUE PASA EL SOFTWARE

Es necesario establecer los estados por los que va pasando el producto o un proceso software: la entrada al proceso es una **necesidad** que, una vez estudiada se convierte en una **especificación de requisitos** que, posteriormente, se transforma en un **diseño del sistema,** para pasar más adelante a ser un **código** y, finalmente un **sistema software completo** e integrado. Este enfoque orientado al producto, focalizado en la transformación del producto, en lugar del proceso que lo transforma, es lo que se llama **ciclo de vida**. Es decir, el ciclo que el producto software sufre a lo largo de su vida, desde que nace (o se detecta la necesidad) hasta que muere (o se retira del sistema). La figura 1.3 muestra las relaciones entre proceso y ciclo de vida.

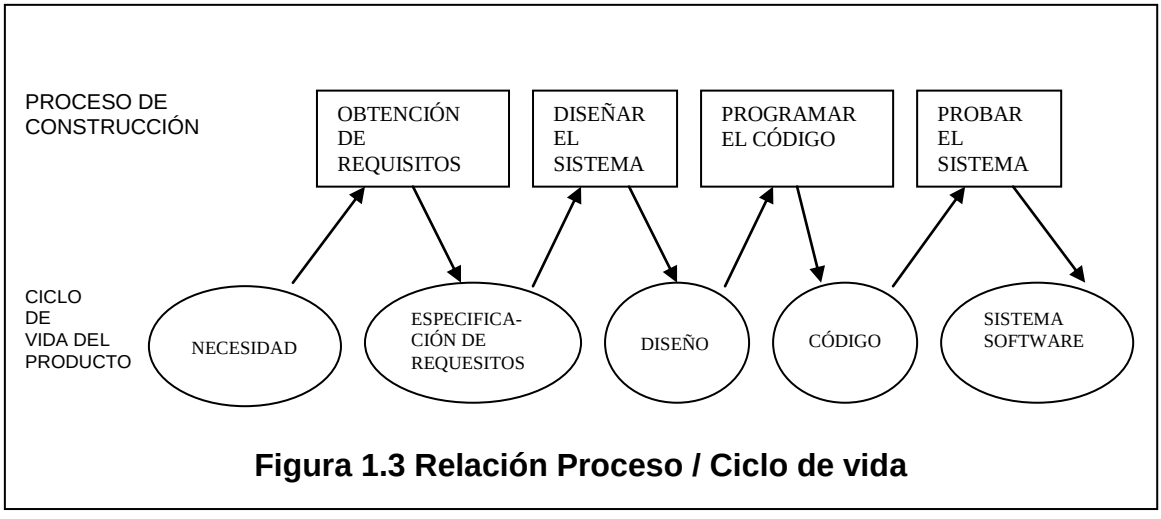


Figura 1.3 Relación Proceso / Ciclo de vida

Este cambio de perspectiva del proceso al producto es muy sutil. De hecho, siempre se está hablando del mismo problema: generación de una solución computarizada que satisfaga una necesidad. Es más, proceso y producto, producto y proceso, están intrínsicamente relacionados, son inseparables. Sin embargo, esta variación en el modo de enfocar la construcción de software tiene un sentido.

Por necesidad histórica, la primera preocupación de la ingeniería de software tenía que ser los programas de la computadora (la tecnología usada para resolver el problema). En los primeros años, los problemas que podían tratar las computadoras estaban muy limitados debido a las limitaciones de la tecnología. Por ejemplo, a pesar de que los comienzos de la inteligencia artificial se datan en 1956, no fue hasta que llegaron los avances en computación en los años 80, cuando alcanzó amplia aceptación y entró en explotación. Según la tecnología mejoraba, la complejidad de los proyectos crecía. Sin embargo, todavía el programa era el tema central de la Informática. A las personas se les enseñaba a escribir programas, y una buena capacidad de programación definía una profesión. Sin embargo, al centrarse en el programa limita la visión a temas de un grano muy fino, de un nivel muy bajo. A menudo, esta problemática ha sido llamada **programación a pequeña escala**. Hoy por hoy, se denomina problemática de este tipo a la programación. Las expectativas y el potencial se encuentra en la **programación a gran escala**. Este nombre se reserva para las decisiones de diseño de alto nivel, para el grano grueso, para las otras fases del proceso que no son la codificación.

Resumiendo a lo largo de la breve historia de la ingeniería de software se ha producido un cambio de perspectiva del producto al proceso. De ahí que, en los últimos años, el nombre de ciclo de vida haya sido relegado, utilizando en su

lugar proceso software. Este cambio de enfoque significa que se está más preocupado por el proceso de resolver un problema del mundo real (quizás utilizando muchos programas para ello) que con el producto en sí mismo. Naturalmente, la mayor parte del esfuerzo se dedicará a la creación y mantenimiento del producto. Pero esa actividad es sólo un medio para conseguir un fin.

El proceso software refleja cómo se usa la experiencia humana en la construcción de software y cómo se aplica a un dominio concreto; es el ciclo de vida del software visto desde fuera; la estructura dentro de la que los ingenieros software deben operar.

1.1.4 PROCESOS DEL CICLO DE VIDA

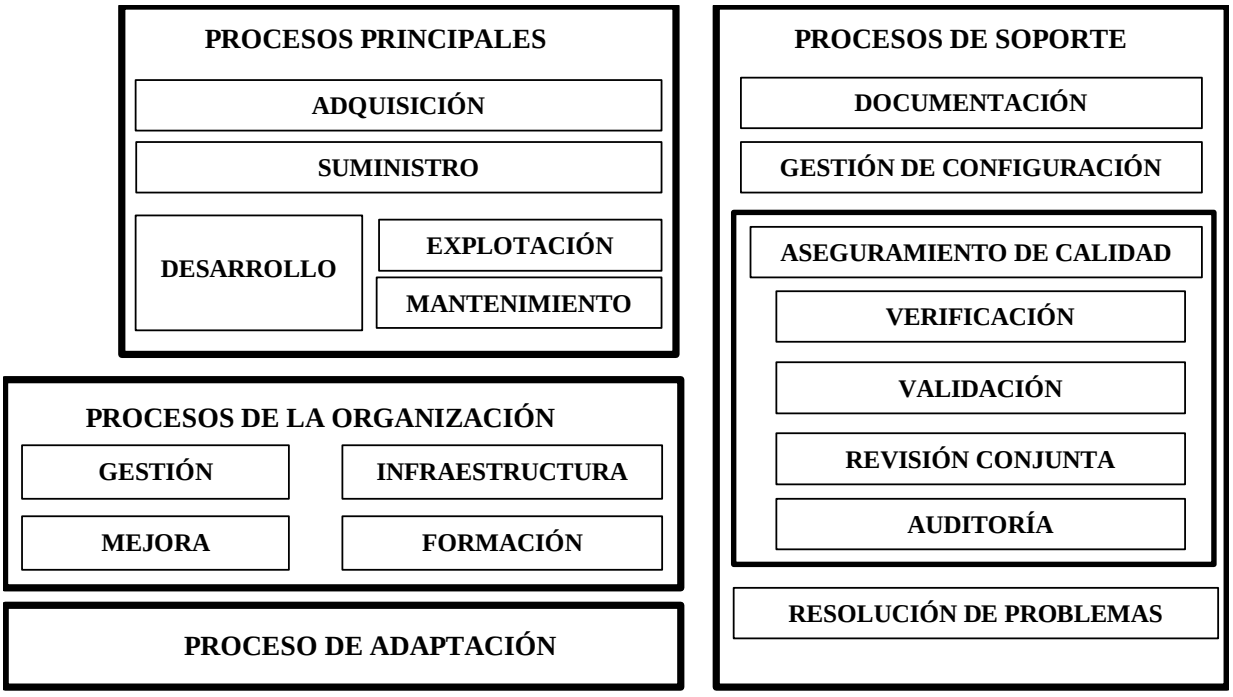


FIGURA 1.4 PROCESOS DE CREACIÓN DEL SOFTWARE

PROCESOS PRINCIPALES

Los procesos principales son útiles a las personas que inician o realizan el desarrollo, la explotación o el mantenimiento del software durante su ciclo de vida así por ejemplo: compradores, suministradores, personal de desarrollo, operadores y personal de mantenimiento del software.

Dentro de este proceso se realizan los siguientes sub-procesos:

- Proceso de Adquisición.- Son actividades y tareas que el comprador, el cliente o el usuario realizan para adquirir un sistema o producto (servicio) software.

- Proceso de Suministro.- Son actividades y tareas que realiza el suministrador. Se inicia al preparar una propuesta para atender una petición de un comprador, o por la firma de un contrato con el comprador para proporcionarle un producto software.

- Proceso de Desarrollo.- Dentro de este proceso se realizan las siguientes actividades:

    - Análisis de Requisitos del Sistema.- Los requisitos del sistema incluyen: funciones y capacidades, requisitos de seguridad, requisitos de interacción hombre-máquina, interfaces del sistema, restricciones aplicables al diseño, requisitos de aceptación.

    - **Diseño de la Arquitectura del Sistema.- En este proceso se identifica la arquitectura de alto nivel del sistema: Se determinan los principales componentes hardware, software y las operaciones manuales. Se asignan los requisitos del sistema a dichos componentes.**

- Análisis de los Requisitos del Software.- Aquí se identifican y documentan los requisitos del software, incluyendo: especificaciones funcionales y de capacidad (rendimiento de la aplicación, etc.), interfaces externas, seguridad y protección (de la información, daños personales, etc.), datos que se van a manejar, requisitos de la base de datos, requisitos de instalación y requisitos de mantenimiento.

- **Diseño de la Arquitectura del Software.- Dentro de este se analiza los componentes principales del software, versión preliminar de los manuales de usuario, requisitos de las pruebas y la planificación de la integración del software.**

- Diseño Detallado del Software.- Dentro de este proceso se realizan los siguientes diseños: diseño detallado de cada componente software, diseño detallado de las interfaces, diseño detallado de la base de datos, se actualizan manuales de usuario, se actualizan los requerimientos de pruebas para la integración del software. También en este proceso se evalúa todo lo anterior y se realizan reuniones de revisión.

- Codificación y Prueba del Software.- Aquí se desarrollan los componentes software y las bases de datos. Se prueban los componentes (prueba de unidad) y se actualizan los manuales de usuario.

- Integración del Software.- Aquí se integran los componentes del software y se prueban según la necesidad.

- Prueba del Software.- Se realizan las pruebas de acuerdo con los requisitos de cualificación (validación) especificados para el software.

- Integración del Sistema.- Aquí se integra: hardware, software y operaciones manuales.

- Prueba del Sistema.- aquí se realiza una prueba análoga del software, pero de acuerdo con los requisitos de cualificación especificados para el sistema.

- **Instalación del Software.- Aquí se procede a la instalación del software en el entorno donde vaya a funcionar**

- Soporte del proceso de Aceptación del Software.- Aquí se debe dar apoyo a la revisión de aceptación y a la prueba del software por el comprador.

- Proceso de Explotación.- Este proceso también es llamado de operación y es la explotación del software y del soporte del mismo (se aplica al sistema completo).

- Proceso de Mantenimiento.- El software o la documentación necesita ser modificado, debido a problemas o a necesidades de mejora o adaptación, por ejemplo: nuevos errores detectados, cambios en la legislación, cambios en el entorno, necesidad de mejoras, migración a un nuevo entorno operativo, etc.

PROCESOS DE SOPORTE

Estos procesos sirven de apoyo al resto de procesos. Contribuyen al éxito y calidad del proyecto software. Se aplican en cualquier momento del ciclo de vida.

Dentro de este proceso se realizan los siguientes sub-procesos:

- Proceso de Documentación.- Registra la información producida por cualquier proceso o actividad del ciclo de vida.

- Proceso de Gestión de la Configuración.- Aquí se realiza la configuración del software: programas, documentación, datos.

- Proceso de Aseguramiento de la Calidad.- Este aporta confianza en que los procesos y los productos software del ciclo de vida cumplen con los requisitos especificados y se ajustan a los planes establecidos.

- Proceso de Verificación.- Indica si los requisitos de un sistema o del software están bien recogidos en cada modelo

- Proceso de Validación.- Indica si el sistema o software final cumple con las necesidades del usuario.

- Proceso de Revisión Conjunta.- Se realiza durante todo el ciclo de vida: a nivel de gestión y a nivel técnico del proyecto

- Proceso de Auditoría.- Permite determinar si se cumplen los requisitos, los planes y el contrato.

- Proceso de Resolución de Problemas.- Aquí se Analizan y eliminan los problemas (diferencias con el contrato o los requisitos) descubiertos durante el desarrollo, el mantenimiento, u otro proceso.

PROCESOS GENERALES

El objetivo de estos procesos es establecer, implementar y mejorar la organización del ciclo de vida.

Dentro de este proceso se realizan los siguientes sub-procesos:

- Proceso de Gestión.- Se incluye en cualquier organización que tenga que gestionar sus procesos. Implica: *planificación, seguimiento y control, revisión y evaluación.*

- Proceso de Infraestructura.- Establece la infraestructura necesaria para el resto de procesos (para el desarrollo, la explotación o el mantenimiento): *hardware, software, herramientas, normas e instalaciones.*

- Proceso de Mejora.- Sirve para establecer, valorar, medir, controlar y mejorar los procesos del ciclo de vida del software.

- Proceso de Formación.- Sirve para mantener el personal formado, desarrollando un plan de formación, junto con materiales adecuados.

PROCESOS DE ADAPTACIÓN

Este proceso permite adaptar el estándar a cada proyecto y organización. Dentro de este proceso también encontramos factores que influencian la forma de adquirir, desarrollar, explotar o mantener un sistema:

- Tamaño y complejidad del proyecto.
- Requisitos del sistema.

- Métodos de desarrollo.
- Variaciones en las políticas y procedimientos de la organización.

CICLOS DE VIDA DEL SOFTWARE

Como todo producto de ingeniería, el software también tiene su ciclo de vida. Éste corresponde al período desde que el sistema se concibe hasta que se deja de usar, pasando por su especificación, desarrollo, transferencia y explotación. En definitiva, el ciclo de vida del software corresponde a las fases involucradas en todo el período del sistema de software.

La ISO 12207-1 expresa que el ciclo de vida del software es: “Un marco de referencia que contiene los procesos, las actividades y las tareas involucradas en el desarrollo, la explotación y el mantenimiento de un producto de software, abarcando la vida del sistema desde la definición de los requisitos hasta la finalización de su uso”.

No existe un único modelo de ciclo de vida que defina los estados por los que pasa cualquier producto software. Dado que existe una variedad de aplicaciones para las que se construyen productos software (software de tiempo real, de gestión, de ingeniería y científico, de sistemas, de computadoras personales, etc.) y que dicha variedad supone situaciones totalmente distintas, es natural que existan diferentes modelos de ciclo de vida. Por ejemplo, en aquellos casos en que el problema sea perfectamente conocido, el grupo de desarrollo tenga experiencia en sistemas del mismo tipo, el usuario sea capaz de escribir claramente sus requisitos, un ciclo de vida tradicional, en cascada o secuencial seria el adecuado. Por el contrario, si el desarrollo conlleva riesgos (sean técnicos o de otro tipo), un ciclo de vida en espiral será el más apropiado. Sin embargo, si se está ante el caso en que es necesario probarle el producto al usuario para demostrarle la utilidad del mismo, se estará ante un ciclo de vida con prototipado, etc.

Un ciclo de vida debe:

- Determinar el orden de las fases del proceso software
- Establecer los criterios de transición para pasar de una fase a la siguiente

A continuación, se revisara los diferentes modelos de ciclo de vida existentes: en cascada, gradual, espiral, prototipado operativo, prototipado de usar y tirar, etc. No existe un modelo de ciclo de vida que sirva para cualquier proyecto, esto debe quedar claro. Cada proyecto debe seleccionar un tipo de ciclo de vida que sea el más adecuado para su caso. El ciclo de vida apropiado se elige en base a la cultura de la corporación, el deseo de asumir riesgos, el área de aplicación, la volatilidad de los requisitos y hasta qué punto se entienden bien dichos requisitos. El ciclo de vida elegido ayuda a relacionar las tareas que forman el proceso software de cada proyecto.

1.1.5 MODELOS DE CICLO DE VIDA TRADICIONALES

Estos tipos de modelos de la evolución del producto software existen, en algún caso desde los primeros días de la ingeniería de software. El ciclo de vida del software clásico o modelo *en cascada* y el *refinamiento sucesivo* están ampliamente tratados en casi todos los libros de ingeniería de software. El modelo de *emisión gradual* está estrechamente relacionado con las prácticas industriales donde aparece con mayor frecuencia. Los *estándares militares* también han marcado ciertas formas de ciclo de vida clásico en la práctica exigida para contratistas del Ministerio de Defensa de los EE.UU. Finalmente, *el prototipado* es uno de los últimos ciclos de vida aparecidos que se han extendido tan rápidamente que, hoy en día, puede considerase clásico. Está rápida extensión del prototipado es debida al aumento en la complejidad de los sistemas software que se construyen, que hace necesario el desarrollo de prototipos antes de poder pasar a la construcción del sistema a escala real. Dado que todos estos modelos se han usado durante algún tiempo es por lo que se consideran tradicionales.

1.1.6 MODELO DE CICLO DE VIDA CLÁSICO O EN CASCADA.

Este modelo fue presentado por primera vez por Royce en 1970. El modelo de desarrollo en cascada se caracteriza debido a que sus fases se distribuyen en forma secuencial, una después de otra. Primero se realiza la fase de análisis. Una vez completada dicha fase, se desarrolla la fase de diseño. Luego, la fase de producción, que incluye el diseño detallado, programación y testeo del producto. Una vez finalizada dicha fase, se sigue a la fase de transferencia del sistema construido al ambiente de producción. Por último, se realiza la fase de operación y mantenimiento del software.

El modelo de desarrollo se llama cascada ya que su dibujo parece una cascada, en donde el producto de una fase va cayendo a la siguiente para su procesamiento.

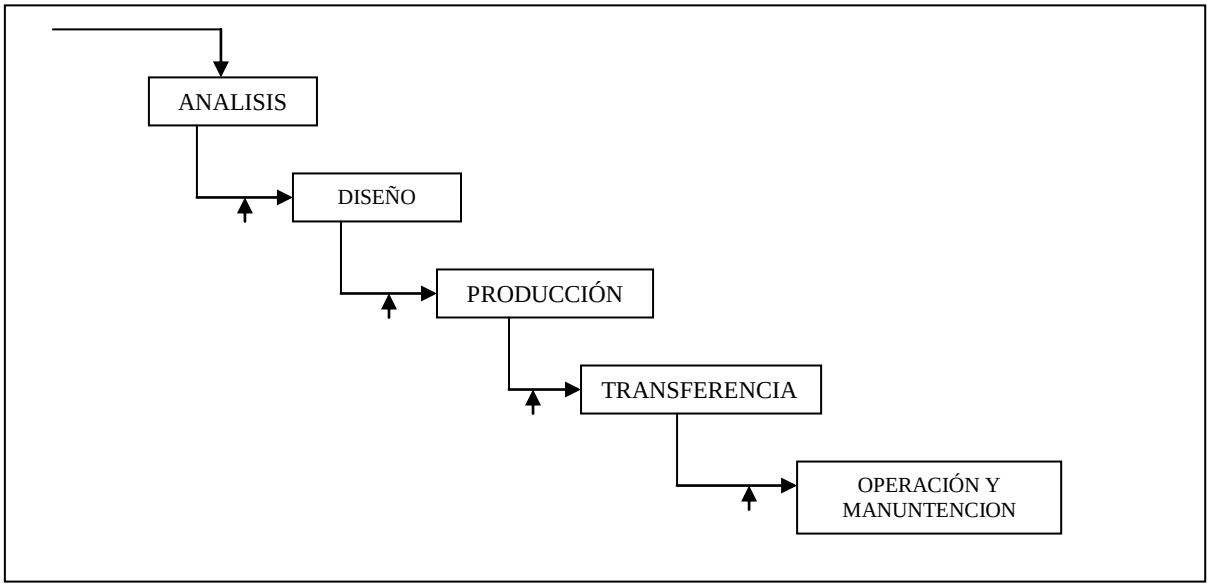


FIGURA 1.5 MODELO DE CICLO DE VIDA EN CASCADA

Esta claro que para utilizar este modelo, es necesario cumplir con la aceptación de cada una de las fases antes de partir con la siguiente, representado en la figura anterior como triángulos negros. Dichos triángulos corresponden a hitos que deben ser aprobados formalmente entre el cliente y el equipo de desarrollo. Esto requiere una gran madurez por parte del equipo de desarrollo y por parte del cliente, ya que no es posible volver a fases anteriores. Cada uno debe conocer exactamente sus responsabilidades en el ciclo.

El modelo en cascada a levantado ciertas criticas que describimos a continuación:

- No refleja realmente el proceso de desarrollo del software
- Se tarda mucho tiempo en pasar por todo el ciclo
- Perpetua el fracaso de la industria del software en su comunicación con el usuario final
- Se convierten las especificaciones en implementaciones de manera informal
- El mantenimiento se realiza en el código fuente
- Las revisiones de proyectos de gran complejidad son muy difíciles

El riesgo principal que se puede presentar en este ciclo de vida es en el análisis ya que si un requisito esta mal especificado o no refleja lo que el usuario explicó, todo el proceso de construcción del software esta mal realizado y se pierde tiempo y dinero ya que se debe realizar todo el proceso nuevamente.

1.1.7 MODELO DE CICLO DE VIDA DE REFINAMIENTO SUCESIVO O MEJORA ITERATIVA

Las etapas que forman este ciclo de vida son las mismas que el modelo en cascada y su realización sigue el mismo orden. Sin embargo, este modelo recomienda desarrollar los sistemas software a través de un refinamiento y mejora continua desde las especificaciones de alto nivel del sistema hasta las componentes del código fuente. Es decir, este modelo asume que el producto generado en cada etapa no se produce de manera lineal, del principio al final de la etapa. Por el contrario, predica la generación de los productos de forma iterativa, mediante un proceso de refinamiento. Debido a la marcha atrás permitida en el modelo en cascada, que abre un camino desde una etapa hacia otra anterior, el

refinamiento iterativo puede producirse también a nivel global de todas las etapas.

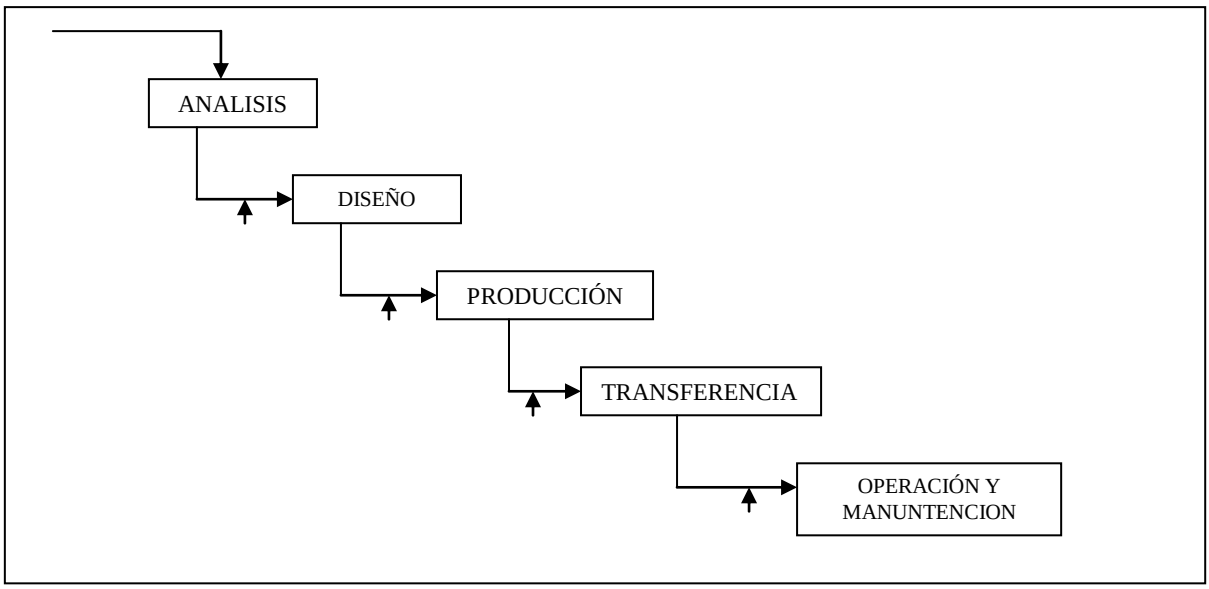


FIGURA 1.6 MODELO DE CICLO DE VIDA DE REFINAMIENTO SUCESIVO O MEJORA ITERATIVA

Estos modelos han sido muy efectivos para enseñar a programadores individuales cómo organizar su trabajo de desarrollo de software, y además reduce el riesgo de que el software no funcione de acuerdo a lo que requiere el usuario.

1.1.8 MODELOS DE CICLO DE VIDA CON EMISIÓN GRADUAL

Este modelo propone desarrollar sistemas produciendo en primer lugar las funciones esenciales de operación y, a continuación, proporcionar a los usuarios mejoras y versiones más capaces del sistema a intervalos regulares. Este modelo combina el ciclo de vida clásico del software con mejoras iterativas a nivel del desarrollo del sistema global. También proporciona una manera para distribuir periódicamente actualizaciones

de mantenimiento de software comercial. Es, por lo tanto, un modelo popular de la evolución del software usado por firmas comerciales.

1.1.9 ESTÁNDARES MILITARES Y PRÁCTICAS INDUSTRIALES

Las empresas industriales adoptan con frecuencia alguna variación del modelo clásico como base para la práctica del desarrollo de software. Muchos suministradores de la administración americana organizan sus actividades de acuerdo con los modelos de ciclo de vida del estándar militar, tal como lo engloba en la norma MIL-STD-2167 de 1987. Tales estándares subrayan no sólo alguna variación de las actividades del ciclo de vida clásico, sino que también contienen los documentos que deben entregarse a los clientes que necesitan sistemas software. Estos estándares se intentan que sean también compatibles con la garantía de la calidad del software, la gestión de configuraciones y la verificación y validación independiente de servicios en un proyecto de desarrollo con más de un contratista. Estos modelos ponen especial énfasis en la definición de productos entregables, revisiones, hitos y técnicas requeridas en cada caso.

Es necesario en este modelo dar a conocer lo que es la norma MIL-STD-2167 y a la norma ESA PSS-05-0 que describimos a continuación.

INTRODUCCIÓN A LA NORMA MIL-STD-2167

Este estándar utilizado por las fuerzas armadas de los EE.UU. En realidad lo utilizan como normativa que debe cumplir los contratistas que se dedican hacer productos software para ellos. En este estándar se contemplaba el desarrollo de productos integrados que incluyen hardware y software, y se establecían ciclos de vida paralelos para ambos. En la última versión, se han separado los conceptos de software y

hardware de manera que, en la actualidad, este estándar no afecta mas que al software.

La nomenclatura de este estándar es un poco complicada, y pesada, por lo que hay que consultar constantemente la lista de acrónimos a no ser que el ingeniero este muy acostumbrado a la misma. En el estándar se considera que existe un sistema que divide en varios CSCI (Computer Software Configuration Item). Cada CSCI se divide a su vez en varios CSC (Computer Software Component). Y cada CSC se divide a su vez en varias CSU (Configuration Software Units). Esta división es importante, ya que afecta directamente a la división en etapas del ciclo de vida.

La descomposición del ciclo de vida de esta norma tiene las siguientes fases:

- Análisis de requisitos del sistema global
- Diseño del sistema
- Análisis de requisitos del software
- Diseño preliminar
- Diseño detallado
- Codificación y verificación de CSUs
- Integración y verificación de CSCs
- Prueba CSCIs
- Integración y prueba del sistema

En cada etapa del ciclo de vida se especifican los documentos que se tienen que generar, al igual que las revisiones que debe sufrir el producto. Este estándar es un poco excesivo en cuanto a documentación requerida, y además pide más de un documento que tiene información redundante.
El estándar no se limita a establecer un ciclo de vida, también se estudian aspectos de cualificación formal, evaluación de productos, gestión de configuración, y transición a la fase de mantenimiento. Finalmente, para cada una de las etapas del ciclo de vida se establece todo lo que se refiere a:

- Gestión de desarrollo
- Ingeniería de software
- Cualificación formal y pruebas
- Evaluación de productos software
- Gestión de configuración

1.1.10 El Estándar ESA PSS-05- 0

Esta es la norma utilizada por la Agencia Espacial Europea (ESA, European Space Agency) para sus desarrollos de software. Al igual que el de la fuerzas armadas americanas, este documento está orientado principalmente a las empresas que desarrollan software bajo contrato, ya que la Agencia desarrolla poco software por sí misma. Estos estándares son bastante generales, y cada proyecto de gran envergadura suele desarrollarlos más, haciendo los estándares propios del proyecto. En caso de conflicto, se suele establecer una jerarquía, en la que prima el estándar más general.

En este estándar, se consideran todos los aspectos de un proyecto software. Además del propio desarrollo y su normativa, se contemplan los aspectos de:

- Gestión de proyecto
- Gestión de configuración
- Control y garantía de calidad

Las etapas que establece este documento para el ciclo de vida son las siguientes:

- Definición de requisitos del usuario
- Definición de requisitos del software
- Diseño de la arquitectura
- Diseño detallado y producción del software
- Transferencia de la tecnología al usuario
- Operación y mantenimiento

La etapa que aparece nueva, respecto al ciclo de vida clásico, es la de transferencia. En esta fase la Agencia, viendo los resultados de las pruebas, da su aceptación provisional al software, y se procede a la instalación en la máquina objetivo, a la formación de los usuarios, etc. Esta fase tiene sentido, en tanto en cuanto, el software se suele desarrollar en países distintos de aquel que se va instalar posteriormente, y por lo tanto, la fase de instalación precisa de desplazamientos de personal, y otras peculiaridades.
En el estándar se contemplan para cada fase los siguientes aspectos:

- Entradas
- Actividades
- Salidas

Además, y para cada uno de los tres aspectos mencionados: gestión del proyecto y de las configuraciones y control de calidad, se describen los planes necesarios para su ejecución, así como los documentos e hitos asociados.

La ventaja fundamental de este estándar es que es muy sencillo y fácil de comprender, con lo que se puede tomar como punto de referencia para desarrollos propios en cualquier otro entorno.

El estándar ESA PSS-05- 0 divide el ciclo de vida del software en seis fases principales y cuatro fases complementarias de revisión. Las fases principales son: **RU** (Definición de Requisitos de Usuarios), **RS** (Definición de Requisitos Software), **DA** (Definición del Diseño Arquitectónico), **DD** (Diseño detallado del Software y Producción del Código), **TR** (Transferencia del Software a Operaciones), **OM** (Operación y Manutención). Estas son detalladas a continuación:

- RU: Definición de requisitos de usuarios.- Corresponde a la especificación de los requisitos del sistema de software, utilizando en lenguaje del usuario. Dentro de las actividades principales de esta fase, se encuentra la determinación del ambiente operacional y la

especificación de los requisitos de usuarios. Lo que se debe entregar en esta fase es el Documento de Requisitos de Usuarios (DRU), el cual se encuentra bajo políticas de control de cambios.

- RS: Definición de requisitos de software.- Corresponde a la especificación de los requisitos del sistema de software, vistos desde la perspectiva del grupo de desarrollo. Dentro de las actividades principales de esta fase está la construcción del modelo lógico del sistema y la especificación de los requisitos de software. Para esto último, es necesario realizar un proceso de traducción de los requisitos de usuarios, convirtiéndolos en requisitos de software. Lo que se debe entregar en esta fase es el Documento de Requisitos de Software (DRS), el cual se encuentra bajo políticas de control de cambios.

- DA: Definición del diseño arquitectónico.- En esta fase se realiza el diseño arquitectónico del sistema de software. Entre sus actividades se encuentra la construcción del modelo físico y la definición de las componentes principales del sistema. Lo que se debe entregar en esta fase es el Documento de Diseño Arquitectónico (DDA), el cual se encuentra regulado por políticas de control de cambios.

- DD: Diseño detallado y producción del código.- En esta fase se completa el diseño realizado en la fase anterior, y se realiza la producción del código de acuerdo a los documentos ya desarrollados. Las actividades también incluyen las tareas de testeo del software. Lo que se debe entregar en esta fase es el Documento de Diseño Detallado (DDD), el código del sistema y el Manual de Usuarios del Software (MUS). Estos tres entregables se encuentran regulados por políticas de control de cambios.

- TR: Transferencia del software a operaciones.- En esta fase, se realiza la instalación del sistema en el ambiente de explotación, y las pruebas de aceptación provisorias. En caso de requerir datos de otras aplicaciones, éstos deben ser migrados adecuadamente con el propósito

de poblar las bases de datos. Lo que se debe entregar en esta fase es el Documento de Transferencia de Software (DTS), el cual se encuentra regulado por políticas de control de cambios. Los hitos principales que indican el término de esta fase son la entrega del DTS, y la aceptación provisoria del sistema por parte del cliente.

- OM: Operación y manutención.- El sistema es puesto en operación, por lo que requiere manutención del código y documentación. En algún momento de esta fase, se realiza la prueba de aceptación final, terminando toda responsabilidad por parte del equipo de desarrollo. Durante toda esta fase, que puede durar muchos años, se completa el Documento de Historial del Proyecto (DHP), que documenta toda la experiencia recogida durante dicha fase en la operación y manutención del sistema. Este documento es utilizado como entrada para el desarrollo del sistema de reemplazo. La entrega del DHP corresponde al último hito de la fase y del sistema de software.

Las fases complementarias son: **RU/R** (Revisión de los Requisitos de Usuarios), **RS/R** (Revisión de los Requisitos de Software), **DA/R** (Revisión del diseño arquitectónico), **DD/R** (Revisión del Diseño detallado del software y Producción del Código). Estas son detalladas a continuación:

- RU/R: Como un anexo a la fase anterior, se incluye una fase complementaria de revisión de los requisitos de usuarios, la que incluye actividades de aseguramiento de la calidad. Su hito principal es la aprobación del DRU por parte del cliente, de acuerdo a procedimientos previamente establecidos.

- RS/R: Como un anexo a la fase anterior, se incluye una fase complementaria de revisión de los requisitos de software, la que incluye actividades de aseguramiento de la calidad. Su hito principal es la aprobación del DRS por parte del cliente, de acuerdo a procedimientos previamente establecidos.

- DA/R: Como un anexo a la fase anterior, se incluye una fase complementaria de revisión del diseño arquitectónico del sistema, la que incluye actividades de aseguramiento de la calidad. Su hito principal es la aprobación del DDA por parte del cliente, de acuerdo a procedimientos previamente establecidos.

- DD/R: Como un anexo a la fase anterior, se incluye una fase complementaria de revisión del diseño detallado del sistema, la que incluye actividades de aseguramiento de la calidad. Su hito principal es la aprobación del DDD, código y MUS por parte del cliente, de acuerdo a procedimientos previamente establecidos.

El modelo de ciclo de vida especificado por el estándar ESA PSS-05-0 es bien claro y reduce al máximo los riesgos que se pueden producir ya que este contempla fases que realizan revisiones periódicas a todas y cada una de las fases del ciclo de vida. Por ejemplo: la norma RU: requisitos del usuario va complementada con la norma RU/R que es una revisión a los requisitos del usuario

1.1.11 MODELO DE CILCO DE VIDA POR PROTOTIPOS

Antes de empezar a hablar sobre el modelo en sí es importante mencionar lo que es un prototipo. Un Prototipo viene del griego protos que significa primero y typos que significa modelo entonces podemos decir que prototipo es el primer modelo que se tiene para desarrollar un software.

El modelo de cascada anterior se sugiere para casos en que el cliente es maduro, siendo capaz de especificar correcta y completamente la aplicación deseada en un período de tiempo definido. No obstante, en la gran mayoría de los casos, lo anterior no es posible. Por ello, el equipo desarrollador debe evaluar el grado de madurez del cliente, y proponer un modelo de desarrollo.

Si el cliente no tiene la madurez requerida, es necesario proponer otro modelo de desarrollo. Una alternativa es el modelo por prototipos, en que se hace madurar al cliente rápidamente en la primera fase de análisis. Esta fase incluye análisis, diseño y construcción de prototipos del sistema, con el propósito de construir una especificación correcta y completa del sistema. Una vez que se logra lo anterior, se sigue el ciclo de igual forma que en el modelo de ciclo de vida en cascada.

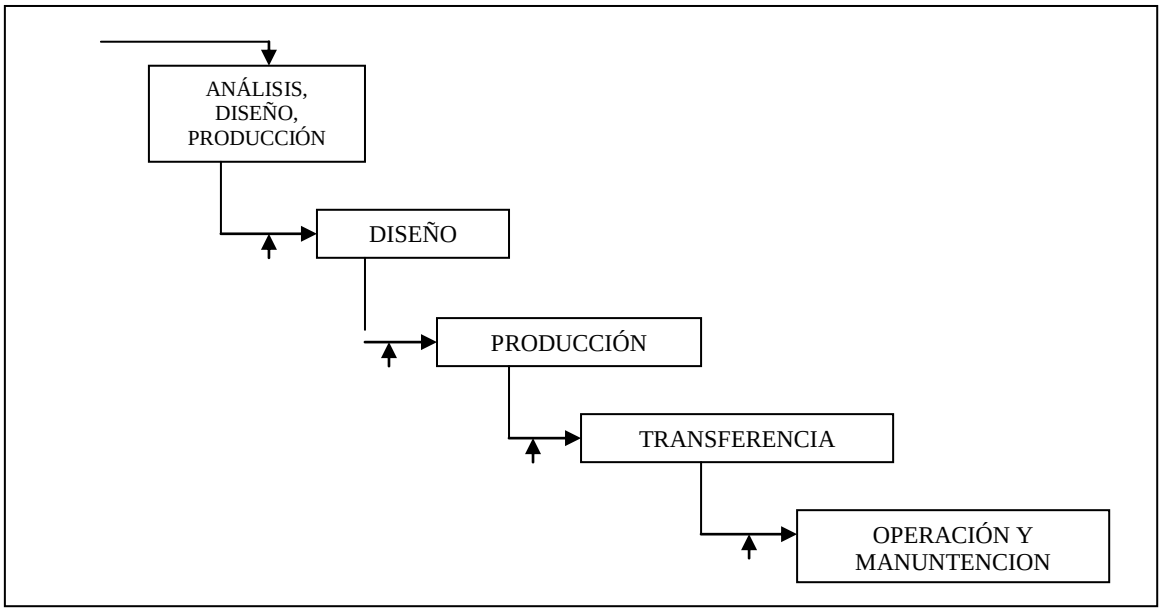


Figura 1.7 MODELO DE CILCO DE VIDA POR PROTOTIPOS

Nótese que en la figura 1.7, la primera fase termina con el hito de aprobación por parte del cliente, de la especificación realizada por prototipos. Los prototipos no constituyen parte del producto mismo, por lo que generalmente no son utilizados en el producto final.

En este modelo se puede implementar, lo que llamamos efecto de amplificación y como es normal el uso de prototipos que describimos a continuación:

1.1.12 EFECTO DE AMPLIFICACIÓN

Resulta importante tener presente el efecto de amplificación que se produce en la construcción de software como producto de la detección tardía de defectos. Detectar y eliminar un defecto al inicio del ciclo de vida no tiene los mismos costos que realizarlo al final del ciclo, cuando el producto ya se encuentra en operación, los usuarios ya han sido capacitados, y los datos migrados.

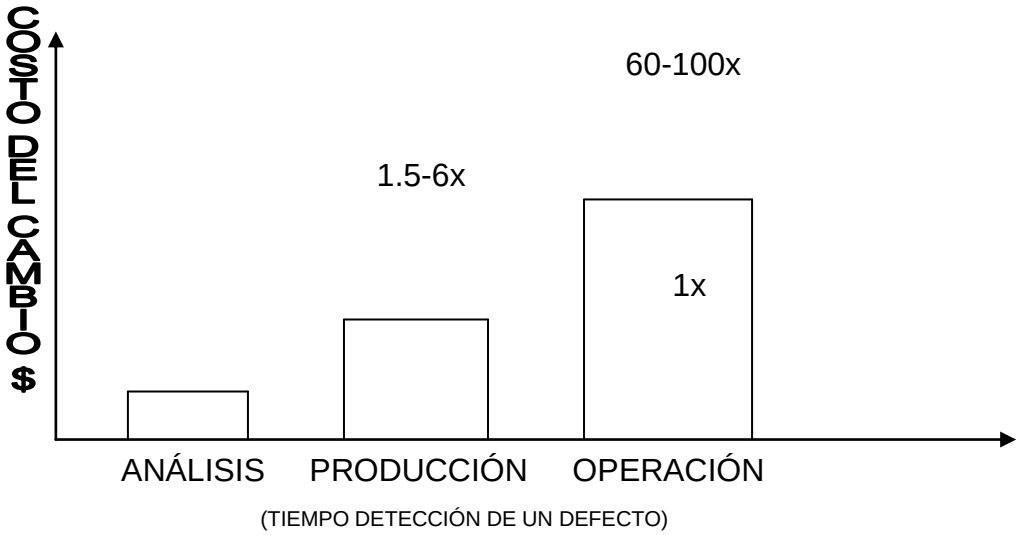


FIGURA 1.8 EFECTO DE AMPLIFICACIÓN

Consideremos que la detección y remoción de un defecto en la etapa de análisis cuesta 1x. Detectar y remover el mismo defecto en la etapa de producción costará entre 1,5 y 6x, un aumento sustancial. Si el sistema entra en operación, detectar y remover el mismo defecto anterior puede llegar a costar entre 60 y 100x (x = Dólares)

¿Dónde queremos gastar entonces nuestros esfuerzos en detectar y remover defectos? La respuesta debiese ser clara, al principio del ciclo, ya que de esa forma, reducimos los costos de amplificación. En la fase de análisis debiesen realizarse esfuerzos importantes para especificar correctamente el software, evitando la introducción de defectos.

Aunque la respuesta anterior parece ser obvia, no corresponde a lo que tradicionalmente realizan los equipos de desarrollo. Para ello, considérese la siguiente tabla estadística de esfuerzos en las fases de análisis, diseño y producción.

FASE	ESFUERZO %
ANÁLISIS	10%
DISEÑO	20%
PRODUCCIÓN :	
DISEÑO DETALLADO Y PROGRAMACION	20%
TESTEO	50%
TOTAL	100%

TABLA 1.1 PORCENTAJE DE ESFUERZOS EN LA FASE DE ANÁLISIS

La fase de producción se dividió en dos, diseño detallado y programación, y testeo, con el propósito de entender mejor el fenómeno que típicamente aparece en los equipos de desarrollo. De la tabla anterior, se visualiza rápidamente que el esfuerzo de detección y remoción de defectos se está realizando tardíamente en el ciclo de vida del software, pagando costos grandes debido al efecto de amplificación.

Los equipos de desarrollo maduros entienden la problemática anterior, y han logrado invertir los esfuerzos realizados, aumentándolo en las fases iniciales, con el propósito de producir trabajo con la menor cantidad de defectos posible. De esa forma, el esfuerzo en etapas siguientes va disminuyendo, debido a la disminución del efecto de amplificación.

Uso de prototipos

La idea de usar prototipos para testear diseño de productos es común a muchas ingenierías. El proceso de realizar prototipos dentro de una fase es una forma útil de reducir el riesgo en un proyecto a través de experiencia práctica. La salida del ejercicio de prototipeo es el conocimiento ganado por la implementación y no usar el software

prototipeado. El objetivo de la actividad de prototipeo debiese estar claramente identificada antes de empezar el proceso. De lo contrario, es fácil que los clientes no entiendan lo que se desea obtener con el ejercicio, produciendo frustración. El proceso de construcción de prototipos con el propósito de definir requisitos se denomina "prototipeo exploratorio", mientras que aquel que permite investigar la factibilidad de las soluciones propuestas es llamado "prototipeo experimental". Los prototipos usualmente implementan requisitos de alto riesgo funcional, rendimiento, o de interfaces de usuario, ignorando calidad, confiabilidad, mantenimiento y requisitos de seguridad. Por lo tanto debe entenderse que el software prototipo es "pre-operacional" y nunca debiese ser entregado como parte de un sistema de software.

1.1.13 EL PROTOTIPADO "RAPIDO"

Las características principales de este modelo son las siguientes:

- No modifica el flujo del ciclo de vida
- Reduce el riesgo de construir productos que no satisfagan las necesidades de los usuarios
- Reduce costos y aumenta la probabilidad de éxito
- Exige disponer de las herramientas adecuadas
- Suele utilizarse principalmente en dos áreas:
    - Prototipado de la interfaz de usuario
    - Prototipado del rendimiento

El prototipado rápido para que sea efectivo:

- Debe ser un sistema con el que se pueda experimentar
- Debe ser comparativamente barato (< 10%)
- Debe desarrollarse rápidamente
- Debe ponerle énfasis en la interfaz de usuario
- El equipo de desarrollo debe ser reducido
- Debe utilizarse herramientas y lenguajes adecuados

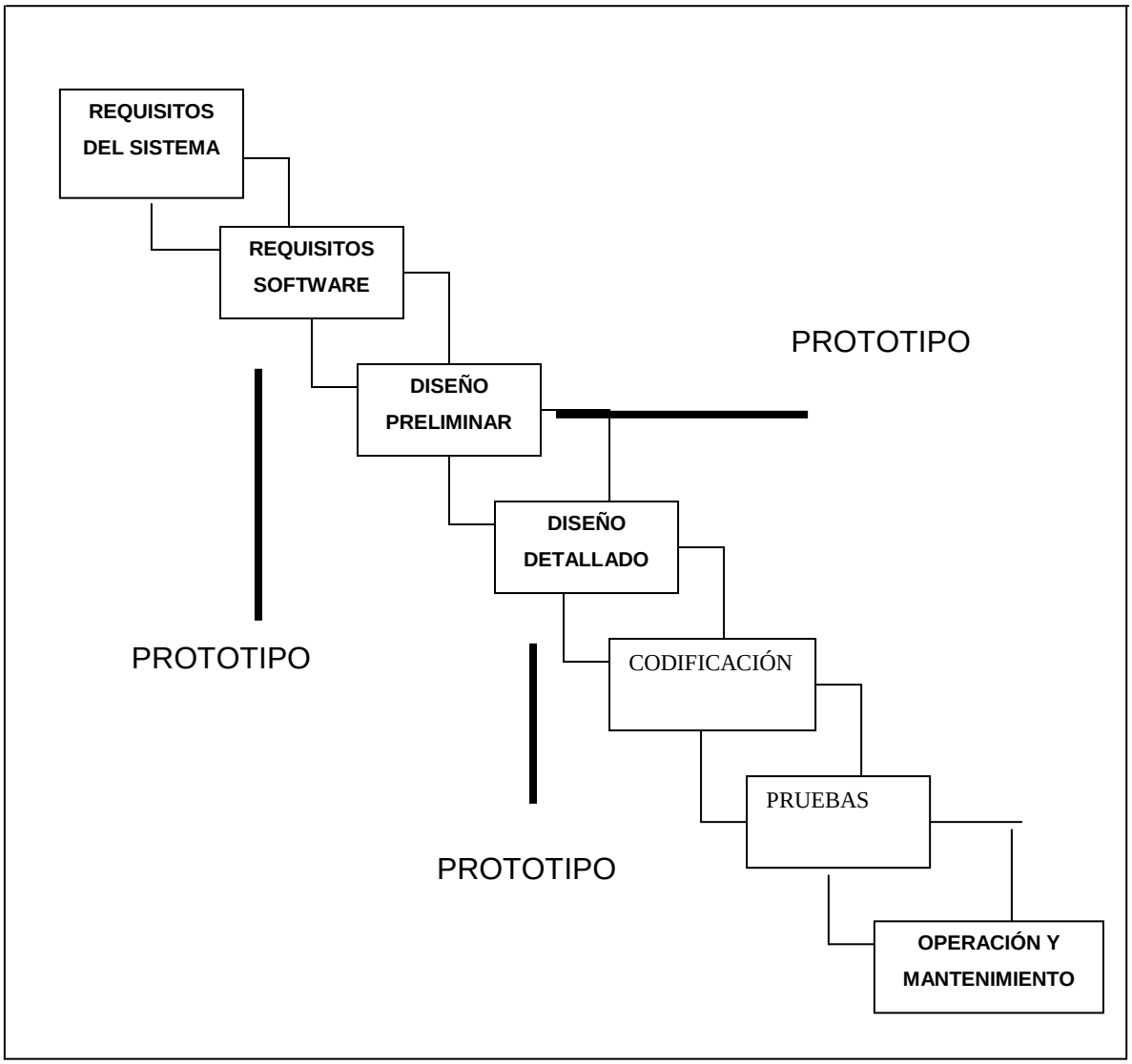


FIGURA 1.9 MODELO DE CICLO DE VIDA PROTOTIPADO RÁPIDO

"El prototipado es un medio excelente para recoger el 'feedback' (realimentación) del usuario final"

1.1.14 MODELO DE CICLO DE VIDA INCREMENTAL

Las características principales de este modelo son:

- Se evitan proyectos largos y se entrega *"Algo de valo*r" a los usuarios con cierta frecuencia
- El usuario se involucra más
- Mayor retorno de la inversión

- Difícil de evaluar el coste total
- Difícil de aplicar a sistemas transaccionales que tienden a ser integrados y a operar como un todo
- Requiere gestores experimentados
- El resultado puede ser muy positivo

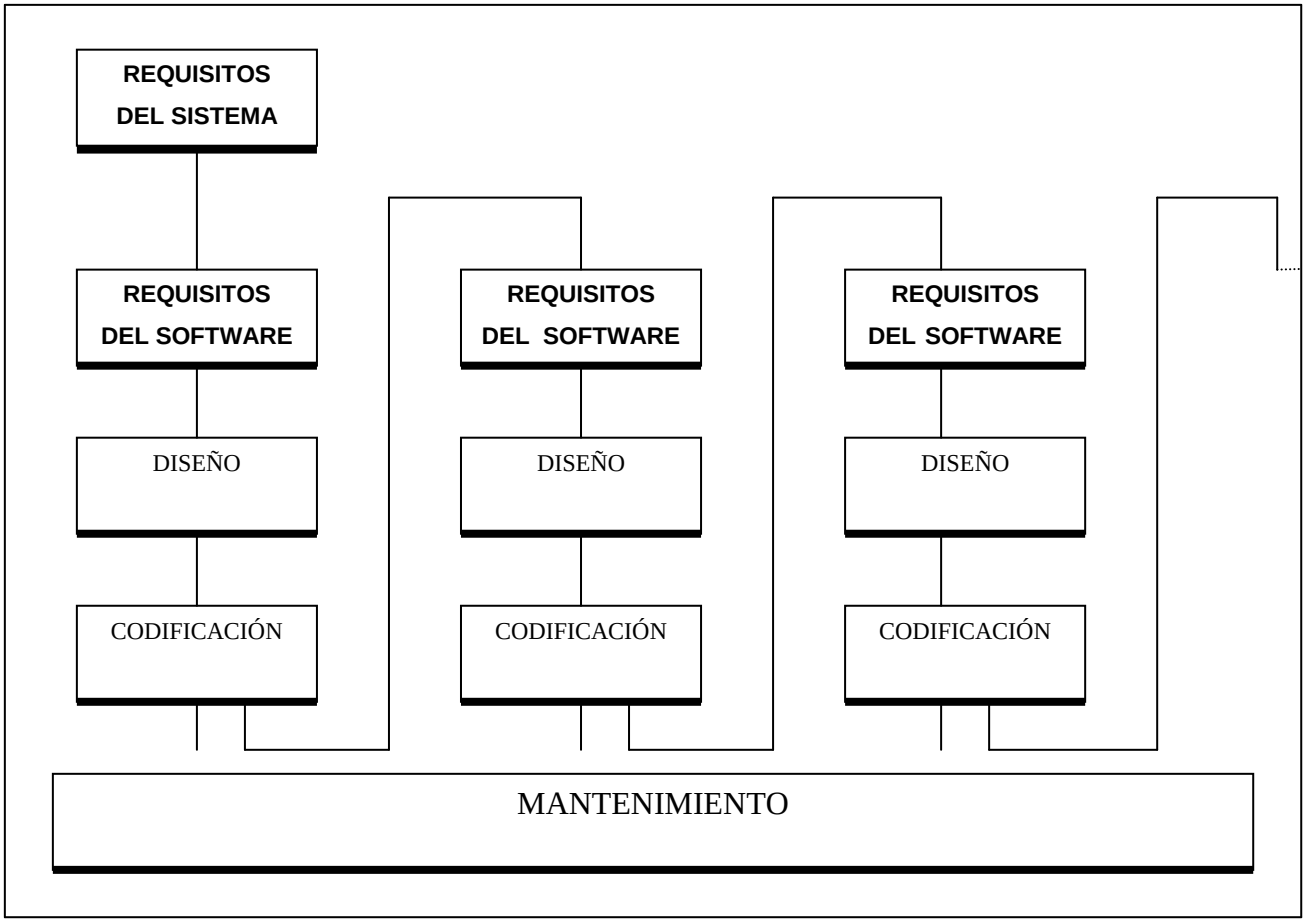


FIGURA 1.9 MODELO DE CICLO DE VIDA INCREMENTAL

1.1.15 MODELOS DE CICLO DE VIDA ALTERNATIVOS

Hay al menos tres conjuntos alternativos a los modelos de evolución de los productos software tradicionales. Estos tres conjuntos centran su atención bien sobre productos distintos a los clásicos (como son uso de componentes reutilizables, etc.) o sobre procesos especiales de producción (como son automatización de la programación, modelo espiral básico en riesgos, etc.) o sobre entornos de producción (que centran su atención en la organización y gestión de estrategias para

producir software). Dado que estos modelos no están aún muy extendidos, se considera fundamental su presentación aquí por las potencialidades que presentan.

1.1.16 MODELOS DE PROCESO DE PRODUCCIÓN DE SOFTWARE

Hay dos tipos de modelos de producción de software: operativos y no operativos. La diferencia entre ambos viene, principalmente, del hecho de que los primeros pueden verse como programas que implementan un régimen particular de inferencia y evolución del software. Los segundos, denotan enfoques conceptuales que aún no han sido suficientemente articulados en una forma deseable para codificar.

1.1.17 MODELOS OPERATIVOS

a) Especificaciones operativas para prototipado rápido

El enfoque operativo para el desarrollo del software supone la existencia de un lenguaje de especificación formal y un entorno de proceso. Las especificaciones están codificadas en el lenguaje y, cuando es posible, constituyen un prototipo funcional del sistema especificado. Cuando tales especificaciones pueden ser desarrolladas y procesadas gradualmente, entonces el prototipo resultante puede refinarse y desarrollarse en sistemas funcionalmente más completos que siempre están operativos durante su desarrollo. Variaciones dentro de este enfoque representan o bien esfuerzos donde el prototipo es el fin buscado, o donde los prototipos especificados se conservan operativos pero refinados dentro de un sistema completo.

b) Automatización de la programación y del proceso software

La automatización del proceso y la programación están relacionados con el desarrollo de las especificaciones formales de cómo una familia de sistemas software debería desarrollarse. Tales especificaciones

deberían, por lo tanto, proporcionar una estimación para la organización y descripción de las distintas cadenas de producción software, cómo están interrelacionadas, cuando iteran, etc. Así como qué herramientas software deberían usarse.
El desarrollo del software utilizando técnicas de cuarta generación (T4G) se caracteriza por facilitar la especificación de algunas de las funcionalidades de alto nivel. La herramienta genera a continuación el código, o parte del código, a partir de la especificación. Esta especificación se hace en un lenguaje lo más próximo al lenguaje natural.

El concepto de desarrollo en T4G se basa en el uso de una serie de herramientas, entre las que se encuentran:

- **Lenguajes no procedimentales para consultas de bases de datos**
- **Lenguajes no procedimentales para generación de informes, definición de pantallas**
- **Lenguajes no procedimentales de generación de código**
- **Capacidades gráficas de alto nivel**
- **Hojas de cálculo**

Con estas herramientas al alcance, el desarrollo de algunas aplicaciones queda bastante simplificado, y se puede llegar a poner en manos de un usuario experimentado en su uso.

Una vez hecha la especificación, la generación de código es prácticamente automática, con lo que el tiempo de desarrollo se ve reducido drásticamente. Con el código generado, se empieza a revisar el funcionamiento, y se le van añadiendo prestaciones nuevas al producto de una forma prácticamente interactiva.

Esta técnica permite la construcción de programas al usuario, y le permite además la revisión y actualización personal, con lo que es muy difícil la equivocación en cuanto a cumplimiento de requisitos.

Hoy por hoy, su utilización se reduce a sistemas, sobre todo de gestión, con un grado de complejidad no muy elevado.

c) Automatización del software basado en conocimientos

Este modelo intenta llevar el proceso de automatización hasta sus limites al suponer que pueden usarse las especificaciones del proceso para desarrollar directamente sistemas software y configurar entornos de desarrollo para soportar las tareas de producción en curso.

Los sistemas expertos son un caso particular en el ciclo de vida del software, ya que su peculiaridad les hace disponer de ciclos de vida propios. En este ciclo de vida, las fases se pueden activar en paralelo, y reactivar en cualquier momento, sin necesidad de ejecutar ciclos completos. Se puede utilizar técnicas de prototipado, pero la expansión al sistema final a partir del prototipo es mucho más directa, ya que puede bastar con incrementar la base de reglas o la base de conocimientos.

Por otra parte, la definición interna de lo que debe hacer el sistema experto no queda clara ni siquiera al final del desarrollo porque lo que se trata de modelizar es el razonamiento de los expertos humanos. Por lo tanto no existen nunca unos requisitos claros para validar el resultado.

Las fases de desarrollo de un sistema experto son las siguientes:

- **Identificación del problema**
- **Estudio de factibilidad**
- **Identificación de subproblemas**
- **Identificación de conceptos**
- **Diseño conceptual**
- **Diseño detallado**
- **Código**

- **Prueba del razonamiento**
- **Prueba del conocimiento**
- **Validación**
- **Conservación/Mantenimiento/Mejora**

Muchas de estas etapas se producen en paralelo, e influyen unos en otros, con lo que el diagrama de bloques que lo representa, en vez de ser secuencial es un grupo de cajas que interactúan, pero que están una al lado de la otra en el tiempo.

El enfoque común a estos tres modelos (especificaciones operativas, automatización del proceso, producción de software basado en conocimientos) es buscar la automatización del modelo de transformación continuo. A su vez, esto implica un entorno automatizable capaz de registrar el desarrollo formalizado de las especificaciones operativas, transformando y refinando, sucesivamente, dichas especificaciones en un sistema implementado, asimilando los requisitos de mantenimiento al insertar las especificaciones nuevas y/o mejoradas, en la derivación de desarrollo y luego llevando el desarrollo revisado a la implementación. Sin embargo, hay que decir que los progresos actuales es este punto han sido menos prometedores de lo esperado.

1.1.18 MODELOS NO OPERATIVOS

a) Modelo en espiral

El modelo en espiral para el desarrollo del software representa un enfoque dirigido por el riesgo para el análisis y estructuración del proceso software. Fue presentado por primera vez por Bôehm en 1986. El enfoque incorpora métodos del proceso dirigidos por las especificaciones y por los prototipos. Esto se lleva a cabo

representando ciclos de desarrollo iterativos en forma de espiral, denotando los ciclos internos del ciclo de vida, análisis y prototipado precoz, y los externos, el modelo clásico. La dimensión radial indica los costes de desarrollo acumulativos y la angular, el progreso hecho en cumplimentar cada desarrollo en espiral. El análisis de riesgos, que busca identificar situaciones que pueden cuasar el fracaso o sobrepasar el presupuesto o plazo, aparece durante cada ciclo de la espiral. En cada ciclo, el análisis del riesgo representa groseramente la misma cantidad de desplazamiento angular, mientras que el volumen desplazado barrido denota crecimiento de los niveles de esfuerzo requeridos para el análisis del riesgo, como se ve en la figura.

La primera ventaja del modelo en espiral es que su rango de opciones permiten utilizar los modelos de proceso de construcción de software tradicionales, mientras su orientación al riesgo evita muchas dificultades. De hecho, en situaciones apropiadas, el modelo en espiral proporciona una combinación de los modelos existentes para un proyecto dado. Otras ventajas son:

- **Se presta atención a las opciones que permiten la reutilización de Software existente**
- **Se centra en la eliminación de errores de y alternativas poco atractivas**
- **No establece una definición entre desarrollo de Software y mantenimiento del sistema.**
- **Proporciona un marco estable para desarrollos integrados Hardware-software.**

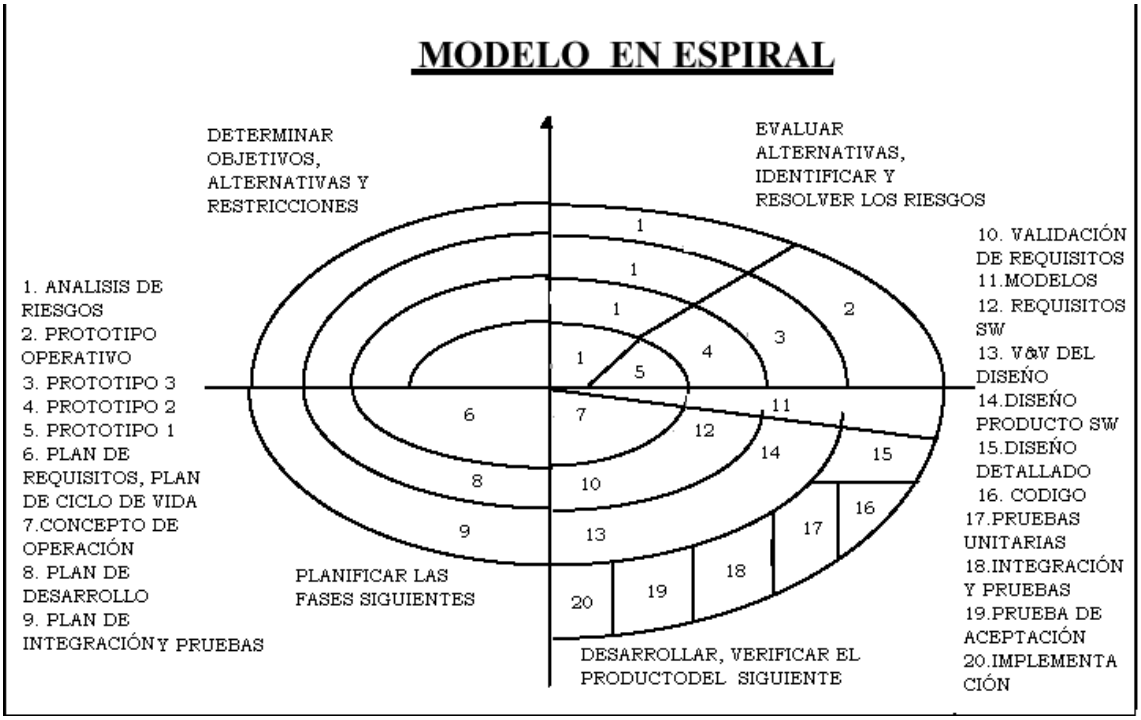


FIGURA 1.10 MODELO DE CICLO DE VIDA EN ESPIRAL

Características:

El modelo en espiral presenta las siguientes características:

- Permite acomodar otros modelos
- Incorpora objetivos de calidad y gestión de riesgos
- Elimina errores y alternativas no atractivas al comienzo
- Permite iteraciones, vuelta atrás y finalizaciones rápidas
- Es difícil de adaptar a los contratos
- Depende de las personas
- Difícil de asegurar que las personas involucradas operan en un contexto consistente

- Cada ciclo empieza identificando:
    - Los objetivos de la porción correspondiente
    - Las alternativas
    - Restricciones
- Se evalúan las alternativas respecto a los objetivos y las restricciones

- Se formula una estrategia efectiva para resolver las fuentes de riesgos (simulación, prototipado, etc.)
- Se plantea el próximo prototipo
- Una vez resueltos los riesgos se sigue el ciclo en cascada
- Cada ciclo se completa con una revisión que incluye todo el ciclo anterior y el plan para el siguiente

b) Modelos de transformación continua

Estos modelos proponen un proceso por el cual los sistemas software se desarrollan a través de una serie de transformaciones continuas de problemas establecidos en especificaciones abstractas dentro de implementaciones concretas. Se propone un esquema por el cual no hay ciclo de vida tradicional ni etapas separadas, en su lugar se lleva a cabo una serie de transformaciones y refinamientos graduales de especificaciones abstractas para llegar a programas concretos. En este sentido, entonces, las fases que definen el problema y los sistemas software pueden emerger de alguna manera juntos y así continuar coevolucionando.

Los modelos de transformación continuada también se acomodan al interés de los formalistas del software que buscan la sentencia precisa de las propiedades formales de las especificaciones de los sistemas software. De acuerdo con ello, los formalismos especificados pueden ser transformados matemáticamente en propiedades que una implementación fuente debería satisfacer. El potencial para automatizar tales modelos es aparente y está sujeto a investigación.

1.1.19 PROBLEMAS COMUNES EN EL DESARROLLO DE SOFTWARE

Los grupos de desarrollo con poca madurez muestran características similares que hacen que su trabajo presente problemas bastante comunes. Entre los que se han detectado en entrevistas con equipos de desarrollo, están los siguientes:

- Falta de claridad en los requisitos. Esto se produce por falta de esfuerzo en las fases tempranas del ciclo de vida del software, específicamente en la fase de análisis. Adicionalmente, es posible que no se haya utilizado el modelo de desarrollo adecuado, lo que no permitió definir una especificación correcta y completa del sistema a construir.

- Los clientes tienden a perderse durante el ciclo de vida. Parten muy entusiasmados y con buena predisposición, y a medida que se avanza en el desarrollo, van desapareciendo.

- Los clientes siempre le echan la culpa de los problemas producidos durante el desarrollo a los informáticos.

- Se hace poca o ninguna documentación. Existe dentro de los desarrolladores, el convencimiento de que la documentación es algo que exige el cliente, pero que no tiene ninguna relevancia para el equipo técnico.

- En general, no se hace administración de la configuración y control de versiones. Las distintas versiones de documentos, código y tests son almacenadas sin una política común, ni en un repositorio compartido con acceso restringido y respaldos frecuentes. Eso hace que se produzcan pérdidas importantes en el trabajo desarrollado, como producto de pérdidas y descoordinación entre los miembros del equipo de desarrollo.

- **Poco o ningún aseguramiento de la calidad. Existen pocos o ningún procedimiento definido y comunes al grupo de desarrollo, ni políticas que permitan monitorear el ajuste del grupo a dichos procedimientos. Esto hace que cada vez que se desarrolla, deba "reinventarse" todos los procedimientos y "recapacitarse" a los miembros del grupo de desarrollo.**

- Se quitan recursos en un proyecto para priorizar otros. En empresas de desarrollo o Gerencias de Informática con poca madurez en el proceso de desarrollo, no es poco frecuente ver que para terminar el trabajo de un grupo en particular, se le quitan recursos humanos a otros grupos. Esta política, también es conocida como “apagar incendios”, es una clara señal de equipos de desarrollo con bajísima madurez.

Todos los síntomas anteriores son claros indicios de falta de madurez del proceso de desarrollo, los que inciden en producir productos de software de baja calidad, en tiempos y costos fuera de lo estimado inicialmente. Se hace necesario seguir un proceso que permita obtener madurez en el proceso de desarrollo, tanto al equipo técnico como a los clientes.

1.1.20 ESTIMACION DEL PROYECTO DE SOFTWARE.

En el principio el costo del Software constituía un pequeño porcentaje del costo total de los sistemas basados en computadoras. Hoy en día el Software es el elemento mas caro de la mayoría de los sistemas informáticos.

Un gran error en la estimación del costo puede ser lo que marque la diferencia entre beneficios y perdidas, la estimación del costo y del esfuerzo del software nunca será una ciencia exacta, son demasiadas las variables: humanas, técnicas, de entorno, políticas, que pueden afectar el costo final del software y el esfuerzo aplicado para desarrollarlo.

Para realizar estimaciones seguras de costos y esfuerzos tienen varias opciones posibles:

- Deje la estimación para mas adelante (obviamente podemos realizar una estimación al cien por ciento fiable después de haber terminado el proyecto).
- Base las estimaciones en proyectos similares ya terminados.
- Utilice técnicas de descomposición relativamente sencillas para generar las estimaciones de costos y esfuerzo del proyecto.

- Desarrolle un modelo empírico para él calculo de costos y esfuerzos del Software.

Desdichadamente la primera opción, aunque atractiva no es practica.

La Segunda opción puede funcionar razonablemente bien si el proyecto actual es bastante similar a los esfuerzos pasados y si otras influencias del proyecto son similares. Las opciones restantes son métodos viables para la estimación del proyecto de software. Desde el punto de vista ideal, se deben aplicar conjuntamente las técnicas indicadas usando cada una de ellas como comprobación de las otras.

Antes de hacer una estimación, el planificador del proyecto debe comprender el ámbito del software a construir y generar una estimación de su tamaño.

ESTIMACIÓN BASADA EN EL PROCESO.

Es la técnica más común para estimar un proyecto, es basar la estimación en el proceso que se va a utilizar, es decir, el proceso se descompone en un conjunto relativamente pequeño de actividades o tareas, y en el esfuerzo requerido para llevar a cabo la estimación de cada tarea.

Al igual que las técnicas basadas en problemas, la estimación basada en el proceso comienza en una delineación de las funciones del software obtenidas a partir del ámbito del proyecto. Se mezclan las funciones del problema y las actividades del proceso. Como último paso se calculan los costos y el esfuerzo de cada función y la actividad del proceso de software.

1.1.21 MODELOS DE ESTIMACION.

Existen diferentes modelos de estimación como son:

- **Los Modelos Empíricos:** Donde los datos que soportan la mayoría de los modelos de estimación obtienen una muestra limitada de proyectos. Por esta razón, el modelo de estimación no es adecuado para todas las clases de software y en todos los entornos de desarrollo. Por lo tanto los resultados obtenidos de dichos modelos se deben utilizar con prudencia.

- **El Modelo COCOMO.** Barry Boehm, en su libro clásico sobre economía de la Ingeniería del Software, introduce una jerarquía de modelos de estimación de Software con el nombre de COCOMO, por su nombre en Ingles (Constructive, Cost, Model) modelo constructivo de costos. La jerarquía de modelos de Boehm esta constituida por los siguientes:

    - **Modelo I.** El Modelo COCOMO básico calcula el esfuerzo y el costo del desarrollo de Software en función del tamaño del programa, expresado en las líneas estimadas.
    - **Modelo II.** El Modelo COCOMO intermedio calcula el esfuerzo del desarrollo de software en función del tamaño del programa y de un conjunto de conductores de costos que incluyen la evaluación subjetiva del producto, del hardware, del personal y de los atributos del proyecto.
    - **Modelo III.** El modelo COCOMO avanzado incorpora todas las características de la versión intermedia y lleva a cabo una evaluación del impacto de los conductores de costos en cada caso (análisis, diseño, etc.) del proceso de ingeniería de Software.

1.1.22 HERRAMIENTAS AUTOMÁTICAS DE ESTIMACIÓN.

Las herramientas automáticas de estimación permiten al planificador estimar costos y esfuerzos, así también variables del proyecto tales como la fecha de entrega o la selección del personal. Aunque existen muchas herramientas automáticas de estimación, todas exhiben las mismas características generales y todas requieren de una o más clases de datos.

A partir de estos datos, el modelo implementado por la herramienta automática de estimación proporciona estimaciones del esfuerzo requerido para llevar a cabo el proyecto, los costos, la carga de personal, la duración, y en algunos casos la planificación temporal de desarrollo y riesgos asociados.

En resumen el planificador del Proyecto de Software tiene que estimar tres cosas antes de que comience el proyecto: cuanto durara, cuanto esfuerzo requerirá y cuanta gente estará implicada. Además el planificador debe

predecir los recursos de hardware y software que va a requerir y el riesgo implicado.

Para obtener estimaciones exactas para un proyecto, generalmente se utilizan al menos dos de las tres técnicas referidas anteriormente. Mediante la comparación y la conciliación de las estimaciones obtenidas con las diferentes técnicas, el planificador puede obtener una estimación más exacta. La estimación del proyecto de software nunca será una ciencia exacta, pero la combinación de buenos datos históricos y técnicas puede mejorar la precisión de la estimación.

Luego de haber estudiado en forma general lo que es un proyecto software es necesario aclarar que este trabajo se va dirigir exclusivamente a los proyectos software de sistemas de información, por lo tanto es necesario exponer o dar a conocer lo que es un Sistema de Información.

Un **Sistema de Información** es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Los componentes básicos de un sistema de información son:

- El equipo computacional: el hardware necesario para que el sistema de información pueda operar.
- El recurso humano que interactúa con el Sistema de Información: el cual está formado por las personas que utilizan el sistema.

Un sistema de información realiza cuatro actividades básicas: entrada, almacenamiento, procesamiento y salida de información.

- **Entrada de Datos:** Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen de otros sistemas o módulos. Esto último se denomina interfases automáticas. Las unidades típicas de entrada de datos a las computadoras son las terminales, las

cintas magnéticas, las unidades de diskette, los códigos de barras, los escáners, la voz, los monitores sensibles al tacto, el teclado y el mouse, entre otras.

- **Almacenamiento de información:** El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros, los discos flexibles o diskettes y los discos compactos (CD-ROM).
- **Procesamiento de Información:** Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general de un año base.
- **Salida de Información:** La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, diskettes, cintas magnéticas, la voz, los graficadores y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo. En este caso, también existe una interfase automática de salida.

1.2 .- OBJETIVOS DE UN PROYECTO SOFTWARE

Las solicitudes de sistemas de información están motivadas por los siguientes tres objetivos generales:

- **Resolver un problema .-** Actividades procesos o funciones que en la actualidad o quizás en el futuro, no satisfacen los estándares de desempeño o las expectativas para lo que es necesario emprender una acción que resuelva las dificultades.

- **Aprovechar una oportunidad .-** Un cambio para ampliar o mejorar el rendimiento económico de la empresa y su competitividad dentro del mercado.

- **Dar respuestas a directivos .-** Proporcionar información en respuesta a ordenes , solicitudes o mandatos originados por una autoridad legislativa o administrativa, llevar acabo tareas de cierta manera, o también cambiar la información o tal vez el desempeño.

Para alcanzar estos objetivos las empresas emprenden proyectos por una o más de las razones denominadas las cinco "C"**:**

- Capacidad
- Comunicación
- Costos
- Control
- Competitividad

Capacidad

Por ejemplo: Las actividades de una organización están influenciadas por la capacidad de ésta para procesar transacciones con rapidez y eficiencia. Los sistemas de información mejoran esta capacidad en tres formas.

- Aumentan la velocidad de procesamiento: Los sistemas basados en computadora pueden ser de ayuda para eliminar la necesidad de cálculos tediosos y comparaciones repetitivas. Un sistema automatizado puede ser de gran utilidad si lo que se necesita es un procesamiento acelerado.

- Aumento en el volumen: La incapacidad para mantener el ritmo de procesamiento no significa el abandono de los procedimientos existentes. Quizá éstos resulten inadecuados para satisfacer las demandas actuales. En estas situaciones el analista de sistemas considera el impacto que tiene la introducción de procesamiento computarizado, si el sistema existente es manual. Es poco probable que únicamente el aumento de la velocidad sea la respuesta. El tiempo de procesamiento por transacción aumenta si se considera la cantidad de actividades comerciales de la empresa junto con su patrón de crecimiento.

- Recuperación más rápida de la información: Las organizaciones almacenan grandes cantidades de datos, por eso, debe tenerse en cuenta donde almacenarlos y como recuperarlos cuando se los necesita. Cuando un sistema se desarrolla en forma apropiada, se puede recuperar en forma rápida la información.

Costo

- Vigilancia de los costos: Para determinar si la compañía evoluciona en la forma esperada, de acuerdo con lo presupuestado, se debe llevar a cabo el seguimiento de los costos de mano de obra, bienes y gastos generales. La creciente competitividad del mercado crea la necesidad de mejores métodos para seguir los costos y relacionarlos con la productividad individual y organizacional.

- Reducción de costos: Los diseños de sistemas ayudan a disminuir los costos, ya que toman ventaja de las capacidades de cálculo automático y de recuperación de datos que están incluidos en procedimientos de programas en computadora. Muchas tareas son realizadas por programas de cómputo, lo cual

deja un número muy reducido de éstas para su ejecución manual, disminuyendo al personal.

Control

- Mayor seguridad de información: Algunas veces el hecho de que los datos puedan ser guardados en una forma adecuada para su lectura por medio de una máquina, es una seguridad difícil de alcanzar en un medio ambiente donde no existen computadoras. Para aumentar la seguridad, generalmente se desarrollan sistemas de información automatizados. El acceso a la información puede estar controlado por un complejo sistemas de contraseñas, limitado a ciertas áreas o personal, si está bien protegido, es difícil de acceder.

- Menor margen de error: (mejora de la exactitud y la consistencia): Esto se puede lograr por medio del uso de procedimientos de control por lotes, tratando de que siempre se siga el mismo procedimiento. Cada paso se lleva a cabo de la misma manera, consistencia y con exactitud: por otra parte se efectúan todos los pasos para cada lote de transacciones. A diferencia del ser humano, el sistema no se distrae con llamadas telefónicas, ni olvidos e interrupciones que sufre el ser humano. Si no se omiten etapas, es probable que no se produzcan errores.

Comunicación

La falta de comunicación es una fuente común de dificultades que afectan tanto a cliente como a empleados. Sin embargo, los sistemas de información bien desarrollados amplían la comunicación y facilitan la integración de funciones individuales.

- Interconexión: (aumento en la comunicación): Muchas empresas aumentan sus vías de comunicación por medio del desarrollo de

redes para este fin, dichas vías abarcan todo el país y les permiten acelerar el flujo de información dentro de sus oficinas y otras instalaciones que no se encuentran en la misma localidad. Una de las características más importantes de los sistemas de información para oficinas es la transmisión electrónica de información, como por ejemplo, los mensajes y los documentos.

- Integración de áreas en las empresas: Con frecuencia las actividades de las empresas abarcan varias áreas de la organización, la información que surge en un área se necesita en otra área, por ejemplo. Los sistemas de información ayudan a comunicar los detalles del diseño a los diferentes grupos, mantienen las especificaciones esenciales en un sitio de fácil acceso y calculan factores tales como el estrés y el nivel de costos a partir de detalles proporcionados por otros grupos.

Competitividad

Los sistemas de información computacionales son un arma estratégica, capaz de cambiar la forma en que la compañía compite en el mercado, en consecuencia éstos sistemas mejoran la organización y la ayudan a ganar "ventaja competitiva", sin embargo, si los competidores de la compañía tienen capacidades mas avanzadas para el procesamiento de información, entonces los sistemas de información pueden convertirse en una "desventaja competitiva".

CONSTANTES DE LOS PROYECTOS DE SOFTWARE

- Retrasos no previstos
- Desbordamiento de costes
- Software no acorde con los requisitos
- Errores en los programas
- Sensibilidad a los errores humanos y a las averías físicas
- Dificultad de puesta en marcha
- Dificultad de evolución

- Mantenimiento

1.3.- CARACTERÍSTICAS DE UN PROYECTO SOFTWARE

Para crear un Proyectos Software es necesario conocer las características principales que presenta el Software para darle su correcto mantenimiento y utilización.

Lo principal:

- El software es un elemento lógico, no físico. Esta característica lo hace muy distinto del hardware.
- El software se desarrolla, no se fabrica en un sentido clásico
- El software no se estropea
- El software sufre cambios. Los cambios introducen nuevos defectos
- La mayoría del software se construye a medida, en lugar de ensamblar componentes existentes
- El hardware se construye (tras una fase de diseño), ensamblando componentes ya construidos (provenientes de catálogos)
- No existen catálogos de componentes de software
- Los avances en reusabilidad del software no están dando buenos resultados

La calidad es una de las características más importantes que debe tener el software y la analizamos a continuación:

CALIDAD DE LOS PRODUCTOS SOFTWARE

Actualmente, la satisfacción hacia el uso de un producto puede marcar una gran diferencia en el mercado de productos similares. Es así como el desarrollo de artículos que satisfacen las expectativas de los clientes y usuarios harán la diferencia entre dos organizaciones que desarrollan productos que compiten en el mercado. La preocupación por ofrecer productos acompañados de altos niveles de calidad no es una actividad

nueva. A lo largo de este siglo han surgido distintas interpretaciones de como brindar calidad.

El desarrollo de productos software no esta ausente de ofrecer calidad. Dicho nivel de calidad, incluido en los productos, considera muchas actividades dentro del desarrollo de los proyectos software. La gestión de la calidad dentro de este tipo de proyectos puede estandarizarse dentro de la organización y certificarse a la comunidad de clientes.

Concepto de Calidad

Antes de empezar hablar acerca de la calidad de los productos software, se debería definir que es lo que se entiende por calidad, a que es aplicable y de que forma puede ser relacionada con productos software.

Según el diccionario, calidad se puede definir como "una característica o atributo de una cosa". De esta forma se podría decir que la calidad de los productos puede medirse como una comparación de sus características y atributos. Así, este concepto puede aplicarse a cualquier producto. Una de las formas de realizar una medida de calidad es observar las diferencias ocurridas en la producción dos productos *iguales.* La producción de artículos de cualquier especie no asegura que dos de ellos sean totalmente iguales. Quizás sea preciso realizar observaciones acuciosas para lograr distinguir las variaciones entre uno y otro, ya que estas pueden no ser obvias. Es más, quizás sea necesario disponer de instrumentos adecuados y de precisión para poder observar dichos cambios de la producción. Uno de los principales objetivos de dar calidad a los productos es minimizar las diferencias entre unidades producidas. Estas diferencias tienen diversos orígenes y, por tanto, distintas y amplias formas de corregirlos, dependiendo de la naturaleza del producto. Lo primordial es tener en cuenta el concepto de brindar calidad a lo que se está realizando.

De este modo, el brindar calidad es una actividad esencial para un negocio que produce productos que serán utilizados por otras personas.

Calidad en los productos Software.

Hasta el momento puede dilucidarse algunos de los atributos que hacen comparable un producto de otro. Quizás podemos considerar formas, colores, tamaños, manejabilidad, entre otros. Estas características pueden ser físicamente mensurables y, por ello, fácilmente comparables. Observando desde esa perspectiva, De qué manera puede ser aplicada la calidad a los productos software? Cómo controlar la variación entre un producto de este tipo? Así como existen medidas para atributos físicos, para el software también existen medidas que pueden hacerlo comparables, tales como puntos de función, líneas de código y otras. Estas medidas aportan a la medida de variación entre productos software.

La principal meta de un equipo desarrollador de software debería ser siempre producir software catalogado como de alta calidad. Pero para ello se deben tener en cuenta algunas ideas previas:

- Los productos software son realizados por personas para personas. Así, las personas desarrolladoras deben tener en cuenta claramente que son otras personas las que utilizarán sus productos, los que pueden estar sujetos a fallos constantes. Aún a pesar de los avances actuales en Inteligencia Artificial, los asistentes software para el desarrollo de software no son demasiado confiables como para que la mano humana no intervenga en este proceso. El desarrollo de productos software es una actividad sujeta a muchos factores que la pueden hacer poco confiable.

- Muchas personas piensan en la calidad como un atributo exclusivo de los productos. Que está empieza a considerarse una vez que las primeras líneas de código son escritas. El concepto de calidad involucra muchos factores previos a esta etapa, debiendo ponerse atención a cada una de estas etapas anteriores.

Sujeto a lo anterior, la calidad que pueden alcanzar los productos software, y en general cualquier producto, esta sometida a como se desarrolla cada una de las etapas de la vida del producto, partiendo por la definición de la idea del producto hasta la entrega y manutención del mismo. Así la entrega de calidad a un producto considera actividades tales como:

- Administración de la calidad, asegurando minimizar las diferencias entre los recursos presupuestados y los recursos realmente utilizados en las distintas etapas. Dichos recursos incluyen el equipamiento y tiempo de desarrollo.

- Uso de tecnología de Ingeniería de Software eficiente, considerando métodos de desarrollo y herramientas.

- Aplicación de técnicas formales a lo largo de todo el proceso.

- Minimización de las variaciones entre los productos, diminuyendo las diferencias y defectos entre versiones.

- Testeo en diferentes etapas del desarrollo.

- Control de la documentación, tanto de apoyo al desarrollo como la entregada al usuario final, generada en cada etapa, y verificación de los posibles cambios y modificaciones que pudiera sufrir.

- Correcto mantenimiento y servicios de post-venta.

Calidad por etapas.

Como ya se observó la calidad esta presente en todas las etapas del proceso de desarrollo de los productos software. A grandes rasgos se puede realizar una clasificación de como interviene la aplicación de la calidad en dichas

etapas. De esta forma podemos distinguir que la calidad se puede asegurar en el diseño, en la producción y la satisfacción final.

- Calidad en el diseño. Aquí se pretenden características definidas para la realización del producto software y que se deberían cumplir posteriormente. Aquí la calidad se basa en definir un listado de especificaciones a seguir. Involucra descripción de los procesos de desarrollo, tareas y responsabilidades de los equipos de desarrollo. Dichos procesos pueden estar estandarizados, por lo cual puede certificarse que el trabajo se realiza bajo alguna norma de calidad, como puede ser la norma de calidad ISO 9000-3:1993 que establece guías de acción para la aplicación de ISO 9001 orientada al desarrollo, suministro y mantenimiento del software.

En esta etapa la calidad aumenta en la medida que se realiza una alta especificación de los procesos y se propone una estrecha tolerancia a la modificación, estableciendo los métodos correctivos a las desviaciones ocurridas.

- Calidad en la producción. Aquí se entiende el logro de la calidad en el grado que la producción cumpla los requerimientos de diseño. Si los requerimientos están bien definidos y especificados el cumplimiento de la calidad en esta etapa no debería tornarse en una tarea titánica, ya que las bases del trabajo estarían previamente definidas.

- Calidad de satisfacción. Esta es la medida de la calidad apreciada por los usuarios finales de los productos software. En cierta medida es el entendimiento y aprecio del producto software. Esta calidad es la culminación de un proceso previo sometido a distintas aplicaciones de calidad de trabajo. No puede esperarse en esta etapa una alta calidad si no hubo preocupación por ella en las etapas anteriores.De gran modo, es en esta etapa en

donde es mas apreciada la calidad dada a un producto pues es aquí cuando se produce la comercialización y uso *masivo* de él. Estas apreciaciones de calidad hacia un determinado producto elevarán el nivel de confianza a la organización desarrolladora, lo que puede elevar su posición en el mercado.. Para lograr una alta calidad del producto final este debe estar soportado por una preocupación de asegurar la calidad en las etapas previas a alcanzar dicho estado final. Lo que permite ir escalando en la oferta de calidad es mantener un riguroso control de la calidad.

Control de la calidad.

Como puede vislumbrase, el control de la calidad es realizar una observación constante acerca del cumplimiento de las tareas que pueden ofrecer una calidad objetiva a la forma en como se está desarrollando un proyecto de Ingeniería de Software. Es decir, una vigilancia permanente a todo el proceso de desarrollo y ciclo de vida del software. Esta meta puede alcanzarse mediante frecuentes inspecciones a las metodologías de trabajo y uso de herramientas, revisiones de prototipos y testeo exhaustivo de los productos finales.

El control de la calidad permite realizar las rectificaciones pertinentes al desarrollo en cuanto este empieza a desviarse de sus objetivos, alejando la inclusión de la calidad al trabajo. Estas rectificaciones son posibles gracias a una retroalimentación de las etapas superiores, creado un aprendizaje al observar las salidas de cada etapa, hasta el producto final, y mejorar los procesos que dan origen al sistema.

La retroalimentación, así como cada etapa realizada, debe generar documentación, tanto como del diseño de los procesos de la etapa como de los resultados obtenidos en cada etapa (y que servirá de entrada a la etapa siguiente). Esto permite realizar el mejoramiento de los procesos débiles, lo que definitivamente desembocará en un aseguramiento de la calidad en los procesos ejecutados por la organización. Por otra parte la documentación generada puede servir a modo de entrenamiento de integrantes recientemente

incorporados a los equipos de desarrollo, los cuales no estarán familiarizados con los conceptos de calidad manejados por dichos equipos.

En el control de calidad se debe tener presente los costos que esta involucra. Si se piensa en las tareas que se debe realizar en este control, puede observase que es necesario llevar a cabo tareas de búsqueda de problemas, testeo, realimentación, rectificación, elaboración, modificación y estudio de la documentación; entre otras actividades. Todas ellas tienen costos involucrados (incluso puede darse la inclusión de equipos destinados al aseguramiento de la calidad: los grupos SQA). Pero debe existir un compromiso, ya que un excesivo costo en el control de la calidad puede hacer que este proceso se torne ineficiente. Pero, por otra parte, el mejoramiento de la calidad implica reducir los costos ya que se tendría un cierto nivel de calidad ya asegurado.

Finalmente, y como consecuencia de la naturaleza del proceso de desarrollo de productos software, el asegurar la calidad en las primeras etapas de este involucra que los costos del control en las etapas posteriores tenderá a disminuir al tener menos aspectos que controlar pues, nuevamente, la calidad estaría asegurada en sus bases.

1.4 ÁMBITO DE UN PROYECTO SOFTWARE.

Es la primera actividad que se lleva a cabo durante la planificación del proyecto de Software.

En esta etapa se deben evaluar la función y el rendimiento que se asignaron al Software durante la Ingeniería del Sistema de Computadora para establecer un ámbito de proyecto que no sea ambiguo, e incomprensible para directivos y técnicos

Describe la función, el rendimiento, las restricciones, las interfaces y la fiabilidad, se evalúan las funciones del ámbito y en algunos casos se refinan para dar mas detalles antes del comienzo de la estimación.

El ámbito se define como un pre-requisito para la estimación y existen algunos elementos que se debe tomar en cuenta como es:

La obtención de la Información necesaria para el software. Para esto el analista y el cliente se reúnen sobre las expectativas del proyecto y se ponen de acuerdo en los puntos de interés para su desarrollo.

CAPITULO II

El presente capitulo trata sobre la teoría de Gestión de riesgos en donde intervienen lo que es Activos, Amenazas, Vulnerabilidad, Impacto, Riesgo, Salvaguarda con sus respectivas definiciones, características, tipos, atributos y métricas. Además se va tratar sobre lo qué es Gestión de Riesgos, su importancia, también se trata como identificar y clasificar a los Riesgos, los componentes, controladores y estrategias del riesgo. También se va tratar sobre la proyección del riesgo y dentro de este tema se analizará la evaluación del impacto del riesgo, evaluación del riesgo y finalmente el planteamiento de Salvaguardas.

2. TEORÍA GENERAL DE GESTIÓN DE RIESGOS

2.1.- RIESGO

2.1.1 .- DEFINICIÓN

En términos generales el riesgo es la proximidad de un daño dentro de nuestro estudio podríamos decir que: el riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización.

2.1.2.- CARACTERÍSTICAS

El Riesgo es el resultado del Análisis de Riesgos que es un proceso complejo que parte de la determinación de los elementos autónomos (los activos del dominio y las amenazas actuantes en él) y prosigue con la estimación de los elementos derivados de aquellos dos (las vulnerabilidades y los impactos).

Este 70gresión complejo se realiza con el objetivo de obtener un resultado concreto es decir un valor calculado de riesgo que permita tomar 70gresión70l para proseguir con la siguiente etapa del proceso. El Riesgo calculado es simplemente un indicador ligado al par de valores

calculados de la 71gresión71lidad y el impacto, ambos derivados a su vez de la relación entre el activo y la Amenaza/71gresión a las que el Riesgo calculado se refiere en última instancia.

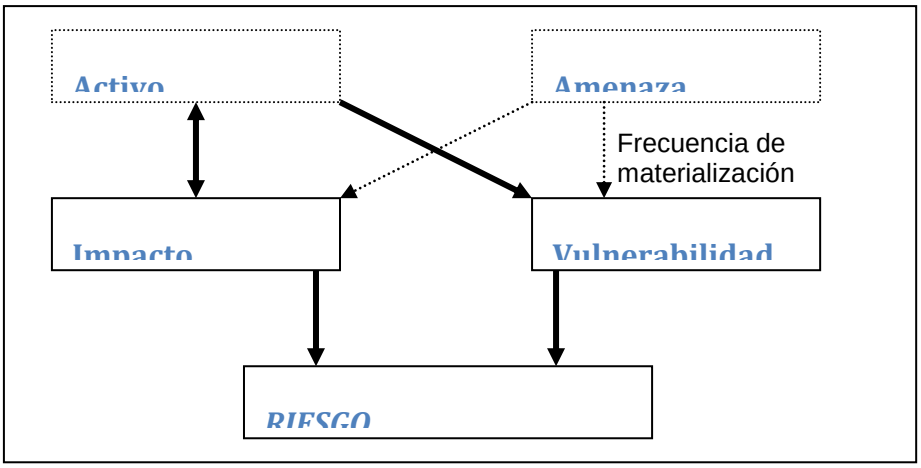


FIGURA 2.1 RIESGO

2.1.3 .- TIPOS

Aquí presentamos una lista de los riesgos que se pueden sucitar:

- El riesgo calculado intrínseco.- se define o calcula antes de aplicar salvaguardas
- El riesgo calculado residual.- se considera como el que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.
- El riesgo efectivo.- se le llama riesgo efectivo al nivel de riesgo resultante una vez aplicadas las salvaguardas existentes en el sistema de información.
- El riesgo de simulación.- se le llama riesgo de simulación al nivel de riesgo resultante una vez introducidos los cambios en los componentes del sistema a través de las simulaciones.

2.1.4.- ATRIBUTOS

Se consideran dos atributos, uno de cada Riesgo y otro de relación entre riesgos:

- Restricción a cada tipo de impacto factible dada la vulnerabilidad de un activo (o grupo de activos) a una amenaza (o conjunto de amenazas).
- Propagación del riesgo para activos dependientes entre sí.

2.1.5.- METRICAS

En el caso más sencillo, la Vulnerabilidad se ha podido estimar como una ***frecuencia*** (por ejemplo de fallos de un componente) y el impacto también se ha podido apreciar como un **valor monetario** de reposición (de ese componente). Entonces el Riesgo calculado se puede apreciar por el impacto acumulado durante un período, por ejemplo un año. El Riesgo será así el coste de las reposiciones del componente durante el año y se podrá comparar, bien con un umbral determinado, bien con el coste también anual de las salvaguardas para reducirlo. La métrica de Riesgos en este caso sencillo (Vulnerabilidad como frecuencia e Impacto monetarizado)

En los casos más complejos, cuando la Vulnerabilidad no se puede recoger como frecuencia o el Impacto no se puede monetarizar, se estima la métrica de Riesgos con ayuda de una tabla cualitativa o su matriz equivalente con los siguientes niveles:

Rango de Riesgos	**Impacto**	**Vulnerabilidades (frecuencia)**
Muy bajo	Muy bajo	Muy baja, Baja, Media, Alta
Bajo	Muy bajo	Muy alta
	Bajo	Muy baja, Baja, Media
	Medio	Muy baja, Baja

Medio	Bajo Medio Alto	Alta, Muy alta Media, Alta, Muy alta Muy baja
Alto	Alto Muy alto	Baja, Media, Alta, Muy alta Muy baja
Muy alto	Muy alto	Baja, Media, Alta, Muy alta

TABLA 2.1 TABLA CUALITATIVA SEGÚN EL RANGO DEL RIESGO

2.2 .- AMENAZA

2.2.1 .- DEFINICIÓN

Las amenazas son los eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

2.2.2 .- CARACTERÍSTICAS

La definición anterior recoge la esencia dinámica de la Amenaza: es decir, es un Evento de tipo potencial (o sea una Acción, interrupción o falta de acción situada fuera del control de los actores de la seguridad; en contraposición de las Acciones de tipo decisión humana); la consecuencia de la amenaza, si se materializa, es un incidente que modifica el estado de seguridad de los Activos amenazados**,** es decir, lo hace pasar de un estado anterior al evento a otro posterior (potencial o realmente, según se trate de Amenaza o de agresión materializada).

La definición de amenaza también sobreentiende que hay diversidad de consecuencias**,** lo que habrá de tenerse en cuenta al examinar la entidad Impacto.

La distancia entre la Amenaza potencial y su materialización como agresión real se mide por la frecuencia histórica o bien por la potencialidad de dicha materialización**.**

2.2.3.- TIPOS

La diversidad de causas de las Amenazas permite clasificarlas según su naturaleza (lo que a su vez podrá orientar sobre las medidas a tomar para neutralizarlas con cierta autonomía sobre sus consecuencias).

Se considera cuatro tipos de causas amenazadoras: no humanas (accidentes); humanas pero involuntarias (errores); humanas intencionales que necesitan presencia física; y humanas intencionales que proceden de Origen Remoto. Se tienen en definitiva estos 4 Grupos:

Grupo A de Accidentes

A1: Accidente físico de origen industrial: incendio, explosión, inundación por roturas, contaminación por industrias cercanas o emisiones radioeléctricas

A2: Avería: de origen físico o lógico, debida a un defecto de origen o sobrevenida durante el funciona-miento del sistema

A3: Accidente físico de origen natural**:** riada, fenómeno sísmico o volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe.

A4: Interrupción de servicios o de suministros esenciales**:** energía, agua, telecomunicación, fluidos y suministros diversos

A5: Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, electrostática

Grupo E de Errores

E1: Errores de utilización ocurridos durante la recogida y transmisión de datos o en su explotación por el sistema

E2: Errores de diseño existentes desde los procesos de desarrollo del software (incluidos los de dimensionamiento, por la posible saturación de los flujos en los sistemas).

E3: Errores de ruta, secuencia o entrega de la información en tránsito

E4: Inadecuación de monitorización, trazabilidad, registro del tráfico de información

Grupo P de Amenazas Intencionales Presenciales

P1: Acceso físico no autorizado con inutilización por destrucción o sustracción (de equipos, accesorios o infraestructura)

P2: Acceso lógico no autorizado con intercepción pasiva simple de la información (requiere sólo su lectura)

P3: Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración (requiere lectura y escritura); es decir, reducción de la confidencialidad del sistema para obtener bienes o servicios aprovechables (programas, datos)

P4: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración

P5: Indisponibilidad de recursos, sean humanos (huelga, abandono, rotación) o técnicos (desvío del uso del sistema, bloqueo).

Grupo T de Amenazas Intencionales de Origen Remoto

T1: Acceso lógico no autorizado con intercepción pasiva (para análisis de tráfico)

T2: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración (requiere lectura y escritura) y usando o no un reemisor o 'man in the middle'**:** es decir, reducción de la integridad y/o disponibilidad del sistema sin provecho directo (sabotaje inmaterial)

T3: Acceso lógico no autorizado con modificación (Inserción, Repetición) de información en tránsito

T4: Suplantación de Origen (del emisor o reemisor, 'man in the middle') o de Identidad

T5: Repudio del Origen o de la Recepción de información en tránsito

2.2.4 .- ATRIBUTOS

El elemento Amenaza no tiene atributos destacables que sean útiles para el Análisis y Gestión de Riesgos.

2.2.5.- METRICAS

La ocurrencia intrínseca de la amenaza tiene sólo un interés genérico si no está asociada como agresión materializada. Al Activo agredido pese a todo, puede ayudar a valorar la Vulnerabilidad que concreta dicha asociación por excepción (o sea si no hubiera valoración específica de dicha Vulnerabilidad); en este caso se expresa según la siguiente escala:

Período Medio entre Ocurrencias	Valor en la Escala Subjetiva
Menor que una vez por semana	Frecuencia muy alta
Menor que cada dos meses	Frecuencia alta
Menor que un año	Frecuencia media
Menor que seis años	Frecuencia baja
Mayor que seis años	Frecuencia muy baja

TABLA 2.2 VALORACIÓN DE LAS AMENAZAS SEGÚN LAS OCURRENCIA

La escala escogida no se basa en consideraciones objetivas, sino que intenta contrarrestar los efectos de la incertidumbre en la determinación de los períodos en base a intervalos que aproximadamente se aumentan de forma exponencial.

2.3.- SALVAGUARDA

2.3.1 .- DEFINICIÓN

Se define la Función o Servicio de salvaguarda como la acción que reduce el Riesgo

Se define el **Mecanismo de salvaguarda** como el procedimiento o dispositivo, físico o lógico que reduce el riesgo.

2.3.2 CARACTERÍSTICAS

Para reducir el riesgo, se necesita la mejora de Salvaguardas existentes o la incorporación de otras nuevas.

Es necesario distinguir entre la entidad más abstracta llamada Función o Servicio de Salvaguarda y la entidad concreta llamada Mecanismo de Salvaguarda.

La distinción terminológica entre 'función de salvaguarda' y 'servicio de salvaguarda' refleja sólo que ambos términos se han acuñado en documentos normativos de orígenes diferentes, aunque encubren un concepto semejante.

La Función o Servicio de Salvaguarda es una *acción* de tipo *actuación* (o de tipo no-actuación, es decir omisión), puesto que es fruto de una *decisión* para reducir un Riesgo (no es una acción de tipo evento).

Dicha *actuación* se materializa en el correspondiente mecanismo de salvaguarda que opera de dos formas posibles, en general alternativas:

- 'Neutralizando' o 'bloqueando' otra acción, que es el evento de materialización de la Amenaza en forma de agresión, con reducción

previa al evento de la Vulnerabilidad mediadora de dicha materialización.

- Modificando el *estado de seguridad* del Activo agredido de nuevo (lo había modificado anteriormente por el Impacto consecuente a la Amenaza materializada), con *reducción posterior al evento productor de dicho Impacto*.

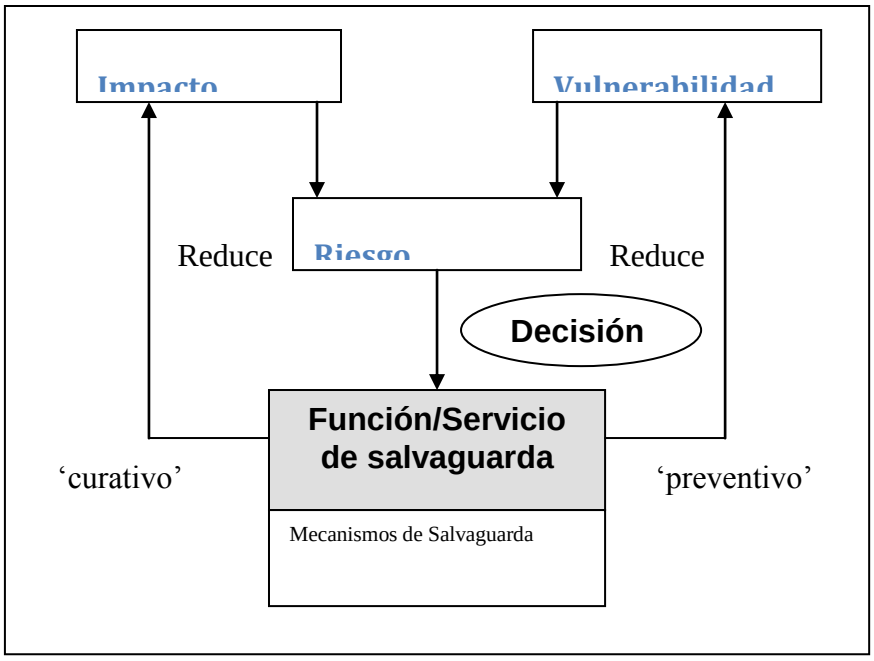


FIGURA 2.2 SALVAGUARDA

2.3.3 TIPOS

Las funciones, servicios y mecanismos de salvaguarda se tipifican, según su forma de actuación**,** en dos grandes tipos:

- **La funciones o servicios preventivos actúan sobre la Vulnerabilidad (antes de la agresión) y reduce la potencialidad de materialización de la Amenaza (no la posibilidad genérica de ésta, que es independiente del Activo amenazado). Este tipo de función o servicio actúa en general contra amenazas humanas.**

- Las funciones o servicios curativos o restablecedores actúan sobre el Impacto (tras la agresión) y reduce su gravedad. Este tipo de función o servicio actúa en general con amenazas de todos los tipos. Las funciones o servicios de salvaguarda, así tipificados según sus formas de actuación, lógicamente pueden clasificarse según:
    - Los tipos de Amenazas generadoras de las Vulnerabilidades para las funciones o servicios preventivos;
    - Los tipos de Impactos para las funciones o servicios curativos.

Las funciones y servicios de salvaguarda pueden especificarse aún con más detalle dentro de cada gran tipo de salvaguardas preventivas o curativas:

Salvaguardas Preventivas

- La Concienciación, información y formación del personal propio y del relacionado establemente con la Organización son un tipo de salvaguarda ‘estructural’ (ligada a la estructura global de la Organización y no sólo a sus Sistemas de Información). Su importancia está justificada por el papel esencial que juega en la seguridad el factor humano.

- La Disuasión es un tipo de salvaguarda que empuja a que el potencial agresor humano intencional reconsidere el inicio de la agresión, a partir de las consecuencias que puedan sobrevenirle contra su propio interés. Este tipo de salvaguarda exige normalmente una difusión lo más amplia y a su vez selectiva posibles. Por poner ejemplos, el establecimiento de condenas es una de las salvaguardas de disuasión más conocidas.

- La Prevención propiamente dicha es un tipo de salvaguarda de protección que no impide el inicio de la materialización de la amenaza, sino su realización completa y por lo tanto la consecución plena del impacto. Como ejemplo de salvaguarda preventiva puede tomarse el control de accesos.

- La Detección preventiva puede llegar a ser hasta disuasoria (si su instalación es conocida por el potencial agresor, consciente de que podría ser descubierto).

Salvaguarda Curativas o Restablecedoras

- La Corrección es un tipo de salvaguarda que impide la propagación del Impacto. Por ejemplo, un impacto en la integridad de una información detectado por su descuadre lleva a tomar medidas para paralizar la circulación de dicha información y de verificar sus fuentes.

- La Recuperación es un tipo de salvaguarda restauradora que repara los daños o reconstruye los elementos dañados para acercarse al estado de seguridad del Activo agredido previo a la agresión. Cuando no basta la recuperación funcional, pueden adoptarse también otras salvaguardas como la transferencia del riesgo a terceros (por ejemplo con los seguros) o la acción ante los tribunales.

- La Detección curativa, 'monitorización' o seguimiento curativo del impacto, en caso de amenaza ya materializada, es previa a toda eficacia en la actuación de las salvaguardas curativas (muchas agresiones son detectadas tarde o nunca). El cuadre de la información sería un buen ejemplo de esta salvaguarda detectora.

Los mecanismos de salvaguarda, tipificados según sus formas de actuación también como preventivos o curativos, se especifican con más detalle dentro de cada tipo según el 'recurso' empleado de la Organización (mecanismos organizativos, físicos, de software específico de seguridad, de contratación de seguros ...). Estos recursos a su vez se pueden relacionar estrechamente con los Activos o Grupos de Activos tipificados en este mismo Submodelo (entorno, sistema de información, información, funcionalidad, otros activos), dando tipos de mecanismos concernientes a la arquitectura básica, los soportes, las

comunicaciones, la explotación, la compra de paquetes y el desarrollo de aplicaciones, etc.

2.3.4 ATRIBUTOS

La eficacia genérica es un atributo de una Función o Servicio de Salvaguarda que hace pasar de la Vulnerabilidad intrínseca del Activo y el Impacto pleno sobre éste a una Vulnerabilidad y un Impacto efectivos (que son los que tienen en cuenta dicha Función o Servicio).

La Eficacia concreta es un atributo de un Mecanismo de Salvaguarda. Esta Eficacia suele ser inespecífica (reduce el riesgo de distintos Activos) por lo que suele estar asociada a la eficacia de otros Mecanismos de Salvaguarda. También transforma la Vulnerabilidad intrínseca y el Impacto pleno del Activo respecto al tipo de Amenaza respectivamente en Vulnerabilidad e Impacto efectivos (que son los que tienen en cuenta dicho Mecanismo de Salvaguarda).

2.3.5 METRICAS

Una función o servicio de salvaguarda no tiene una métrica propia, sino derivada de su poder reductor del Riesgo. El valor de la Eficacia genérica de una función o servicio de salvaguarda viene marcado por la experiencia de los analistas de seguridad y depende del tipo de dicha función o servicio de salvaguarda (o sea de su forma de actuación) y del tipo de Amenaza.

2.4 ACTIVO

2.4.1 DEFINICIÓN

Los Activos son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

2.4.2 CARACTERÍSTICAS

Cada Activo (o bien un conjunto homogéneo de Activos) se caracteriza por su estado en materia de seguridad; estado que se concreta estimando los 4 niveles que son: de Autenticación, Confidencialidad, Integridad, Disponibilidad (A-C-I-D):

- **Subestado A de Autenticación.-** Se define como la característica de dar y reconocer la autenticidad de los Activos del Dominio (de tipo *Información)* y/o la identidad de los actores.

- **Subestado C de Confidencialidad.**- Se define como la característica que previene la divulgación no autorizada de activos del Dominio. Concierne sobre todo a Activos de tipo Información, y a menudo se relaciona con la Intimidad o 'privacidad', cuando esa información se refiere a personas físicas, que trata la LORTAD, Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal. El término divulgación debe tomarse en su sentido más estricto: el simple acceso físico o lógico al activo altera este subestado, aunque no haya modificaciones aparentes ni difusión posterior.

- **Subestado I de Integridad. -** Se define como la característica que previene la modificación o destrucción no autorizadas de Activos del Dominio. La integridad está vinculada a la fiabilidad funcional del sistema de información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél) y suele referirse (no siempre) a Activos de tipo Información. Por ejemplo, son típicos los problemas causados por la amenaza de un virus (llegado con un disquete externo o por la red) a la integridad de los datos almacenados en el disco duro de un PC.

- **Subestado D de Disponibilidad.-** Se define como la característica que previene la denegación no autorizada de acceso a Activos del Dominio. La disponibilidad se asocia a la fiabilidad técnica (tasa de fallos) de los componentes del sistema de información.

2.4.3 TIPOS

Se consideran 5 grandes tipos o categorías de Activos:

1. El entorno del Sistema de Información comprende los activos que se precisan para garantizar los siguientes niveles

   Ejemplos:

   - Equipamientos y suministros (energía, climatización, comunicaciones)
   - Personal (de dirección, de operación, de desarrollo, otro)
   - Otros tangibles (edificaciones, mobiliario, instalación física)

2. El sistema de información en sí. Ejemplos:
   - Hardware (de proceso, de almacenamiento, de interfaz, servidores, firmware, otros)
   - Software (de base, paquetes, producción de aplicaciones, modificación de firmware)
   - Comunicaciones (redes propias, servicios, componentes de conexión, etc.)

3. La propia información tratada por las aplicaciones del sistema de información. Ejemplos:
   - Datos (informatizados, concurrentes al o resultantes del Sistema de Información)
   - Meta-información (estructuración, formatos, códigos, claves de cifrado)
   - Soportes (tratables informáticamente, no tratables)

4. Las funcionalidades de la organización**,** que justifican la existencia de los Sistemas de Información anteriores y les dan finalidad. Ejemplos:
   - Objetivos y misión de la organización
   - Bienes y servicios producidos

- Personal usuario y/o destinatario de los bienes o servicios producidos

5. Otros activos, ya que el tratamiento de los activos es un método de evaluación de riesgos que debe permitir la inclusión de cualquier activo, sea cual sea su naturaleza. Ejemplos:
    - **Credibilidad (ética, jurídica, etc.) o buena imagen de una persona jurídica o física,**
    - Conocimiento acumulado,
    - Independencia de criterio o de actuación,
    - Intimidad de una persona física,
    - Integridad material de las personas, etc.

Las 5 categorías o niveles citados implican una tipificación según la naturaleza propia o intrínseca de los Activos. Los 3 primeros constituyen el Dominio estricto genérico de todo proyecto de Seguridad de Sistemas de Información, mientras que los dos últimos son exteriores al Sistema de Información propiamente dicho o extrínsecos, pero no exentos de consecuencias desde el punto de vista de la seguridad.

2.4.4 ATRIBUTOS

Cada Activo o Grupo de Activos incorpora como atributos esenciales dos indicadores sobre dos tipos de valoraciones, que ofrecen una orientación para calibrar el posible impacto que la materialización de una amenaza puede provocar en el activo:

- La valoración intrínseca al Activo considerado tiene dos aspectos

    - Uno cualitativo como valor de uso del Activo; este atributo permite responder al ¿para qué sirve el Activo? y soporta la clasificación anterior en tipos por naturaleza;

- Otro cuantitativo como valor de cambio**,** o sea cuánto vale; este atributo es válido para ciertos tipos de Activo y útil tanto a efectos indirectos de la valoración del Impacto causable por las amenazas, como para soportar la decisión entre la valoración del Riesgo y la de las salvaguardas para reducirlo.

- La valoración del estado de seguridad del Activo considerado, expuesta anteriormente como característica por su importancia, se concreta en sus 4 subestados *A*-*C*-*I*-D: autenticación, confidencialidad, integridad, disponibilidad.

2.4.5 METRICAS

Las valoraciones anteriores reposan sobre sendas métricas. **Las métricas de valoración intrínseca de los Activos** se apoyan en estas situaciones:

- Ciertos Activos pueden estar inventariados: una parte importante de los Activos de los niveles 1 (Entorno) y 2 (Sistema de información) pueden tomarse de los Inventarios preestablecidos en la Entidad y por tanto seguirán las clasificaciones de dichos inventarios (relacionadas a menudo con su contabilización patrimonial).

- Otros Activos pueden estar inventariados o no: así las Aplicaciones existentes que cubren la obtención de determinada Información (nivel 3) o ciertas Funcionalidades de la Organización (nivel 4) suelen estar inventariadas si se compran en el mercado o si se pueden valorar, por ejemplo por su coste de producción.

- Una parte de Activos del Sistema en estudio no son inventariables en el sentido contable del término, es decir como ‘valor de cambio’ (apto por

ejemplo para reposición en caso de deterioro). No por ello dejan de tener un ‘valor de uso’ para la Organización, que a menudo se suele apreciar cualitativamente por su carencia.

Las métricas de valoración del estado de seguridad del Activo considerado permiten estimar los niveles de sus 4 *subestados A-C-I-D* (autenticación, confidencialidad, integridad, disponibilidad).

- **Subestado A de Autenticación.** Su escala está ligada a la menor o mayor necesidad de formalización, de autorización y de responsabilización probatoria en el conocimiento o la comunicación de Activos del Dominio***.***

- **Subestado C de Confidencialidad de Información.** usa una escala con 4 niveles (para cada uno se adjunta un tipo de dato tomado de las categorías implícitas en la LORTAD Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal)

    1. Libre, sin restricciones en su difusión (datos de carácter NO personal)

    2. Restringida, con restricciones normales (dato de carácter personal)

    3. Protegida, con restricciones altas (dato especialmente protegido o ‘sensible’, por ejemplo sobre ideología, religión, salud o etnia)

    4. Confidencial, no difundible por su carácter crítico

- **Subestado I de Integridad.** Su escala usa 4 niveles, referibles a una característica práctica, la facilidad mayor o menor de reobtener el Activo con calidad suficiente**,** o sea completo y no ‘corrompido’ para el uso que se desea darle:

1. Bajo**,** si se puede reemplazar fácilmente con un Activo de igual calidad (por ejemplo, información redundante o imprecisa).

2. Normal, si se puede reemplazar con un Activo de calidad semejante con una molestia razonable.

3. Alto, si la calidad necesaria es reconstruible, difícil y costoso.

4. Crítico, si no puede volver a obtenerse una calidad semejante.

- **Subestado D de Disponibilidad.** Su escala emplea niveles definidos por el período de tiempo máximo de carencia del Activo sin que las consecuencias o Impactos sean graves para la Organización.

    1. Menos de una hora, considerado como fácilmente recuperable

    2. Hasta un día laborable, coincidente con un plazo habitual de recuperación con ayuda telefónica de especialistas externos o de reposición con existencia local.

    3. Hasta una semana, coincidente con un plazo normal de recuperación grave con ayuda presencial de especialistas externos, de reposición sin existencia local o con el arranque del centro alternativo.

    4. Más de una semana, considerado como interrupción catastrófica.

Otros sistemas tienen tiempos máximos de carencia distintos, que por ejemplo son inferiores a una centésima de segundo para un ordenador embarcado en un satélite; o a una décima para el controlador de una unidad de vigilancia intensiva hospitalaria; o a un segundo en una sala de contratación bursátil electrónica; o a diez segundos en cualquier transacción; etc. En ciertos sistemas, la carencia es menos aceptable en unos períodos que en otros (nóminas a fin de mes, balances en torno al fin de año, etc).

2.5 VULNERABILIDAD

2.5.1 DEFINICIÓN

Vulnerabilidad de un Activo es la potencialidad o posibilidad de ocurrencia de la materialización de una Amenaza sobre dicho Activo.

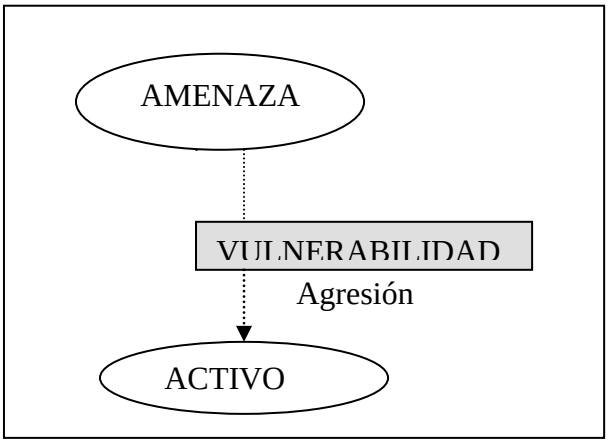


FIGURA 2.3 VULNERABILIDAD

2.5.2 CARACTERÍSTICAS

La Vulnerabilidad es una propiedad de la relación entre un Activo y una Amenaza. La Vulnerabilidad se ha venido vinculando más al Activo como una 'no-calidad' de éste, pero se puede utilizar con una mayor vinculación a la Amenaza cuando el problema lo considere conveniente (en todo caso,

Vulnerabilidad no es sólo una ‘debilidad’ o sea una ‘propiedad negativa’ del elemento ‘Activo’). La Vulnerabilidad es un concepto con dos aspectos:

- La Vulnerabilidad como propiedad ejerce una función de mediación (o de predicación en sentido lingüístico) entre la Amenaza como acción y el Activo como objeto de cambio del estado de seguridad. Por este aspecto estático la Vulnerabilidad forma parte del estado de seguridad del Activo.

- La Vulnerabilidad es asimismo en su aspecto dinámico el mecanismo obligado de paso o conversión de la Amenaza a una agresión materializada sobre un Activo. Por poner ejemplos, la Amenaza ‘Inundación por desbordamiento de torrente’ combinada con el Activo ‘centro de cálculo’ situado en zona inundable, se plasma en una Vulnerabilidad de dicho Activo respecto a esa Amenaza. Esta Vulnerabilidad depende del propio ‘ciclo de recurrencia’ (frecuencia) de las avenidas en la zona y de la ubicación del propio centro de cálculo (cercanía al lecho, situación en un sótano, etc.).

2.5.3 TIPOS

Se consideran dos acepciones principales:

- La Vulnerabilidad intrínseca del Activo respecto al tipo de Amenaza sólo depende de estas dos entidades, Activo y Amenaza.

- La Vulnerabilidad efectiva del Activo tiene en cuenta las Salvaguardas aplicadas en cada momento a dicho Activo y se tiene en cuenta en forma de un factor que estima la eficacia global de dichas Salvaguardas.

2.5.4.- ATRIBUTOS

La Vulnerabilidad intrínseca puede descomponerse, si conviene y para análisis muy detallados (sobre todo de amenaza intencional), según los aspectos siguientes:

- Potencialidad autónoma respecto al Activo amenazado de ocurrencia de la Amenaza (por ejemplo la frecuencia de inundaciones en un lugar determinado).
- Potencialidad derivada de la relación entre Activo y Amenaza (intencional sobre todo)
- Factores subjetivos generadores de más o menos 'fuerza' (motivación, disuasión)
- Oportunidad de acceso al Dominio con capacidad y recursos, según 4 aspectos:
    - Accesibilidad física presencial: número de personas o entidades autorizadas por su función a acceder normalmente al entorno del Activo, con una escala de 4 niveles
        - Una sola persona o entidad
        - Pocas personas de una entidad
        - Bastantes personas de pocas entidades distintas
        - Bastantes personas de varias entidades distintas

    - **Accesibilidad física calificada: calificación (formación general y experiencia) de los usuarios autorizados a acceder físicamente al entorno del Activo, con esta escala:**
        - No se requiere calificación
        - Se requiere poca formación para manejar la documentación técnica
        - Se requiere cierta experiencia para manejar la documentación técnica
        - Se requiere alta formación y experiencia para manejar la documentación

- Accesibilidad lógica competencial. Conocimiento técnico específico sobre el Activo atacable, con una escala de 4 niveles
    - No requiere competencia especial
    - Es fácil de realizar por un usuario
    - Requiere la competencia de un desarrollador
    - Necesita un experto muy calificado

- Accesibilidad lógica instrumental. Disponibilidad del instrumental que corresponde a la tecnología del Activo amenazable, con una escala de 4 niveles.

    - No requiere instrumental o éste es muy accesible
    - No requiere instrumental especial pero su acceso es restringido (coste ...)
    - Requiere instrumental especial aunque accesible de la tecnología considerada
    - Requiere instrumental especial y de acceso muy difícil

2.5.5.- METRICAS

La Métrica de la Vulnerabilidad consiste en considerar la ‘distancia’ entre la Amenaza (potencial) y su materialización como agresión (real) sobre el Activo.

Para ciertos Activos existen datos cuantitativos precisos (fiabilidad de un componente hardware, número de fallos de software) y se usa la métrica [0,1], donde la cota 0 implica que la Amenaza no afecta al Activo y la cota 1 no es alcanzable pues indicaría una agresión permanente. Pero como en general estas medidas no están disponibles, una primera aproximación cualitativa a la frecuencia o posibilidad de materialización de la Amenaza lleva a emplear la escala vista en las Amenazas potenciales (consideradas ahora reales, o sea agresiones).

Se puede 'objetivar' o sea hacer más objetiva esa escala de niveles comparando el periodo medio entre ocurrencias con una unidad. En unos casos conviene que sea mayor (el año, a efectos contables) y en otros menor (por ejemplo el día, pues una ocurrencia 'diaria' de fallo de un Activo es un límite superior psicológica y materialmente inaceptable en condiciones de productividad normales, no de investigación de incidentes).

PERIODO MEDIO ENTRE OCURRENCIAS	ESCALA SUBJETIVA	ESCALAS OBJETIVAS	
		POR DÍA	POR AÑO
Menos que 1 semana	Frecuencia muy alta	≅ 0.2	≅ 50
Menos que 2 meses	Frecuencia alta	≅ 0.02	≅ 5
Menos que 1 año	Frecuencia media	≅ 0.002	≅ 1
Menos que 6 años	Frecuencia baja	≅ 0.0002	≅ 0.2
Superior a 6 años	Frecuencia muy baja	≅ 0	≅ 0.02

TABLA 2.3 MÉTRICAS DE LA VULNERABILIDAD

Esta métrica de Vulnerabilidad no sólo es inviable en muchas ocasiones, sino que puede ser inconveniente para ciertos tipos de sectores, Activos o Amenazas. Sectores como por ejemplo defensa, energía nuclear, transporte de personas, etc. ejercen su función como 'misión' y trabajan con Activos que requieren seguridad crítica por su propia naturaleza. En estos casos la Vulnerabilidad para una amenaza es un mecanismo de nada (no le afecta) o todo (el riesgo es el propio impacto pleno).

La descomposición de la Vulnerabilidad intrínseca en Potencialidad genérica de ocurrencia de la Amenaza y Accesibilidad de la Amenaza al Dominio conlleva una métrica de Vulnerabilidad que combina la Métrica anterior (para la posibilidad genérica) con una corrección por factores incrementadores que tienen en cuenta la Accesibilidad

2.6 IMPACTO

2.6.1 DEFINICIÓN

El Impacto en un Activo es la consecuencia sobre éste de la materialización de una Amenaza.

2.6.2 CARACTERÍSTICAS

El Impacto es, visto de una manera dinámica, la diferencia en las estimaciones del estado de seguridad del Activo obtenidas antes y después de la agresión o materialización de la Amenaza sobre éste. Dicho de otra forma, el evento Amenaza (materializada en agresión) produce en el estado de seguridad del Activo anterior (a la amenaza) un cambio a un nuevo estado posterior (a la amenaza), midiendo el impacto la diferencia entre ambos estados.

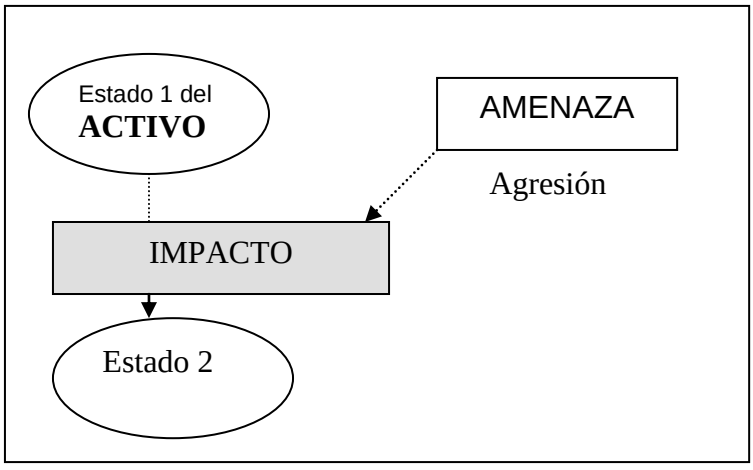


FIGURA 2.4 IMPACTO

2.6.3.- TIPOS

Se emplea una tipología de Impactos orientada a la naturaleza de las consecuencias de las combinaciones Activo-Amenaza (estas combinaciones son tan numerosas que no sería útil tomarlas como causas o 'naturaleza' de los Impactos para clasificarlos, como se hizo con las Amenazas).

Por tanto, una simple disfunción de un Activo no constituye normalmente un Impacto si no entraña una consecuencia de deterioro y perjuicio apreciable como cambio de estado. Por ejemplo no se considera Impacto la interrupción del tratamiento de una aplicación en un sistema por microcorte de energía o el reenvío automático de un mensaje por un servicio que tenga mecanismos de auto-recuperación (aunque implique incluso formas más o menos degradadas de funcionamiento, pero normalmente ya se cuenta con ellas).

Se consideran tres grandes grupos de Impactos, según que sus Consecuencias sean reductoras directamente de los subestados de seguridad A-C-I-D del Activo agredido; o bien indirectamente (y en este caso, de forma cuantitativa o cualitativa).

El Impacto será cualitativo con pérdidas funcionales (de los subestados de seguridad); cualitativo con pérdidas orgánicas (de fondo de comercio, daño de personas, etc.); y cuantitativo si las pérdidas se pueden traducir en dinero directa o indirectamente.

Impactos con consecuencias cualitativas funcionales

- El deterioro del Subestado de Autenticación (SA) no suele ser evolutivo (multiplicación en cadena) pero produce directamente anulación de documentos y procedimientos e indirectamente inseguridad jurídica (muy importante en la Administración pública) El deterioro del Subestado de Confidencialidad (SC) no suele ser evolutivo y tiene consecuencias de distintos órdenes, unas directas (divulgación de información no revelable o revelada anticipadamente, sustracción puntual o masiva) y otras indirectas (desconfianza, incomodidades, chantaje).

- El deterioro del Subestado de Integridad (SI) puede ser evolutivo y tiene consecuencias directas como la alteración de información sensible o vital en mayor o menor escala, e indirectas como la posible contaminación de programas (pérdida, tratamiento erróneo, etc).

- El deterioro del Subestado de Disponibilidad (SD) puede ser evolutivo y causar de inmediato desde la degradación de la productividad del activo como recurso o la interrupción de su funcionamiento de forma más o menos duradera y profunda (de unos datos, de una aplicación, de un servicio o de todo un sistema). Indirectamente esto se traduce en caída de margen por falta de resultados; así como en gastos suplementarios para recuperar o mantener la funcionalidad precedente a la amenaza.

Una parte de los deterioros anteriores tienen Impactos con consecuencias cuantitativas de diversos tipos:

N1: Pérdidas de valor económico, ligadas a activos inmobiliarios o inventariables, que comprenden todos los costes de reposición de la funcionalidad, incluyendo los gastos de tasar, sustituir, reparar o limpiar lo dañado: edificios y obras, instalaciones, computadores, redes, accesorios, etc.

N2: Pérdidas indirectas, valorables económicamente y ligadas a intangibles en general no inventariados: gastos de tasación y restauración o reposición de elementos no materiales del sistema: datos, programas, documentación**,** procedimientos, etc.

N3: Pérdidas indirectas, valorables económicamente y unidas a disfuncionalidades tangibles: se aprecian por el coste del retraso o interrupción de funciones operacionales de la organización; la perturbación o ruptura de los flujos y ciclos productivos (de productos, servicios o expedientes, por ejemplo),

incluido el deterioro de la calidad de éstos; y la incapacidad de cumplimentar las obligaciones contractuales o estatutarias.

N4: Pérdidas económicas relativas a responsabilidad legal (civil, penal o administrativa) del ‘propietario’ del sistema de información por los perjuicios causados a terceros ((incluidas, por ejemplo, sanciones de la Agencia de Protección de Datos).

Otros deterioros de los subestados de seguridad tienen Impactos con consecuencias cualitativas orgánicas de varios tipos:

L1: Pérdida de fondos patrimoniales intangibles: conocimientos (documentos, datos o programas) no recuperables, información confidencial, 'know-how'.

L2: Responsabilidad penal por Incumplimiento de obligaciones legales.

L3: Perturbación o situación embarazosa político-administrativa (deontología, credibilidad, prestigio, competencia política).

L4: Daño a las personas

2.6.4.- ATRIBUTOS

Desde el punto de vista de las Consecuencias directas sobre el estado de seguridad del Activo, el Impacto conjunta dos atributos o factores, la Gravedad intrínseca del resultado y el Agravante (o Atenuante) circunstancial. Ambos atributos hacen cambiar al menos uno de los niveles de los 4 subestados de seguridad del Activo: Autenticación, Confidencialidad, Integridad, Disponibilidad.

Desde el punto de vista de las Consecuencias indirectas y como se ha visto, un Impacto tiene como atributo importante:

- El aspecto cuantitativo de la consecuencia provocada, sea material (por ejemplo una pérdida monetaria para la reposición) o inmaterial (pérdidas como datos, programas, documentación o procedimientos);
- O bien su aspecto cualitativo (por ejemplo, pérdidas de fondo de comercio, pérdidas o daño de vidas, situación embarazosa político-administrativa, atentados a la intimidad personal).

2.6.5.- MÉTRICAS

Las diferencias en los atributos implican variaciones de medición y tratamiento del Impacto, aunque todas son generalmente cualitativas (por carencia de datos estadísticos cuantitativos).

Se indican dos formas básicas de valorar los impactos, apoyadas ambas en escalas cualitativas:

- Valoración en tiempo de la falta de disponibilidad de algún activo importante;
- Valoración en unidades monetarias de una escala con niveles meramente orientativos, que representa las cantidades a emplear para paliar los daños producidos por una amenaza materializada en la organización.

2.7 QUÉ ES GESTIÓN DE RIESGOS

Riesgo: Según Robert Charette el riesgo afecta a los futuros acontecimientos, implica cambio, elección y por consiguiente la incertidumbre que trae la elección.

El riesgo implica dos características:

- Incertidumbre: El acontecimiento que caracteriza al riesgo puede o no puede ocurrir.

- Pérdida: Si el riesgo se presenta, ocurrirán consecuencias no deseadas ó pérdidas.

El objetivo de la Gestión de Riesgos es identificar, estudiar y eliminar las fuentes de riesgo antes de que empiecen a amenazar el cumplimiento satisfactorio de un proyecto software.

2.8 MPORTANCIA DE LA GESTIÓN DE RIESGOS

Es muy importante en la actualidad el realizar gestión de riesgos ya que esta nos permite tener una visión general de lo que puede ocurrir en el transcurso del desarrollo o funcionamiento de un proyecto software para estar preparados con el equipo humano, material y económico necesario para sacar adelante al proyecto.

Cuando se considera el riesgo en el contexto de la ingeniería del software, los tres pilares conceptuales de Charette se hacen continuamente evidentes. Los mismos que expresan: el futuro es lo que nos debe importar, es decir, al momento de realizar el proyecto se de tener en cuenta los riesgos que a futuro pueden hacer que nuestro proyecto fracase; el cambio es nuestra preocupación, es decir, como afectarán los cambios en los requisitos del cliente, en las tecnologías de desarrollo, en el proyecto y todas las entidades relacionadas con él, y de manera significante en el cumplimiento de la planificación temporal y en el éxito general del proyecto; enfrentar de manera correcta las elecciones, en cuanto a métodos y herramientas que deberíamos emplear, cuanta gente debería estar implicada, entre otras.

Peter Drucker dijo una vez: "Mientras que es inútil intentar eliminar el riesgo y cuestionable el poder minimizarlo, es esencial que los riesgos que se tomen sean los riesgos adecuados". Antes de poder identificar los "riesgos adecuados" que se pueden tomar en un proyecto de software, es importante poder identificar todos los riesgos que sean obvios a jefes de proyectos y profesionales del software.

2.9 IDENTIFICACIÓN DE RIESGOS

La identificación del riesgo es un intento sistemático para especificar las amenazas al plan del proyecto (estimaciones, planificación temporal, carga de recursos, etc). Identificando los riesgos conocidos y predecibles, el gestor del proyecto da un paso adelante para evitarlos cuando sea posible y controlarlos cuando sea necesario

Existen dos tipos diferenciados de riesgos para cada categoría presentada en el apartado anterior: genéricos y específicos del producto. Los riesgos **genéricos** son una amenaza potencial para todos los proyectos de software. Los **específicos** de producto sólo los pueden identificar los que tienen una clara visión de la tecnología. el personal y el entorno específico del proyecto en cuestión. Para identificar los riesgos específicos del producto se examinan el plan del proyecto y la declaración del ámbito del software y se desarrolla una respuesta a la siguiente pregunta: ¿Qué características especiales de este producto pueden estar amenazadas por nuestro plan del proyecto'?"

Tanto los riesgos genéricos como los específicos del producto se deberían identificar sistemáticamente. Tom Gilb tiene toda la razón cuando dice: "Si no atacas activamente a los riesgos. ellos te atacarán activamente a ti", Un método para identificar riesgos es crear una lista de comprobación de elementos de riesgo.

2.9.1 RIESGOS DEL TAMAÑO DEL PRODUCTO

Estos riesgos están asociados con el tamaño general del software a construir o a modificar.

Pocos gestores experimentados discutirían la siguiente frase: El riesgo del proyecto es directamente proporcional al tamaño dcl producto. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con el tamaño del producto (software):

- ¿Tamaño estimado del producto en LDC (líneas de código) o FP (puntos de función)?
- ¿Grado de seguridad en la estimación del tamaño?
- ¿Tamaño estimado del producto en número de programas, archivos y transacciones?
- ¿Porcentaje de desviación en el tamaño del producto respecto a la medida de productos anteriores?
- ¿Tamaño de la base de datos creada o empleada por el producto?
- ¿Número de usuarios del producto?
- ¿Número de cambios previstos a los requisitos del producto? ¿Antes de la entrega? ¿ Después de la entrega?
- ¿Cantidad de software reutilizado?

En cada caso, la información del producto a desarrollar debe compararse con la experiencia anterior. Si ocurre una gran desviación del porcentaje o si las magnitudes son similares. pero si los resultados anteriores fueron poco satisfactorios, el riesgo es grande.

2.9.2 RIESGOS DEL IMPACTO EN EL NEGOCIO

Son los riesgos asociados con las limitaciones impuestas por la gestión o por el mercado.

Un gestor de ingeniería de una gran compañía de software colocó una placa con el texto: "¡dios me concedió el cerebro para ser un buen jefe de proyectos y el sentido común para correr como un diablo cuando marketing establece las fechas límite del proyecto!". Al departamento de marketing le guían las consideraciones del negocio, y éstas entran a veces en conflicto directo con las realidades técnicas. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con el impacto en el negocio:

- ¿Efecto de este producto en los ingresos de la compañía?

- ¿Viabilidad de este producto para los gestores expertos?
- ¿Es razonable la fecha límite de entrega?
- ¿Número de clientes que usarán este producto y la consistencia de sus necesidades relativas al producto?
- ¿Número de otros productos/sistemas con los que este producto debe tener interoperatividad?
- ¿Sofisticación del usuario final?
- ¿Cantidad y calidad de la documentación del producto que debe ser elaborada y entregada al cliente?
- ¿Limitaciones gubernamentales en la construcción del producto?
- ¿Costos asociados por un retraso en la entrega?
- ¿Costos asociados con un producto defectuoso?

Cada respuesta para el producto a desarrollar debe compararse con la experiencia anterior. Si se obtiene una gran desviación del porcentaje o si las magnitudes son similares, pero los resultados anteriores fueron poco satisfactorios, el riesgo es grande.

2.9.3 RIESGOS RELACIONADOS CON EL CLIENTE

Son riesgos asociados con la satisfacción del cliente y la habilidad del desarrollador para comunicarse con el cliente en los momentos oportunos. No todos los clientes son iguales. Pressman y Herron tratan este aspecto cuando dicen: Los clientes tienen diferentes necesidades. Algunos saben lo que quieren; otros saben lo que no quieren. Algunos están deseando saber todos los detalles, mientras que otros se quedan satisfechos con vagas promesas.

Los clientes tienen diferentes personalidades. Algunos disfrutan siendo clientes (la tensión, la negociación, las recompensas psicológicas de un buen producto). Otros preferirían no ser clientes en absoluto. Algunos aceptarían felizmente cualquier cosa que se les entregara y le sacarían el mejor provecho a un producto pobre. Otros se quejarán amargamente cuando les falte calidad; algunos darán las gracias cuando la calidad es buena; unos pocos se quejarán

por todo.

Los clientes también tienen varios tipos de asociaciones con sus suministradores. Algunos conocen bien a sus proveedores y sus productos; otros no se han visto nunca las caras y se comunican siempre mediante correspondencia escrita y algunas llamadas telefónicas breves. Los clientes se contradicen a menudo. Quieren todo para ayer y gratis. A menudo, el producto se ve cogido entre las propias contraindicaciones del cliente.

Un "mal" cliente puede tener un profundo impacto en la habilidad del equipo de software para completar el proyecto a tiempo y dentro de presupuesto. Un mal cliente representa una amenaza significativa al plan del proyecto y un sustancial riesgo para el jefe del proyecto. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con diferentes clientes:

- ¿Ha trabajado con el cliente anteriormente?
- ¿Tiene el cliente una idea formal de lo que se requiere? ¿Se ha molestado en escribirlo?
- ¿Aceptará el cliente gastar su tiempo en reuniones formales de requisitos para identificar el ámbito del proyecto?
- ¿Está dispuesto el cliente a establecer una comunicación fluida con el desarrolador?
- ¿Está dispuesto el cliente a participar en las revisiones?
- ¿Es sofisticado técnicamente el área del producto?
- ¿Está dispuesto el cliente a dejar a su personal hacer el trabajo? Es decir, ¿ resistirá la tentación de mirar por encima del hombro durante el trabajo técnico?
- ¿Entiende el cliente el proceso del software?

Si la respuesta a alguna de estas preguntas es "no", se debería hacer una investigación más profunda para valorar el potencial de riesgo.

2.9.4 RIESGOS DEL PROCESO

Si el proceso del software no está bien definido; si el análisis, diseño y pruebas se realizan sobre la marcha; si la calidad es un concepto que todo el mundo estima importante, pero por la que nadie actúa de manera tangible para alcanzarla, entonces el proyecto está en peligro. Las siguientes preguntas se han extraído sobre la evaluación de la ingeniería del software desarrollado por R. S. Pressman & Associates. Inc. Las preguntas se han adaptado del cuestionario de evaluación del proceso del software del Instituto de Ingeniería del Software (IIS).

Aspectos del proceso

- ¿Apoyan sus gestores senior unas normas escritas que hagan hincapié en la importancia de un proceso estándar para el desarrollo del software?
- ¿Ha desarrollado su organización una descripción escrita del proceso del software a emplear en este proyecto?
- ¿Están de acuerdo los miembros del personal con el proceso del software tal y como está documentado y estan dispuestos a usarlo?
- ¿Se emplea este proceso del software para otros proyectos?
- ¿Ha desarrollado o adquirido su organización cursos de formación de ingeniería del software para jefes de proyecto y personal técnico?
- ¿Se ha proporcionado una copia de los estándares de ingeniería del software publicados a cada desarrollador y gestor de software?
- ¿Se han desarrollado diseños de documentos y ejemplos para todas las entregas definidas como parte del proceso del software?
- ¿Se llevan a cabo regularmente revisiones técnicas formales de las especificaciones de requisitos, diseño y código?

- ¿Se llevan a cabo regularmente: revisiones técnicas de los procedimientos de prueba y de los casos de prueba?
- ¿,Se documentan todos los resultados de las revisiones técnicas, incluyendo los errores encontrados y recursos empleados?
- ¿Existe algún mecanismo para asegurarse de que el trabajo realizado en un proyecto se ajusta a los estándares de ingeniería del software?
- ¿Se emplea una gestión de configuración para mantener la consistencia entre los requisitos del sistema/software, diseño, código y casos de prueba?
- ¿Hay algún mecanismo de control de cambios de los requisitos del cliente que impacten en el software?
- ¿Hay alguna declaración de trabajo documentada, una especificación de requisitos software y un plan de desarrollo del software para cada subcontratación?
- ¿Se sigue algún procedimiento para hacer un seguimiento y revisar el rendimiento de las subcontraciones?

Aspectos técnicos

- ¿Se emplean técnicas de especificación de aplicaciones para ayudar en la comunicación entre el cliente y el desarrollador?
- ¿Se emplean métodos específicos para el análisis del software?
- ¿Emplea un método específico para el diseño de datos y arquitectónico?
- ¿Está escrito su código en más de un 90 por ciento en lenguaje de alto nivel?
- ¿Se han definido y empleado reglas específicas para la documentación del código?
- ¿Emplea métodos específicos para el diseño de casos de prueba?

- ¿Se emplean herramientas de software para apoyar la planificación y el seguimiento de las actividades?
- ¿Se emplean herramientas de software de gestión de configuración para controlar y seguir los cambios a lo largo de todo el proceso del software?
- ¿Se emplean herramientas de software para apoyar los procesos de análisis y diseño del software?
- ¿Se emplean herramientas para crear prototipos software?
- ¿Se emplean herramientas de software para dar soporte a los procesos de prueba?
- ¿Se emplean herramientas de software para soportar la producción y gestión de la documentación?
- ¿Se han establecido métricas de calidad para todos los proyectos de software?
- ¿Se han establecido métricas de productividad para todos los proyectos de software?

Si la mayoría de las cuestiones anteriores se han respondido negativamente, el proceso del software es débil y el riesgo es alto.

2.9.5 RIESGOS TECNOLOGICOS

Alcanzar los límites de la tecnología es un reto excitante. Es el sueño de casi todos los técnicos, porque fuerza al profesional a emplear su talento al máximo. Pero también es muy arriesgado. La ley de Murphy parece mantener su imperio en esta parte del universo del desarrollo, haciendo extremadamente difícil predecir los riesgos, y mucho menos hacer ningún plan sobre ellos. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con la técnica a construir.

- ¿Es nueva para su organización la tecnología a construir?
- ¿Demandan los requisitos del cliente la creación de nuevos algoritmos o tecnología de entrada o salida?
- ¿El software interactúa con hardware nuevo o no probado?

- ¿Interactúa el software a construir con productos software suministrados por el vendedor que no se hayan probado?
- ¿Interactúa el software a construir con un sistema de base de datos cuyo funcionamiento y rendimiento no se han comprobado en esta área de aplicación?
- ¿Demandan los requisitos del producto una interfaz de usuario especial?
- ¿Demandan los requisitos del producto la creación de componentes de programación distintos de; los que su organización haya desarrollado hasta ahora?
- ¿Demandan los requisitos el empleo de nuevos métodos de análisis, diseño o pruebas?
- ¿Demandan los requisitos el empleo de métodos de 'desarrollo del software no convencionales, tales como los métodos formales, enfoques basados .... en IA y redes neuronales?
- ¿Imponen excesivas restricciones de rendimiento los requisitos del producto?
- ¿No está seguro el cliente de que la funcionalidad pedida sea factible?

Si la respuesta a alguna de estas preguntas es afirmativa, se debería realizar una investigación más profundidad para valorar el riesgo potencial.

2.9.6 RIESGOS DEL ENTORNO DE DESARROLLO

Si a un carpintero se le pidiera que construyera un mueble de calidad con una simple sierra de mano, se dudaría de la calidad del producto final. Las herramientas inapropiadas o ineficaces pueden estropear los esfuerzos de incluso un experimentado profesional.

El entorno de ingeniería del software soporta al equipo del proyecto. al

proceso y al producto. Pero si el entomo es malo. puede ser una fuente de riesgos significativa. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados com el entomo de desarrollo:

- ¿Tenemos disponible una herramienta de gestión de proyectos de software?
- ¿Tenemos disponible una herramienta de gestión del proceso del software?
- ¿Existen herramientas de análisis y diseño disponibles?
- ¿Proporcionan las herramientas de análisis y diseño, métodos apropiados para el producto a construir?
- ¿Hay disponible? compiladores o generadores de código apropiados para el producto a construir?
- ¿Hay disponibles herramientas de pruebas apropiadas para el producto a construir?
- ¿Tenemos disponibles herramientas de gestión de configuración software?
- ¿Hace uso el entorno de bases de datos o información almacenada?
- ¿Están todas las herramientas de software integradas entre sí?
- ¿Se ha formado a los miembros del equipo del proyecto en todas las herramientas,?
- ¿Existen expertos disponibles para responder todas las preguntas que surjan sobre las herramientas?
- ¿Es adecuada la ayuda en línea y la documentación de las herramientas?

Si se ha contestado negativamente a la mayoría de las preguntas anteriores, el entorno de desarrollo es débil y el riesgo es alto.

2.10 COMPONENTES Y CONTROLADORES DEL RIESGO

Las Fuerzas Aéreas de Estados Unidos han redactado un documento que contiene excelentes directrices para identificar riesgos software y evitarlos. El enfoque de las Fuerzas Aéreas requiere que el gestor del proyecto identifique los controladores del riesgo que afectan a los componentes de riesgo software (rendimiento, coste, soporte y planificación temporal). En el contexto de este estudio, los componentes de riesgo se definen de la siguiente manera:

- Riesgo de rendimiento: el grado de incertidumbre con el que el producto encontrará sus requisitos y se adecue para su empleo pretendido.
- Riesgo de coste: el grado de incertidumbre que mantendrá el presupuesto del proyecto.
- Riesgo de soporte: el grado de incertidumbre de la facilidad del software para corregirse, adaptarse y ser mejorado.
- Riesgo de la planificación temporal: el grado de incertidumbre con que se podrá mantener la planificación temporal y de que el producto se entregue a tiempo.

El impacto de cada controlador de riesgo en el componente de riesgo se divide en cuatro categorías de impacto -despreciable. marginal, crítico y catastrófico.

2.11 ESTRATEGÍAS DE RIESGO

Dentro de las estrategias de riesgo tenemos dos grandes grupos que son: las estrategias reactivas y las proactivas.

Las estrategias de riesgo **reactivas** se han denominado humorísticamente "Escuela de gestión del riesgo de Indiana Jones". En las películas, Indiana Jones, cuando se enfrentaba a una dificultad insuperable, siempre decía "¡No te preocupes, pensaré en algo!". Nunca se preocupaba de los problemas hasta que ocurrían, entonces le reaccionaba como un héroe.

Como el jefe del proyecto de software normalmente no es Indiana Jones y los miembros de su equipo no son sus fiables colaboradores, la mayoría de los

equipos de software confían solamente en las estrategias de riesgo reactivas. En el mejor de los casos, la estrategia **reactiva** supervisa el proyecto en previsión de posibles riesgos. Los recursos se ponen aparte, en caso de que pudieran convertirse en problemas reales. Pero lo más frecuente es que el equipo de software no haga nada respecto a los riesgos hasta que algo va mal. Después el equipo vuela para corregir el problema rápidamente. éste es el método denominado a menudo "de bomberos". Cuando falla, "la gestión de crisis" entra en acción y el proyecto se encuentra en peligro real.

Una estrategia considerablemente más inteligente para el control del riesgo es ser **proactivo.** La estrategia **proactiva** empieza mucho antes de que comiencen los trabajos técnicos. Se identifican los riesgos potenciales, se valoran su probabilidad y su impacto y se establece una prioridad según su importancia.

Después el equipo de software establece un plan para controlar el riesgo. El primer objetivo es evitar el riesgo, poco común no se pueden evitar todos los riesgos. el equipo trabaja para desarrollar un plan de contingencia que le permita responder de una manera eficaz y controlada.

A lo largo de lo que queda de este capitulo, estudiamos la estrategia proactiva para el control de riesgos.

2.12 PROYECCIÓN DEL RIESGO

La proyección del riesgo, también denominada estimación del riesgo, intenta medir cada riesgo de dos maneras -la probabilidad de que el riesgo sea real y las consecuencias de los problemas asociados con el riesgo, si ocurriera. El jefe del proyecto, junto con otros gestores y personal técnico, realiza cuatro actividades de proyección del riesgo:

1. Establecer una escala que refleje la probabilidad percibida del riesgo;
2. Definir las consecuencias del riesgo;
3. Estimar el impacto del riesgo en el proyecto y en el producto; y

4. Apuntar la exactitud general de la proyección del riesgo de manera que no haya confusiones.

2.12.1 EVALUACIÓN DEL IMPACTO DEL RIESGO

Tres factores afectan a las consecuencias probables de un riesgo, si ocurre: su naturaleza, su alcance y cuando ocurre. La naturaleza del riesgo indica los problemas probables que aparecerán si ocurre. Por ejemplo, una interfaz externa mal definida para el hardware del cliente (un riesgo técnico) impedirá un diseño y pruebas tempranas y probablemente lleve a problemas de integración más adelante en el proyecto. El alcance de un riesgo combina la severidad (¿cómo de serio es el problema?) con su distribución general (¿qué proporción del proyecto se verá afectado y cuantos clientes se verán perjudicados?). Finalmente, la temporización de un riesgo considera cuándo y por cuánto tiempo se dejará sentir el impacto. En la mayoría de los casos, un jefe de proyecto prefiere las "malas noticias" cuanto antes, pero en algunos casos, cuanto más tarden, mejor.

Volviendo una vez más al enfoque del análisis de riesgo propuesto por las Fuerzas Aéreas de Estados Unidos, se recomiendan los siguientes pasos para determinar las consecuencias generales de un riesgo:

1. Determinar la probabilidad media de que ocurra un valor para cada componente de riesgo.

2. Empleando la Figura 2.1, determinar el impacto de cada componente basándose en los criterios mostrados.

3. Completar la tabla de riesgo y analizar los resultados como se describe en las secciones precedentes.

2.12.2 EVALUACIÓN DEL RIESGO

En este punto del proceso de gestión del riesgo, debemos establecer un conjunto de ternas de la forma.

[ri,li,xi]

Donde r es el riesgo, l la probabilidad del riesgo y x el impacto del riesgo. Durante la evaluación del riesgo, se sigue examinando la exactitud de las estimaciones que fueron hechas durante la proyección del riesgo, se intenta dar prioridades a los riesgos que no se habían cubierto y se empieza a pensar las maneras de controlar y/o impedir los riesgos que sean más probables que aparezcan.

Para que sea útil la evaluación, se debe definir un nivel de referencia de riesgo. Para la mayoría de los proyectos, los componentes de riesgo estudiados anteriormente tienen un nivel de degradación del rendimiento, exceso de coste, dificultades de soporte o retrasos de la planificación temporal (o cualquier combinación de los cuatro) que provoquen que se termine el proyecto. Si una combinación de riesgos crea problemas de manera que uno o más de estos niveles de referencia se excedan, se parará el trabajo. En el contexto del análisis de riesgos del software, un nivel de referencia de riesgo tiene un solo punto, denominado punto de referencia o punto de ruptura, en el que la decisión de seguir con el proyecto o dejarlo (los problemas son demasiado graves) son igualmente aceptables.

Por tanto, durante la evaluación del riesgo, se realizan los siguientes pasos:

1. Definir los niveles de referencia de riesgo para el proyecto.
2. Intentar desarrollar una relación entre cada [ri, li, xi] y cada uno de los niveles de referencia.
3. Intentar predecir como afectarán las combinaciones compuestas de riesgos a un nivel de referencia.

2.13 PLANTEAMIENTO DE SALVAGUARDAS

La Etapa tiene como Objetivo la Selección de los mecanismos de salvaguarda que materialicen las funciones y servicios de salvaguarda, respeten las restricciones y reduzcan los riesgos por debajo de los umbrales deseados.

Esta etapa parte de los resultados de las etapas anteriores:

- Identificación de los mecanismos de salvaguarda implantados actualmente y de las funciones y En esta etapa, el especialista selecciona los mecanismos de salvaguarda que materialicen las funciones y servicios seleccionados, en función de la efectividad de éstos. Una vez elegidos estos mecanismos, se estudian sus relaciones, costes, tipos y otras características. Tras analizar posibles contradicciones o contraindicaciones en su aplicación, la Etapa establece un orden de prioridades para su implantación, reflejado en cronogramas tentativos de puesta en práctica. servicios de salvaguarda que cubren, así como el grado de su implantación.

- Funciones y servicios de salvaguarda seleccionados, capaces de reducir el riesgo hasta alcanzar los umbrales previamente elegidos (o bien actualizados, si se ha visto su necesidad).

Por último la etapa posibilita la recopilación de todos los informes obtenidos, para generar el documento final del Análisis y Gestión de Riesgos, además de los documentos de presentación de resultados a los diversos niveles de la Organización.

Las actividades de esta Etapa son:

1. Identificación de los mecanismos.- Se identifican de los mecanismos que puedan materializar las funciones y servicios de salvaguarda.
2. Selección de mecanismos de salvaguarda.- Se seleccionan y estudian los mecanismos de salvaguarda anteriores que cumplan las

restricciones y alcancen una efectividad suficiente en la reducción del nivel de riesgo.

3. Especificación de los mecanismos a implantar.- La tarea especifica para los mecanismos de salvaguarda seleccionados ciertas características importantes.
4. Orientación a la planificación de la Implantación.- La priorización de los mecanismos seleccionados junto a la estimación de los recursos necesarios permiten realizar una aproximación a los cronogramas de implantación.
5. Integración de resultados.- En esta actividad final se recopilan los informes de Etapa para generar el informe final y los documentos correspondientes para realizar presentaciones a diversos niveles.

Identificar mecanismos posibles

La tarea procede a confeccionar una lista inicial de posibles mecanismos de salvaguarda que materialicen las funciones y servicios de salvaguarda elegidos, parte de dichas funciones y servicios de salvaguarda.

Éstos, habitualmente asociados a impactos y vulnerabilidades de los activos ante las amenazas, permiten identificar un conjunto de mecanismos de salvaguarda posibles.

En esta tarea no se tiene en cuenta aún el análisis del coste, efectividad, necesidades de mantenimiento, etc. de los mecanismos posibles para materializar las funciones y servicios de salvaguarda.

Estudiar mecanismos implantados

Algunos de los mecanismos de salvaguarda identificados por la tarea anterior pueden estar ya implantados en el Dominio en estudio.

Esta tarea recupera la información obtenida en la recogida de datos del Dominio que identificaba los mecanismos ya implantados y sus características. Estos mecanismos se agrupan en dos bloques:

- Mecanismos coincidentes con alguno de los contenidos en la lista de mecanismos potenciales confeccionada en la tarea anterior
- Mecanismos no incluidos en dicha lista. Los mecanismos incluidos en ambos bloques se analizan según diversos criterios:
    - Su grado de implantación,
    - Los costes tanto de su implantación inicial como de su mantenimiento

CAPITULO III

En este capitulo se trata los antecedentes, conceptos, objetivos, aplicaciones y usos de la Metodología Magerit, el encuadre de Magerit en la Gestión de Riesgos. Además como Magerit se comporta en proyectos de complejidad media y alta, estructura de la fase de Análisis y Gestión de riesgos, visión global de las etapas del proceso Magerit.

También se realiza un estudio de la Herramienta de Gestión de Riesgos Ris2k en la que se destaca los cálculos del Riesgo Efectivo, Simulado, Intrínseco y Residual

Además se realiza el estudio de la Herramienta de Gestión de Riesgos Chinchon en la que se destaca los cálculos del Riesgo Efectivo, Mínimo e Intrínseco.

Para finalmente realiza un análisis comparativo entre la dos herramienta Ris2k y Chinchon.

3. - ESTUDIO DE LA METODOLOGÍA MAGERIT

3.1.- INTRODUCCIÓN AL MAGERIT

3.1.1 .- ANTECEDENTES DE CREACIÓN DEL MAGERIT

El Consejo Superior de Informática de la Unión Europea ha elaborado la Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas, MAGERIT, cuya utilización promueve, como respuesta a la dependencia creciente de éstas (y en general de toda la sociedad) de las Tecnologías de la Información. La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con

medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información para que generen confianza cuando se utilicen tales medios.

3.2.- QUE ES EL MAGERIT

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

MAGERIT ha sido el paso fundamental para la creación de herramientas de gestión de riesgos como son el RIS2K y el CHINCHON ya que esta metodología es muy fácil de entender y manejar.

3.3.- OBJETIVOS DEL MAGERIT

El método MAGERIT tiene un **objetivo inmediato** doble**:**

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un **análisis de los riesgos** que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

- Los resultados del análisis de riesgos permiten a la **gestión de riesgos recomendar las medidas** apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios

.

3.4.- APLICACION DEL MAGERIT

La Aplicación de MAGERIT permite:

- Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad
- Ayudar a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- La incrustación de mecanismos de seguridad en el corazón mismo de los sistemas de información:

    a. Para paliar las insuficiencias de los sistemas vigentes
    b. Para asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento.

3.4.1 TIPOS DE PROYECTOS

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

- **Situación.-** se refiere al marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- **Envergadura**: complejidad e incertidumbre relativas del Dominio estudiado, tipo de estudio más adecuado a la situación (corto, simplificado), granularidad adoptada.

- **Problemas específicos** que se desee solventar: Seguridad lógica, seguridad de redes y comunicaciones, planes de emergencia y contingencia, estudios técnicos para homologación de sistemas o productos , auditorías de seguridad, etc.

3.4.2 DERECHOS DE UTILIZACIÓN

MAGERIT es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas (MAP). Su utilización no requiere autorización previa del mismo.

3.4.3 RESPONSABLE DEL PRODUCTO

- Secretaría de Estado para la Administración Pública
- Dirección General de Organización Administrativa
- Subdirección General de Coordinación de Recursos Tecnológicos de la Administración General del Estado

Es importante mencionar que estos organismos pertenecen a la Unión Europea específicamente a España.

3.4.4 USOS DE MAGERIT

Diferentes usos se le puede dar a MAGERIT en cuanto a seguridad se refiere así tenemos:

- Tratar de que no haya elementos en el sistema de información que queden fuera del análisis
- Incrustar mecanismos de seguridad en el corazón mismo de los sistemas de información:
    - Para paliar las insuficiencias de los sistemas
    - Para asegurara el correcto desarrollo y funcionamiento de los sistemas

3.5 ELEMENTOS DEL MAGERIT

Dos elementos conforman la estructura de Magerit:

1. Un conjunto de guías compuesto básicamente por:

    - Guía de procedimientos.- Representa el núcleo del método, que se completa con la Guía de Técnicas. Ambas

constituyen un conjunto autosuficiente, puesto que basta su contenido para comprender la terminología y para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información

- Guía de aproximaciones.- Presenta los conceptos básicos de seguridad de los sistemas de información, con la finalidad de facilitar su comprensión por personal no especializado y ofrece una introducción al núcleo básico de MAGERIT, constituido por las Guías de Procedimientos y de Técnicas.

- Guía de técnicas.- Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.

- Guía para desarrolladores de aplicaciones.- Está diseñada para ser utilizada por los desarrolladores de aplicaciones, y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información.

- Guía para responsables del dominio protegible.- Explica la participación de los directivos "responsables de un dominio" en la realización del análisis y gestión de riesgos de aquellos sistemas de información relacionados con los activos cuya gestión y seguridad les están encomendados.

- Referencia de normas legales y técnicas.- lista de normas a seguir en materia de seguridad

2. Un panel de herramientas de apoyo, con sus correspondientes guías de uso y con la arquitectura de información y especificaciones de la interfaz para el intercambio de datos.

Esta estructura de MAGERIT permite realizar:

- El análisis de los riesgos para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el Sistema de Información (conocidos como 'activos'). Para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

- **La gestión de los riesgos, basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.**

3.6 EL MODELO MAGERIT

3.6.1.- ENCUADRE DE MAGERIT

Encuadre de MAGERIT en la Gestión de la Seguridad de los SI

MAGERIT, como método de Análisis y Gestión de Riesgos, cubre sólo una fase de la GESTIÓN global de la Seguridad de un Sistema de Información determinado. La Gestión global de Seguridad (representada en la figura 3.1)

es una acción permanente, cíclica y recurrente (es decir, se ha de reemprender continuamente debido a los cambios del sistema y de su entorno).

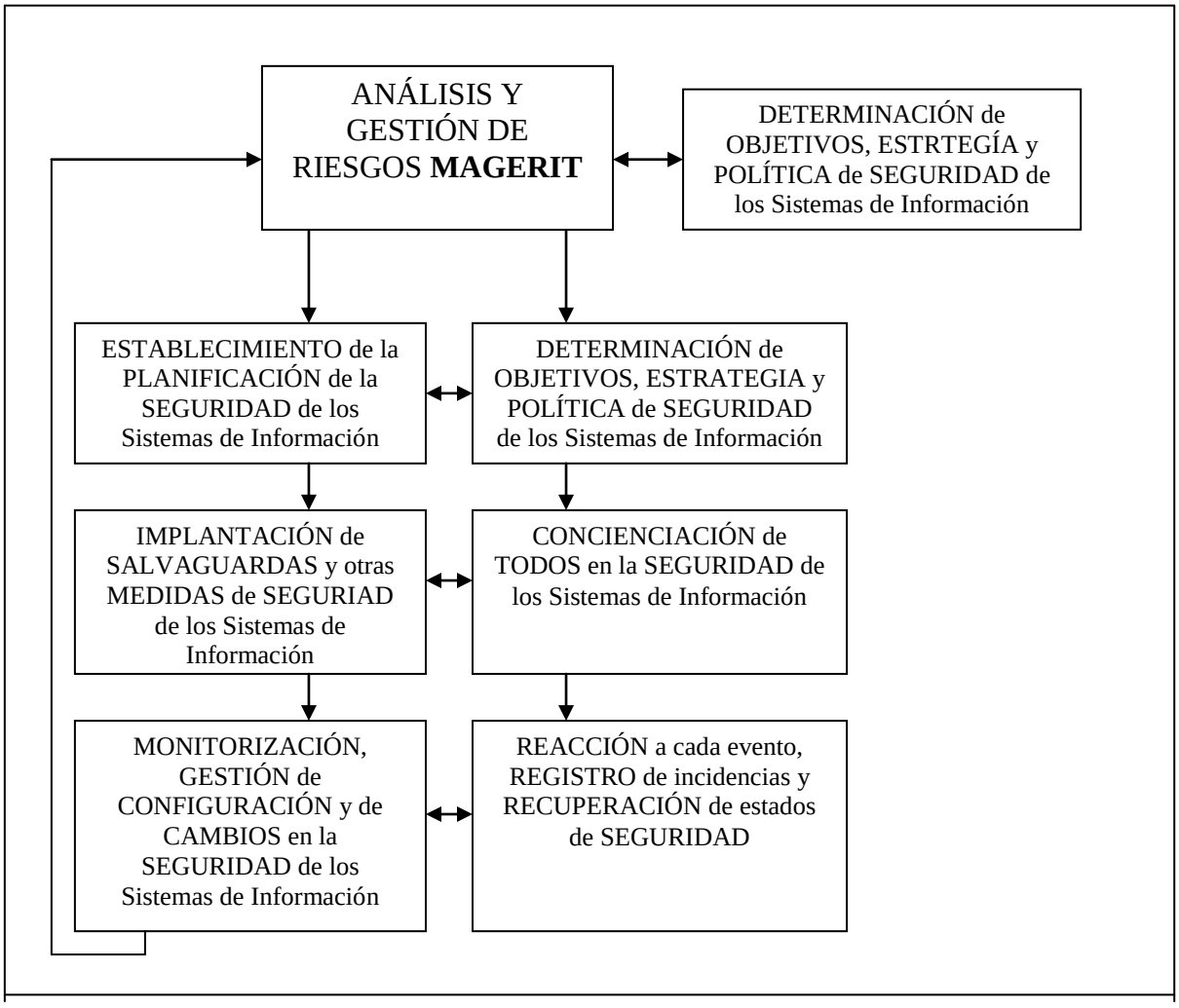


FIGURA 3.1 ENCUADRE DE MAGERIT EN LA GESTIÓN DE LA SEGURIDAD DE LOS SI

- El ANÁLISIS Y GESTIÓN DE RIESGOS es la fase nuclear de 'medición' y cálculo en el ciclo de gestión de la seguridad, es el punto de arranque del ciclo de Gestión de Seguridad y además requiere técnicas de proceso especiales (propias del ámbito de la seguridad).

- La fase de Determinación de OBJETIVOS, ESTRATEGIA y POLÍTICA de Seguridad de los Sistemas de Información se nutre de y nutre a su vez la fase de Análisis y Gestión de Riesgos. En el ciclo inicial de la

Gestión de Seguridad, un Análisis y Gestión de Riesgos de carácter global ayuda a determinar los objetivos, estrategia y política, que influirán durante los ciclos sucesivos en el Análisis y Gestión de Riesgos más detallado (que a su vez puede modificarlos para ciclos sucesivos).

- La fase de Establecimiento de la PLANIFICACION de la Seguridad de los Sistemas de Información se deriva de la fase de Análisis y Gestión de Riesgos como su consecuencia funcional más inmediata. Utiliza técnicas generales de planificación (resultados, secuenciación, hitos de decisión), pero adaptadas al ámbito de la seguridad).

- La fase de Determinación de la ORGANIZACION de la Seguridad de los Sistemas de Información se deriva de la fase de Análisis y Gestión de Riesgos como su consecuencia orgánica más inmediata. Utiliza técnicas generales de organización (compromiso gerencial, roles, responsabilidades, documentación normativa), aunque adaptadas al ámbito de la seguridad.

- La Fase de IMPLANTACION de SALVAGUARDAS y otras medidas de Seguridad para los Sistemas de Información se deriva de las fases de Planificación y Organización, utilizando técnicas generales de Gestión de Proyectos y Gestión de Configuración, aunque adaptadas al ámbito de la seguridad.

- La Fase de CONCIENCIACIÓN de TODOS en la SEGURIDAD de los Sistemas de Información deriva de las fases de Planificación y Organización. Tiene en cuenta el papel fundamental del recurso humano interno en todo proyecto de seguridad y utiliza técnicas generales de gestión de proyectos y gestión de formación, comunicación y recursos humanos, aunque adaptadas al ámbito de la seguridad.

- La fase de REACCIÓN a cada evento, de MANEJO y REGISTRO de las incidencias y de RECUPERACIÓN de estados aceptables de Seguridad tiene un carácter básicamente operacional y utiliza por tanto técnicas

generales de Gestión cotidiana y de Atención a Emergencias adaptadas al ámbito de la seguridad.

- La Fase de MONITORIZACIÓN, GESTIÓN de CONFIGURACIÓN y de CAMBIOS en la Seguridad de los Sistemas de Información tiene un carácter básicamente de mantenimiento, con técnicas generales de monitorización, gestión de configuración y gestión de cambios adaptadas al ámbito de la seguridad.

3.6.2 MAGERIT EN PROYECTOS DE COMPLEJIDAD MEDIA Y ALTA

Los proyectos de complejidad media o alta en materia de seguridad requieren la realización de más de un ciclo de Gestión global de seguridad (figura 3.2). La *primera aplicación del ciclo de Gestión* abarca todo el sistema en estudio: arranca de la fase de Análisis y Gestión de Riesgos, enfocada a grandes rasgos para conseguir una primera dicotomía o clasificación en dos grandes bloques de los componentes del sistema:

- Los componentes que implican ***riesgos menores,*** a los que bastará aplicar globalmente medidas básicas de seguridad;

- Los componentes que implican ***riesgos mayores,*** a cada uno de los cuales será necesario aplicar un nuevo Análisis y Gestión de Riesgos más detallado.

Esta primera aplicación ofrece así una primera visión sintética de la seguridad con ayuda de las otras fases del ciclo de Gestión de Seguridad, es decir:

- Una determinación global de objetivos, estrategia y política de seguridad;

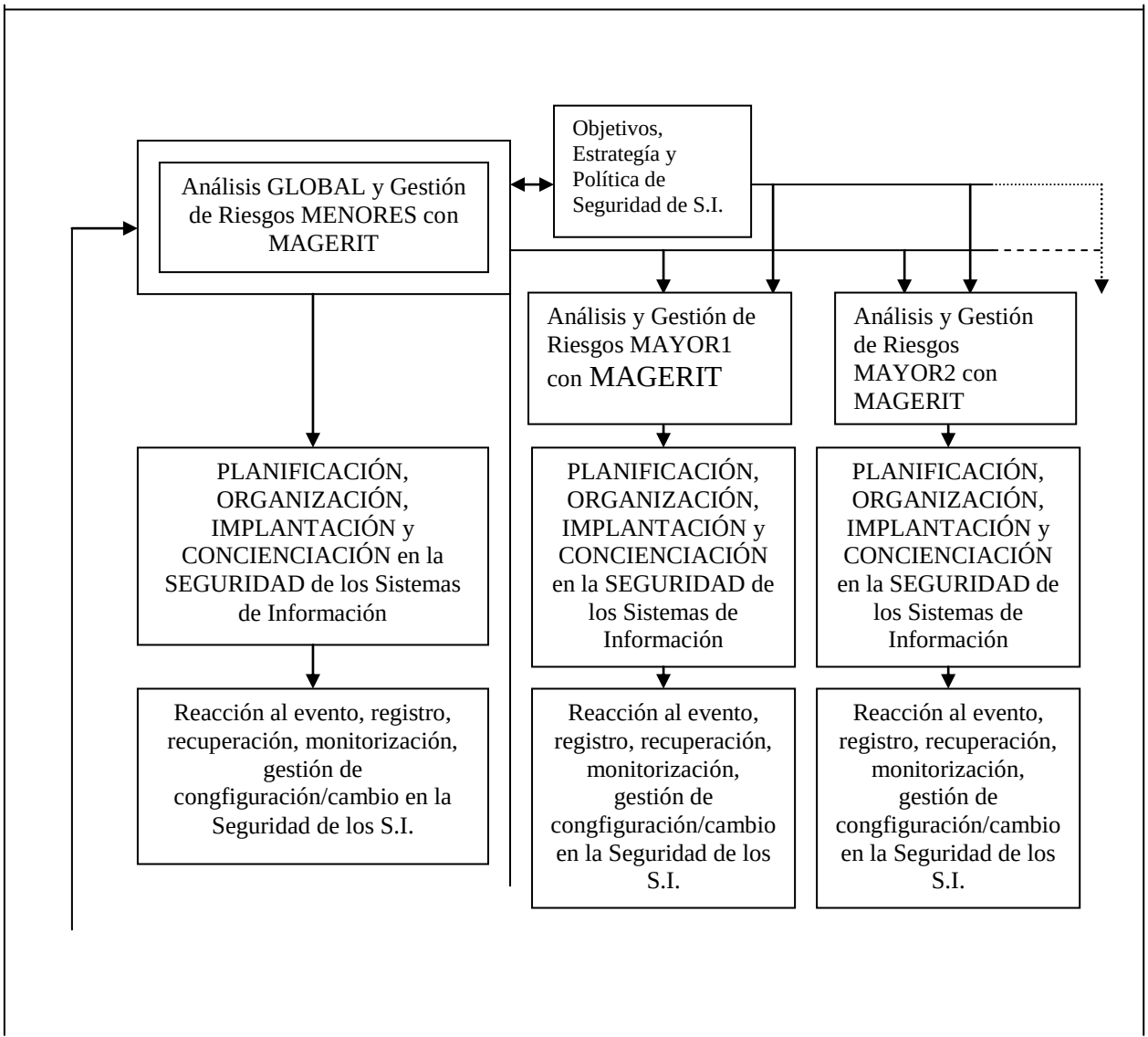
- Una planificación inicial de la seguridad

- Una primera determinación de la organización necesaria para la seguridad;

- La Implantación de las salvaguardas generales en los componentes de riesgos bajos;

- El entrenamiento a la participación en la seguridad de componentes de riesgos bajos;

- La preparación a la reacción ante cada evento, el manejo y registro de las incidencias y la recuperación de estados aceptables de seguridad ligados a los componentes de riesgo bajo.



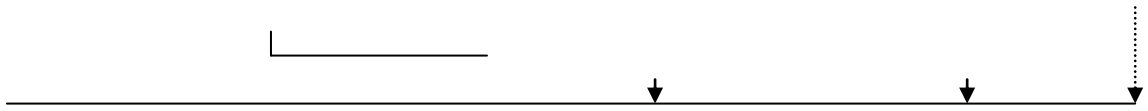


FIGURA 3.2 MAGERIT EN PROYECTOS DE COMPLEJIDAD MEDIA Y ALTA

3.6.3 ESTRUCTURA DE LA FASE DE ANÁLISIS Y GESTIÓN DE RIESGOS

El método MAGERIT se empieza por definir aquí en su nivel más genérico (para que pueda adaptarse a cada situación concreta). MAGERIT maneja así una visión estratégica global sobre la Seguridad de los Sistemas de Información de las Administraciones Públicas; visión que arranca de un Modelo de Análisis y Gestión de Riesgos que comprende 3 Submodelos (figura 3.3):

- Submodelo de Elementos
- Submodelo de Eventos
- Submodelo de Procesos

El Submodelo de Elementos proporciona los componentes que el Submodelo de Eventos relacionará entre sí y con el tiempo, mientras que el Submodelo de Procesos es la descripción funcional (el esquema explicativo) del proyecto de seguridad a construir. Para construir un proyecto de seguridad específico, el esquema, es decir el Submodelo de Procesos, ayuda por una parte a seguir el *procedimiento* general y por otra a adaptarlo al problema concreto, teniendo siempre en cuenta la política de seguridad que haya marcado la dirección de la entidad afectada. Si esta adaptación es compleja o tiene elementos de incertidumbre, debe hacerse con ayuda de un especialista de seguridad de los Sistemas de Información.

El procedimiento particularizado para el proyecto concreto de seguridad determina las Funciones y Servicios de Salvaguarda adecuados a los problemas detectados al aplicar el método e indica tipos de Mecanismos de Salvaguarda para resolverlos. Aunque no forman parte de MAGERIT, éste prepara la Planificación, la Organización y las otras fases posteriores necesarias para implementar y explotar adecuadamente dichos Mecanismos.

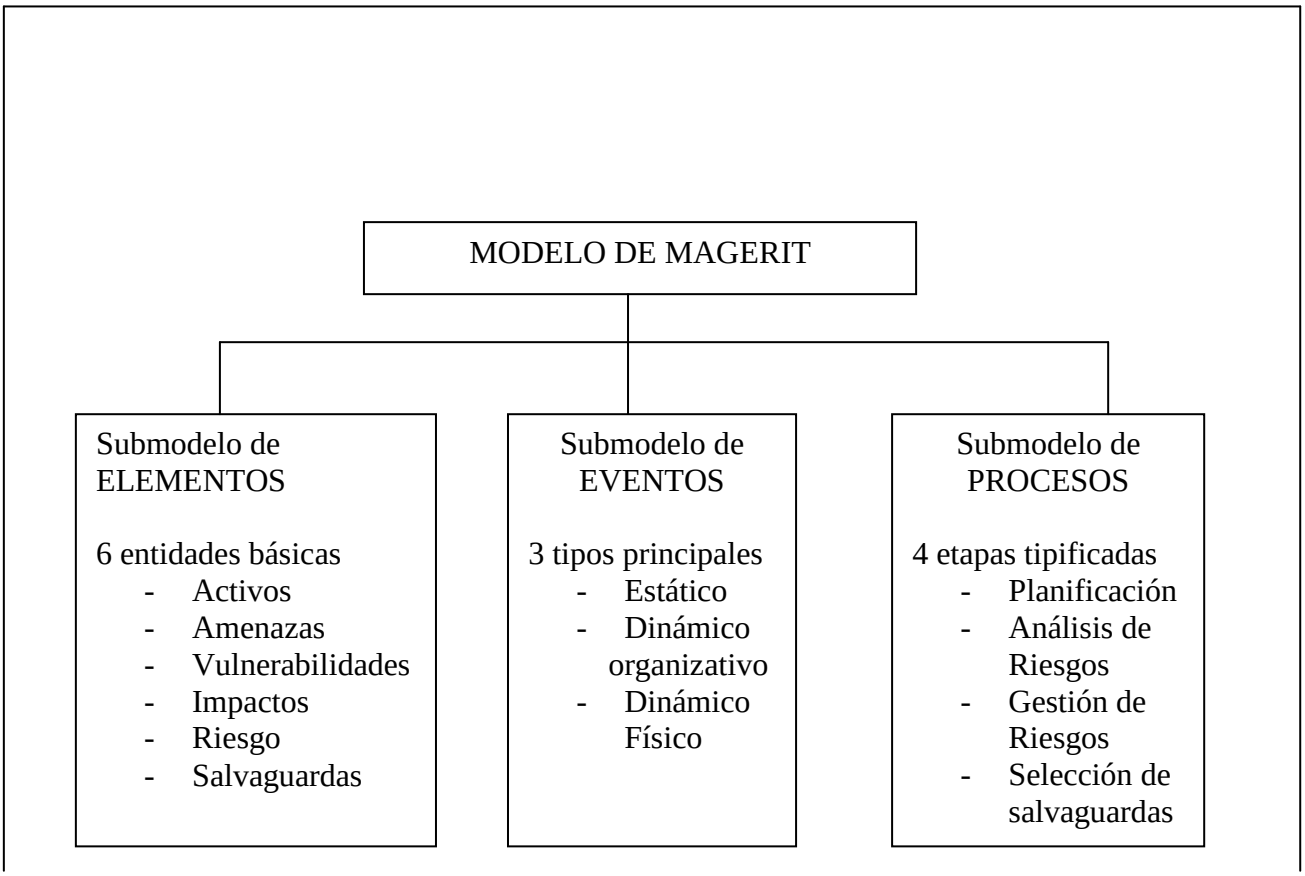


FIGURA 3.3 MODELO MAGERIT

3.6.3.1 SUBMODELO DE ELEMENTOS

El Submodelo de Elementos de MAGERIT comprende las seis Entidades básicas siguientes, así como sus procesos de adquisición y actualización:

• Activos
• Amenazas
• Vulnerabilidades
• Impactos
• Riesgos
• Salvaguardas (Funciones, Servicios y Mecanismos)

Activos.- Los Activos son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Amenazas.- **Las amenazas son los eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.**

Vulnerabilidad.- *Vulnerabilidad de un Activo es la potencialidad o posibilidad de ocurrencia de la materialización de una Amenaza sobre dicho Activo.*

Impacto.- El Impacto en un Activo es la consecuencia sobre éste de la materialización de una Amenaza.

Riesgo.- **El riesgo es la posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.**

Salvaguardas.- **MAGERIT define la Función o Servicio de salvaguarda como la acción que reduce el Riesgo. MAGERIT define el Mecanismo de salvaguarda como el procedimiento o dispositivo, físico o lógico que reduce el riesgo.**

3.6.3.2 SUBMODELOS DE EVENTOS

El Submodelo de Elementos ya estudiado ha proporcionado los componentes que el Submodelo de Eventos va a relacionar entre sí y con

el tiempo, mientras que el Submodelo de Procesos será la descripción funcional (el esquema explicativo) del proyecto de seguridad a construir. Como se acaba de citar anteriormente, la estructura y el funcionamiento de los Modelos de Análisis y Gestión de Riesgos se ha venido presentando intuitivamente hasta ahora en forma de 'ciudad amurallada': los activos están dentro, las amenazas son el enemigo exterior, las salvaguardas existentes son las murallas y las vulnerabilidades son sus 'brechas'. El ataque de las amenazas aprovecha las brechas y causa impactos en los activos. El reforzamiento de las murallas de salvaguarda reduce las brechas-vulnerabilidades y permite reparar los Impactos.

Esta visión ***estática de la seguridad*** cada vez está más superada, tanto por la naturaleza de los nuevos tipos de amenazas (más intencionales), de Activos (Sistemas de Información como 'ciudades abiertas') y por tanto de salvaguardas: en cada urbanización de Activos habrá que incrustar como mecanismos de salvaguarda ***agentes dinámicos*** que crezcan con la urbanización, la patrullen y hasta se camuflen para burlar a unos agresores cada vez más inteligentes.

En una situación de cambio de modelo como la descrita, conviene precisar con especial rigor la intuición anterior. MAGERIT ofrece un Submodelo de Eventos del método con tres 'vistas' relacionadas con las herramientas que ayuden a automatizar la metodología:

- La sencilla ***vista estática relacional*** es esencial para el entendimiento básico de MAGERIT

- La ***vista dinámica organizativa*** es conveniente para una comprensión profunda del funcionamiento de las etapas de MAGERIT.

- La ***vista dinámica física*** es una aproximación complementaria y más compleja a la realidad descrita por las vistas anteriores, aunque no es imprescindible para la comprensión de MAGERIT y sólo será necesaria en ciertas situaciones (por ejemplo como 'esqueleto' para productos o herramientas avanzadas de apoyo a MAGERIT).

3.6.3.3 VISTA ESTÁTICA RELACIONAL DEL SUBMODELO DE EVENTOS

La vista estática relacional del Submodelo de Eventos recoge el esquema de las relaciones generales entre las entidades indicadas en el Submodelo de Elementos . MAGERIT retiene como esquema de relaciones básico el reflejado en la siguiente figura:

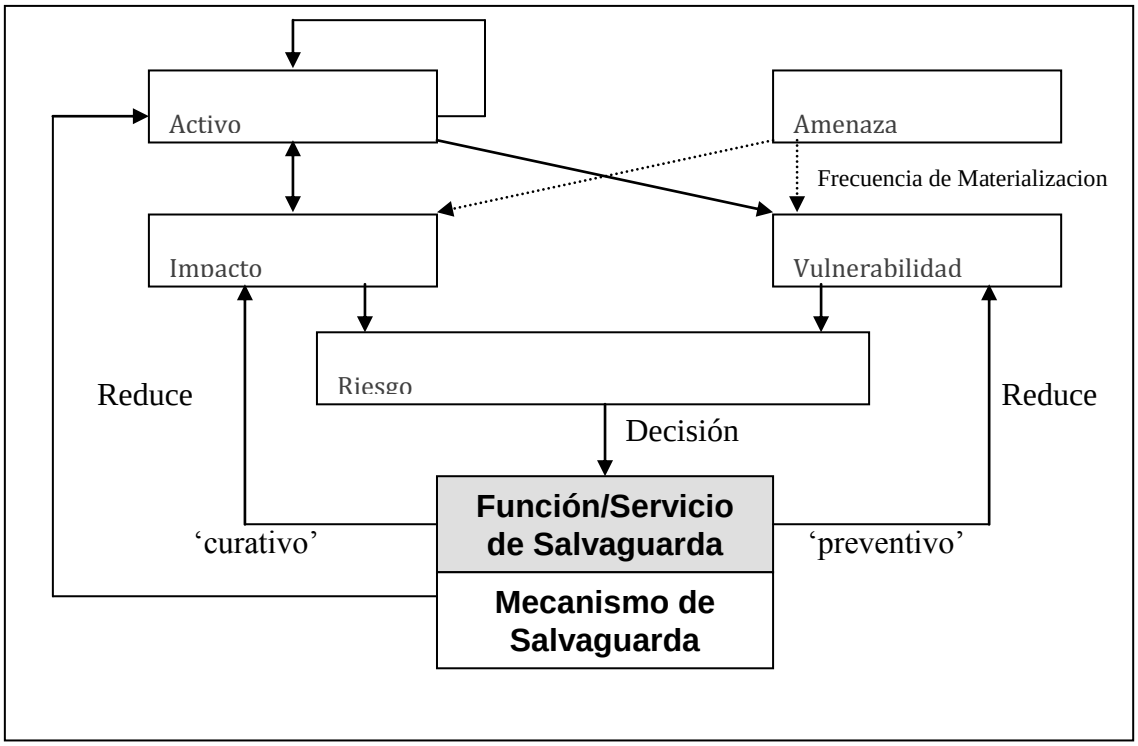


FIGURA 3.4 VISTA ESTÁTICA DEL SUBMODELO DE EVENTOS

El Submodelo estático de Eventos recoge simplemente las siguientes relaciones directas entre las entidades (representadas por los vectores de la figura anterior) :

Relaciones Directas del Activo; éste:

- Puede ser componente o dependiente de otro Activo
- Puede tener vulnerabilidades respecto a diversas amenazas
- Puede estar afectado por Impactos acumulables procedentes de diversas amenazas
- Puede estar protegido por un mecanismo de salvaguarda

Relaciones Directas de la Amenaza (si se materializa); ésta:

- Puede ser componente o dependiente de otra Amenaza
- Ha de explotar una vulnerabilidad para afectar a un activo
- Puede causar un impacto sobre el activo

Relaciones Directas de la Vulnerabilidad; ésta:

- Se relaciona con un activo
- Puede ser explotada por una amenaza para materializarse en agresión
- Puede ser afectada por una Función o un Servicio de salvaguarda
- Contribuye al riesgo.

Relaciones Directas del Impacto; éste:

- Se relaciona con un activo
- Puede causarlo la materialización de una amenaza
- Puede ser afectado por una Función o un Servicio de salvaguarda
- Contribuye al riesgo.

Relaciones Directas del Riesgo; éste:

- Se refiere a la vulnerabilidad de un activo respecto a una amenaza
- Se refiere al impacto propiciado por la vulnerabilidad de un activo
- Puede relacionarse con una Función o un Servicio de salvaguarda

Relaciones Directas de la Función o Servicio de Salvaguarda; éstos:

- Están relacionados con un riesgo
- Pueden complementar otra función o servicio de salvaguarda
- Pueden afectar al impacto de una amenaza
- Pueden afectar a la vulnerabilidad de una amenaza
- Permiten elegir entre Mecanismos de Salvaguarda

Relaciones Directas del Mecanismo de Salvaguarda; éste:

- Materializa una Función o un Servicio de Salvaguarda
- Protege un activo
- Puede afectar al impacto de una amenaza
- Puede afectar a la vulnerabilidad de una amenaza

3.6.3.4 VISTA DINÁMICA ORGANIZATIVA DEL SUBMODELO DE EVENTOS: ORGANIZACIÓN, DOMINIO Y ENTORNO

Esta vista del Submodelo, más detallada y compleja que la anterior, se muestra en la figura 3.5. Parte de una primera delimitación del Dominio de Información que MAGERIT ayuda a analizar desde el punto de vista de la seguridad; así como de la distinción, en el Entorno del Dominio delimitado, de una parte interna a la Organización y de otra externa (a efectos de posibles Restricciones o Condiciones, que la vista del Submodelo tendrá en cuenta). El Dominio está formado por Activos, ordenados de la mejor forma posible para facilitar el análisis de su seguridad y la gestión de su aseguramiento. Dicho Dominio, definido en cada momento por su 'estado' de seguridad, puede estar sometido a amenazas materializables, que son acciones de tipo 'evento' modificadoras de ese estado de seguridad. Las salvaguardas existentes permiten realizar otras acciones de tipo 'actuación', también modificadoras del estado de seguridad, que responden de forma anticipada o diferida pero en tiempo 'real' (o sea con intención de influir en el evento).

El Dominio tiene como Actor principal el Responsable del Dominio o de los Activos protegibles, que es quien determina su valor y necesidad de seguridad en forma de objetivos, de criterios de decisión o de decisiones.

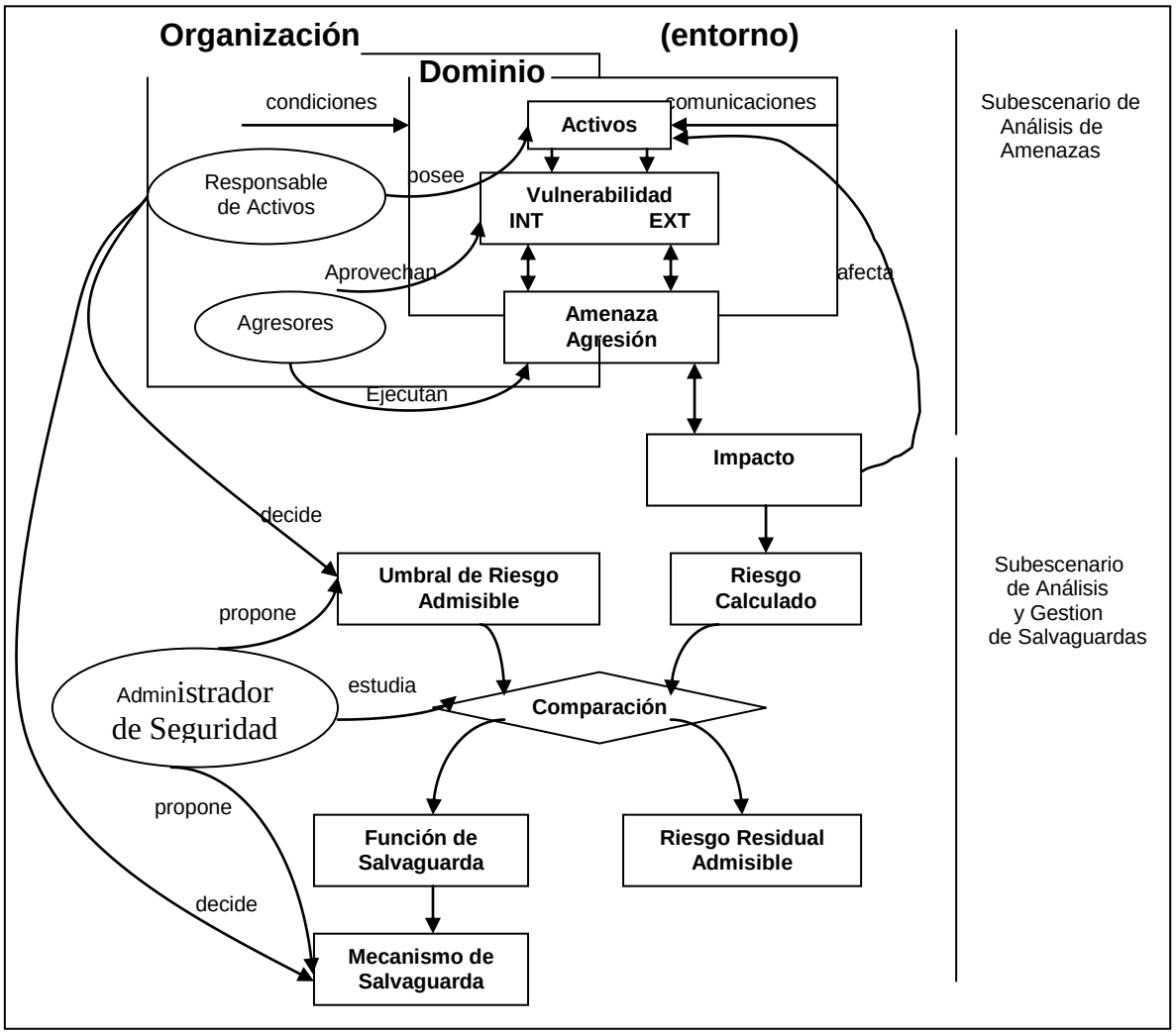


FIGURA 3.5 VISTA DINÁMICA ORGANIZATIVA DEL SUBMODELO DE EVENTOS: ORGANIZACIÓN, DOMINIO Y ENTORNO

3.6.3.5 LA MATERIALIZACIÓN DE LA AMENAZA COMO EVENTO DESENCADENANTE

El evento Amenaza desencadena una o más posibles disfunciones en el Dominio estudiado, según una distribución intrínseca de frecuencias, poco

precisas y en general pequeñas (sean históricas o previsibles) ligadas a las Vulnerabilidades de los Activos del Dominio. Cada disfunción puede quedar latente hasta que se activa como nuevo evento o bien genera uno o más siniestros, que a su vez pueden actuar como nuevos eventos desencadenantes de otros siniestros.

A partir de esa 'materialización' desencadenante, el Submodelo funciona dinámicamente como un escenario de 'aseguramiento' (acción para obtener seguridad) con 2 subescenarios:

- El subescenario de análisis de las amenazas o de ataque coincide con el análisis de los riesgos. Parte de una secuencia, o sea una cadena evento-disfunción-siniestro; y analiza las consecuencias reales o simuladas de ese ataque a uno o varios tipos de Activos del dominio, sean componentes de su Sistema de Información o bien otros Activos (infraestructuras, personal, ingresos, credibilidad, imagen, etc.).
- El subescenario de análisis y gestión de salvaguardas o de defensa coincide con la gestión de los riesgos y describe, frente a cada secuencia de ataque, la articulación y gestión de las funciones o servicios de salvaguarda apropiados (que funcionan de una forma más o menos específica).

Gestión de Salvaguardas

La incorporación de Salvaguardas depende del Riesgo, es decir de forma inmediata del Impacto sobre el Activo y de su Vulnerabilidad a la Amenaza y, de forma mediata, de los propios Tipos de Activos y Amenazas. Las salvaguardas actúan en distintos momentos y formas: unas son previas a la materialización de la Amenaza (Salvaguardas Concienciadoras, Disuasorias, Preventivas); y otras son consecuentes o consecutivas a esa materialización (Salvaguardas Correctivas y Recuperadoras), mientras que algunas salvaguardas actúan antes o después según las circunstancias (como las Salvaguardas Detectoras).

El Subescenario de defensa incorpora las Salvaguardas en dos niveles:

- **La incorporación funcional de Funciones o Servicios de Salvaguarda ayuda a la toma de decisiones.**
- La incorporación material de Mecanismos de Salvaguarda se caracteriza por su eficacia: un mismo Mecanismo de Salvaguarda tendrá más o menos eficacia según sea el alcance de la agresión.

3.6.3.6 VISTA DINÁMICA 'FÍSICA' DEL SUBMODELO DE EVENTOS

La **vista dinámica física** recoge otra forma de articular los escenarios de funcionamiento de los Elementos de MAGERIT, asimilando el Submodelo de sus Elementos de Seguridad concretos a las Entidades y Relaciones más abstractas que se emplean en otros modelos físicos, cuyo funcionamiento está ampliamente experimentado ya están dotados de numerosas técnicas de análisis y de simulación así como de herramientas para su gestión. Esta vista se puede necesitar para dar soporte tanto a ciertas técnicas y herramientas sofisticadas de cálculo de riesgos y de selección de salvaguardas, como a algunos especialistas que usen MAGERIT para enfrentarse a sistemas o problemas críticos que requieran modelos específicos de simulación de su proceso, con objeto de observar su funcionamiento y determinar los parámetros estratégicos óptimos de su seguridad.

3.6.3.7 SUBMODELO DE PROCESOS

De los dos Submodelos ya estudiados, el Submodelo de Elementos proporciona los componentes que el Submodelo de Eventos relaciona entre sí y con el tiempo. El Submodelo de Procesos realiza ahora la descripción funcional (el esquema explicativo) del proyecto de seguridad a construir. Para construir un proyecto de seguridad específico, el esquema explicativo, es decir el Submodelo de Procesos, ayuda por una parte a seguir el ***procedimiento*** general y por otra a adaptarlo al problema concreto, teniendo siempre en cuenta la Política de seguridad que haya marcado la Dirección de la Entidad

afectada. Si esta adaptación es compleja o tiene elementos de incertidumbre, el proyecto debe hacerse con ayuda de un especialista de seguridad de los Sistemas de Información.

3.6.3.8 ESTRUCTURA DEL SUBMODELO

El Submodelo de Procesos del Modelo MAGERIT agrupa y ordena las acciones a realizar a lo largo de un proyecto de análisis y gestión de riesgos. Este marco de trabajo define:

- Una estructuración del proyecto que sirve de guía al equipo de trabajo y que permite involucrar en aquél a los responsables del Dominio protegible y a los usuarios.
- Un conjunto de productos a obtener
- Un conjunto de técnicas para obtener los productos
- Las funciones y responsabilidades de los distintos 'actores' en el proyecto.

El Submodelo de Procesos de MAGERIT formaliza y describe detalladamente la sucesión de acciones y se estructura en tres niveles: etapas, compuestas por actividades y éstas desglosadas en tareas**:**

- **Las ETAPAS agrupan un conjunto de Actividades y corresponden al término de fase empleado por el método Métrica v.2.1, es decir, establece los hitos de decisión y entrega de productos. Exige al final de cada etapa una aceptación formal de sus resultados y usa el producto final de cada etapa como inicio de la siguiente.**
- **Las ACTIVIDADES agrupan un conjunto de tareas con criterios generalmente de carácter funcional.**
- **Las TAREAS La descripción de cada Tarea especifica los siguientes conceptos:**
    - Acciones a realizar

- Actores, (que intervienen o están afectados por la cumplimentación de las acciones) productos y documentos a obtener como producto de las acciones
- Validaciones y aprobaciones a realizar de los resultados obtenidos
- Enunciado de las técnicas a emplear

El término ‘Unidades’ se utiliza en un sentido general para recoger diferentes ámbitos de la organización dentro de una Administración o Entidad (Direcciones generales, Organismos Autónomos, Subdirecciones, etc.).

3.6.3.9 ETAPAS DE MAGERIT

MAGERIT propone las cuatro Etapas siguientes:

Etapa 1. Planificación del Análisis y Gestión de Riesgos

La Etapa establece las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos; permite investigar la oportunidad de realizarlo; definir los objetivos que ha de cumplir y el dominio (ámbito) que abarcará; planificar los medios materiales y humanos para su realización; e iniciar el lanzamiento del proyecto

Etapa 2. Análisis de Riesgos

La Etapa permite identificar y valorar los elementos que intervienen en el riesgo; obtener una evaluación de éste en las distintas áreas del dominio; y estimar los umbrales de riesgo deseables.

Etapa 3. Gestión de Riesgos

La Etapa permite identificar las posibles funciones o servicios de salvaguarda reductores del riesgo detectado; seleccionar las salvaguardas aceptables en función de las ya existentes y de las restricciones; simular diversas combinaciones; y especificar las finalmente elegidas.

Etapa 4. Selección de Salvaguardas

La Etapa permite seleccionar los mecanismos de salvaguarda a implantar; elaborar una orientación del plan de implantación de los mecanismos de salvaguarda elegidos; establecer los mecanismos de seguimiento para la implantación; recopilar los documentos de trabajo del proceso de Análisis y Gestión de Riesgos; obtener los documentos finales del proyecto; y realizar las presentaciones de los resultados a los diversos niveles.

3.6.3.10 VISIÓN GLOBAL DE LAS ETAPAS DEL PROCESO MAGERIT

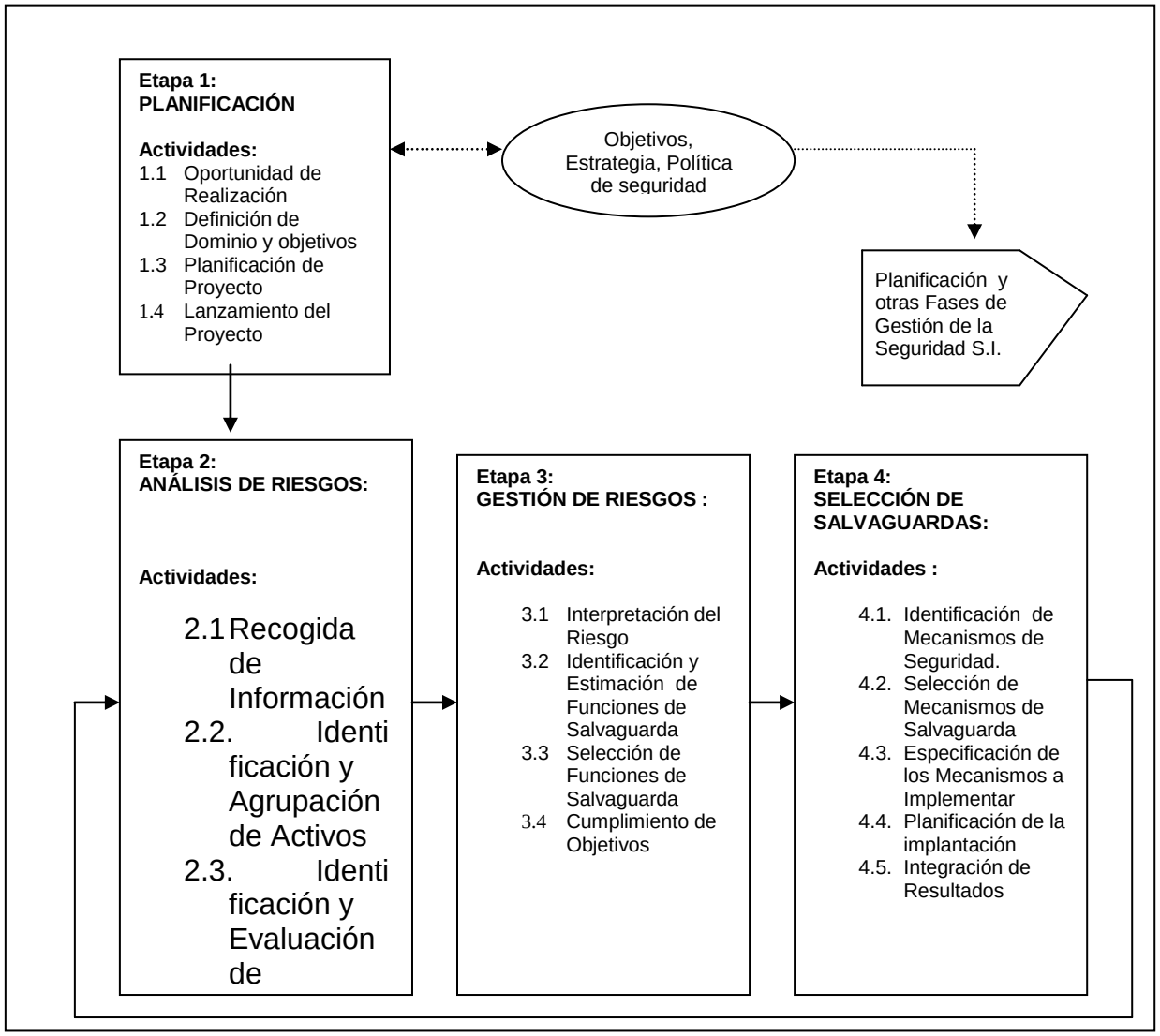


FIGURA 3.6 VISIÓN GLOBAL DE LAS ETAPAS DEL PROCESO MAGERIT

La figura 3.6 representa el Ciclo de Etapas (iterativo) del Proceso cubierto por MAGERIT que constituye la Fase de Análisis y Gestión de Riesgos dentro de la Gestión de la Seguridad de los Sistemas de Información. Así mismo se anotan los enlaces de este ciclo MAGERIT con la Fase de 'Objetivos, Estrategia y Política de Seguridad' (que es anterior y concomitante con MAGERIT) y con la Fase de 'Planificación de los Mecanismos de Salvaguarda' (que inicia el resto de la Gestión de la Seguridad). El esquema completo de Etapas, Actividades y Tareas del Submodelo de Procesos de MAGERIT es el siguiente:

ETAPA 1. PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS

Actividad 1.1: Oportunidad de Realización

- Tarea 1.1.1:(única) Clarificar la oportunidad de realización

Actividad 1.2: Definición de Dominio y Objetivos

- Tarea 1.2.1: Especificar los objetivos del proyecto
- Tarea 1.2.2: Definir el dominio y los límites del proyecto
- Tarea 1.2.3: Identificar el entorno y restricciones generales
- Tarea 1.2.4: Estimar dimensión, coste y retornos del proyecto

Actividad 1.3: Planificación del Proyecto

- Tarea 1.3.1: Evaluar cargas y planificar entrevistas
- Tarea 1.3.2: Organizar a los participantes
- Tarea 1.3.3: Planificar el trabajo

Actividad 1.4: Lanzamiento del Proyecto

- Tarea 1.4.1: Adaptar los cuestionarios
- Tarea 1.4.2: Seleccionar criterios de evaluación y técnicas para el proyecto
- Tarea 1.4.3: Asignar los recursos necesarios
- Tarea 1.4.4: Sensibilizar (campaña informativa)

ETAPA 2. ANÁLISIS DE RIESGOS

Actividad 2.1: Recogida de Información

- Tarea 2.1.1: Preparar la información
- Tarea 2.1.2: Realización de las entrevistas
- Tarea 2.1.3: Analizar la información recogida

Actividad 2.2: Identificación y Agrupación de ACTIVOS

- Tarea 2.2.1: Identificar activos y grupos de activos
- Tarea 2.2.2: Identificar mecanismos de salvaguarda existentes
- Tarea 2.2.3: Valorar activos

Actividad 2.3: Identificación y Evaluación de AMENAZAS

- Tarea 2.3.1: Identificar y agrupar amenazas
- Tarea 2.3.2: Establecer los árboles de fallos generados por amenazas

Actividad 2.4: Identificación y Estimación de VULNERABILIDADES

- Tarea 2.4.1: Identificar vulnerabilidades
- Tarea 2.4.2: Estimar vulnerabilidades

Actividad 2.5: Identificación y Valoración de IMPACTOS

- Tarea 2.5.1: Identificar impactos
- Tarea 2.5.2: Tipificar impactos
- Tarea 2.5.3: Valorar impactos

Actividad 2.6: Evaluación del RIESGO

- Tarea 2.6.1: Evaluar el riesgo intrínseco
- Tarea 2.6.2: Analizar las funciones de salvaguarda existentes
- Tarea 2.6.3: Evaluar el riesgo efectivo

ETAPA 3. GESTIÓN DE RIESGOS

Actividad 3.1: Interpretación del Riesgo

- Tarea 3.1.1:(única) Interpretar los riesgos

Actividad 3.2: Identificación y Estimación de Funciones de Salvaguarda

- Tarea 3.2.1: Identificar funciones de salvaguarda
- Tarea 3.2.2: Estimar la efectividad de las funciones de salvaguarda

Actividad 3.3: Selección de Funciones de Salvaguarda

- Tarea 3.3.1: Aplicar los parámetros de selección
- Tarea 3.3.2: Evaluar el riesgo

Actividad 3.4: Cumplimiento de Objetivos

- Tarea 3.4.1 (única): Determinar el cumplimiento de los objetivos

ETAPA 4. SELECCIÓN DE SALVAGUARDAS

Actividad 4.1: Identificación de Mecanismos de Salvaguarda

- Tarea 4.1.1: Identificar mecanismos posibles
- Tarea 4.1.2: Estudiar mecanismos implantados
- Tarea 4.1.3: Incorporar restricciones

Actividad 4.2: Selección de Mecanismos de Salvaguarda

- Tarea 4.2.1: Identificar mecanismos a implantar
- Tarea 4.2.2: Evaluar el riesgo (mecanismos elegidos)
- Tarea 4.2.3: Seleccionar mecanismos a implantar

Actividad 4.3 Especificación de los Mecanismos a Implantar

- Tarea 4.3.1 (única): Especificar los mecanismos a implantar

Actividad 4.4: Planificación de la Implantación

- Tarea 4.4.1 Priorizar mecanismos
- Tarea 4.4.2: Evaluar los recursos necesarios
- Tarea 4.4.3: Elaborar cronogramas tentativos

Actividad 4.5: Integración de Resultados

- Tarea 4.5.1 (única): Integrar los resultados

3.6.3.11 ESTRUCTURA DE LA ETAPA DE PLANIFICACIÓN

Objetivos de la Etapa

El Objetivo principal de esta etapa de planificación es establecer y definir el marco general de referencia para todo proyecto de realización de análisis y gestión de riesgos. Otros objetivos complementarios son:

- **Motivar a la Dirección de la Unidad implicada.**
- Demostrar la oportunidad de realizar un Análisis y Gestión de Riesgos.
- Afirmar y dar a conocer la voluntad política de la realización por parte de la Dirección.
- Crear las condiciones para el buen desarrollo del proyecto.

Contenido de la Etapa

Esta Etapa de Planificación de Análisis y Gestión de Riesgos se enmarca, como ocurre con cualquier otra planificación concreta, en la Planificación Estratégica de la Organización, como una concreción a corto y medio plazo de ésta. No sólo será lógico, sino conveniente, que muchos de los conceptos de esta etapa de MAGERIT retomen y readapten elementos de la Fase de Planificación de Sistemas de Información.

Así, la Planificación Estratégica de la Organización tiene como finalidad principal definir las metas de ésta a largo plazo (en cuanto a funcionalidades y servicios futuros a prestar, perspectivas de crecimiento y/o previsiones de evolución), así como estimar las necesidades de información en función de dichas metas (considerando tanto la situación de la Organización frente a su entorno, como la visión de los responsables de la misma).

Esta etapa de planificación concreta la realización táctica de las metas estratégicas definidas en la planificación estratégica, con dos grandes resultados:

- La definición precisa del proyecto de Análisis y Gestión de Riesgos y de su dominio

- **La programación ajustada para desarrollar el proyecto, teniendo en cuenta las prioridades y los recursos necesarios, es decir:**
    - La definición de la serie de hitos a considerar en el desarrollo del proyecto
    - La obtención de unos resultados que sirvan de punto de partida al desarrollo del proyecto.

Como consecuencia lógica, esta Etapa de Planificación requiere:

    - Un ámbito organizativo más restringido y un horizonte temporal más limitado
    - Un trabajo sucesivo de refinamiento y revisión a lo largo del desarrollo del proyecto, de manera que se pueda valorar el cumplimiento de su programación en el marco de metas establecidas por la Planificación Estratégica (y teniendo en cuenta que la Planificación de la Implantación de medidas de seguridad forma parte de otra Etapa de este Submodelo de Procesos).

- La participación imprescindible de los responsables de las Unidades implicadas, puesto que les corresponde definir los objetivos y las estrategias de evolución de dichas Unidades, así como patrocinar todos los trabajos encaminados a obtener la seguridad de sus sistemas como uno de los retos básicos de un entorno en constante evolución.

En resumen, el contenido de esta Etapa como marco general de referencia incluye:

- La justificación y oportunidad de abordar el proyecto.
- La definición del dominio a considerar y de los objetivos del proyecto.
- La planificación del proyecto, considerando los participantes, los recursos necesarios y el cronograma de realización.
- La particularización de las técnicas a emplear en las actividades del proyecto.

Resumen del Contenido de las Actividades

MAGERIT define en esta Etapa de Planificación del proyecto de Análisis y Gestión de Riesgos las 4 actividades siguientes:

1. **Oportunidad de Realización**

Se estudian los aspectos básicos para la realización de un proyecto de Análisis y Gestión de Riesgos, fundamentando la oportunidad de ésta. Se inicia una primera aproximación a los objetivos asignados al proyecto, al dominio -o ámbito- a incluir y a los medios necesarios para su elaboración.

2. **Definición de dominio y objetivos**

Se definen los objetivos finales del proyecto, su dominio y sus límites. Se realiza una primera identificación del entorno y de las restricciones generales a considerar. Se establecen los medios (responsables, técnicos, usuarios, etc.) a considerar para la recogida de información.

3. **Organización y Planificación del proyecto**

Se determina la carga de trabajo que supone la realización del proyecto y las características del grupo de trabajo a constituir. Se planifican las entrevistas a realizar para la recogida de información. Se establece quiénes son el resto de

participantes, así como su modo de actuación. Se elabora el plan de trabajo para la realización del proyecto.

4. Lanzamiento del proyecto

Se adaptan los cuestionarios para la recogida de información en función al entorno retenido. Se eligen las técnicas principales de evaluación de riesgo a utilizar y se asignan los recursos necesarios para el comienzo del proyecto. También se realiza una campaña informativa de sensibilización a los afectados sobre las finalidades y requerimientos en su participación.

Resultados

Documentación Intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Análisis de los resultados, con la detección de las áreas críticas claves.
- Información existente utilizable por el proyecto (por ejemplo inventario de Activos)
- Resultados de posibles aplicaciones de métodos de Análisis y Gestión de Riesgos realizadas anteriormente (por ejemplo catalogación, agrupación y valoración de activos, amenazas, vulnerabilidades, impactos, riesgo, mecanismos de salvaguarda, etc.).

Documentación final

- Informe de *"Planificación del Análisis y Gestión de riesgos"* que contendrá una síntesis de los productos obtenidos en las actividades realizadas en la etapa.

3.6.3.12 ESTRUCTURA DE LA ETAPA DE ANÁLISIS DE RIESGOS

Objetivos de la Etapa

Esta etapa tiene los siguientes objetivos:

- **Evaluar el riesgo del sistema en estudio, tanto el riesgo intrínseco (sin salvaguardas), como el riesgo efectivo (incluyendo el efecto de las salvaguardas implementadas si se trata de un sistema actual, no de un sistema previsto). Mostrar al Comité director las áreas del sistema con mayor riesgo.**
- **Presentar y obtener la aprobación de los umbrales de riesgo aceptables o asumibles.**

Contenido de la Etapa

El punto de partida de esta Etapa en el ciclo del proceso de MAGERIT es la documentación de la anterior Etapa 1 referente a los objetivos del proyecto, los planes de entrevistas, la evaluación de cargas, la composición y reglas de actuación del equipo de participantes, el plan de trabajo y el informe de presentación del proyecto. El Análisis del Riesgo identifica, evalúa y combina los Elementos definidos en el correspondiente Submodelo, con el resultado de una evaluación del Riesgo en el Dominio del proyecto que sea utilizable para la Identificación y Gestión de las Salvaguardas que puedan contrarrestar el Riesgo no asumible. La Etapa de Análisis del Riesgo sigue en cierta forma el subescenario de ataque de la vista dinámica organizativa del Submodelo de Eventos, combinando en cada uno de los pasos del subescenario operaciones relacionadas con los Elementos de seguridad. Así y tras definir más detalladamente el contenido del Dominio (es decir el conjunto de los Activos), la Etapa considera los posibles eventos (osea las Amenazas), la potencialidad de la materialización de éstas y las consecuencias de dicha materialización (los

Impactos). Con ayuda de todos estos materiales, suficientemente Identificados y evaluados, el cálculo o la estimación de los distintos tipos de riesgo es una labor bastante rutinaria, cuyos resultados (tipos de Riesgo) deberán interpretarse adecuadamente en la Etapa 3 siguiente.

Resumen del Contenido de las Actividades

1. Recogida de información

Obtención de la información sobre el sistema, de sus componentes, y de los factores que pueden influir en la seguridad.

2. Identificación y agrupación de ACTIVOS

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de los Activos en cuanto a su contribución a la evaluación del riesgo.

3. Identificación y evaluación de AMENAZAS

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de las Amenazas en cuanto a su contribución a la evaluación del riesgo.

4. Identificación y estimación de VULNERABILIDADES

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de las Vulnerabilidades en cuanto a su contribución a la evaluación del riesgo.

5. Identificación y valoración de IMPACTOS

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de los Impactos en cuanto a su contribución a la evaluación del riesgo.

6. Evaluación del RIESGO

Valoración del riesgo intrínseco y del riesgo efectivo, a partir de los resultados de las Actividades anteriores.

Resultados

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelo de datos, etc.
- Resultados de la catalogación, clasificación y valoración de activos, de salvaguardas existentes, de amenazas, de vulnerabilidades, de impactos y del riesgo obtenido.
- Análisis de los resultados, con la detección de las áreas críticas claves.

Documentación final

- Riesgo global, riesgo distribuido por áreas, áreas críticas y umbrales de riesgo.

3.6.3.13 ESTRUCTURA DE LA ETAPA DE GESTIÓN DE RIESGOS

Objetivos de la Etapa

Esta Etapa tiene por **objeto** identificar y seleccionar las funciones de salvaguarda apropiadas para reducir el riesgo a un nivel aceptable.

Contenido de la Etapa

Los puntos de partida para esta etapa están constituidos por la documentación de la etapa anterior, referida a la descripción de los componentes del riesgo (activos, funciones y mecanismos de salvaguarda

existentes, amenazas, vulnerabilidades e impactos), a los niveles de riesgos calculados y a los umbrales de riesgo aceptados por el comité director.

La métrica del Riesgo subyace a toda posible estimación de las distintas funciones de salvaguarda con 'priorización' o no entre ellas para argumentar, entre las decisiones alternativas, las que consiguen la neutralización de los riesgos de la forma más eficaz y económica posible. El especialista en seguridad es así el protagonista de esta Etapa.

Resumen del Contenido de las Actividades

1. Interpretación del Riesgo

Interpretación de los resultados generados en las actividades anteriores, orientada a descubrir las principales áreas críticas.

2. Identificación de Funciones de Salvaguarda y Estimación de su Efectividad

Identificación y estimación de la efectividad de las funciones o servicios de salvaguarda necesarias para reducir el riesgo a los umbrales aceptados.

3. Selección de las Funciones de Salvaguarda

Selección de las funciones o servicios de salvaguarda óptimos que cumplan los objetivos de reducción del riesgo.

4. Cumplimiento de Objetivos

Estudio de los riesgos residuales obtenidos por la aplicación de las funciones o servicios de salvaguarda seleccionados, para determinar si se encuentran dentro de los umbrales de riesgo elegidos.

Resultados

Documentación intermedia

- Lista de funciones y servicios de salvaguarda ordenados según su efectividad, con una descripción de sus características.
- Informe de funciones y servicios de salvaguarda existentes, estimando su efectividad.
- Informe de funciones y servicios de salvaguarda seleccionados, con justificación de cada uno.
- Nuevos valores del riesgo al aplicar las funciones y servicios de salvaguarda propuestos
- Informe del estudio comparativo de resultados en las simulaciones.

Documentación final

- Lista final de funciones y servicios de salvaguarda propuestos.

3.6.3.14 ESTRUCTURA DE LA ETAPA DE SELECCIÓN DE SALVAGUARDAS

Objetivos de la Etapa

La Etapa tiene como Objetivo la Selección de los mecanismos de salvaguarda que materialicen las funciones y servicios de salvaguarda, respeten las restricciones y reduzcan los riesgos por debajo de los umbrales deseados.

Contenido de la Etapa

Esta etapa parte de los resultados de las etapas anteriores:

- **Identificación de los mecanismos de salvaguarda implantados actualmente y de las funciones**

- **Funciones y servicios de salvaguarda seleccionados, capaces de reducir el riesgo hasta alcanzar los umbrales previamente elegidos (o bien actualizados, si se ha visto su necesidad). Por último la etapa posibilita la recopilación de todos los informes obtenidos, para generar el documento final del Análisis y Gestión de Riesgos,**

además de los documentos de presentación de resultados a los diversos niveles de la Organización.

En esta etapa, el especialista selecciona los mecanismos de salvaguarda que materialicen las funciones y servicios seleccionados, en función de la efectividad de éstos. Una vez elegidos estos mecanismos, se estudian sus relaciones, costes, tipos y otras características. Tras analizar posibles contradicciones o contraindicaciones en su aplicación, la Etapa establece un orden de prioridades para su implantación (excluida de MAGERIT), reflejado en cronogramas tentativos de puesta en práctica.

Resumen del Contenido de las Actividades

Las actividades de esta Etapa son:

- Identificación de los mecanismos.- Se identifican de los mecanismos que puedan materializar las funciones y servicios de salvaguarda.

- **Selección de mecanismos de salvaguarda.- Se seleccionan y estudian los mecanismos de salvaguarda anteriores que cumplan las restricciones y alcancen una efectividad suficiente en la reducción del nivel de riesgo.**

- **Especificación de los mecanismos a implantar.- La tarea especifica para los mecanismos de salvaguarda seleccionados ciertas características importantes.**

- **Orientación a la planificación de la Implantación.- La priorización de los mecanismos seleccionados junto a la estimación de los recursos necesarios permiten realizar una aproximación a los cronogramas de implantación.**

- **Integración de resultados.- En esta actividad final se recopilan los informes de Etapa para generar el informe final y los documentos correspondientes para realizar presentaciones a diversos niveles.**

Resultados

Documentación intermedia

- Documentos relativos a los mecanismos seleccionados y sus características, su modo de implantación y los recursos necesarios para ésta.

Documentación final

- Documento principal del trabajo realizado: "Informe final del Análisis y Gestión de Riesgos"

3.7 ANÁLISIS DE LA HERRAMIENTA RIS2K

La herramienta RIS2K permite implementar la mayoría de los conceptos y procesos propuestos por la metodología MAGERIT con relación al Efecto 2000.

La proximidad del año 2000 ha puesto de manifiesto el riesgo existente de que los sistemas informáticos fallen o realicen tratamientos erróneos debido al empleo de formatos de fecha para el año con sólo dos posiciones. A ello hay que añadir la posible no consideración del año 2000 como bisiesto.

Como consecuencia, un número indeterminado pero aparentemente alto de los sistemas de información y de control del tipo más diverso, están potencialmente amenazados por el Efecto 2000. Afrontar con garantía de éxito este problema requiere identificar y evaluar los riesgos para, a continuación, emprender las acciones precisas para reducir o, mejor, eliminar dichos riesgos.

RIS2K es una ayuda para decidir qué medidas de salvaguarda son las más apropiadas para reducir el riesgo al mínimo tolerable. A tal fin, RIS2K relaciona activos, amenazas y vulnerabilidades, calcula el riesgo y posibilita, mediante simulaciones, seleccionar las salvaguardas que reduzcan el riesgo a ese mínimo aceptable.

Así mismo, RIS2K propone un esquema (que se funda en el análisis y la gestión de los riesgos) para elaborar los planes de contingencia, es decir, la preparación metódica de tareas para reaccionar en el caso de que los sistemas no se comporten según lo esperado.

RIS2K es un programa interactivo, fácil de manejar con un ambiente de trabajo similar a Word o cualquier otro programa. RIS2K para realizar gestión de riesgos maneja activos, amenazas, salvaguardas, vulnerabilidades e impactos los cuales describimos a continuación:

Activos

RIS2K permite identificar y valorar los activos componentes de un sistema de información posibilitando asociar activos con grupos de activos. Permite realizar el Alta, Baja o Modificación de los activos.

Muchas veces es difícil valorar económicamente un activo. RIS2K presenta la opción parámetros, dentro de esta opción creamos una tabla de correspondencias entre los valores de una escala cualitativa de 0 a 10 y magnitudes económicas, que identifican el valor relativo de un activo asociándolo a una magnitud económica.

La valoración del riesgo depende en gran medida del valor del activo amenazado. De este valor, de la ubicación dentro del árbol de activos, de la vulnerabilidad del activo ante distintas amenazas y del impacto que causa la materialización de estas amenazas, se obtendrá el riesgo ante estas amenazas.

Agrupación/Agrupamiento de Activos

La Agrupación de Activos constituye una forma de definir un conjunto de activos que se quiere agrupar por un concepto distinto al de Grupo de Activos en que todos los activos corresponden al mismo tipo dentro de los cinco grandes tipos considerados por la metodología MAGERIT (ya tratados anteriormente).

De esta forma bajo el concepto agrupación se permite crear conjuntos de activos que pueden ser afectados por un determinado tipo de amenaza de una forma simultanea. Por ejemplo, si consideramos todos los activos que están situados en la sala de ordenadores, edificio, departamento, etc., son activos que cada uno de ellos puede pertenecer a un grupo distinto con relación a los restantes dentro de la agrupación hardware, software, equipo auxiliar, documentación, etc.- y que pueden ser atacados simultáneamente por una amenaza común incendio, inundación, etc.

En este caso se debería definir en la pantalla de agrupación la denominada: Sala de ordenadores, o departamento, y bajo agrupamiento se deberán incluir todos los activos de grupos de activos iguales o distintos, definidos previamente, de que se compone este agrupamiento.

Amenazas

Este proceso identifica los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. A través de esta opción, el usuario podrá asociar a la amenaza, grupos de amenaza, tipos de amenaza, activos y funciones que reducen la vulnerabilidad y el impacto de la amenaza sobre el activo. Permite realizar el Alta, Baja o Modificación de las Amenazas.

Amenazas por Grupo de Activos

Este proceso permite la creación de pares amenaza/activo de forma masiva, de forma que al proporcionar una amenaza y un grupo de activos, se genera un par amenaza/activo por cada activo perteneciente al grupo de activos seleccionado.

Grupos de amenazas

Esta clasificación permite y describe la agrupación de amenazas por su origen (accidentales, errores, intencionadas). Permite realizar el Alta, Baja y Modificación de los grupos de amenazas.

Tipos de Amenazas

Esta clasificación permite y describe la tipificación de amenazas por su efecto sobre los estados de la seguridad (disponibilidad, integridad, confidencialidad, autenticación). RIS2K permite realizar el Alta, Baja y Modificación de los tipos de Amenazas.

Salvaguardas

Las salvaguardas son acciones para reducir el riesgo que pude sufrir un activo determinado.

Funciones de Salvaguarda

Este proceso identifica las funciones o servicios de salvaguarda capaces de actuar contra las amenazas. Permite asociar mecanismos de salvaguarda existentes a las funciones de salvaguarda. Permite realizar el Alta, Baja y Modificación de las de funciones de salvaguarda.

Mecanismos de Salvaguarda

Permite identificar y valorar los dispositivos capaces de reducir el riesgo. También se identifican los mecanismos existentes en la organización y se establecen las relaciones con otros mecanismos,

agrupando los mecanismos que son complementarios e identificando los excluyentes.

- **Mecanismos complementarios:.- Puede crear grupos con mecanismos complementarios, que luego se utilizarán en la proposición de salvaguardas y en el proceso de simulación. Todos los mecanismos complementarios se incluirán en un mismo grupo.**
- **Mecanismos excluyentes: Puede dar para un mecanismo sus excluyentes, que luego se utilizarán en la proposición de salvaguardas y en el proceso de simulación**

Tipos de Funciones de Salvaguarda

Esta clasificación permite y describe la tipificación de funciones de salvaguarda por funcionalidad (Detección, Disuasión, Prevención, Corrección, Recuperación, Monitorización, Concienciación, Información).

Luego de ingresar todos los datos mencionados y descritos anteriormente la herramienta procede al Calculo de los Riesgos (efectivo, simulado, residual e intrínsico).

Cálculo del Riesgo Efectivo

Se calcula el riesgo efectivo, para lo cual hay que considerar la efectividad de las funciones de salvaguarda, obtenida por la implementación de los mecanismos que se han detectado como existentes. Una vez conocida la efectividad de las funciones se evalúa su capacidad para disminuir el riesgo y se aplica a los activos amenazados.(Se llama riesgo efectivo al nivel del riesgo resultante una vez aplicadas las salvaguardas existentes en el sistema de información).

En la pantalla aparecerá una relación de los mecanismos (código y descripción). A través de una serie de columnas MAGERIT informa sobre

qué mecanismos existen. Al mismo tiempo se ofrece la posibilidad de establecer el grado de implementación, ya que pueden existir mecanismos no implementados en su totalidad.

Una vez establecido el grado de implementación, se puede proceder a calcular el riesgo efectivo. La formula es la siguiente:

Riesgo Efectivo (RE) = Vulnerabilidad Disminuida (VD) * Impacto Disminuido (ID)

Cálculo del Riesgo Intrínseco

Se calcula el riesgo intrínseco de cada activo amenazado, teniendo en cuenta la degradación que la amenaza puede producir en el activo y el valor relativo o dependencia acumulada del activo en el árbol de activos, así como la propia vulnerabilidad del activo.(Se llama riesgo intrínsico al nivel del riesgo que de por si contiene el activo antes de aplicar las salvaguardas). Aquí es importante conocer lo que es un Árbol de Activos.

Árbol de Activos .- **En este proceso se establecen las relaciones y dependencias entre activos, posibilitando la construcción del árbol. La misión del árbol de activos es servir de base para calcular la propagación de riesgos entre activos.**

- **Activo padre es aquel que puede verse afectado si una amenaza se materializase en alguno de sus activos hijo.**
- **Activo hijo es aquel que, si se materializa una amenaza sobre él, provoca disfunciones sobre el activo padre al cual pertenece.**

La formula para el cálculo es la siguiente:

Riesgo Intrínseco (RI)= Impacto (I) * Vulnerabilidad (V)

Riesgo Residual.

Se le llama riesgo residual al nivel de riesgo resultante una vez aplicadas las salvaguardas propuestas por MAGERIT. La formula para el calculo es la siguiente:

Riesgo Residual (RR)= Vulnerabilidad Máxima (VM)* Impacto Máximo(IM)

Simulación

En este proceso, se calcula el riesgo de simulación, para lo cual hay que considerar la efectividad de las funciones de salvaguarda, obtenida por la implementación de los mecanismos que se han seleccionado para la simulación. Una vez conocida la efectividad de las funciones se evalúa su capacidad para disminuir el riesgo y se aplica a los activos amenazados.

En la pantalla aparecerá una relación de los mecanismos (código y descripción). A través de una serie de columnas MAGERIT informa sobre qué mecanismos existen y cuáles han sido propuestos. Al mismo tiempo se ofrece la posibilidad de seleccionar aquellos mecanismos que se van a utilizar para la simulación, es decir para calcular el riesgo de simulación. Opcionalmente es posible añadir a la selección los mecanismos complementarios y descartar los mecanismos excluyentes. La formula para el cálculo es la siguiente:

Riesgo Simulado (RS)= Vulnerabilidad Disminuida (VD) * Impacto Disminuido (ID)

Riesgo de Simulación.

Se le llama riesgo de simulación al nivel de riesgo resultante una vez introducidos los cambios en los componentes del sistema a través de las simulaciones.

3.8 ANÁLISIS DE LA HERRAMIENTA CHINCHON

La herramienta CHINCHON ha sido elaborada por el Dr. José Antonio Mañas profesor de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid en 1998.

El software consiste en una herramienta para el análisis de riesgo bajo la metodología Magerit. CHINCHON analiza cuantitativamente el riesgo de un sistema de información. La entrada de datos se escribe en XML, y realiza un análisis de la posición de riesgos, sirviendo de apoyo a su gestión. De momento CHINCHON no incluye ninguna facilidad para generar los modelos en formato XML. La salida del análisis realizado por CHINCHON consiste en:

- Listados en HTML (visibles en cualquier navegador estándar)
- Resultados para importar en hojas de cálculo (exel)

Los derechos de propiedad intelectual pertenecen al autor quien ha puesto la herramienta en el dominio público. CHINCHON además interactúa con RIS2K ya que tiene como objeto intercambiar el modelo de datos:

- Importa datos exportados por RIS2K
- Exporta datos para importar en RIS2K

CHINCHON es una herramienta muy poco conocida en materia de gestión de riesgos por lo tanto no se tiene a la mano mucha información que facilite su conocimiento.

La herramienta CHINCHON sigue el modelo MAGERIT.

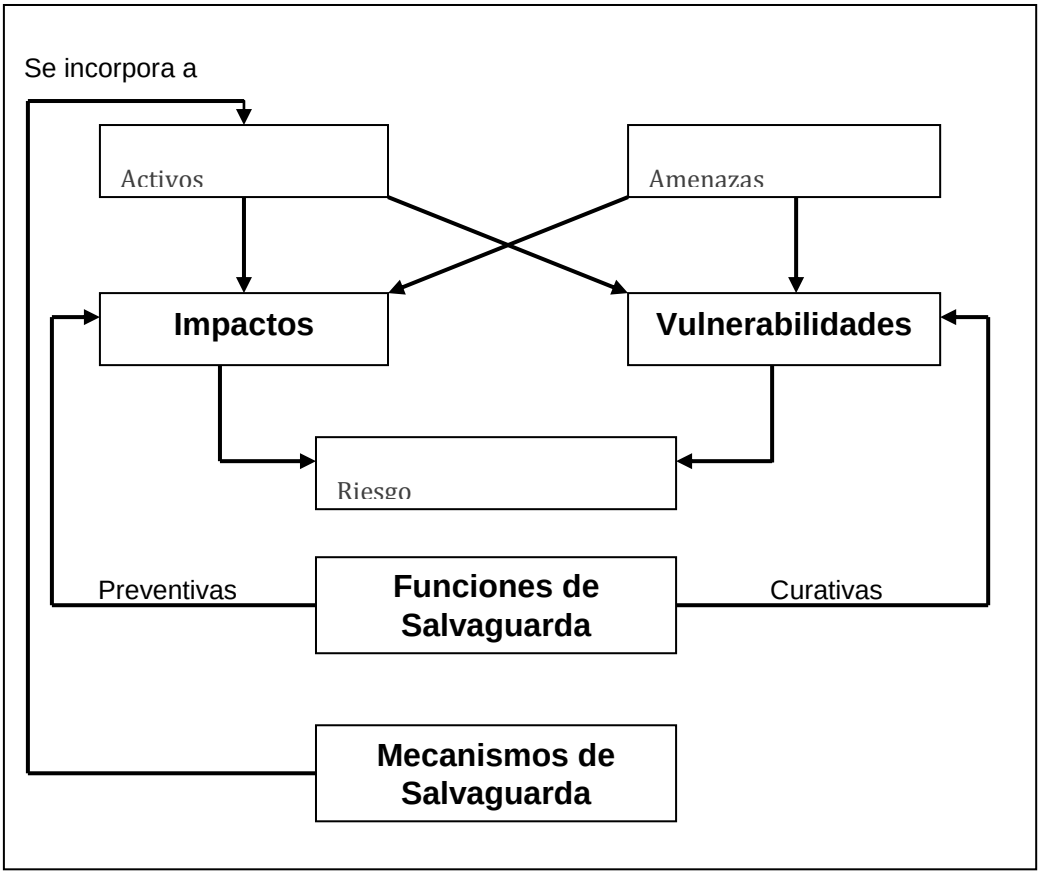


FIGURA 3.7 MODELO MAGERIT

Componentes del Modelo

- Activos
- Amenazas

- Funciones de Salvaguarda
- Mecanismos de Salvaguarda

Agrupamientos

- Grupos de Activos
- Grupos de Amenazas
- Grupos de Funciones
- Grupos de Mecanismos

Relaciones entre Componentes

- Dependencia entre activos
- Efecto de las amenazas sobre los activos
- Mitigación de las amenazas gracias a las funciones de salvaguarda
- Provisión de las funciones por medio de mecanismos de salvaguarda

Criterios Cualitativos de Valoración

- Valoración de activos
- Grado de dependencia entre activos
- Vulnerabilidad de un activo frente a una amenaza
- Degradación de un activo por causa de una amenaza
- Disminución de la vulnerabilidad gracias a una salvaguarda
- Disminución del impacto gracias a una salvaguarda
- Coste de las salvaguardas
- Coste de los mecanismos de salvaguarda

Uso

Para utilizar chinchon se requiere un runtime de Java 2, y conocimientos de XML para el ingreso de datos.

Valoraciones

La especificación de un sistema de información para proceder a su análisis de riesgo supone la introducción de multitud de datos numéricos que alimentan las funciones matemáticas.

Muchos de estos valores numéricos son meras estimaciones cualitativas. Por ello, la herramienta prevé una serie de nombres simbólicos para recoger los niveles cualitativos más frecuentes.

La especificación de parámetros de valoración es opcional, en su conjunto y en sus componentes.

Activos

Chinchon reconoce a los activos como los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Los activos se organizan en grupos, simplemente a efectos de clasificación.

Grupos de Activos

Un grupo puede contener activos o, a su vez, más grupos, permitiendo una clasificación a tantos niveles como sea pertinente en cada caso.

Amenazas Sobre los Activos

Cuando una amenaza se materializa sobre un activo, éste se ve perjudicado.

Amenazas

Chinchon define a la amenazas como los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las amenazas se organizan en grupos, simplemente a efectos de clasificación.

Grupos de Amenazas

Un grupo puede contener amenazas o, a su vez, más grupos, permitiendo una clasificación a tantos niveles como sea pertinente en cada caso.

Mecanismos para Proveer Funciones

Para disponer de las funciones de salvaguardas se necesitan mecanismos de salvaguarda concretos.

Funciones de Salvaguarda

Las funciones de salvaguarda son acciones para reducir un riesgo; pueden ser de tipo actuación u omisión. Las funciones se organizan en grupos, simplemente a efectos de clasificación.

Grupos de Funciones de Salvaguarda

Un grupo puede contener funciones o, a su vez, más grupos, permitiendo una clasificación a tantos niveles como sea pertinente en cada caso.

Las funciones de salvaguarda se implantan para mitigar el efecto potencial de las amenazas.

Funciones para Mitigar Amenazas

Para mitigar el efecto de las amenazas se despliegan funciones de salvaguarda. Las funciones preventivas (PR) reducen la vulnerabilidad de los activos, mientras que las funciones curativas (CU) reducen la degradación. Hay funciones de carácter mixto (PC).

Las funciones se materializan en mecanismos de salvaguarda:.

- Una función preventiva (PR) se ejerce como acción sobre la vulnerabilidad, previniendo su ocurrencia.
- Una función curativa (CU) actua sobre el impacto, reduciendo el efecto de la agresión.
- Una función preventiva/curativa (PC) previene la ocurrencia y reduce el impacto.

Grupos de Funciones de Salvaguarda

Un grupo puede contener funciones o, a su vez, más grupos, permitiendo una clasificación a tantos niveles como sea pertinente en cada caso.

Grupos de Mecanismos de Salvaguarda

Un grupo puede contener funciones o, a su vez, más grupos, permitiendo una clasificación a tantos niveles como sea pertinente en cada caso.

Cálculo del Riesgo Intrínseco

Valor del riesgo si no se aplicara ninguna salvaguarda. Se estima como el impacto ponderado por la vulnerabilidad (probabilidad de que ocurra). La formula para el calculo es la siguiente:

Riesgo Insico (RI) = Impacto (I) * Vuerabilidad(V);

Cálculo del Riesgo Efectivo

Valor del riesgo si se aplican las salvaguardas existentes. Toma en consideración la disminución del impacto y la disminución de la vulnerabilidad. La formula para el calculo es la siguiente

Riesgo Efectivo (RE) = Vulnerabilidad Disminuida (VD) * Impacto Disminuido (ID)

Cálculo del Riesgo Mínimo

Valor del riesgo si se aplicaran al 100% todas las salvaguardas conocidas. Toma en consideración la disminución del impacto y la disminución de la vulnerabilidad. La formula para el calculo es la siguiente:

Riesgo Mínimo (RM) = Disminución Impacto (DI) * Disminución Vulnerabilidad (DV)

Cálculo del Riesgo Intrínseco

Valor acumulado del riesgo intrínseco de todas las amenazas sobre este activo. La formula para el calculo es la siguiente:

*Riesgo Intrínseco (RI)= Impacto (I) * Vulnerabilidad (V)*

3.9 ANÁLISIS COMPARATIVO ENTRE LA HERRAMIENTA RIS2K Y CHINCHON

Semejanzas:

- CHINCHON y RIS2K son herramientas de Análisis y Gestión de Riesgos
- CHINCHON y RIS2K calculan el riesgo cuantitativamente
- CHINCHON y RIS2K utilizan las mismas formulas para el calculo de riesgos.
- CHINCHON y RIS2K siguen la metodología MAGERIT para el Análisis y Gestión de Riesgos de los Proyectos Software
- CHINCHON y RIS2K toman como base el modelo propuesto por Magerit para la Gestión de Riesgos.

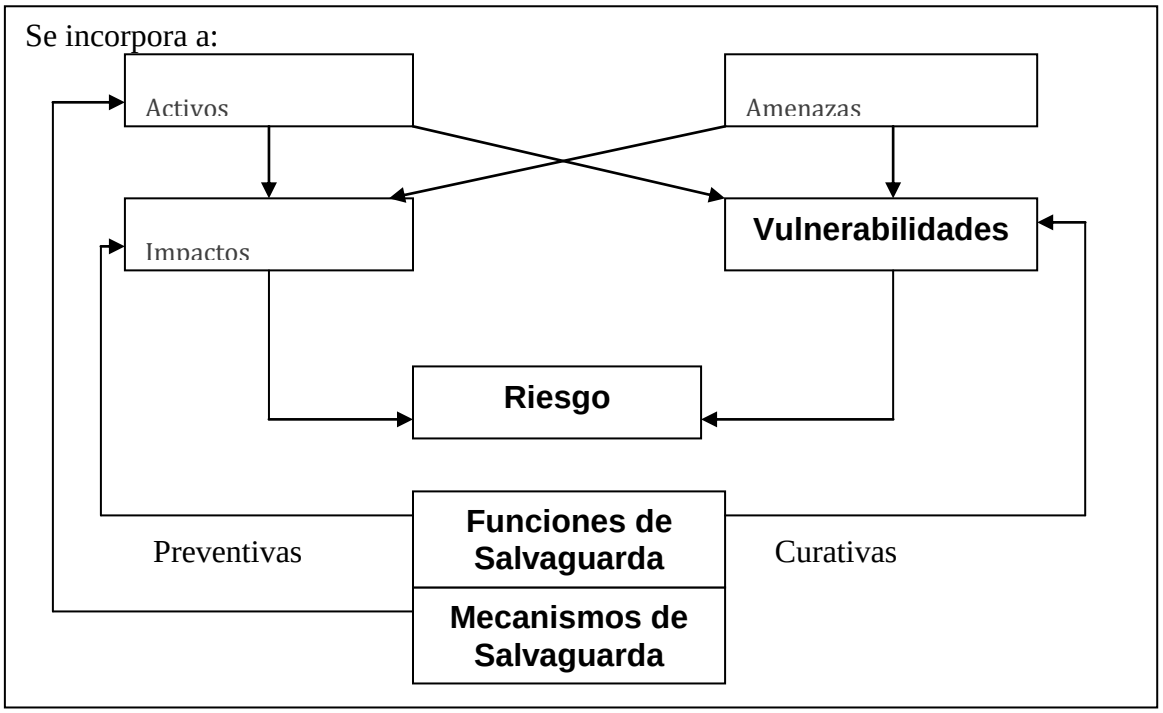


FIGURA 3.7 MODELO MAGERIT

- CHINCHON y RIS2K manejan Activos, Amenazas y Salvaguardas para calcular el riesgo

- CHINCHON y RIS2K permiten hacer Altas, Bajas o Modificaciones de Activos, Amenazas y Salvaguardas

- CHINCHON y RIS2K presentan resultados certeros sobre los Riesgos que pude sufrir un Proyecto Software.

- CHINCHON Y RIS2K presentan los resultados gráficamente para una mejor comprensión e interpretación de los resultados.

- CHINCHON y RIS2K son de distribución gratuita y los podemos encontrar en la pagina http://www.csi.map.es

Diferencias:

RIS2K	CHINCHON
Creado por el Ministerio de la Administraciones Públicas de España (MAP)	Creado por el Dr. José Antoño Manñas profesor de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Escuela Politécnica de Madrid
Funciona independientemente de otros lenguajes de programación.	Para su funcionamiento necesita interactuar con Java 2.1 y XML
El ambiente de trabajo es similar a Windows	El ambiente de trabajo es similar al

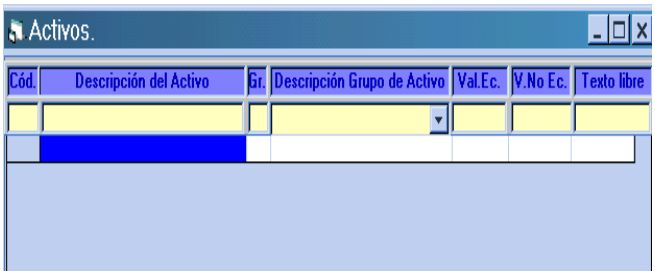
<table>
<tr><td></td><td>lenguaje de programación C++</td></tr>
<tr><td>Para empezar a utilizar RIS2K no se necesita previos conocimientos de otros lenguajes de programación.</td><td>Para empezar a manejar CHINCHON es necesario conocer sobre el funcionamiento y manejo de Java 2.1 y XML.</td></tr>
<tr><td>La valoración de activos, amenazas, salvaguardas se lo hace en cifras numéricas y/o porcentajes según el caso. Es importante mencionar que en algunos casos ingresa el usuario los valores mientras que en otros el sistema mismo se encarga de asignar los valores.

POR EJEMPLO:
Al ingresar los mecanismos de salvaguarda en la herramienta se necesita ingresar el mecanismo y el grado de cumplimiento del mismo. Este valor se ingresa en porcentaje y no tiene un rango especifico.</td><td>La valoración de activos, amenazas, salvaguardas se lo hace en códigos que reemplazan a la valoración numérica

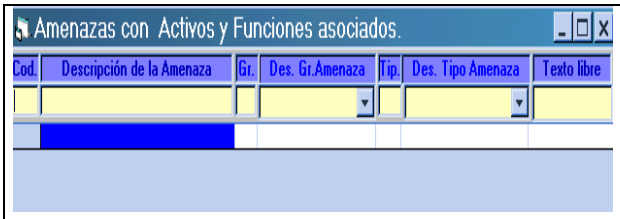
POR EJEMPLO:

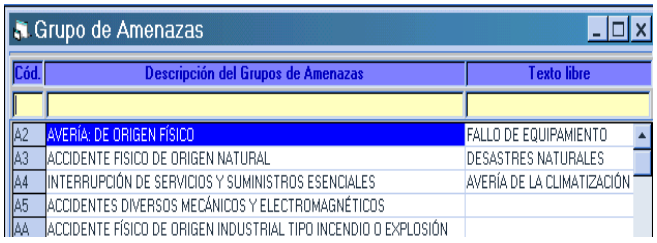
<table><tr><th>código</th><th>valor</th><th>código</th><th>valor</th></tr><tr><td>M</td><td>100</td><td>F</td><td>2%</td></tr><tr><td>M+</td><td>120</td><td>F+</td><td>2.4%</td></tr><tr><td>M-</td><td>80</td><td>F-</td><td>1.6%</td></tr></table>TABLA 3.1 VALORACIONES DE LOS ACTIVOS EN CHINCHON

La asignación de un código resulta en ocasiones molesta pues se desearía especificar "algo más que" o "algo menos que". Para estas ocasiones se puede añadir un carácter adicional: "+" para indicar un 20% arriba, "-" para indicar un 20% abajo.</td></tr>
<tr><td></td><td></td></tr>
</table>

RIS2K permite identificar y valorar los activos componentes de un sistema de información posibilitando asociar activos con grupos de activos.	Chinchon reconoce a los activos como los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Los activos se organizan en grupos simplemente a efectos de clasificación.
El ingreso de activos en RIS2K se lo realiza de la siguiente manera. ▪ En la Barra de Herramientas se encuentra la opción Datos y dentro de esta la opción Activos se da un clic sobre esta opción y se presenta una pantalla para el ingreso de los datos correspondientes al Activo.  	El ingreso de activos en Chinchon se lo realiza mediante el Lenguaje XML de la siguiente manera: <activos cod="xxx" [opcional] valor="nnn" [opcional] > nombre del grupo <activos> ... </activos> ... <activo ... > ... </activo> ... </activos>
Para ingresar un grupo de activos y árbol de activos se realiza el mismo procedimiento.	**En CHINCHON no es necesario especificar el árbol de activos pero si los grupos de activos y se lo realiza de la manera descrita en el Ejemplo:** <activos cod="I1">

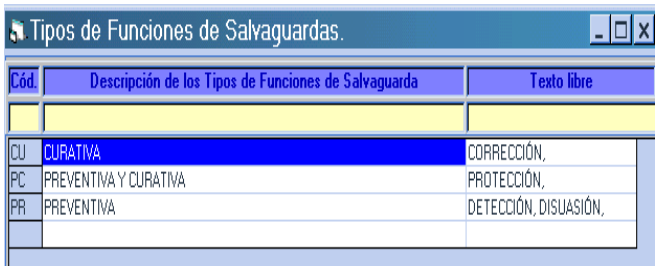
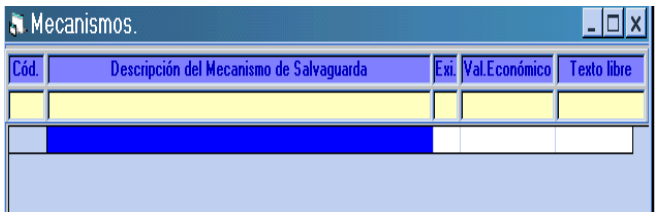
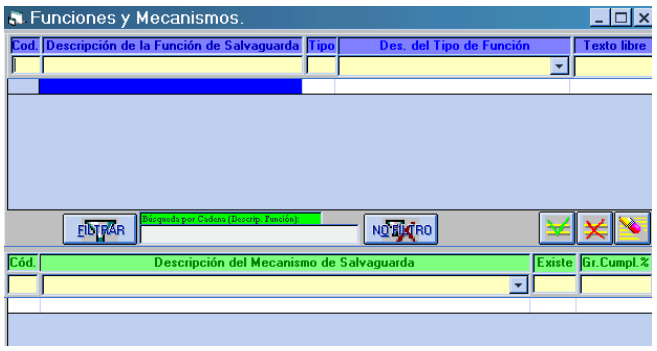
	Información <activocod="0051"valor="1000000"> Datos de la gestión de expedientes </activo> <activo cod="0053" valor="700000"> Ficheros de información </activo> </activos>
RIS2K define a las amenazas como procesos que identifican los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. A través de esta opción, el usuario podrá asociar a la amenaza, grupos de amenaza, tipos de amenaza, activos y funciones que reducen la vulnerabilidad y el impacto de la amenaza sobre el activo.	Chinchon define a la amenazas como los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. Las amenazas se organizan en grupos simplemente a efectos de clasificación.
El ingreso de amenazas a la herramienta RIS2K se lo realiza de la siguiente manera: ▪ Dentro de la barra de Herramientas se encuentra la opción Datos y dentro de esta la opción Amenazas para seleccionar esta opción se da un clic sobre la misma e ingresamos la información. Ejemplo	El ingreso de amenazas se lo realiza en XML de la siguiente manera: <amenazas cod="xxx" [opcional] v="x%" [opcional] d="x%" [opcional] >

<table>
<tr>
<td> 
</td>
<td>nombre del grupo
<amenazas> ... </amenazas>
...
<amenaza ... > ... </amenaza>
...
</amenazas></td>
</tr>
<tr>
<td>Para ingresar los Grupos de Amenazas seguimos el procedimiento anterior y finalmente se ingresa todos los datos que requiere la nueva ventana.

 
</td>
<td>El ingreso de los Grupos de amenazas se realiza siguiendo el procedimiento anterior.
EJEMPLO:

<amenazas cod="P3">
acceso lógico no autorizado, con alteración o sustracción de la información
<amenaza cod="021" tipo="A">
acceso no autorizado a recursos y servicios
</amenaza>
<amenaza cod="008" tipo="C">
sustracción de información
</amenaza>
<amenaza cod="023" tipo="I">
modificación de información
</amenaza>
<amenaza cod="024" tipo="I">
modificación de programas
</amenaza>
</amenazas></td>
</tr>
<tr>
<td>Funciones de Salvaguarda</td>
<td>Funciones de salvaguarda</td>
</tr>
</table>

Este proceso identifica las funciones o servicios de salvaguarda capaces de actuar contra las amenazas. Permite asociar mecanismos de salvaguarda existentes a las funciones de salvaguarda. Permite realizar el Alta, Baja y Modificación de las de funciones de salvaguarda.	***Las funciones de salvaguarda son acciones para reducir un riesgo; pueden ser de tipo actuación u omisión. Las funciones se organizan en grupos simplemente a efectos de clasificación.***
Mecanismos de Salvaguarda **Permite identificar y valorar los dispositivos capaces de reducir el riesgo. También se identifican los mecanismos existentes en la organización y se establecen las relaciones con otros mecanismos, agrupando los mecanismos que son complementarios e identificando los excluyentes.** **Mecanismos complementarios:.- Puede crear grupos con mecanismos complementarios, que luego se utilizarán en la proposición de salvaguardas y en el proceso de simulación. Todos los mecanismos complementarios se incluirán en un mismo grupo.** Mecanismos excluyentes: Puede dar para un mecanismo sus excluyentes, que luego se utilizarán en la proposición de salvaguardas y en el proceso de simulación **Tipos de Funciones de Salvaguarda** **Esta clasificación permite y describe la tipificación de funciones de salvaguarda**	En Chinchon las funciones se materializan en mecanismos de salvaguarda. Una función preventiva (PR) se ejerce como acción sobre la vulnerabilidad, previniendo su ocurrencia. Una función curativa (CU) actúa sobre el impacto, reduciendo el efecto de la agresión. Una función preventiva/curativa (PC) previene la ocurrencia y reduce el impacto.

por funcionalidad (Detección, Disuasión, Prevención, Corrección, Recuperación, Monitorización, Concienciación, Información).	
Para ingresar las salvaguardas, mecanismos de salvaguardas, funciones de salvaguardas realizamos el siguiente proceso: - Dentro de la barra de Herramientas se encuentra el menú Datos y dentro de esta las opciones: Salvaguarda, Mecanismos de Salvaguarda, Funciones de Salvaguarda para seleccionar estas opción se da un clic sobre las mismas y se ingresan los datos correspondientes. Ejemplo:    	Para ingresar las salvaguardas, mecanismos de salvaguarda, funciones de salvaguardas realizamos el siguiente procedimiento en XML: ***Formato*** <funcion-mecanismo> <fm fun="xxx" mec="xxx" grado="nnn" /> ... </funcion-mecanismo> ***Ejemplo*** <funcion-mecanismo> <fm fun="FNC1" mec="MEC1" grado="30%" /> <fm fun="FNC1" mec="MEC2" grado="30%" /> <fm fun="FNC1" mec="MEC3" grado="40%" /> <fm fun="FNC2" mec="MEC3" grado="60%" /> <fm fun="FNC2" mec="MEC4" grado="20%" /> <fm fun="FNC2" mec="MEC5" grado="20%" />

	<fm fun="FNC3" mec="MEC6" grado="50%" /> <fm fun="FNC3" mec="MEC7" grado="50%" /> </funcion-mecanismo> ***Formato*** <funciones cod="xxx" [opcional] coste="nnn" [opcional] e="x%" [opcional: "100%"] > nombre del grupo <funciones> ... </funciones> ... <funcion ...> ... </funcion> ... </funciones> ***Ejemplo*** <funciones cod="POLICY"> Organizational security policies <funcion cod="P.Audit" tipo="CU"> Audit </funcion> <funcion cod="P.Crypt_Std" tipo="PC"> Cryptographic standards </funcion> </funciones> Las funciones de salvaguarda se implantan

	para mitigar el efecto potencial de las amenazas.
RIS2K calcula el riesgo efectivo, riesgo intrínseco, riesgo residual y riesgo simulado que pueden sufrir un activo.	CHINCHON calcula el riesgo efectivo, el riesgo intrínsico y el riesgo mínimo que puede sufrir un activo.

CAPITULO IV

El presente capitulo trata sobre la construcción misma del software. Inicia con la Especificación de Requisitos Software, Definición de los Casos de Uso de Alto Nivel y la Definición del Modelo Conceptual.

A continuación se desarrolla la Fase de Análisis en donde se vera la Definición de los Casos de Uso Expandidos, Diagramas de Caso de Uso, Diagramas de Secuencia, Definición de los Contratos de Operación y Diagramas de Colaboración. En la fase de diseño se verá los diagramas de objetos. En la fase de implementación se verá el diagrama de clases.

Finalmente se realizaran las pruebas al sistema que se desarrolló.

4.- DESARROLLO DE LA HERRAMIENTA DE GESTIÓN DE RIESGOS DE PROYECTOS SOFTWARE

Para el desarrollo de la Herramienta de Gestión de Riesgos de Proyectos Software se utilizará la Metodología Orientada a Objetos UML por su fácil utilización y entendimiento en el desarrollo de Software.

4.1 Especificación de Requisitos Software

4.1.1 Introducción

Este documento es una especificación de requisitos software (ERS) para el Sistema de Gestión de Riesgos de Proyectos Software la documentación ha sido elaborada de acuerdo a la metodología de análisis y gestión de riesgos MAGERIT. Esta especificación de requisitos se ha estructurado tomando cómo base las directrices dadas por el standard “IEEE Recommended Practice for Software Requerements Specification ANSI/IEEE 830 1998”

4.1.2 Propósito.

El objeto del presente documento es definir de manera clara y precisa todas las funcionalidades y restricciones del sistema a ser desarrollado, el cual deberá: Presentar los posibles riesgos que puede afectar a un proyecto software, lo que implica que deberá soportar, Gestión de Grupos de Activos, Gestión de Activos, Gestión de Árbol de Activos, Gestión de Grupos de Amenazas, Gestión de Tipos de Amenazas, Gestión de Mecanismos de Salvaguarda, Gestión de Tipos y Funciones de Salvaguardas, Gestión Amenazas, Gestión Amenazas por Función de Salvaguarda, Gestión de Amenazas por Activos, Gestión Funciones por Mecanismos de Salvaguarda, Gestión Parámetros, Gestión Eliminar Información, Gestión Cálculo del riesgo Efectivo, Gestión Calculo del Riesgo Intrínsico, Gestión Calculo del riesgo Residual, Gestión Calculo del riesgo Simulado, Gestión de Resultados, Gestión Gráficos.

4.1.3 Ámbito del Sistema.

El sistema recibirá el nombre de Sistema de Gestión de Riesgos de Proyectos Software

El motor que impulsa la realización del presente sistema es la necesidad de conocer con anterioridad los constantes problemas que se suscitan al realizar proyectos ya sea en cuanto a tiempo, recursos materiales, recursos humanos, espacio físico, limitaciones tecnológicas, etc.

La situación de partida es que existe dos sistemas informáticos que cubren las actividades de Gestión de Riesgos de Proyectos Software estos son: RIS2K y CHINCHON de los mismos que se van a extraer las ventajas para crear la nueva herramienta denominada Sistema de Gestión de Riesgos de Proyectos Software

El sistema será fácil de manejar por los usuarios que lo requieran, los resultados que mostrara serán veraces y confiables.

4.1.4 Definiciones, Acrónimos y Abreviaturas.

Definiciones

Usuario	Persona que usa el sistema para realizar gestión de riesgos de un determinado proyecto software.

Tabla 4.1 Definiciones

Acrónimos

ERS	Especificación de requisitos de Software
ARS	Análisis de requisitos del Sistema

Tabla 4.2 Acrónimos

Abreviaturas

Ris2k	Herramienta para el Análisis y Gestión de riesgos bajo la metodología magerit

	desarrollado por el Ministerio de las Administraciones Públicas de España.
Chinchon	Herramienta de Análisis y Gestión de Riesgos bajo la metodología magerit desarrollado por Dr. José Antoño Mañas profesor de la Escuela Politécnica de Madrid

Tabla 4.3 Abreviaturas

4.1.5 Referencias

IEEE Recommended Practice for Software Requeriments Specification. ANSI/IEEE std 830, 1998.

4.1.6 Visión General del Documento

Este documento consta de tres secciones, esta sección es la introducción y proporciona una visión general de la ERS. En la sección 2 se da una descripción general del sistema, con el fin de conocer las principales funciones que debe realizar, los datos asociados y los factores, restricciones y dependencias que afectan al desarrollo, en la sección 3 se detallan los requisitos que debe satisfacer el sistema.

4. 2 Descripción General

En esta sección nos presenta una descripción general del sistema, con el fin de conocer las principales funciones que debe realizar, los datos asociados, las restricciones impuestas, y cualquier factor que pueda afectar al desarrollo del mismo.

4.2.1 Perspectiva del Producto

El sistema en esta versión, no interactuará con ningún otro sistema informático.

4.2.1.1 Funciones del Sistema

En términos generales, el sistema deberá proporcionar soporte a las siguientes tareas de gestión.

- Gestión de Grupos de Activos
- Gestión de Activos
- Gestión de Árbol de Activos
- Gestión Grupos de Amenazas
- Gestión Tipos de Amenazas
- Gestión Mecanismos de Salvaguarda
- Gestión Tipos de Funciones de Salvaguarda
- Gestión Funciones de Salvaguarda
- Gestión de Amenazas
- Gestión de Amenaza por Función de Salvaguarda
- Gestión de Amenazas por Activo
- Gestión Funciones por Mecanismos de Salvaguarda
- Gestión Parámetros
- Gestión Eliminar Información
- Gestión Cálculo del Riesgo Efectivo
- Gestión Cálculo del Riesgo Intrínseco
- Gestión Cálculo del Riesgo Simulado
- Gestión Cálculo del Riesgo Residual
- Gestión de Resultados
- Gestión Gráficos

Gestión de Grupos de Activos

Permitirá realizar las funciones de altas, bajas, cambios de un grupo de activos..

Alta

Para dar de alta un grupo de activos se da un clic sobre la opción nuevo, se ingresa el código en caso de no existir el código el sistema permite ingresar los siguientes datos: descripción del grupo de activo y observación, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de activos en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un grupo de activos, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar un grupo de activos dando un clic sobre el código de grupo de activos y luego dando un clic en el botón eliminar. Se borrará la información referente al grupo de activos de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cambios

Para modificar un grupo de activos, se deberá realizar los siguientes pasos:

1. Seleccionar un grupo de activos dando un clic sobre el código de grupo de activos y luego sobre el botón editar. Automáticamente el grupo de activos aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos Descripción del Grupo de Activo y Observación .
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Gestión de Activos

Permitirá realizar las funciones de altas, bajas, cambios de activos.

Alta

Para dar de alta un activo se da un clic en la opción nuevo, automáticamente se nos genera el código correspondiente al activo y a continuación el sistema permite el ingreso de los siguientes datos: descripción del activo, código del grupo de activo, valor económico, valor no económico y observación, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior derecha de la pantalla. Si el usuario pulsa este botón significará que se acepta el activo en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un activo, es decir para borrarlo de la base de datos se debe efectuar los siguiente: Seleccionar un activo dando un clic sobre el código del activo y luego dar un clic en el botón eliminar. Se borrará la información referente al activo de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como activos existan en la base de datos.

Cambios

Para modificar un activo, deberán efectuarse los siguientes pasos:

1. Seleccionar un activo dando un clic sobre el código de activo y luego sobre el botón editar. Automáticamente el activo aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción del activo, código del grupo de activo, valor económico, valor no económico y observación
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como activos existan en la base de datos.

Gestión de Árbol de Activos

Permitirá realizar las funciones de altas, bajas, de un activo padre y/o activo hijo y salir.

Alta

Para dar de alta una relación entre activos es necesario llevar a cabo los siguientes pasos:

1. El usuario debe seleccionar el activo existente contenido en el combo, automáticamente el sistema levantara el código del mismo para que aparezca en la ventana principal además debe ingresar el grado de dependencia, de no ser así aparecerá el mensaje de error correspondiente.
2. Una vez seleccionado el dato del activo padre seleccionamos los activos hijos de la misma manera que en el paso 1 se da un clic sobre el botón grabar situado en la parte inferior derecha de la pantalla correspondiente, se aceptarán los datos.
3. Una vez aceptados los datos se dará la posibilidad de asociar al activo introducido (activo padre), tantos activos (activos hijos) como se desee, siempre que sean correctos y aparezcan contenidos en la base de datos.

Esta operación podrá repetirse tantas veces como activos aparezcan en el Combo. La relación se grabará en la base de datos de la herramienta.

Baja

Para dar de baja una relación entre activos, es decir para borrarla de la base de datos se debe efectuar los siguientes pasos:

1. Seleccionar un activo (padre o hijo) dando un clic sobre el código de activo (padre o hijo) o sobre la descripción del activo (padre o hijo) o sobre el grado de dependencia.
2. Dar un clic sobre el eliminar, situado en la parte inferior derecha de la pantalla. Se borrará la información referente a la relación padre - hijo de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como relaciones existan en la base de datos

Nota: Para dar de baja una relación el usuario puede seleccionar tanto un activo hijo como un activo padre. En ambos casos se pedirá confirmación de la baja de la relación padre - hijo.

Gestión de Grupos de Amenazas

Permitirá realizar las funciones de altas, bajas, cambios de un grupo de amenazas y salir.

Alta

Para dar de alta un grupo de amenazas se da un clic sobre la opción nuevo, ingresamos el código en caso de no existir el código ingresado el sistema permitirá ingresar los siguientes datos: descripción del grupo de amenaza y observación, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de amenazas en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un grupo de amenazas, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar un grupo de activos dando un clic sobre el código de grupo de amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente al grupo de amenaza de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cambios

Para modificar un grupo de amenazas, deberán efectuarse los siguientes pasos:

1. Seleccionar un grupo de amenazas dando un clic sobre el código de grupo de amenazas y luego sobre el botón editar. Automáticamente el grupo de amenazas aparecerá en la ventana de edición.

2. Realizar las modificaciones a los campos descripción del grupo de amenaza y observación

3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como grupos de amenazas existan en la base de datos.

Gestión de Tipos de Amenazas

Permitirá realizar las funciones de altas, bajas, cambios de un tipo de amenaza.

Alta

Para dar de alta un tipo de amenaza se da un clic sobre la opción nuevo, ingresamos el código del tipo de amenaza en caso de no existir el código el sistema permite ingresar los siguientes datos: descripción del tipo de menaza y observación, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el tipo de amenaza en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un tipo de amenaza, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar un tipo de amenaza dando un clic sobre el código de tipo de amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente al tipo de amenaza de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como tipos de amenaza existan en la base de datos.

Cambios

Para modificar un tipo de amenaza, deberán efectuarse los siguientes pasos:

1. Seleccionar un tipo de amenaza dando un clic sobre el código del tipo de amenaza y luego sobre el botón editar. Automáticamente el tipo de amenaza aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción del tipo de menaza y observación
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como tipos de amenaza existan en la base de datos.

Gestión Mecanismos de Salvaguarda

Permitirá realizar las funciones de altas, bajas, cambios de mecanismos de salvaguarda.

Alta

Para dar de alta un mecanismo de salvaguarda se da un clic sobre la opción nuevo, ingresamos el código del mecanismo de salvaguarda en caso de no existir el código ingresado el sistema permitirá ingresar los siguientes datos: descripción del mecanismo de salvaguarda, la existencia del mecanismo de salvaguarda, valoración económica y texto libre el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de activos en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un mecanismo de salvaguarda es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar un mecanismo de salvaguarda dando un clic sobre el código de mecanismo de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente al mecanismo de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como mecanismos de salvaguarda existan en la base de datos.

Cambios

Para modificar un mecanismo de salvaguarda, deberán efectuarse los siguientes pasos:

1. Seleccionar un mecanismo de salvaguarda dando un clic sobre el código de mecanismo de salvaguarda y luego sobre el botón editar. Automáticamente el mecanismo de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción del mecanismo de salvaguarda, la existencia del mecanismo de salvaguarda, valoración económica y texto libre
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como mecanismos de salvaguarda existan en la base de datos.

Gestión de Tipos de Funciones de Salvaguarda

Permitirá realizar las funciones de altas, bajas, cambios de un tipo de función de salvaguarda.

Alta

Para dar de alta un tipo de función de salvaguarda se da un clic sobre la opción nuevo, ingresamos el código de tipo de función de salvaguarda en caso de no existir el código ingresado el sistema permite ingresar los siguientes datos: descripción de tipo de función de salvaguarda y observación, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de activos en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un tipo de función de salvaguarda, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar un tipo de función de salvaguarda dando un clic sobre el código del tipo de función de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente al tipo de función de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cambios

Para modificar un tipo de función de salvaguarda, deberán efectuarse los siguientes pasos:

1. Seleccionar un tipo de función de salvaguarda dando un clic sobre el código de tipo de función de salvaguarda y luego sobre el botón editar. Automáticamente el tipo de función de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción de tipo de función de salvaguarda y observación
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Gestión funciones de Salvaguarda

Permitirá realizar las funciones de altas, bajas, cambios de una función de salvaguarda.

Alta

Para dar de alta una función de salvaguarda se da un clic sobre la opción nuevo, ingresamos el código de la función de salvaguarda si el código ingresado no existe el sistema permitirá ingresar los siguientes datos: descripción de la función de salvaguarda, código del tipo de la función de salvaguarda, descripción del tipo de la función de salvaguarda, código del mecanismo de salvaguarda, descripción del mecanismo de salvaguarda y grado de Cumplimentación, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la función de salvaguarda en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja una función de salvaguarda, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar un grupo de activos dando un clic sobre el código de función de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente a la función de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como funciones de salvaguarda existan en la base de datos.

Cambios

Para modificar una función de salvaguarda, deberán efectuarse los siguientes pasos:

1. Seleccionar una función de salvaguarda dando un clic sobre la función de salvaguarda y luego sobre el botón editar. Automáticamente la función de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción de la función de salvaguarda, código del tipo de la función de salvaguarda, descripción del tipo de la función de salvaguarda, código del mecanismo de salvaguarda, descripción del mecanismo de salvaguarda y grado de Cumplimentación

3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como funciones de salvaguarda existan en la base de datos.

Gestión de Amenazas

Permitirá realizar las funciones de altas, bajas, cambios de una amenaza.

Alta

Para dar de alta una amenaza se da un clic sobre la opción nuevo, ingresamos el código de la amenaza en caso de no existir el código de ingresado el sistema permitirá ingresar los siguientes datos: descripción de la amenaza, código del grupo de amenaza, descripción del grupo de amenaza, código del tipo de la amenaza, descripción del tipo de amenaza, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la amenaza en curso dándose de alta automáticamente en la base de datos.

Nota: En esta pantalla no se pueden dar de alta grupos de amenaza, tipos de amenaza. Esa operación se realizará en las pantallas y opciones establecidas para ello.

Baja

Para dar de baja una amenaza, es decir para borrarla de la base de datos se debe efectuar lo siguiente: Seleccionar una amenaza dando un clic sobre el código de amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente a la amenaza de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como amenazas existan en la base de datos.

Cambios

Para modificar una amenaza, deberán efectuarse los siguientes pasos:

1. Seleccionar una amenaza dando un clic sobre el código de amenaza y luego sobre el botón editar. Automáticamente la amenaza aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción de la amenaza, código del grupo de amenaza, descripción del grupo de amenaza, código del tipo de la amenaza, descripción del tipo de amenaza
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como amenazas existan en la base de datos.

Gestión Amenazas por Función de Salvaguarda

Permitirá realizar las funciones de altas, bajas, cambios de una amenaza por función de salvaguarda.

Alta

Para dar de alta una amenaza por función de salvaguarda se da un clic sobre la opción nuevo, una vez ingresado tanto el código de la amenaza, función de salvaguarda, porcentaje de reducción de vulnerabilidad, porcentaje de reducción del impacto, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la amenaza por función de salvaguarda en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja una amenaza por función de salvaguarda, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar una amenaza por función de salvaguarda dando un clic sobre el código de la amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente a la amenaza por función de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como amenazas por función de salvaguarda existan.

Cambios

Para modificar una amenaza por función de salvaguarda, deberán efectuarse los siguientes pasos:

1. Seleccionar una amenaza por función de salvaguarda dando un clic sobre el código de amenaza y luego sobre el botón editar. Automáticamente la amenaza por función de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos función de salvaguarda, porcentaje de reducción de vulnerabilidad, porcentaje de reducción del impacto
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como amenazas por función de salvaguarda existan en la base de datos.

Gestión Amenaza por Activos

Permitirá realizar las funciones de altas, bajas, cambios de una amenaza por activo.

Alta

Para dar de alta una amenaza por activo se da un clic sobre la opción nuevo, se nos presenta una ventana donde tenemos diferentes combos que nos

muestran la descripción de las amenazas, activos, vulnerabilidad y degradación existentes, una vez seleccionados los datos que deseamos, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la amenaza por activo en curso dándose de alta automáticamente en la base de datos. El código de grupo de amenaza será presentado automáticamente en la ventana principal

Baja

Para dar de baja una amenaza por activo, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar una amenaza por activo dando un clic sobre el código de grupo de amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente a la amenaza por activo de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como amenazas por activo existan en la base de datos.

Cambios

Para modificar una amenaza por activo, deberán efectuarse los siguientes pasos:

1. Seleccionar una amenaza por activo dando un clic sobre el código de grupo de amenaza y luego sobre el botón editar. Automáticamente el la amenaza por activo aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción de las amenazas, activos, vulnerabilidad y degradación
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como amenazas por activos existan en la base de datos.

Gestión Funciones por Mecanismos de Salvaguarda

Permitirá realizar las funciones de altas, bajas, cambios de funciones por mecanismos de salvaguarda.

Alta

Para dar de alta una función por mecanismo de salvaguarda se da un clic sobre la opción nuevo, se nos presenta una ventana donde tenemos diferentes combos que nos muestran la descripción de la función de salvaguarda, los mecanismos de salvaguarda y el grado de cumplimiento, una vez seleccionados los datos que deseamos, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la función por mecanismo de salvaguarda en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja una función por mecanismo de salvaguarda, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar una función por mecanismo de salvaguarda dando un clic sobre la función de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente a la función por mecanismo de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como funciones por mecanismo de salvaguarda existan en la base de datos.

Cambios

Para modificar una función por mecanismo de salvaguarda, deberán efectuarse los siguientes pasos:

1. Seleccionar una función por mecanismo de salvaguarda dando un clic sobre la función por mecanismo de salvaguarda y luego sobre el botón editar. Automáticamente la función por mecanismo de salvaguarda aparecerá en la ventana de edición.

2. Realizar las modificaciones a los campos descripción de la función de salvaguarda, los mecanismos de salvaguarda y el grado de cumplimiento

3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como funciones por mecanismo de salvaguarda existan en la base de datos.

Gestión Parámetros

Permitirá realizar las funciones de altas, bajas, cambios de un parámetro.

Alta

Para dar de alta un parámetro se da un clic sobre la opción nuevo, escogemos el código del parámetro y luego ingresamos la descripción del parámetro y el valor del mismo, el usuario puede grabar los datos en la base de datos dando un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el parámetro en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un parámetro, es decir para borrarlo de la base de datos se debe efectuar lo siguiente: Seleccionar un parámetro dando un clic sobre el código de parámetro y luego se da un clic en el botón eliminar. Se borrará la información referente al parámetro de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como parámetros existan en la base de datos.

Cambios

Para modificar un parámetro, deberán efectuarse los siguientes pasos:

1. Seleccionar un parámetro dando un clic sobre el código de parámetro y luego sobre el botón editar. Automáticamente el grupo de activos aparecerá en la ventana de edición.
2. Realizar las modificaciones a los campos descripción del parámetro y el valor
3. Dar un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como parámetros existan en la base de datos.

Gestión Análisis

Dentro de la Gestión de análisis tenemos: calculo del riesgo efectivo, calculo del riesgo simulado, calculo del riesgo intrínsico, calculo del riesgo residual

Cálculo del Riesgo Efectivo

Se calcula el riesgo efectivo, para lo cual hay que considerar la efectividad de las funciones de salvaguarda, obtenida por la implementación de los mecanismos que se han detectado como existentes. Una vez conocida la efectividad de las funciones se evalúa su capacidad para disminuir el riesgo y se aplica a los activos amenazados.

En la pantalla aparecerá una relación de los mecanismos (código y descripción).. Al mismo tiempo se ofrece la posibilidad de establecer el grado de implementación, ya que pueden existir mecanismos no implementados en su totalidad.

Una vez establecido el grado de implementación, se puede proceder a calcular el riesgo efectivo dando un clic sobre el botón la opción análisis del menú principal y a continuación un clic en la opción Riesgo Efectivo como resultado obtendremos una tabla con los valores de riesgo efectivo para cada uno de los activos existentes

Cálculo del Riesgo Intrínseco

Se calcula el riesgo intrínseco de cada activo amenazado, teniendo en cuenta la degradación que la amenaza puede producir en el activo y el valor relativo o dependencia acumulada del activo en el árbol de activos, así como la propia vulnerabilidad del activo.

Se puede proceder a calcular el riesgo intrínseco dando un clic sobre al opción análisis del menú principal y luego un clic sobre la opción riesgo intrínsico como resultado obtendremos una tabla con los valores de riesgo intrínsico para cada uno de los activos existentes

Cálculo del Riesgo Residual

Se le llama riesgo residual al nivel de riesgo resultante una vez aplicadas las salvaguardas propuestas. Para calcular el riesgo residual se da un clic sobre la opción análisis del menú principal y luego sobre la opción riesgo residual y a continuación se nos presentara una tabla con los valores de riesgo residual para cada activo existente.

Cálculo del Riesgo Simulado

En este proceso, se calcula el riesgo de simulación, para lo cual hay que considerar la efectividad de las funciones de salvaguarda, obtenida por la implementación de los mecanismos que se han seleccionado para la simulación. Una vez conocida la efectividad de las funciones se evalúa su capacidad para disminuir el riesgo y se aplica a los activos amenazados.

En la pantalla aparecerá una relación de los mecanismos (código y descripción). Al mismo tiempo se ofrece la posibilidad de seleccionar aquellos mecanismos que se van a utilizar para la simulación, es decir para calcular el riesgo de simulación. Opcionalmente es posible añadir a la selección los mecanismos complementarios y descartar los mecanismos excluyentes.

Una vez seleccionados los mecanismos para la simulación se puede proceder a calcular el riesgo de simulación dando un clic sobre la opción análisis del menú principal y luego un clic sobre la opción riesgo simulado y a continuación se nos presentar una tabla con los valores correspondientes al riesgo simulado de los activos existentes.

Gestión Resultados

En esta opción el sistema permitirá listar todos y cada uno del los resultados de los cálculos realizados. Para utilizar esta opción se da un clic sobre la opción resultados del menú principal y luego un clic sobre el listado de resultados que deseemos.
La Gestión Resultados presenta: Gráficos, Listados de Tablas, Listados de Resultados, Niveles Totales de Riesgo

Gráficos

En esta opción podemos observar gráficamente los valores de riesgos que afectan a los activos existentes para hacer uso de esta opción se da un clic sobre la opción gráficos del menú principal y luego un clic sobre el grafico que deseemos observar en la parte inferior del grafico se desplegara una tabla con los valores correspondientes a los gráficos para una mejor comprensión de los mismos.

Listados de Tablas

En esta opción se puede observar los resultados en listados que permiten una mejor compresión e interpretación de los datos. Para hacer uso de esta opción se da un clic sobre la opción resultados y luego un clic sobre listados de tablas, se escoge el listado que deseemos y el sistema despliega la información.

Listados de Resultados

En esta opción se puede observar los resultados en listados de resultados que permiten una mejor compresión e interpretación de los resultados obtenidos. Para hacer uso de esta opción se da un clic sobre la opción resultados y luego un clic sobre listados de resultados, se escoge el listado que deseemos y el sistema despliega la información.

Niveles Totales de Riesgo

En esta opción el sistema presenta un formulario electrónico con el grafico de los niveles totales del proyecto. Para hacer uso de esta opción se da un clic sobre la opción resultados y luego un clic sobre Niveles Totales de Riesgo y el sistema despliega la información.

4.2.2 Características de los Usuarios

El sistema deberá proporcionar una interfaz de usuario fácil de aprender y sencillo de manejar, además deberá presentar un alto grado de usabilidad.

4.2.3 Restricciones

Se requerirá instalar Visual Basic y Microsoft Access para el funcionamiento correcto del sistema, además se deberá crear un ODBC para la conexión con las bases de datos.

4.2.4 Suposiciones

Los requisitos aquí descritos son estables dado que fueron revisados y aprobados por el director y codirector de la tesis en desarrollo.

4.2.5 Dependencias

El sistema a desarrollar no tiene dependencia respecto a otros sistemas.

3. Requisitos Específicos

En este apartado se describirá los requisitos funcionales que deberán ser satisfechos por el sistema.

4.3 Requisitos Funcionales

4.3.1 Gestión de Grupos de Activos

El sistema deberá permitir:

- Req(01) Ingresar un grupo de activos.
- Req(02) Dar de baja un grupo de activos.
- Req(03) Modificar los datos de un grupo de activos

4.3.2 Gestión de Activos

El sistema deberá permitir:

- Req(04) Ingresar activos
- Req(05) Dar de baja un activo .
- Req(06) Modificar los datos de un activo

4.3.3 Gestión de Árbol de Activos

El sistema deberá permitir:

- Req(7) Ingresar activos padres
- Req(8) Ingresar activos hijos
- Req(9) Dar de baja un activo padre
- Req(10) Modificar un activo padre y/o hijo

4.3.4 Gestión de Grupo de Amenazas

El sistema deberá permitir:

- Req(11) Ingresar un grupo de amenazas
- Req(12) Eliminar un grupo de amenazas
- Req(13) Modificar un grupo de amenazas

4.3.5 Gestión Tipo de Amenazas

El sistema deberá permitir:

- Req(14) Ingresar un tipo de amenaza
- Req(15) Eliminar un tipo de amenaza
- Req(16) Modificar un grupo de amenaza

4.3.6 Gestión Mecanismo de Salvaguarda

El sistema deberá permitir:

- Req(17) Ingresar un mecanismo de salvaguarda
- Req(18) Eliminar un mecanismo de salvaguarda
- Req(19) Modificar un mecanismo de salvaguarda

4.3.7 Gestión Tipos de Funciones de Salvaguarda

El sistema deberá permitir:

- Req(20) Ingresar un tipo de función de salvaguarda
- Req(21) Eliminar un tipo de función de salvaguarda
- Req(22) Modificar un tipo de función de salvaguarda

4.3.8 Gestión Función de Salvaguarda

El sistema deberá permitir:

- Req(23) Ingresar una función de salvaguarda
- Req(24) Eliminar una función de salvaguarda
- Req(25) Modificar una función de Salvaguarda

4.3.9 Gestión Amenazas

El sistema deberá permitir:

- Req(26) Ingresar una amenaza
- Req(27) Eliminar una amenaza
- Req(28) Modificar una amenaza

4.3.10 Gestión Amenazas por Función de Salvaguarda

El sistema deberá permitir:

- Req(29) Ingresar una amenaza por función de salvaguarda

- Req(30) Eliminar una amenaza por función de salvaguarda
- Req(31) Modificar una amenaza por función de salvaguarda

4.3.11 Gestión Amenazas por Activo

El sistema deberá permitir:

- Req(32) Ingresar una amenaza por activo
- Req(33) Eliminar una amenaza por activo
- Req(34) Modificar una amenaza por activo

4.3.12 Gestión de Función por Mecanismo de Salvaguarda

El sistema deberá permitir:

- Req(35) ingresar una función por mecanismo de salvaguarda
- Req(36) Eliminar una función por mecanismo de salvaguarda
- Req(37) Modificar una función por mecanismo de salvaguarda

4.3.13 Gestión Parámetros

El sistema deberá permitir:

- Req(38) Ingresar un parámetro
- Req(39) Eliminar un parámetro
- Req(40) Modificar un parámetro

4.3.14 Gestión Análisis

El sistema deberá permitir:

- Req(41) Calcular el riesgo efectivo
- Req(42) Calcular el riesgo simulado
- Req(43) Calcular el riesgo residual
- Req(44) Calcular el riesgo intrinsico

4.3.15 Gestión de Resultados

El sistema deberá permitir:

- Req(45) Mostrar resultados en forma gráfica
- Req(46) Mostrar resultados en listados de tablas
- Req(47) Mostrar resultados en listados de resultados
- Req(48) Mostrar Niveles Totales de Riesgo

4.4 Requisitos de Interfaces Externas

4.4.1 Interfaces de Usuario

La interfaz del sistema debe ser orientada a ventanas, y el manejo del programa se realizará a través del teclado y ratón.

4.4.2 Interfaces Hardware

Se trabajará en un computador Pentium4

4.4.3 Interfaces Software.

De momento, no habrá ninguna interfaz software con sistemas externos.

4.5 Requisitos de Rendimiento

No se ha definido.

4.5.1 Requisitos de Desarrollo

El ciclo de vida para desarrollar el producto es el secuencial básico, o en cascada.

4.5.2 Requisitos Tecnológicos

La aplicación se ejecutará sobre un PC con la siguiente configuración:

- Procesador Pentium 4
- Memoria 128 Mb
- Espacio libre en disco 50 Mb

- Visual Basic 6.0
- Microsoft Access

El sistema operativo en la que se debe ejecutar la aplicación será el Windows 98 o superior

Para el acceso a la base de datos se utilizará un ODBC de nombre VARIABLES

CASOS DE USO DE ALTO NIVEL

Gestión Activos

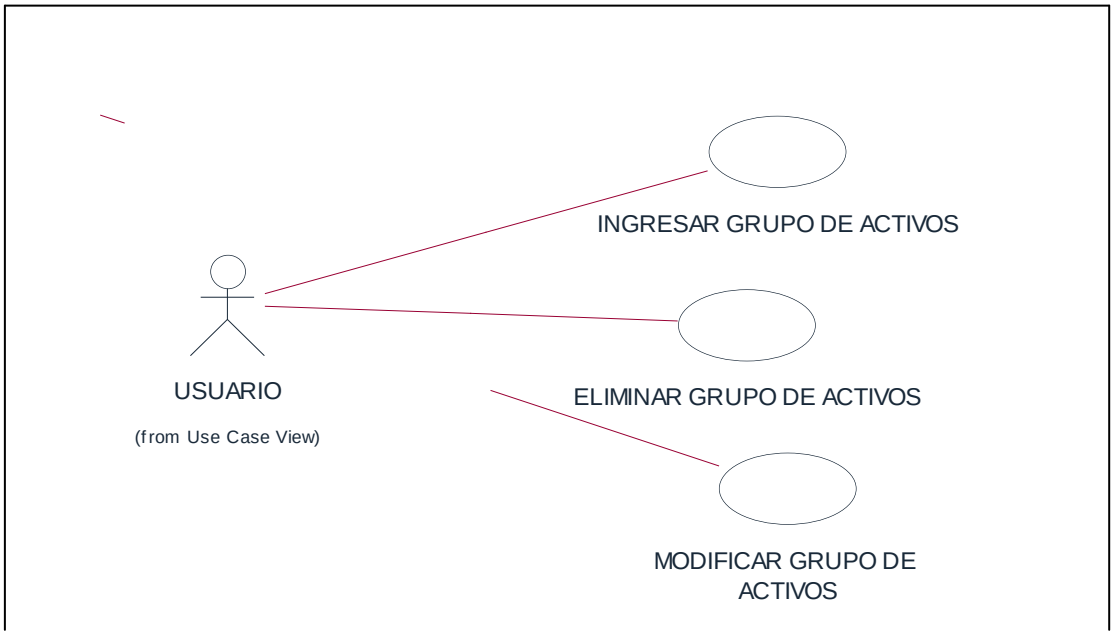


FIGURA 4.1 CASO DE USO DE ALTO NIVEL ACTIVOS

Caso de Uso de Alto Nivel Ingresar Activos

Nombre del Caso de Uso: Ingresar Activos

Actor: Usuario

Tipo: Primario

Descripción: El usuario selecciona la opción ingresar activos, el sistema presenta el formulario de ingreso de nuevos activos, el usuario ingresa los datos solicitados, el sistema almacena los datos y termina el caso de uso.

Caso de Uso de Alto Nivel Eliminar Activos

Nombre del Caso de Uso: Eliminar Activos

Actor: Usuario

Tipo: Primario

Descripción: El usuario selecciona la opción eliminar activos, el sistema presenta los activos existentes, el usuario señala el activo a eliminar, el sistema lo elimina y termina el caso de uso

Caso de Uso de Alto Nivel Modificar Activos

Nombre del Caso de Uso: Modificar Activos

Actor: Usuario

Tipo: Primario

Descripción: El usuario señala la opción Modificar activos, el sistema presenta la lista de activos existentes, el usuario señala el activo a modificar y modifica los datos, el sistema almacena la información y termina el caso de uso

NOTA: *Los demás Casos de Uso de Alto Nivel correspondientes a las Gestiones especificadas en los Requisitos se encuentran en el Anexo 4*

DEDFINICION DEL MODELO CONCEPTUAL

En este punto se recogen todas las entidades a ser procesadas o consultadas por el sistema y todas las relaciones existentes entre las entidades de manera que pueden acceder a la información proporcionada por el sistema.

Información del Modelo de Datos

Nombre del Proyecto: Sistema de Gestión de Riesgos de Proyectos Software

Código del Proyecto: Sistema de Gestión de Riesgos de Proyectos software

Nombre: Modelo Conceptual del Sistema de Gestión de Riesgos

Descripción: Modelo Conceptual del Sistema de Gestión de Riesgos

Autor: Desarrollador del sistema de Gestión de Riesgos

Versión: 1.0

DIAGRAMA DEL MODELO CONCEPTUAL

DECRIPCION DE LAS ENTIDADES

NOMBRE	CODIGO	DOMINIO	TIPO
Codigo_tipoamenaza	Cod_tipoamenaza	Código	A4
Descripción_tipoamenaza	Descripción_tipoamenaza	Descripción	A40
Texto_tipoamenaza	Texto_tipoamenaza	Texto	A4
Codigo_grupoamenaza	Codigo_grupoamenaza	Código	A40

Descripción_grupoamenaza	Descripción_grupoamenaza	Descripción	A40
Texto_grupoamenaza	Texto_grupoamenaza	Texto	NO
Serial_arbolactivos	Serial_arbolactivos	Serial	A4
Codigo_arbolactivos	Codigo_arbolactivos	Código	A40
Descripción_arbolactivos	Descripción_arbolactivos	Descripción	A40
Codigo_activohijo	Codigo_activohijo	Código	A40
Descripción_activohijo	Descripción_activohijo	Descripción	NO
Porcentaje	Porcentaje	Porcentaje	A4
Codigo_activo	Codigo_activo	Código	A40
Descripción_activo	Descripción_activo	Descripción	A4
Codigo_grupoactivo	Codigo_grupoactivo	Código	NO
Valor_economico	Valor_economico	Valor	NO
Valor_noeconomico	Valor_noeconomico	Valor	A40
Texto_activo	Texto_activo	Texto	NO
Valor_DA	Valor_DA	Valor	A4
Codigo_grupoactivo	Codigo_grupoactivo	Código	A40
Descripción_grupoactivo	Descripción_grupoactivo	Descripción	A40
Texto_grupoactivo	Texto_grupoactivo	Texto	A4
Codigo_amenaza	Codigo_amenaza	Código	A40
Descripción_amenaza	Descripción_amenaza	Descripción	A4
Codigo_tipoamenaza	Codigo_tipoamenaza	Código	A4

Codigo_grupoamenaza	Codigo_grupoamenaza	Código	A40
Texto_amenaza	Texto_amenaza	Texto	A4
Codigo_param	Codigo_param	Código	A40
Descripción_param	Descripción_param	Descripción	NO
Valor_param	Valor_param	Valor	NO
Serial_param	Serial_param	Serial	NO
Copiaserial_param	Copiaserial_param	Copiaserial	NO
Serial_amenazas	Serial_amenazas	Serial	NO
Codigo_grupoamenaza	Codigo_grupoamenaza	Código	A4
Codigo_funcionsalvaguarda	Codigo_funcionsalvaguarda	Código	A4
Porcentaje_vulnerabilidad	Porcentaje_vulnerabilidad	Porcentaje	NO
Porcentaje_impacto	Porcentaje_impacto	Porcentaje	NO
Copiaserial_amenazas	Copiaserial_amenazas	Copiaserial	NO
Valor_DVE	Valor_DVE	Valor	NO
Valor_DIE	Valor_DIE	Valor	NO
Valor_DIS	Valor_DIS	Valor	NO
Valor_DVS	Valor_DVS	Valor	NO
Codigo_tipofuncionsalvaguarda	Codigo_tipofuncionsalvaguarda	Código	A4
Descripción:tipofuncionsalvaguarda	Descripción:tipofuncionsalvaguarda	Descripción	A40
Texto_funcionsalvaguar	Texto_funcionsalvaguar	Texto	A40

da	da		
Codigo_mecanismosalvaguarda	Codigo_mecanismosalvaguarda	Código	A4
Descripción_mecanismosalvaguarda	Descripción_mecanismosalvaguarda	Descripción	A40
Existente_mecanismosalvaguarda	Existente_mecanismosalvaguarda	Existente	A2
Codigo_salvaguarda	Codigo_salvaguarda	Código	A4
Texto_mecanismosalvaguarda	Texto_mecanismosalvaguarda	Texto	A40
Simulado_mecanismosalvaguarda	Simulado_mecanismosalvaguarda	Simulado	A2
Copiaserial_funmeca	Copiaserial_funmeca	Copiaserial	NO
Serial_funmeca	Serial_funmeca	Serial	NO
Codigo_mecanismo	Codigo_mecanismo	Código	A4
Codigo_función	Codigo_función	Código	A4
Grado	Grado	Grado	NO
Codigo_funcionsalvaguarda	Codigo_funcionsalvaguarda	Código	A4
Descripción_funcionsalvaguarda	Descripción_funcionsalvaguarda	Descripción	A40
Codigo_tipofuncionsalvaguarda	Codigo_tipofuncionsalvaguarda	Código	A4
Texto_funcionsalvaguarda	Texto_funcionsalvaguarda	Texto	A40
Valor_EFE	Valor_EFE	Valor	NO
Valor_EFESimulado	Valor_EFESimulado	Valor	NO

Serial_amenazaactivo	Serial_amenazaactivo	Serial	NO
Codigo_grupoamenaza	Codigo_grupoamenaza	Código	A4
Codigo_activo	Codigo_activo	Código	A4
Codigo_vulnerabilidad	Codigo_vulnerabilidad	Código	A4
Porcentaje_degradación	Porcentaje_degradación	Porcentaje	NO
Copiaserial_amenazaactivo	Copiaserial_amenazaactivo	Copiaserial	NO
Valor_IMP	Valor_IMP	Valor	NO
Valor_ID	Valor_ID	Valor	NO
Valor_VD	Valor_VD	Valor	NO
Valor_RE	Valor_RE	Valor	NO
Valor_IDS	Valor_IDS	Valor	NO
Valor_VDS	Valor_VDS	Valor	NO
Valor_RS	Valor_RS	Valor	NO
Valor_RR	Valor_RR	Valor	NO
Valor_RI	Valor_RI	Valor	NO

TABLA 4.4 DESCRIPCION DE LAS ENTIDADES

LISTADO DE DATOS POR ENTIDADES

ENTIDAD TIPO_AMENAZA

Nombre: Tipo_amenaza
Código: Tipo_amenaza
Descripción: Identificador de la entidad Tipo_amenaza
Dominio: Tipo

ENTIDAD_GRUPOAMENAZA

Nombre: Grupo_amenaza
Código: Grupo_amenaza
Descripción: Identificador de la entidad Grupo_amenaza
Dominio: Grupo

ENTIDAD ÁRBOL_ACTIVOS

Nombre: Árbol_activos
Código: Árbol_activos
Descripción: Identificador de la entidad Árbol_activos
Dominio: Árbol

ENTIDAD ACTIVO

Nombre: Activo
Código: Activo
Descripción: Identificador de la entidad Activo
Dominio: Activo

ENTIDAD AMENAZA

Nombre: Amenaza
Código: Amenaza
Descripción: Identificador de la entidad Amenaza
Dominio: Amenaza

ENTIDAD GRUPO_ACTIVO

Nombre: Grupo_activo
Código: Grupo_activo
Descripción: Identificador de la entidad Grupo_activo
Dominio: Grupo

ENTIDAD PARÁMETRO

Nombre: Parámetro
Código: Parámetro
Descripción: Identificador de la entidad Parámetro
Dominio: Parámetro

ENTIDAD FUNCIÓN_MECANISMO

Nombre: Función_mecanismo
Código: Función_mecanismo
Descripción: Identificador de la entidad Función_mecanismo
Dominio: Función_mecanismo

ENTIDAD FUNCIÓN_SALVAGUARDA

Nombre: Función_salvaguarda
Código: Función_salvaguarda
Descripción Identificador de la entidad Función_salvaguarda
Dominio: Función_salvaguarda

ENTIDAD MECANISMO_SALVAGUARDA

Nombre: Mecanismo_salvaguarda
Código: Mecanismo_salvaguarda
Descripción: Identificador de la entidad Mecanismo_salvaguarda
Dominio: Mecanismo_salvaguarda

ENTIDAD AMENAZA_ACTIVO

Nombre: Amenaza_activo
Código: Amenaza_activo
Descripción: Identificador de la entidad Amenaza_activo
Dominio: Amenaza_activo

ENTIDAD AMENAZA_GRUPOAMENAZA

Nombre: Amenaza_grupoamenaza
Código: Amenaza_grupoamenaza
Descripción: Identificador de la entidad Amenaza_grupoamenaza
Dominio: Amenaza_grupoamenaza

ENTIDAD AMENAZA_FUNCIONSALVAGUARDA

Nombre: Amenaza_funcionsalvaguarda
Códiogo: Amenaza_funcionsalvaguarda
Descripción: Identificador de la entidad Amenaza_funcionsalvaguarda
Dominio: Amenaza_funcionsalvaguarda

ENTIDAD TIPO_FUNCIONSALVAGUARDA

Nombre: Tipo_funcionsalvaguarda

Código: Tipo_funcionsalvaguarda

Descripción: Identificador de la entidad Tipo_funcionsalvaguarda

Dominio: Tipo_funcionsalvaguarda

DIAGRAMA CONCEPTUAL

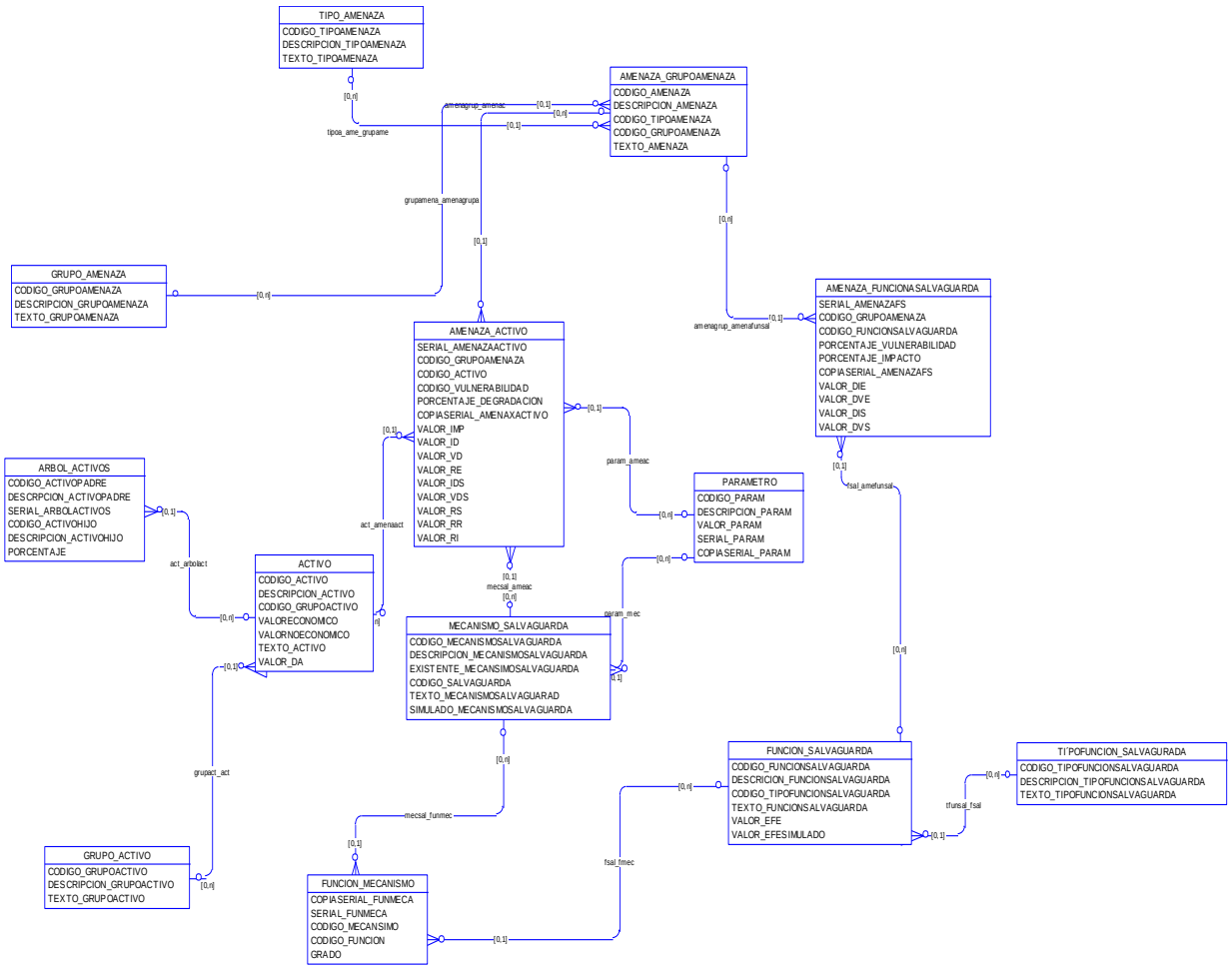


FIGURA 4.2 DIAGRAMA CONCEPTUAL

4.6.- ANÁLISIS Y DISEÑO

DEFINICIÓN DE LOS CASOS DE USO EXPANDIDOS

Gestión Activos

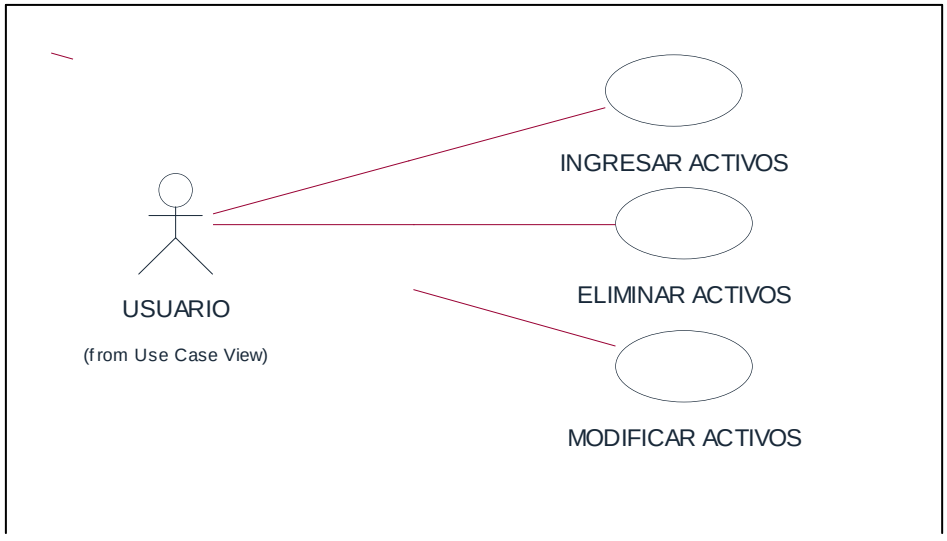


FIGURA 4.3 CASO DE USO EXPANDIDO ACTIVOS

Caso de Uso Expandido Ingresar Activos

Nombre del Caso de Uso: Ingresar Activos

Propósito: Ingresar los activos en el sistema

Actor: Usuario

Requisito: 04

Tipo: Primario Real

Visión General: Este caso de uso comienza cuando el usuario ingresa al sistema y escoge la opción activos el sistema presenta un listado de los activos existente a continuación el usuario da un clic sobre la opción nuevo y el sistema presenta una pantalla en donde el usuario debe llenar los siguientes campos: código del activo, descripción del activo, grupo de activo al que pertenece, valor económico, valor no económico y texto que es una referencia sobre el activo, una vez ingresados estos datos el usuario da un clic sobre el botón grabar y el sistema almacena los datos y termina el caso de uso.

Curso Típico de Eventos

ACTOR	SISTEMA
1) Escoge Opción Activos	2) Presenta Formulario Electrónico con los Activos Existentes
3) Escoge Opción Nuevo	4) Presenta el Formulario Electrónico de Ingreso de Activos
5) Ingresar los Datos a la Base de Datos	6) Grabar la Información en la Base de Datos

TABLA 4.5 CURSO TÍPICO DE EVENTOS INGRESAR ACTIVOS

Cursos Alternativos

2) No existe activos

4) No existe formulario de ingreso de activos

Caso de Uso Expandido Eliminar Activos

Nombre del Caso de Uso: Eliminar Activos
Propósito: Eliminar un activo que se encuentra ingresado en el sistema
Actor: Usuario
Requisito: 05
Tipo: Primario Real
Visión General: Este caso de uso comienza cuando el usuario ingresa al sistema y escoge la opción activos el sistema presenta una pantalla donde se encuentran todos los activos que contiene la base de datos a continuación el usuario escoge el activo que desea eliminar dando un clic sobre el código del mismo, el sistema presenta la información sobre ese activo y el usuario da un clic sobre el botón eliminar automáticamente se elimina el activo del sistema y termina el caso de uso.

Curso Típico de Eventos

ACTOR	*SISTEMA*
1) Escoge Opción Activos	2) Presenta Formulario Electrónico con los Activos existentes
3) Selecciona el Activo que Desea Eliminar	4) Presenta Formulario con los Datos del Activo Seleccionado
5) Confirmar Eliminación	6) Elimina el Activo de la Base de Datos

Tabla 4.6 Curso Típico de Eventos Eliminar Activos

Cursos Alternativos

2) No existe activos
4) No existe formulario de datos del activo seleccionado

Caso de Uso Expandido Modificar Activos

Nombre del Caso de Uso: Modificar Activos

Propósito: Modificar los datos de un activo existente en el sistema

Actor: Usuario

Requisito: **06**

Tipo: Primario Real

Visión General: Este caso de uso comienza cuando el usuario ingresa al sistema y escoge la opción activos el sistema presenta una pantalla donde se encuentran todos los activos que contiene la base de datos a continuación el usuario escoge el activo que desea modificar dando un clic sobre el código del mismo, el sistema presenta la información sobre ese activo y el usuario puede ir modificando los siguientes datos: descripción activo, grupo de activo al que pertenece, valor económico, valor no económico y texto que es una referencia sobre el activo luego da un clic sobre el botón grabar y automáticamente el sistema graba las modificaciones realizadas y termina el caso de uso.

Curso Típico de Eventos

ACTOR	*SISTEMA*
1) Escoger Opción Activos	2) Presenta Formulario Electrónico con los Activos Existentes
3) Seleccionar el Activo a Modificar	4) Presenta Formulario Electrónico de Modificación de Activos
5) Modificar Datos Deseados	6) Grabar los Cambios en la Base de Datos

TABLA 4.7 CURSO TÍPICO DE EVENTOS MODIFICAR ACTIVOS

CURSOS ALTERNATIVOS

2) No existe activos

4) No existe formulario de modificación de activos

NOTA: *Los demás Casos de Uso Expandidos correspondientes a las Gestiones especificadas en los Requisitos se encuentran en el Anexo 4*

DIAGRAMAS DE SECUENCIA

Gestión Activos

FIGURA 4.4 DIAGRAMA DE SECUENCIA INGRESAR ACTIVOS

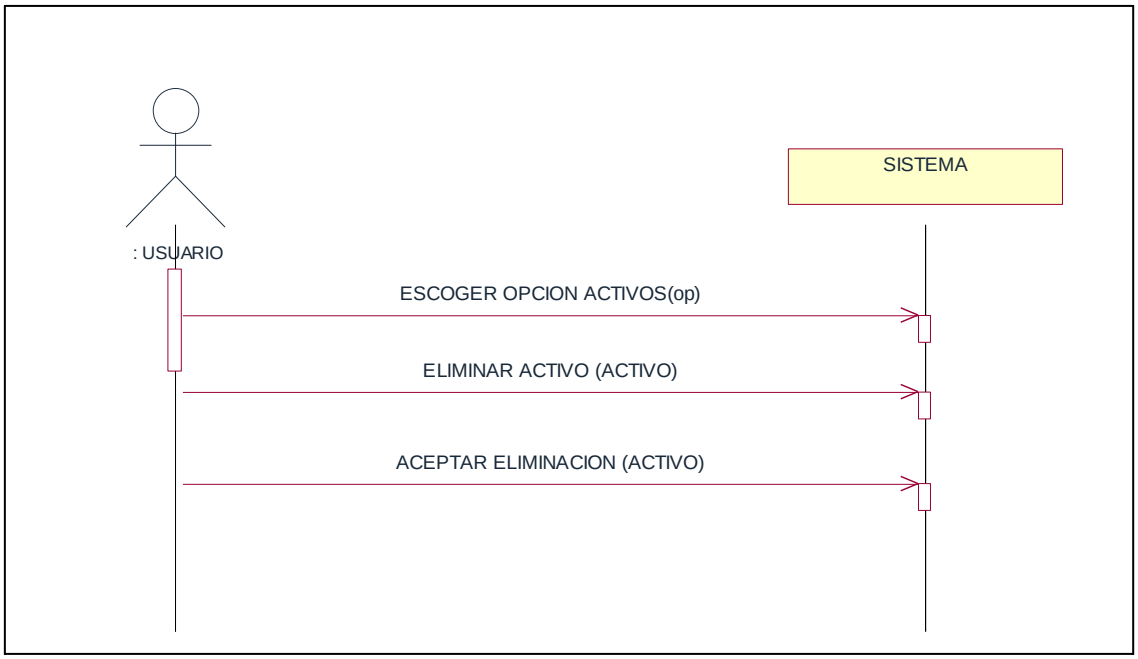


FIGURA 4.5 DIAGRAMA DE SECUENCIA ELIMINAR ACTIVOS

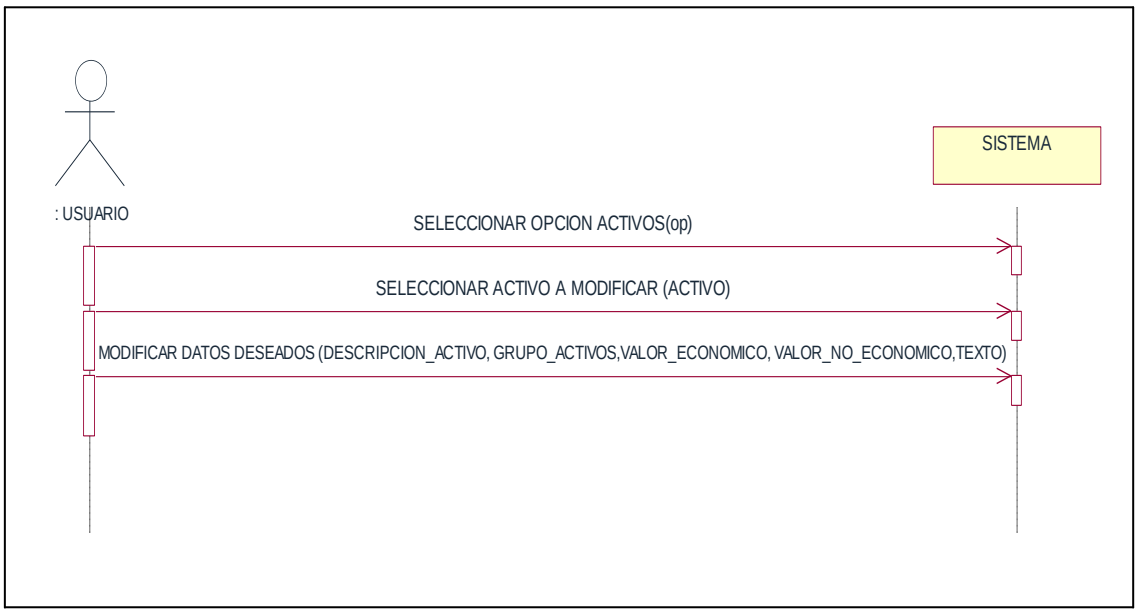


FIGURA 4.6 DIAGRAMA DE SECUENCIA MODIFICAR ACTIVOS

NOTA: *Los demás Diagramas de Secuencia correspondiente a las Gestiones especificadas en los Requisitos se encuentran en el Anexo 4*

DEFINICIÓN DE LOS CONTRATOS DE OPERACIÓN

Gestión Activos

Ingresar Activos

CONTRATO DE OPERACION (Escoger Opción Activos)

Nombre del Contrato: Escoger Opción Activos (op)
Propósito: Presentar Formulario Electrónico con los Activos Existentes
Tipo: Sistema
Referencia: Caso de Uso Ingreso de Activos
Salida: Lista de Activos Existentes
Excepción: No exista formulario electrónico de activos
Pre-condición: Exista formulario electrónico de activos , exista activos
Pos-condición:

CONTRATO DE OPERACION (Escoger Opción Nuevo)

Nombre del Contrato: Escoger Opción Nuevo (nop)

Propósito: Presentar Formulario Electrónico para el Ingreso de Activos Nuevos

Tipo: Sistema

Referencia: Caso de Uso Ingresar Activos

Salida: Formulario con los Datos de los Activos para Ingresar

Excepción: No exista formulario de ingreso de nuevos activos

Pre-condición: Exista formulario de ingreso de activos

Pos-condición:

CONTRATOS DE OPERACION (Ingresar Datos)

Nombre del Contrato: Ingresar Datos (activo)
Propósito: Ingresar al Sistema los Datos del Nuevo Activo
Tipo: Sistema
Referencia: Caso de Uso Ingresar Activos
Salida: Información Completa del Nuevo Activo
Excepción: No presente campos para llenar la Información sobre el nuevo activo
Pre-condición: Que exista formulario electrónico de ingreso de datos, que el activo no exista
Pos-condición:

Eliminar Activos

1. CONTRATO DE OPERACION (Escoger Opción Activos)

Nombre del Contrato: Escoger Opción Activos (op)

Propósito: Presentar Formulario Electrónico con los Activos Existentes

Tipo: Sistema

Referencia: Caso de Uso Eliminar Activos

Salida: Lista de Activos Existentes

Excepción: No exista formulario de activos

Pre-condición: Exista formulario de activos, que existan activos

Pos-condición:

2. CONTRATO DE OPERACIÓN (Eliminar Activo)

Nombre del Contrato: Eliminar Activo (activo)
Propósito: Seleccionar el Activo que se Desea Eliminar
Tipo: Sistema
Referencia: Caso de Uso Eliminar Activos
Salida: Activo a Eliminar Seleccionado
Excepción: No existe formulario electrónico de eliminación de activos
Pre-condición: Que exista formulario electrónico de eliminación de activos
Pos-condición:

3. CONTRATO DE OPERACION (Aceptar Eliminación)

Nombre del Contrato: Aceptar Eliminación (activo)
Propósito: Aceptar la Eliminación del Activo Seleccionado
Tipo: Sistema
Salida: Mensaje "Activo Eliminado"
Excepción: No exista la opción de aceptar eliminación del activo
Pre-condición: Que exista formulario electrónico de eliminar activo, que la información del activo a eliminar este correcta.
Pos-condición: Activo inexistente en la base de datos

Modificar Activos

1. CONTRATO DE OPERACION (Escoger Opción Activos)

Nombre del Contrato: Escoger Opción Activos (op)
Propósito: Presentar Formulario electrónico con los Activos Existentes
Tipo: Sistema
Referencia: Caso de Uso Modificar Activos
Salida: Lista de activos existentes
Excepción: No exista formulario electrónico de activos
Pre-condición: Exista formulario electrónico de activos , exista activos
Pos-condición:

2. CONTRATO DE OPERACIÓN (Seleccionar el Activo a Modificar)

Nombre del Contrato: Seleccionar el Activo a Modificar (activo)

Propósito: Seleccionar un activo para modificar los datos que no estén correctos

Tipo: Sistema

Referencia: Caso de Uso Modificar Activos

Salida: Presentación del activo a modificar con sus datos

Excepción: No exista formulario electrónico de modificación de activos

Pre-condición: Que exista formulario electrónico de modificación de activos, que exista activos.

Pos-condición:

3. CONTRATO DE OPERACION (Modificar Datos Deseados)

Nombre del Contrato: Modificar Datos Deseados (Descripcion_Activo, Grupo_Activos,Valor_Económico, Valor_No_Económico,Texto)

Propósito: Modificar los datos del activo seleccionado

Tipo: Sistema

Referencia: Caso de Uso Modificar Activos

Salida: Lista de Datos Modificados

Excepción: No exista formulario electrónico de modificación de activos

Pre-condición: exista formulario electrónico de modificación de activos, que existan activos

Pos-condición:

NOTA: *Los demás Contratos de Operación correspondientes a las Gestiones especificadas en los Requisitos se encuentran en el Anexo 4*

DIAGRAMAS DE COLABORACIÓN

Gestión Activos

Ingresar Activos

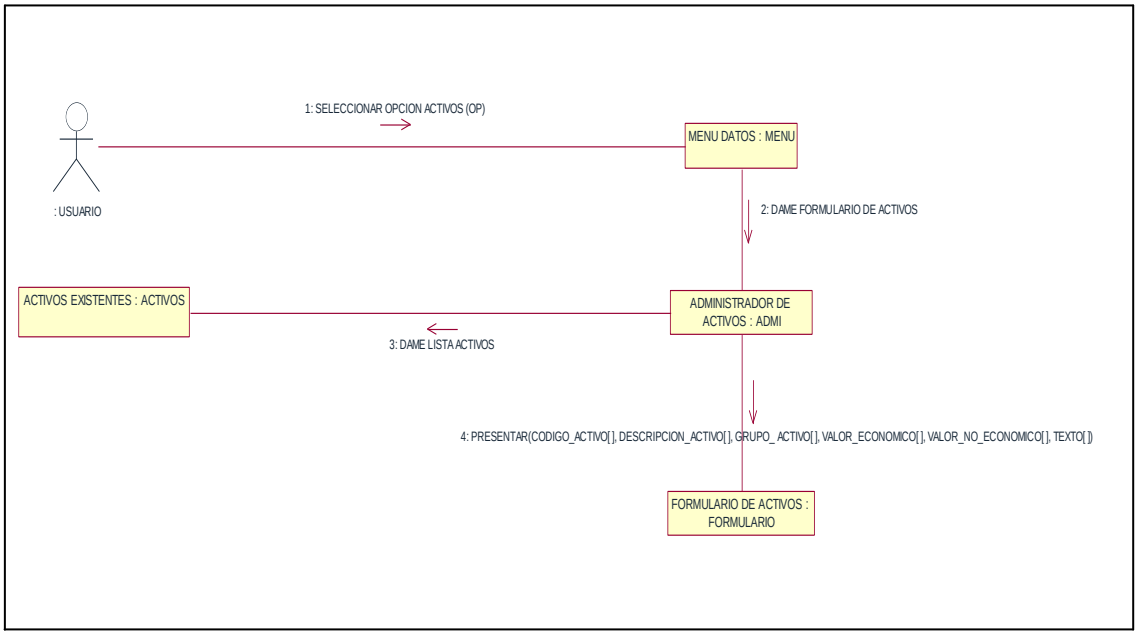


FIGURA 4.7 DIAGRAMA DE COLABORACIÓN SELECCIONAR OPCIÓN ACTIVOS

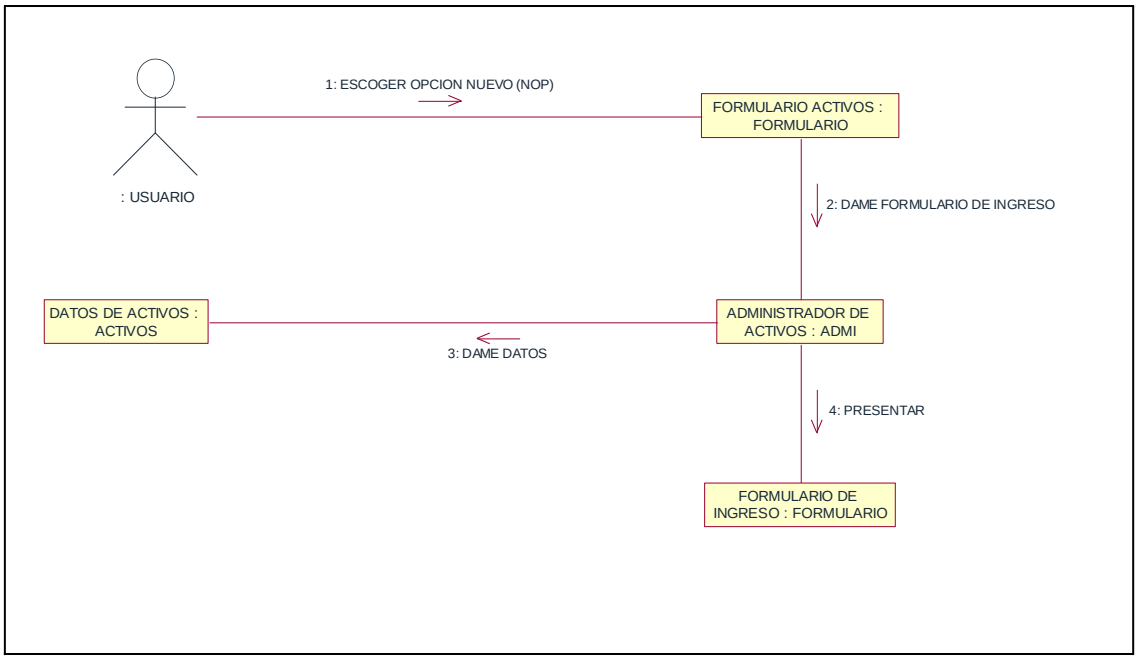


FIGURA 4.8 DIAGRAMA DE COLABORACIÓN SELECCIONAR OPCIÓN NUEVO

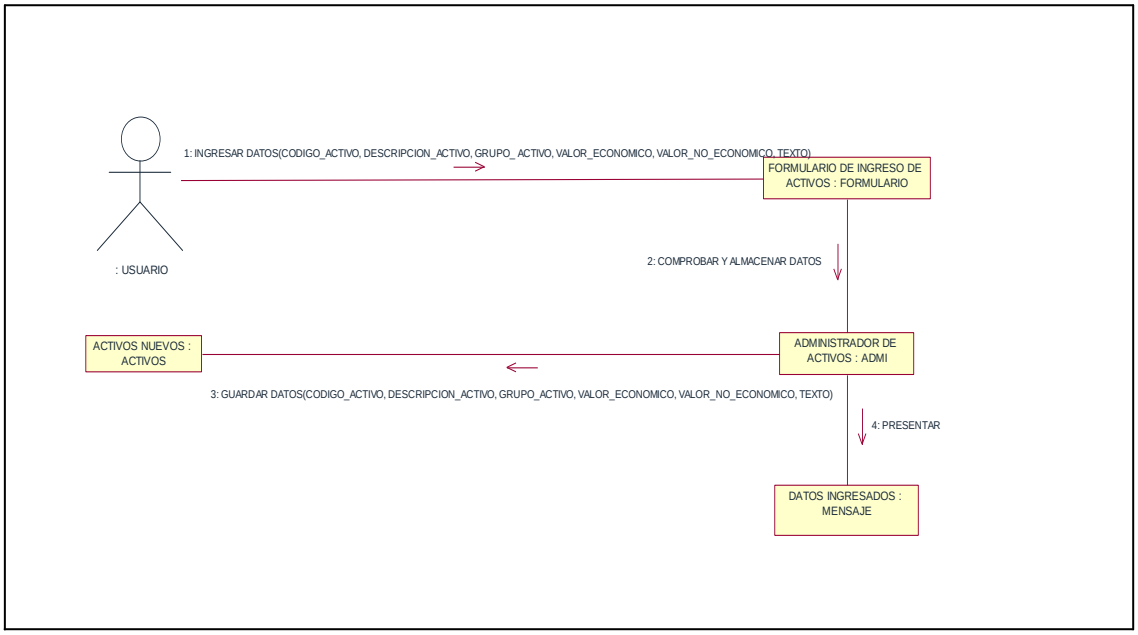


FIGURA 4.9 DIAGRAMA DE COLABORACIÓN INGRESAR DATOS DEL ACTIVO

Eliminar Activos

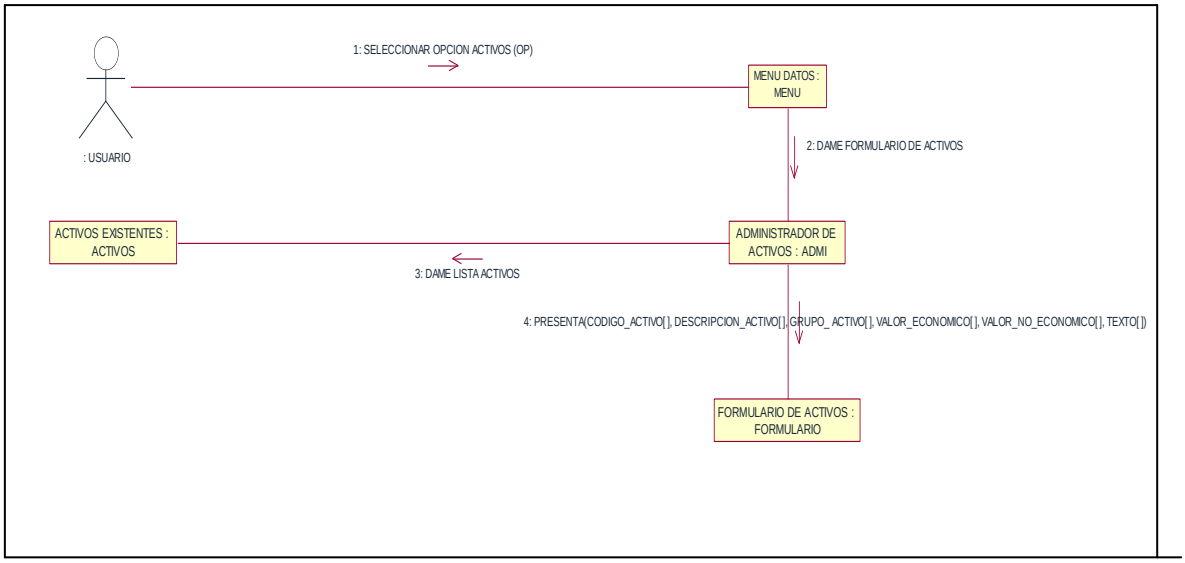


FIGURA 4.10 DIAGRAMA DE COLABORACIÓN SELECCIONAR OPCIÓN ACTIVOS

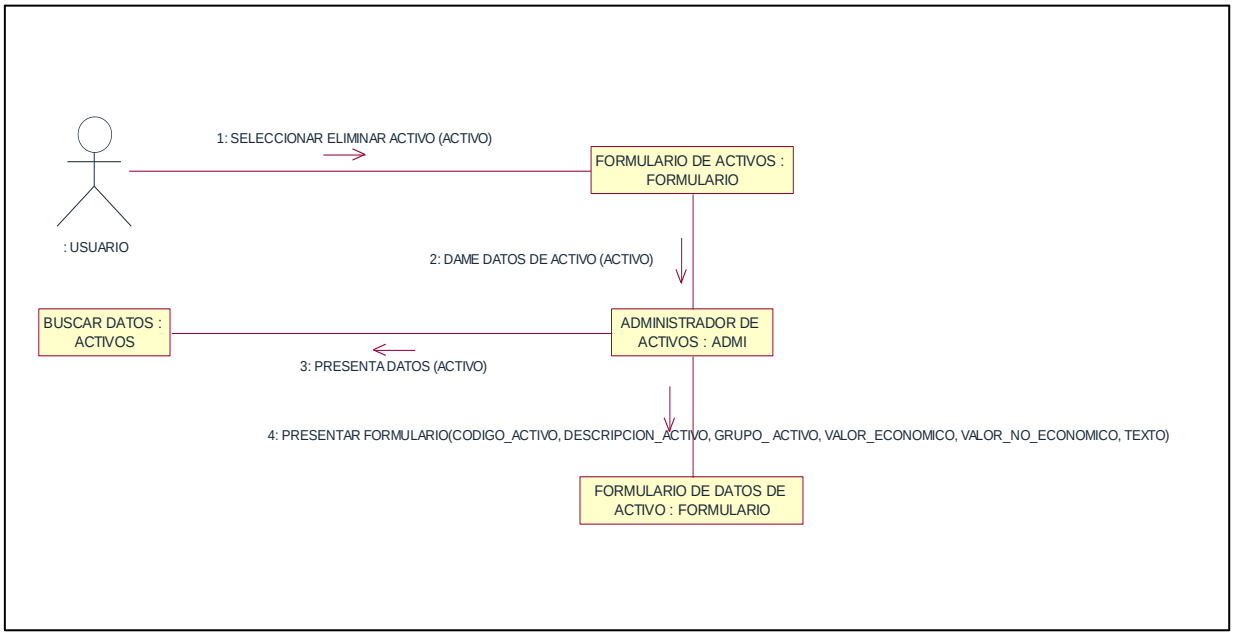


FIGURA 4.11 DIAGRAMA DE COLABORACIÓN SELECCIONAR EL ACTIVO A ELIMINAR

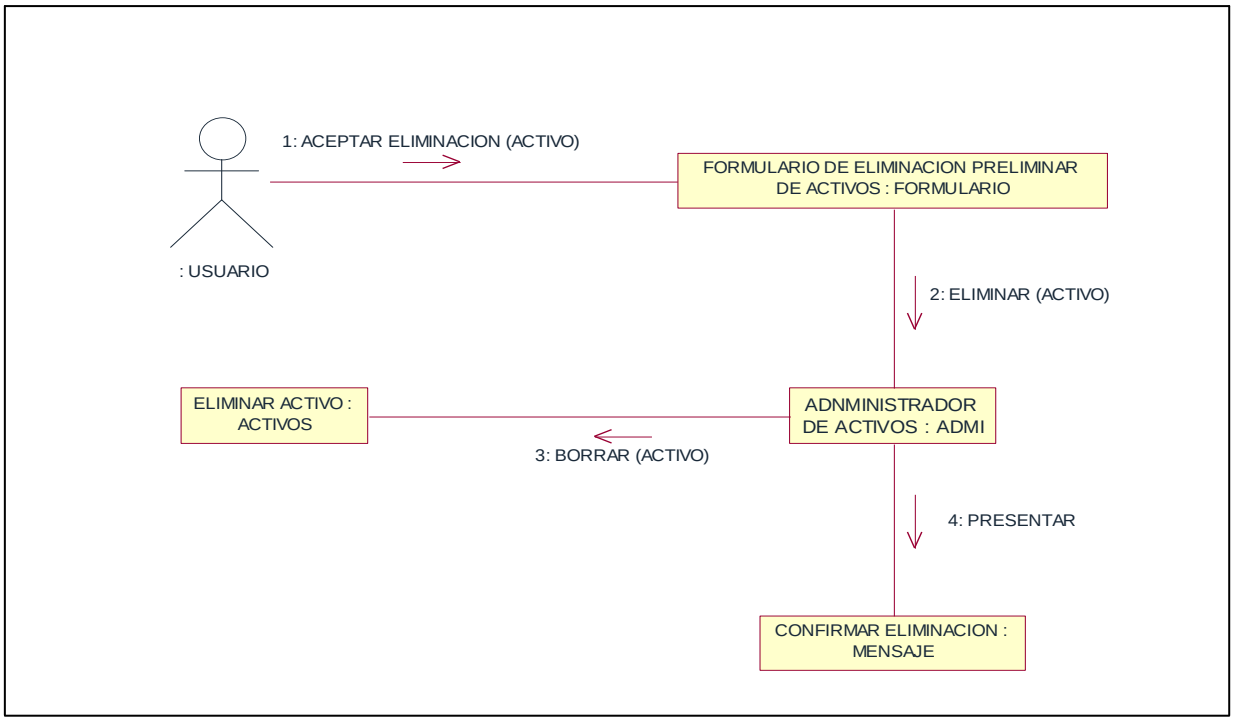


FIGURA 4.12 DIAGRAMA DE COLABORACIÓN ACEPTAR ELIMINACIÓN

Modificar Activos

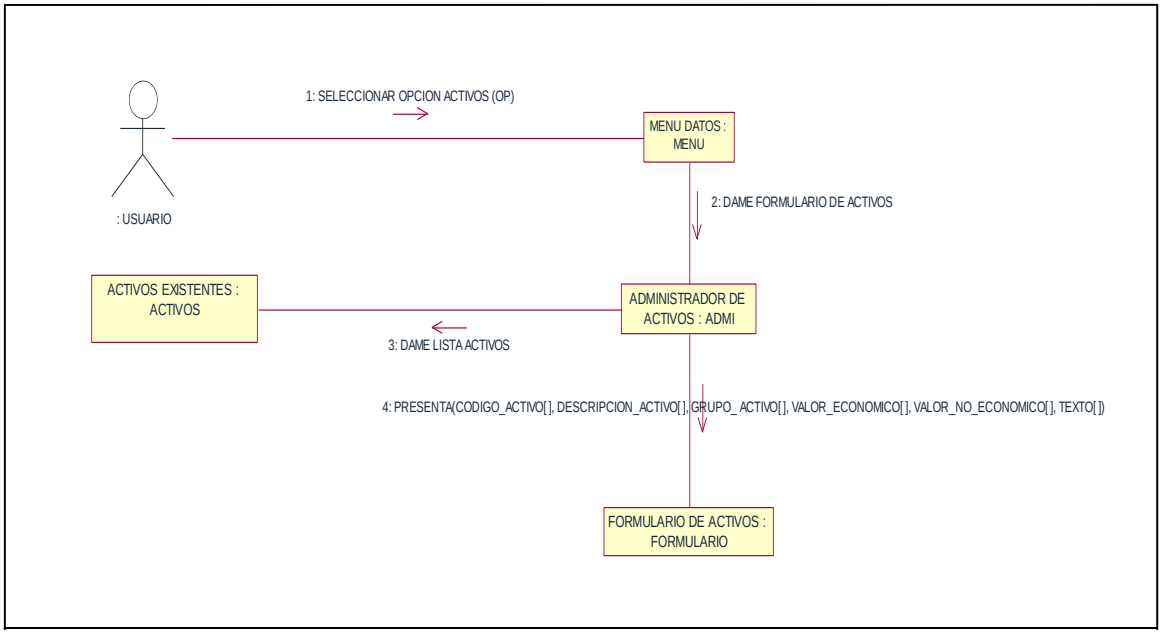


Figura 4.13 Diagrama de Colaboración Seleccionar Opción Activos

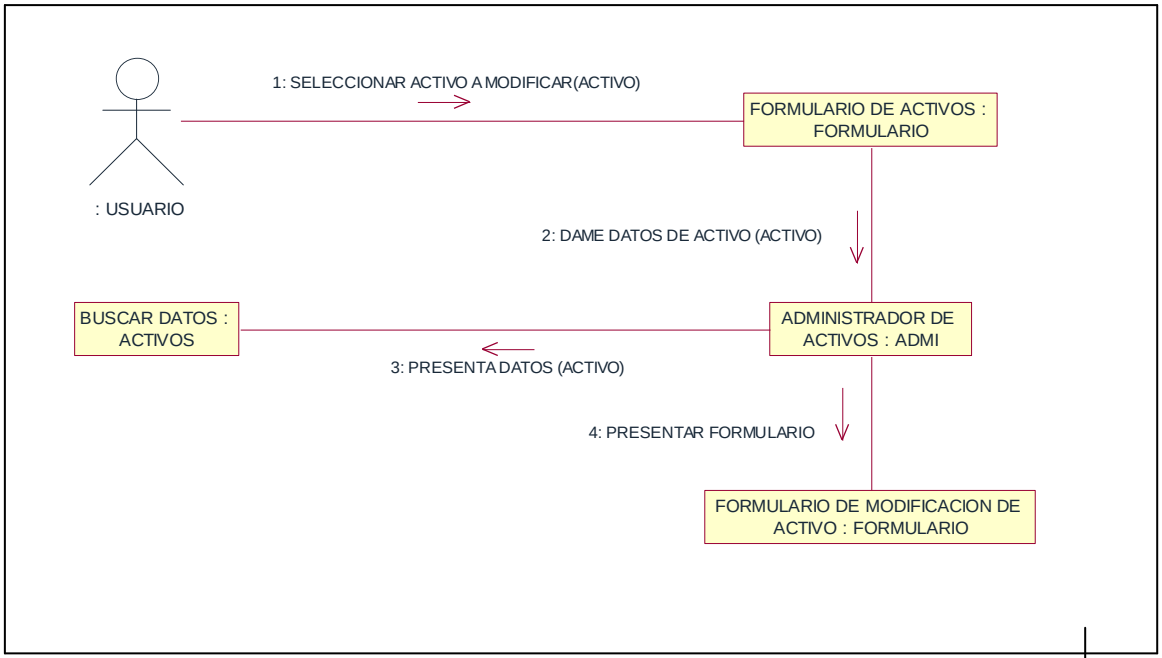


FIGURA 4.14 DIAGRAMA DE COLABORACIÓN SELECCIONAR ACTIVO A MODIFICAR

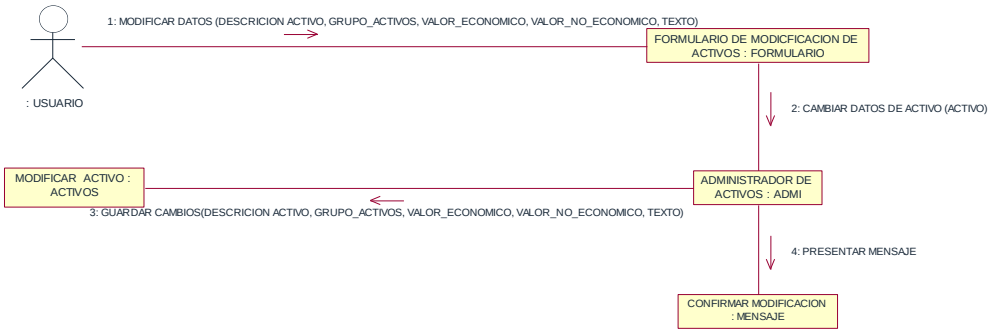


FIGURA 4.15 DIAGRAMA DE COLABORACIÓN MODIFICAR DATOS DESEADOS

NOTA: *Los demás Diagramas de Colaboración correspondientes a las Gestiones especificadas en los Requisitos se encuentran en el Anexo 4*

DIAGRAMA DE OBJETOS

Ingresar Activos

Seleccionar Ingresar Activos

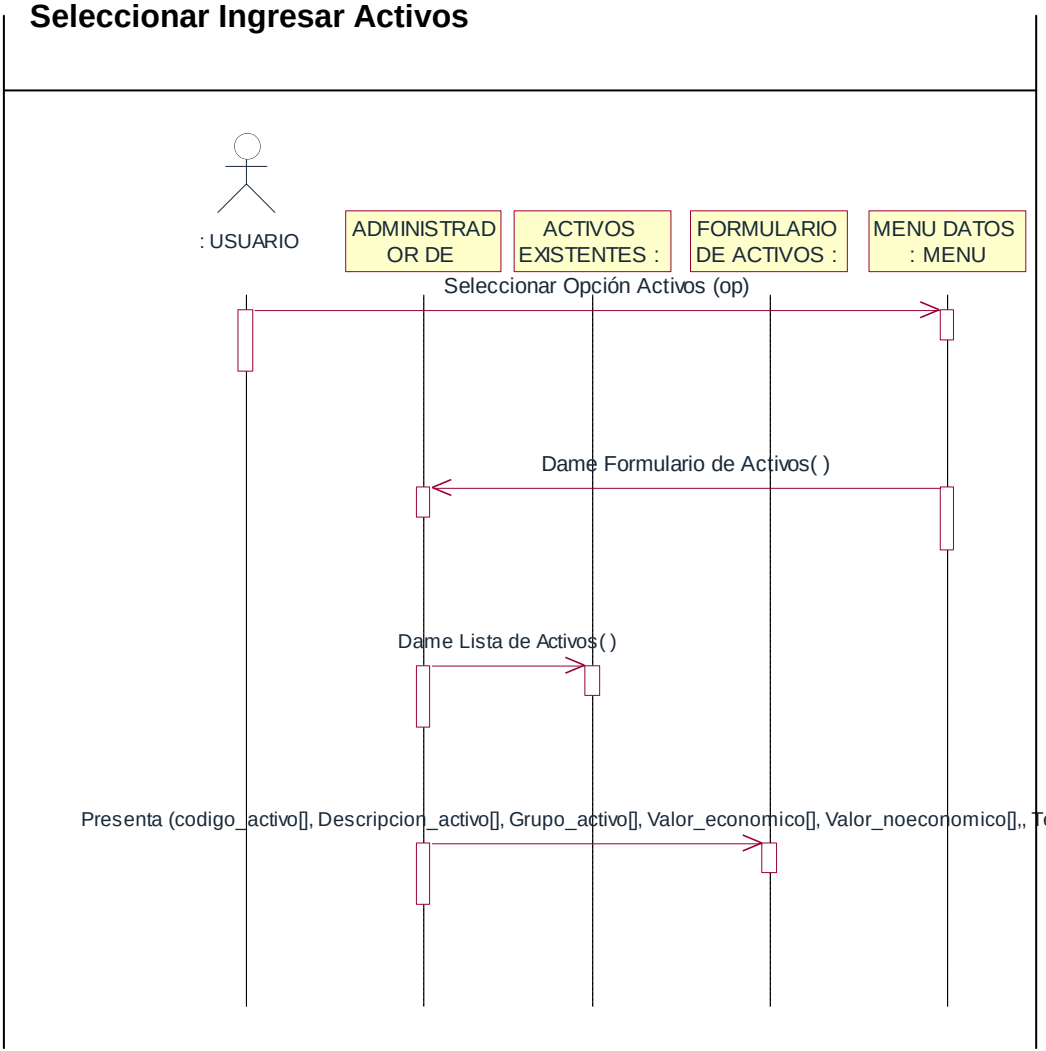


FIGURA 4.16 DIAGRAMA DE OBJETOS SELECCIONAR INGRESAR ACTIVOS

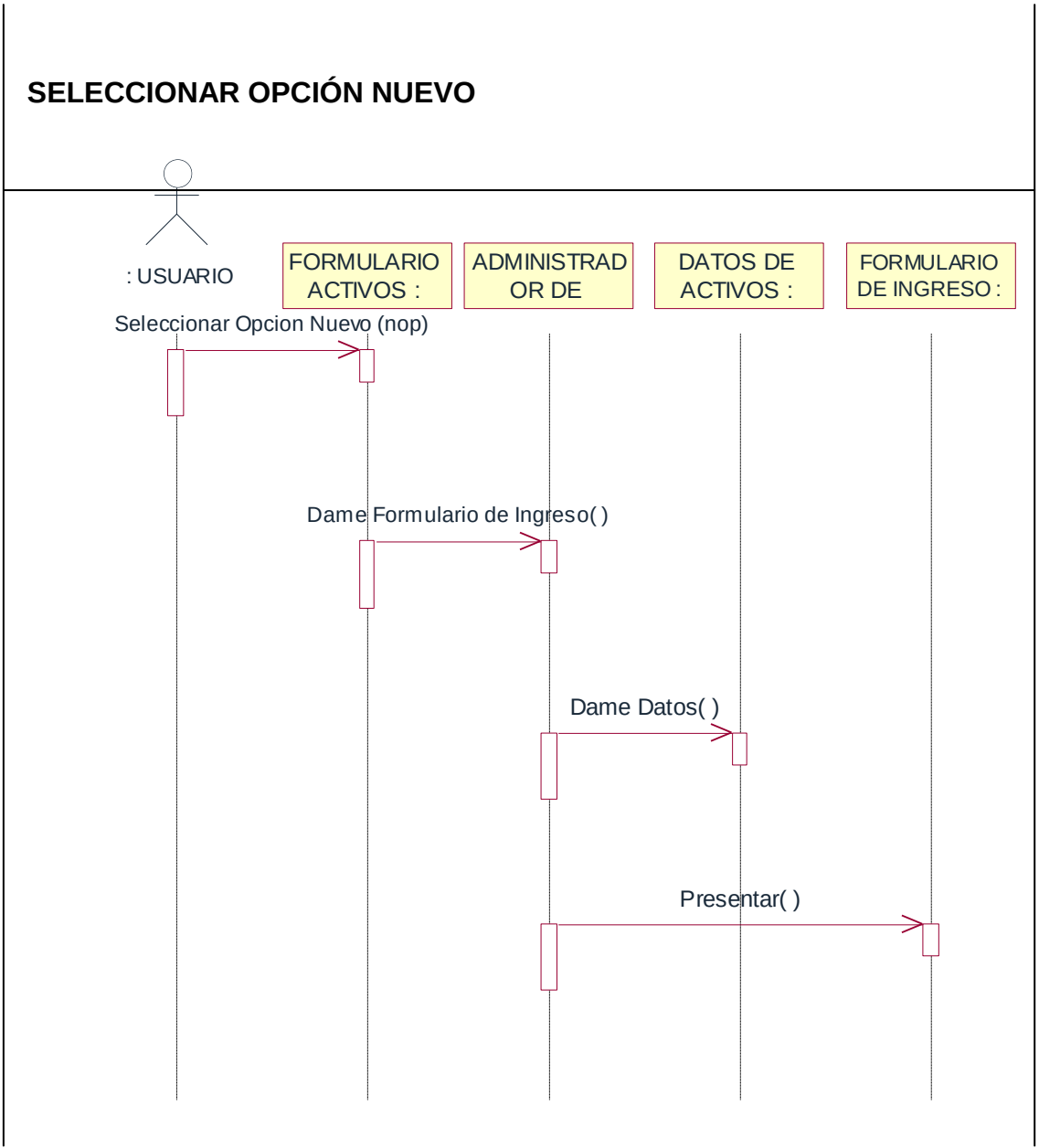


FIGURA 4.17 DIAGRAMA DE OBJETOS SELECCIONAR OPCIÓN NUEVO

INGRESAR DATOS

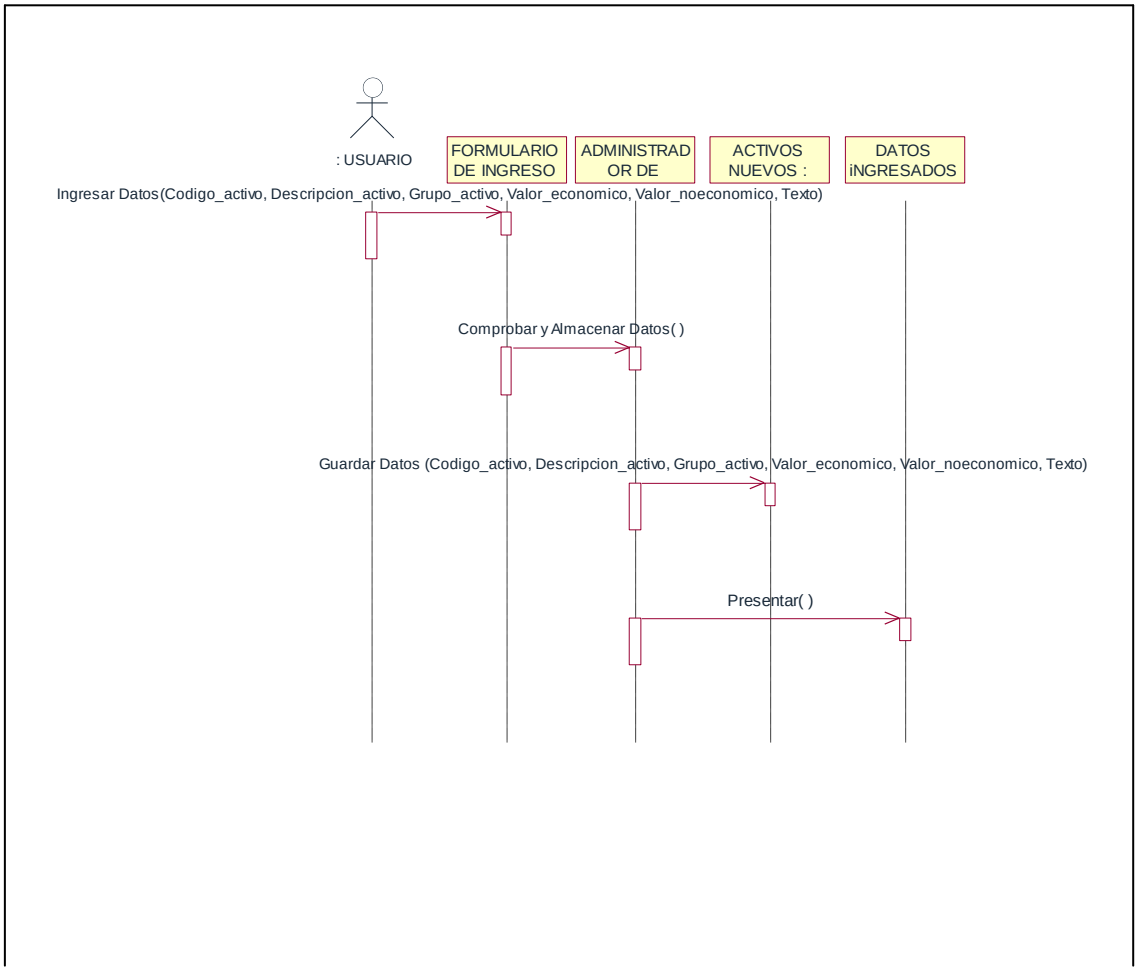


FIGURA 4.18 DIAGRAMA DE OBJETOS INGRESAR DATOS

Eliminar Activos

Seleccionar Opción Activos

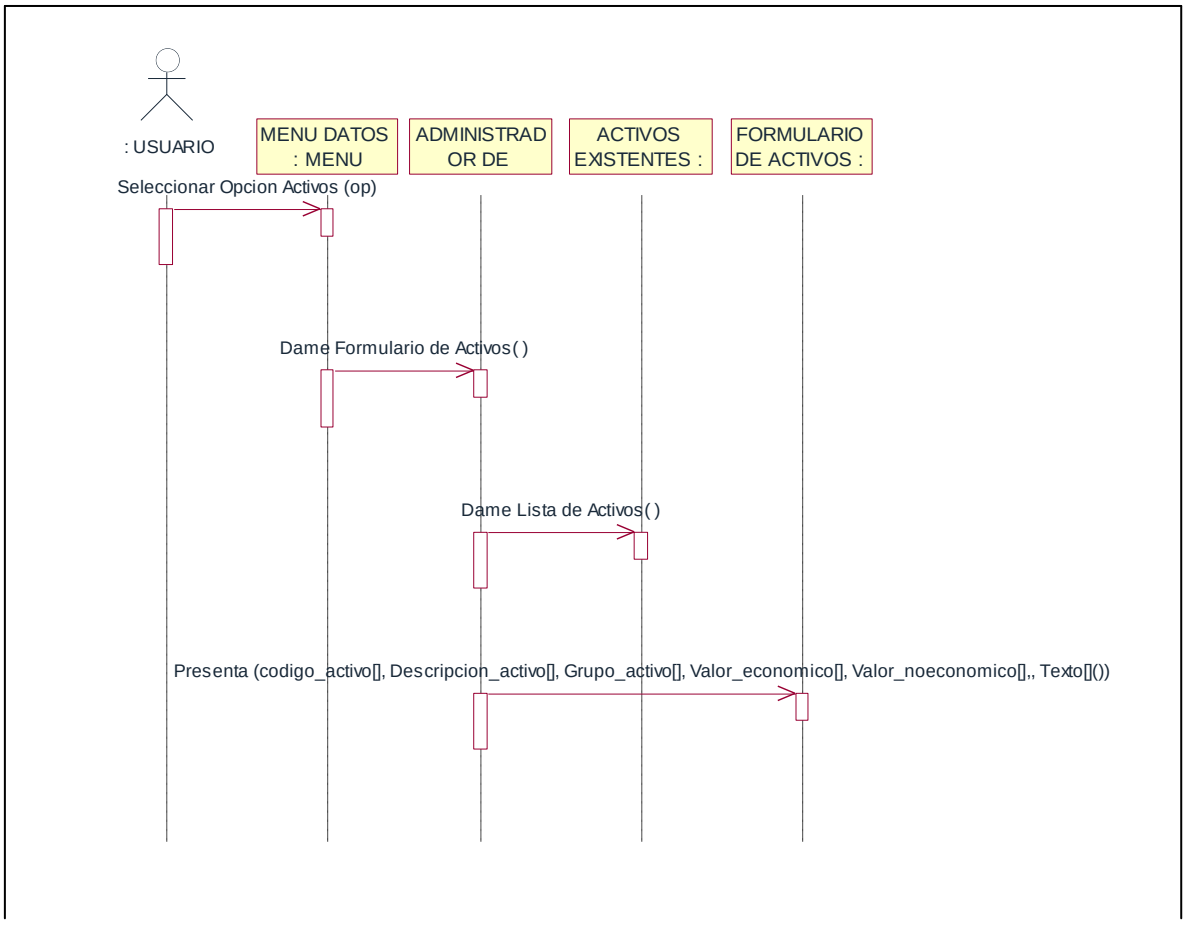


FIGURA 4.19 DIAGRAMA DE OBJETOS SELECCIONAR OPCIÓN ACTIVOS

Eliminar Activo

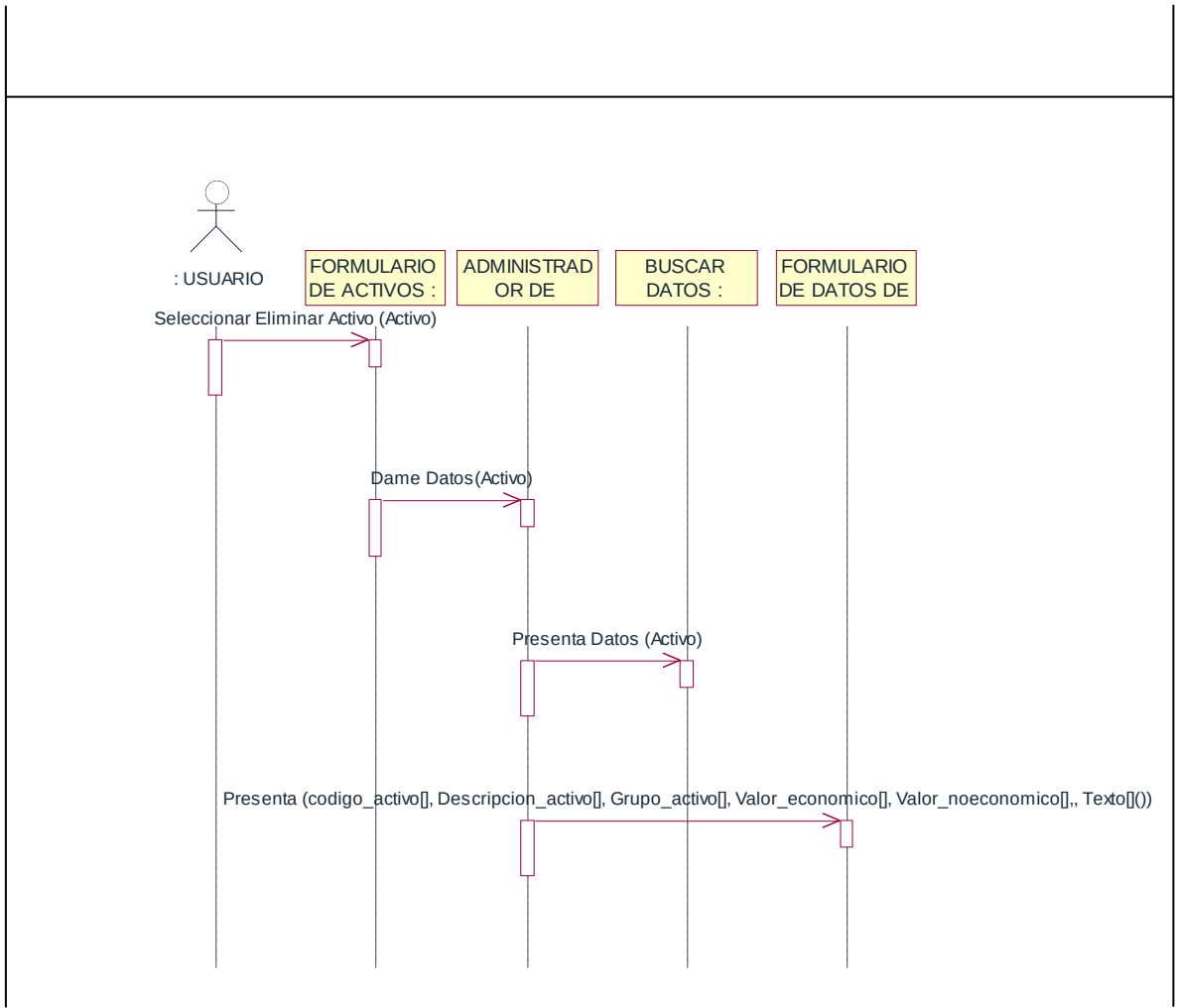


FIGURA 4.20 DIAGRAMA DE OBJETOS SELECCIONAR ACTIVO A ELIMINAR

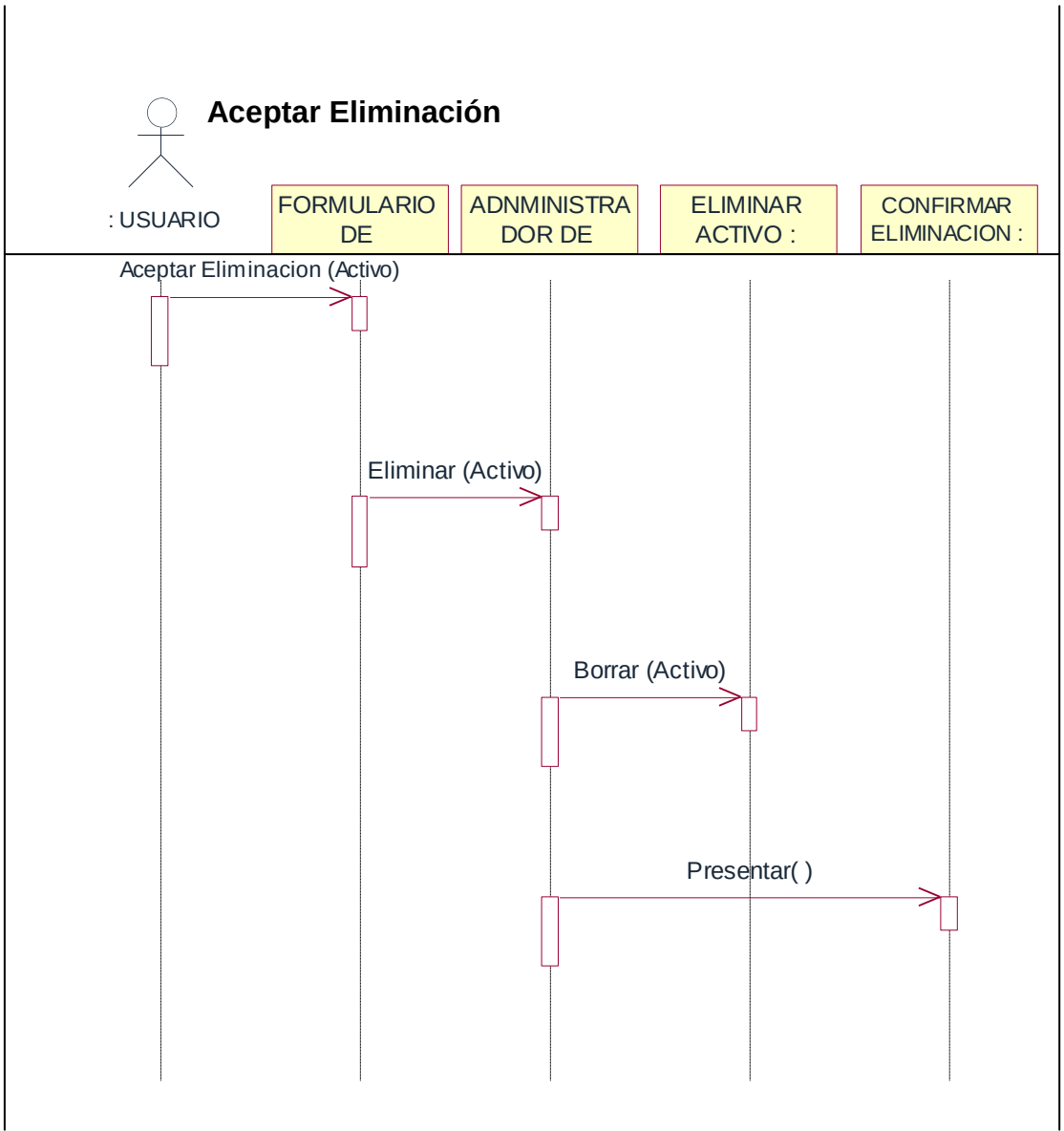


FIGURA 4.21 DIAGRAMA DE OBJETOS ACEPTAR ELIMINACIÓN

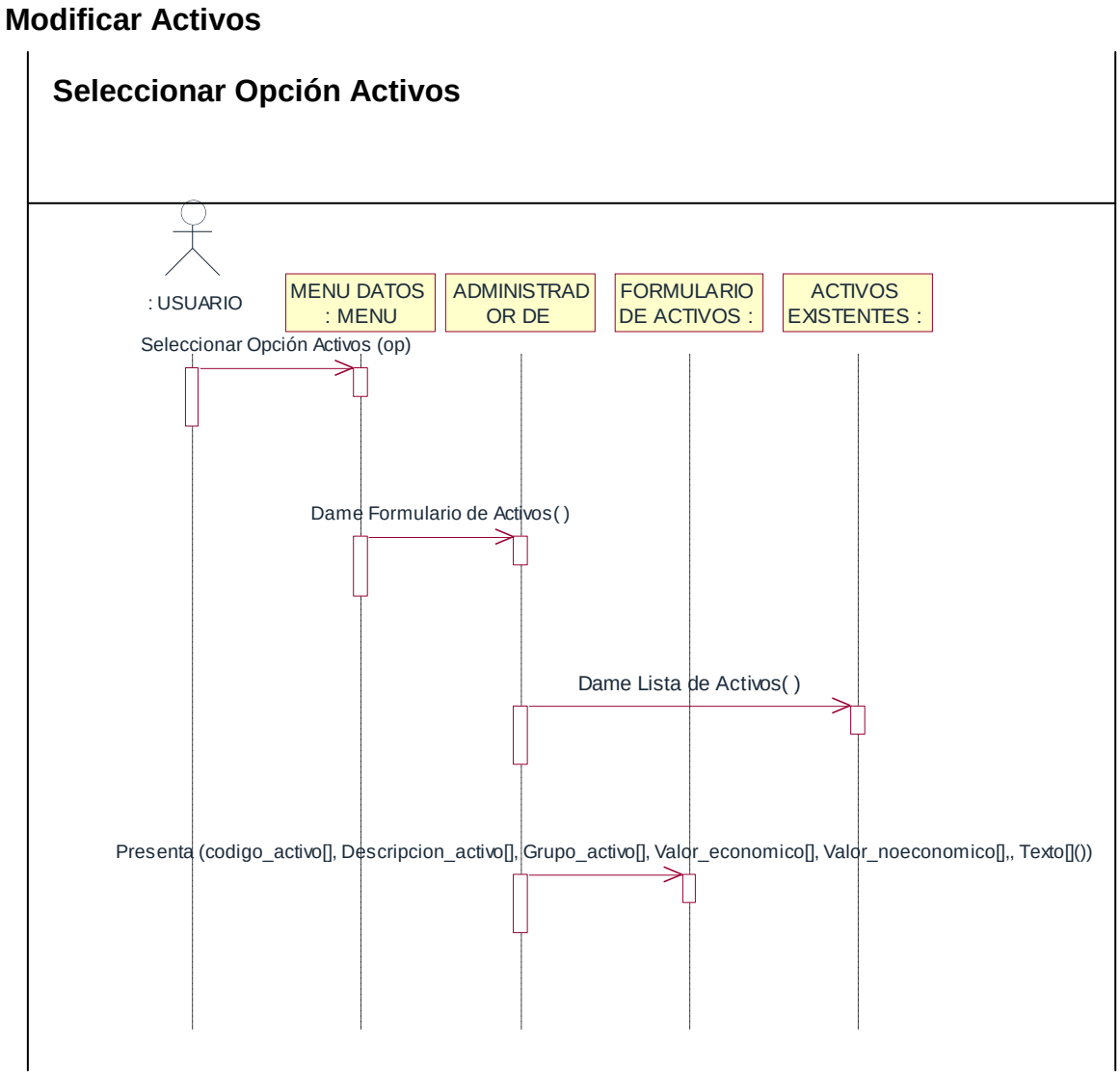


FIGURA 4.22 DIAGRAMA DE OBJETOS SELECCIONAR OPCIÓN ACTIVOS

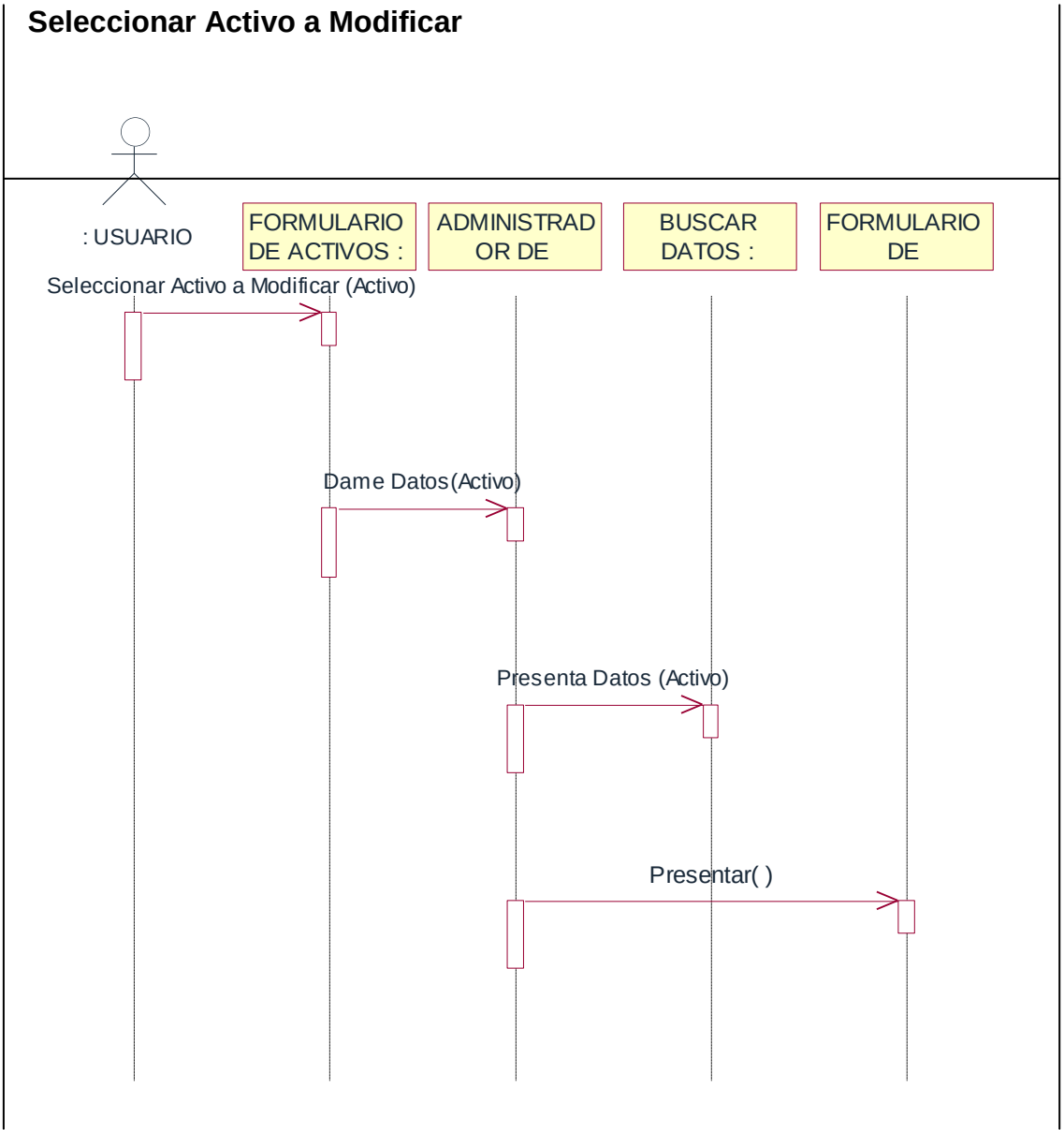


FIGURA 4.23 DIAGRAMA DE OBJETOS SELECCIONAR ACTIVO A MODIFICAR

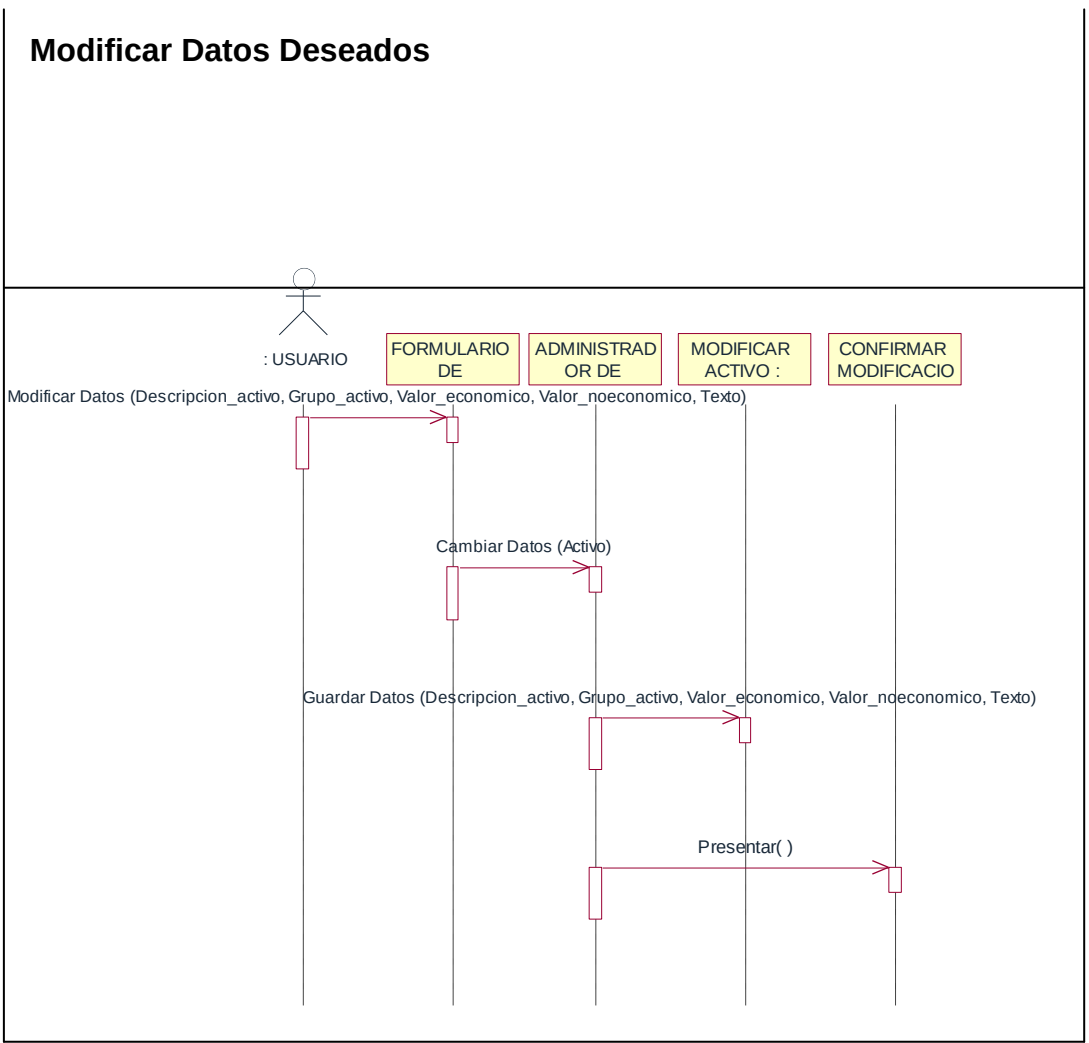


FIGURA 4.24 DIAGRAMA DE OBJETOS MODIFICAR DATOS DESEADOS

4.7 IMPLEMENTACION

En la implementación se presenta el diagrama de clases que no es más que las clases junto con los atributos y las relaciones entre ellas.

DIAGRAMA DE CLASES

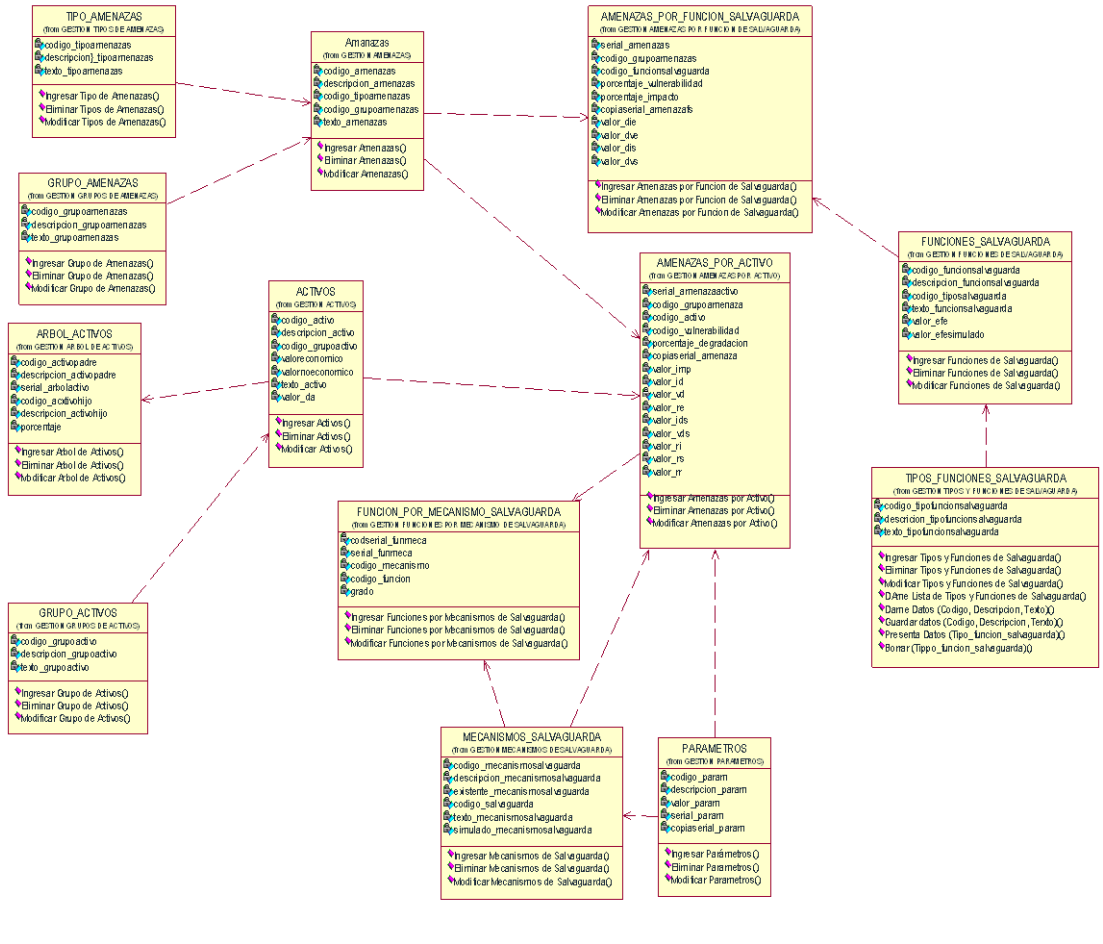


FIGURA 4.25 DIAGRAMA DE CLASES

4.8 PRUEBAS

4.8.1 Propósito

El propósito del Plan de Pruebas es recoger toda la información necesaria para planear y controlar el esfuerzo de las pruebas dadas.

Este Plan de Pruebas para el Sistema de Gestión de Riesgos de Proyectos Software GRPS tiene los siguientes objetivos:

- **Identificar las pruebas que se realizarán en el sistema.**
- **Identificar problemas en el funcionamiento del sistema.**
- **Establecer recursos requeridos para la realización de cada una de las pruebas.**

4.8.2 Alcance

El Plan de Pruebas describe los niveles de comprobación del sistema; es decir, las pruebas de unidad e integración y los tipos de comprobación como la funcionalidad, utilidad, fiabilidad las mismas que serán dirigidas por este plan de prueba.

4.8.3 Personas al que se dirige el plan

Este Plan de Pruebas esta dirigido exclusivamente para la o las personas encargadas de la verificación funcional del sistema o para aquellas personas que vean en este documento una ayuda al uso impropio del sistema.

4.8.4 Preparación del Plan de Pruebas

La siguiente tabla que se presenta a continuación, permitirá determinar para cada requisito la característica a ser probada y los tipos de prueba que se emplearán.

Requisito	Característica a probar	Tipos de prueba
Gestión Grupo de Activos	• Crear un Grupo de Activos y almacenar datos. • Crear un Grupo de Activos con código existente. • Crear un Grupo de Activos con campos obligatorios vacíos. • Crear un Grupo de Activos con valores que no admiten los campos. • Modificar los datos de un Grupo de Activos y actualizar datos. • Modificar los datos de un Grupo de Activos con campos obligatorios vacíos. • Modificar los datos de un Grupo de Activos con valores que no admiten los campos. • Eliminar Grupo de Activos • Buscar datos de un Grupo de Activos y desplegar información	Pruebas de caja negra. • Valores típicos de error • Valores imposibles
Gestión Activos	• Crear un Activo y almacenar datos. • Crear un Activo con código existente. • Crear un Activo con campos obligatorios vacíos. • Crear un Activo con valores que no admiten los campos.	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

	• Modificar los datos de un Activo y actualizar datos. • Modificar los datos de un Activo con campos obligatorios vacíos. • Modificar los datos de un Activo con valores que no admiten los campos. • Eliminar Activos • Buscar datos de un Activo y desplegar información	
Gestión Árbol de Activos	• Crear un Árbol de Activos y almacenar datos. • Crear un Árbol de Activos con campos obligatorios vacíos. • Crear un Árbol de Activos con valores que no admiten los campos. • Modificar los datos de un Árbol de Activos y actualizar datos. • Modificar los datos de un Árbol de Activos con campos obligatorios vacíos. • Modificar los datos de un Árbol de Activos con valores que no admiten los campos. • Eliminar Árbol de Activos • Buscar datos de un Árbol de Activos y desplegar información	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

Gestión Tipos de Funciones de Salvaguarda	• Crear Tipos de Funciones de Salvaguarda y almacenar datos. • Crear Tipos de Funciones de Salvaguarda con código existente. • Crear Tipos de Funciones de Salvaguarda con campos obligatorios vacíos. • Crear Tipos de Funciones de Salvaguarda con valores que no admiten los campos. • Eliminar Tipos de Funciones de Salvaguarda • Eliminar Tipos de Funciones de Salvaguarda con información relacionada • Modificar los datos de un Tipo de Función de Salvaguarda y actualizar datos • Modificar los datos de un Tipo de Función de Salvaguarda con campos obligatorios vacíos. • Modificar los datos de un Tipo de Función de Salvaguarda con valores que no admiten los campos. • Buscar datos de un Tipo de Función de Salvaguarda y desplegar información	Pruebas de caja negra. • Valores típicos de error • Valores imposibles
Gestión Funciones de Salvaguarda	• Crear Funciones de Salvaguarda y almacenar datos . • Crear Funciones de Salvaguarda con campos obligatorios vacíos • Crear Funciones de Salvaguarda con valores que no admiten los	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

	campos. • Eliminar una Función de Salvaguarda • Eliminar una Función de Salvaguarda con información relacionada. • Modificar los datos de una Función de Salvaguarda y actualizarlos. • Modificar los datos de una Función de Salvaguarda con campos obligatorios vacíos. • Modificar los datos de una Función de Salvaguarda con valores que no admiten los campos. • Buscar datos de una Función de Salvaguarda y desplegar información. • Buscar datos de una Función de Salvaguarda con código no existente. • Buscar datos de una Función de Salvaguarda con campo código vacío.	
Gestión Mecanismos de Salvaguarda	• Crear Mecanismos de Salvaguarda y almacenar datos. • Crear Mecanismos de Salvaguarda con código existente. Crear Mecanismos de Salvaguarda con campos obligatorios vacíos. • Crear Mecanismos de Salvaguarda con valores que no admiten los campos.	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

	• Eliminar Mecanismos de Salvaguarda • Eliminar Mecanismos de Salvaguarda con información relacionada • Modificar los datos de un Mecanismo de Salvaguarda y actualizar datos • Modificar los datos de un Mecanismo de Salvaguarda con campos obligatorios vacíos. • Modificar los datos de un Mecanismo de Salvaguarda con valores que no admiten los campos. • Buscar datos de un Mecanismo de Salvaguarda y desplegar información • Buscar datos de un Mecanismo de Salvaguarda con código de Mecanismo de Salvaguarda no existente. • Buscar datos de un Mecanismo de Salvaguarda con código de Mecanismo de Salvaguarda vacío.	
Gestión Función por Mecanismo de Salvaguarda	• Crear Funciones por Mecanismos de Salvaguarda y almacenar datos. • Crear Funciones por Mecanismos de Salvaguarda con campos obligatorios vacíos. • Crear Funciones por Mecanismos de Salvaguarda con valores que no admiten los campos. • Eliminar Funciones por Mecanismos de Salvaguarda	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

	• Eliminar Funciones por Mecanismos de Salvaguarda con información relacionada • Modificar los datos de una Función por Mecanismo de Salvaguarda y actualizar datos • Modificar los datos de una Función por mecanismos de Salvaguarda con campos obligatorios vacíos. • Modificar los datos de una Función por Mecanismo de Salvaguarda con valores que no admiten los campos. • Buscar datos de una Función por Mecanismo de Salvaguarda y desplegar información	
Gestión Grupo de Amenazas	• Crear un Grupo de Amenazas y almacenar datos. • Crear un Grupo de Amenazas con código existente. • Crear un Grupo de Amenazas con campos obligatorios vacíos. • Crear un Grupo de Amenazas con valores que no admiten los campos. • Eliminar Grupo de Amenazas • Eliminar un Grupo de Amenazas con información relacionada • Modificar los datos de un Grupo de Amenazas y actualizar datos • Modificar los datos de un Grupo de Amenazas con campos obligatorios vacíos. • Modificar los datos de un Grupo de	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

	Amenazas con valores que no admiten los campos. • Buscar datos de un Grupo de Amenazas y desplegar información • Buscar datos de un Grupo de Amenazas con código de Grupo de Amenazas no existente. • *Buscar datos de un Grupo de Amenazas con código de Grupo de Amenazas vacío.*	
Gestión Tipo de Amenazas	• Crear un Tipo de Amenazas y almacenar datos. • Crear un Tipo de Amenazas con código existente. • Crear un Tipo de Amenazas con campos obligatorios vacíos. • Crear un Tipo de Amenazas con valores que no admiten los campos. • Eliminar un Tipo de Amenazas • Eliminar un Tipo de Amenazas con información relacionada • Modificar los datos de un Tipo de Amenaza y actualizar datos • Modificar los datos de un Tipo de Amenaza con campos obligatorios vacíos. • Modificar los datos de un Tipo de Amenaza con valores que no aten los campos. • Buscar datos de un Tipo de Amenaza y desplegar información • Buscar datos de un Tipo de	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

	Amenaza con código de Tipo de Amenaza no existente. • Buscar datos de un Tipo de Amenaza con código de Tipo de Amenaza vacío.	
Gestión Amenazas	• Crear Amenazas y almacenar datos. • Crear Amenazas con código existente. • Crear Amenazas con campos obligatorios vacíos. • Crear Amenazas con valores que no admiten los campos. • Eliminar Amenazas • Eliminar Amenazas con información relacionada • Modificar los datos de una Amenaza y actualizar datos • Modificar los datos de una Amenaza con campos obligatorios vacíos. • Modificar los datos de una Amenaza con valores que no admiten los campos. • Buscar datos de una Amenaza y desplegar información • Buscar datos de una Amenaza con código de Amenaza no existente. • Buscar datos de una Amenaza con código de Amenaza vacío.	Pruebas de caja negra. • Valores típicos de error • Valores imposibles
Gestión Amenazas por Función de Salvaguarda	• Crear Amenazas por Función de Salvaguarda y almacenar datos. • Crear Amenazas por Función de Salvaguarda con campos	Pruebas de caja negra. • Valores típicos de error

	obligatorios vacíos. • Crear Amenazas por Función de Salvaguarda con valores que no admiten los campos. • Eliminar Amenazas por Función de Salvaguarda • Eliminar Amenazas por Función de Salvaguarda con información relacionada • Modificar los datos de una Amenaza por función de Salvaguarda y actualizar datos • Modificar los datos de una Amenaza por Función de Salvaguarda con campos obligatorios vacíos. • Modificar los datos de una Amenaza por función de Salvaguarda con valores que no admiten los campos. • Buscar datos de una Amenaza por Función de Salvaguarda y desplegar información	• Valores imposibles
Gestión Amenazas por Activos	• Crear Amenazas por Activos y almacenar datos. • Crear Amenazas por Activos con campos obligatorios vacíos. • Crear Amenazas por Activos con valores que no admiten los campos. • Eliminar Amenazas por Activos • Eliminar Amenazas por Activos con información relacionada • Modificar los datos de una Amenaza	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

	por Activos y actualizar datos • Modificar los datos de una Amenaza por Activos con campos obligatorios vacíos. • Modificar los datos de una Amenaza por Activo con valores que no admiten los campos. • Buscar datos de una Amenaza por Activo y desplegar información	
Gestión Parámetros	• Crear Parámetros y almacenar datos. • Crear Parámetros con código existente • Crear Parámetros con campos obligatorios vacíos. • Crear Parámetros con valores que no admiten los campos. • Eliminar Parámetros • Eliminar Parámetros con información relacionada • Modificar los datos de un Parámetro y actualizar datos • Modificar los datos de un Parámetro con campos obligatorios vacíos. • Modificar los datos de un Parámetro con valores que no admiten los campos. • Buscar datos de un Parámetro y desplegar información	
Gestión Análisis	▪ Calcular Riesgo Efectivo	Pruebas de caja

	▪ Imprimir Reporte ▪ Calcular Riesgo Residual ▪ Imprimir Reporte ▪ Calcular Riesgo Simulado ▪ Seleccionar Mecanismos a Simular ▪ Imprimir Repote ▪ Calcular Riesgo Intrínseco ▪ Imprimir Reporte	negra. • Valores típicos de error • Valores imposibles
Gestión Resultados	▪ Presentar Resultados Gráficamente ▪ Imprimir Gráficos ▪ Presentar Resultados en Listados de Tablas ▪ Imprimir Tablas ▪ Presentar Resultados en Listados de Resultados ▪ Imprimir Listados ▪ Presentar Valores Totales de Riesgo del Proyecto ▪ Imprimir Totales	Pruebas de caja negra. • Valores típicos de error • Valores imposibles

TABLA 4.8 PREPARACION DEL PLAN DE PRUEBAS

4.8.5 Referencias

- Especificación de Casos de Prueba

4.8.6 Pruebas planeadas

Se ha diseñados un conjunto de pruebas para comprobar el cumplimiento de las especificaciones de requisitos.

Se van a desarrollar las siguientes pruebas:

4.8.7 Pruebas Unitarias

El objetivo de esta prueba es verificar la lógica y las funciones de cada uno de los módulos, comprobando la integridad de los datos como también de la de la base de datos.

Las Pruebas Unitarias del plan de pruebas debe enfocarse en cualquier requisito para probar y puede remontarse en los casos de uso o funciones de negocio y reglas del negocio. Las metas de estas pruebas son verificar la aceptación de los datos apropiados, el procesamiento, recuperación, y la aplicación apropiada de las reglas del negocio. Este tipo de comprobación está basado en las técnicas de caja negra; que verifican la aplicación y sus procesos interiores actuando recíprocamente con la aplicación a través la Interfaz Gráfica de Usuario (GUI) y analizan el rendimiento o resultado.

La siguiente tabla identifica un contorno de la comprobación recomendada para cada aplicación.

Objetivo de la técnica:	La funcionalidad de la Comprobación del funcionamiento, incluye la navegación, la entrada de los datos, procesamientos, y recuperación para observar las conductas entre ellos.
Técnica:	Ejecutar cada caso de uso en su propia interfaz , de manera individual cada flujo de eventos de cada caso de uso así como cada función., usando datos válidos e inválidos, para verificar que: ▪ Los resultados esperados ocurren cuando se usan datos válidos ▪ Los mensaje de error o alerta apropiados se despliegan cuando se usan datos inválidos. Que cada regla del negocio se aplica propiamente
Criterios de Exito :	La técnica apoya la comprobación de: ▪ Todas las especificaciones de casos de uso

TABLA 4.9 PRUEBAS UNITARIAS

4.8.8 Prueba de Integración de Componentes

El objetivo de esta prueba es comprobar el correcto funcionamiento de la relación que existe entre las interfaces de cada uno de los componentes.

4.8.9 Comprobación del Ciclo del Negocio

La comprobación del Ciclo del Negocio deben emular las actividades realizadas en el Sistema de Gestión de Riesgos de Proyectos Software GRPS, en el tiempo actual.

Objetivo de la Técnica:	El objetivo es probar y respaldar que los procesos se realizan según el modelo del negocio
Técnica:	Se simularán varios ciclos del negocio.
Criterios de éxito:	La técnica apoya la comprobación de todos los ciclos del negocio.

TABLA 4.10 COMPROBACION DEL CICLO DEL NEGOCIO

4.8.10 Especificación de la Plantilla para los Casos de Prueba

4.8.11 Descripción

Resumen lo que realiza el caso de prueba.

4.8.12 Condiciones de Ejecución

Especifica los usuarios que pueden realizar el caso de prueba.

4.8.13 Criterios de Entrada

Especifica el criterio que se usará para determinar si la ejecución de la Prueba puede empezar.

4.8.14 Criterios de Salida

Especifica el criterio que se usará para determinar si la ejecución de la Prueba está completa o su ejecución no proporciona beneficio.

4.8.15 Resultado Esperado

Proporciona un contorno breve de la forma y contenido de los resúmenes de evaluación de la prueba.

4.8.16 Evaluación de la Prueba

Proporciona un contorno breve de la forma y contenido de los informes que miden la magnitud de la prueba.

4.8.17 Recursos Requeridos

4.8.17.1 Hardware Base del Sistema

La siguiente tabla muestra los recursos del sistema para realizar el Plan de Pruebas.

Recursos del Sistema		
Recurso	**Cantidad**	**Nombre y Tipo**
Computador	1	Petium IV

TABLA 4.11 RECURSOS DEL SISTEMA

4.8.17.2 Software Base del Sistema

La siguiente tabla muestra los recursos del sistema para realizar el Plan de Pruebas.

Nombre del Elemento Software	Tipo y otras Notas
Windows 2000	Sistema Operativo
Microsoft Visual Studio 6.0	Software en el que esta desarrollado el sistema
Microsoft Access	Software donde se crea la base de datos

TABLA 4.12 SOFTWARE BASE DEL SISTEMA

CAPITULO V

En el presente capitulo se exponen las conclusiones y recomendaciones una vez terminado el desarrollo de la Herramienta de Gestión de Riesgos de Proyectos Software.

5.1 CONCLUSIONES:

- El desarrollo de la presente tesis ha sido oportuno, pues se ha dado importancia a lo que realmente las instituciones publicas, instituciones privadas, personas naturales, etc deberían tomar en cuenta antes de desarrollar o de poner en funcionamiento un Proyecto de Software, los riesgos que se puede suscitar y las perdidas económicas que a estos grupos les puede representar

- La Metodología de Análisis y Gestión de Riesgos Magerit, ayuda a enfocar el problema de la seguridad desde una perspectiva completa, y evolucionable en el tiempo

- Los activos son los elementos Físicos, lógicos y organizativos que dan soporte a la realización de análisis y gestión de riesgos

- Las Herramientas Ris2k y Chinchon son herramientas que realizan gestión de Riesgos siguiendo la metodología magerit, en estas herramientas se ha basado nuestro proyecto de tesis para su realización, además .las formulas de calculo de los riesgos que puede sufrir un proyecto software son iguales tanto para Ris2k, Chinchon y la nueva herramienta que se ha desarrollado.

- Las herramientas empleadas para el desarrollo de este proyecto son de licencia gratuita rompiendo el paradigma de que “lo gratis no es bueno”.

- El software que se presenta en esta tesis es fácil de utilizar ya que su ambiente es similar Windows y no es necesario el previo conocimiento de otras herramientas para su manejo básico.

- Los resultados que la nueva herramienta de gestión de riesgos de proyecto software presenta son fáciles de comprender y confiables para ponerlos en práctica cuando se los requiera.

- La instalación de la nueva herramienta de gestión de riesgos se lo puede realizar sobre cualquier plataforma Windows por lo tanto es recomendable su uso.

5.2 RECOMENDACIONES

- Estudiar opcionalmente las herramientas de distribución libre Ris2k y Chinchon para el Análisis y gestión de riesgos

- Identificar correctamente los activos y realizar adecuadamente su clasificación ya que es éxito de la gestión de riesgos.

- Desarrollar y poner y funcionamiento el software de acuerdo a los resultados entregados por las herramientas al realizar gestión de riesgos.

- Aplicar la Metodología Magerit en proyectos de Software ya que es una metodología completa para crear o desarrollar Software

- Utilizar la nueva herramienta de gestión de riesgos propuesta para esta tesis ya que es fácil de utilizar, se la puede instalar sobre cualquier plataforma Windows, no es necesario el previo conocimiento de otras herramientas de gestión de riesgos y los resultados que presenta son tan confiables como los resultados que presenta las herramientas Chinchon y Ris2k.

Latacunga, Octubre del 2005

Sandra Sorayda Rubio Rubio

050252977-9

AUTOR

Ing. Santiago Jácome G.

DECANO DE LA FACULTAD

DE SISTEMAS E INFORMATICA

Dr. Rodrigo Vaca Corrales

SECRETARIO ACADEMICO

ESPE-L

ANEXO 4

ESPECIFICACIÓN DE REQUISITOS SOFTWARE PARA EL SISTEMA DE GESTIÓN DE RIESGOS DE PROYECTOS SOFTWARE "SAMBA"

1. Archivo

- Salir

2. RIS2K

- **Grupos de Activos**

Campos	**Tipo de dato**	**Longitud**
Código de grupo de activo	alfanumérico	2
Descripción	alfanumérico	80
Texto libre	alfanumérico	indefinido

Alta

Para dar de alta un grupo de activos damos un clic sobre la opción nuevo, una vez rellenado tanto el código de grupo de activo como la descripción, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de activos en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un grupo de activos, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar un grupo de activos haciendo un clic sobre el código de grupo de activos y luego dar un clic en el botón eliminar.

Se borrará la información referente al grupo de activos de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cambios

Para modificar un grupo de activos, deberán efectuarse los siguientes pasos:
1. Seleccionar un grupo de activos haciendo un clic sobre el código de grupo de activos y luego sobre el botón editar. Automáticamente el grupo de activos aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Activos**

Campos	**Tipo de dato**	**Longitud**
Código del activo	numérico	4

Descripción del activo	alfanumérico	80
Código del grupo de activo	alfanumérico	2
Descripción del grupo de activo	alfanumérico	80
Valor económico	numérico	9
Valor no económico	alfanumérico	255
Texto libre	alfanumérico	indefinido

Alta

Para dar de alta un activo damos un clic en la opción nuevo, una vez rellenado tanto el grupo de activo como su descripción, el código de grupo de activo y su descripción a la que pertenece y su peso, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior derecha de la pantalla. Si el usuario pulsa este botón significará que se acepta el activo en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un activo, es decir para borrarlo de la base de datos debe efectuar los siguiente: Seleccionar un activo haciendo un clic sobre el código del activo y luego dar un clic en el botón eliminar. Se borrará la información referente al activo de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como activos existan en la base de datos.

Cambios

Para modificar un activo, deberán efectuarse los siguientes pasos:

1. Seleccionar un activo haciendo un clic sobre el código de activo y luego sobre el botón editar. Automáticamente el activo aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como activos existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Árbol de Activos**

Campos	**Tipo de dato**	**Longitud**
Código del Activo Padre	numérico	4
Descripción del Activo Padre	alfanumérico	80
Código del Activo Hijo	numérico	4
Descripción del Activo Hijo	alfanumérico	80
Porcentaje de Dependencia	Numérico sin decimales	3

Alta

Para dar de alta una relación entre activos es necesario llevar a cabo los siguientes pasos:

1. El usuario debe seleccionar el activo existente contenido en el combo, automáticamente el sistema levantara el código del mismo para que aparezca en la ventana principal además debe ingresar el grado de dependencia, de no ser así aparecerá el mensaje de error correspondiente.
2. Una vez seleccionado el dato del activo padre seleccionamos los activos hijos de la misma manera que en el paso 1 damos un clic sobre el botón grabar situado en la parte inferior derecha de la pantalla correspondiente, se aceptarán los datos.
3. Una vez aceptados los datos se dará la posibilidad de asociar al activo introducido (activo padre), tantos activos (activos hijos) como se desee, siempre que sean correctos y aparezcan contenidos en la base de datos.

Esta operación podrá repetirse tantas veces como activos aparezcan en el Combo. La relación se grabará en la base de datos de la herramienta.

Baja

Para dar de baja una relación entre activos, es decir para borrarla de la base de datos deberán efectuarse los siguientes pasos:

1. Seleccionar un activo (padre o hijo) haciendo un clic sobre el código de activo (padre o hijo) o sobre la descripción del activo (padre o hijo) o sobre el grado de dependencia.
2. Hacer un clic sobre el eliminar, situado en la parte inferior derecha de la pantalla. Se borrará la información referente a la relación padre - hijo de la base de datos, con lo que también desaparecerá de la pantalla.

El proceso puede repetirse tantas veces como relaciones existan en la base de datos

Nota: Para dar de baja una relación el usuario puede seleccionar tanto un activo hijo como un activo padre. En ambos casos se pedirá confirmación de la baja de la relación padre - hijo.

Cambios

Los activos (padre e hijo) no podrán modificarse, pero si la relación padre - hijo, es decir que el usuario podrá cambiar las relaciones existentes o modificar el grado de dependencia, siguiendo los mismos pasos llevados a cabo para la realización de un alta.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Grupos de Amenazas**

Campos	**Tipo de dato**	**Longitud**
Código del Grupo de Amenaza	alfanumérico	2
Descripción del Grupo de Amenaza	alfanumérico	80
Texto libre	alfanumérico	indefinido

Alta

Para dar de alta un grupo de amenazas damos un clic sobre la opción nuevo, una vez rellenado tanto el código de grupo de amenaza como la descripción, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el

botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de amenazas en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un grupo de amenazas, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar un grupo de activos haciendo un clic sobre el código de grupo de amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente al grupo de amenaza de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cambios

Para modificar un grupo de amenazas, deberán efectuarse los siguientes pasos:
1. Seleccionar un grupo de amenazas haciendo un clic sobre el código de grupo de amenazas y luego sobre el botón editar. Automáticamente el grupo de amenazas aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como grupos de amenazas existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Tipos de Amenazas**

Campos	**Tipo de dato**	**Longitud**
Código del Tipo de Amenaza	alfanumérico	2
Descripción del Tipo de Amenaza	alfanumérico	80
Texto libre	alfanumérico	indefinido

Alta

Para dar de alta un tipo de amenaza damos un clic sobre la opción nuevo, una vez rellenado tanto el código del tipo de amenaza como la descripción, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el tipo de amenaza en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un tipo de amenaza, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar un tipo de amenaza haciendo un clic sobre el código de tipo de amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente al tipo de amenaza de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como tipos de amenaza existan en la base de datos.

Cambios

Para modificar un tipo de amenaza, deberán efectuarse los siguientes pasos:

1. Seleccionar un tipo de amenaza haciendo un clic sobre el código del tipo de amenaza y luego sobre el botón editar. Automáticamente el tipo de amenaza aparecerá en la ventana de edición.

2. Realizar las modificaciones.

3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como tipos de amenaza existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Mecanismos de Salvaguarda**

Campos	**Tipo de dato**	**Longitud**	
Código del Mecanismo de Salvaguarda	alfanumérico	3	
Descripción del Mecanismo de Salvaguarda	alfanumérico	80	
Mecanismo de Salvaguarda existente	alfanumérico	1	S: si ya existe N: si no existe
Valoración económica	numérico	9	

Texto libre	alfanumérico	indefinido	

Alta

Para dar de alta un mecanismo de salvaguarda damos un clic sobre la opción nuevo, una vez rellenado tanto el código del mecanismo de salvaguarda, descripción del mecanismo de salvaguarda, la existencia del mecanismo de salvaguarda y la valoración económica, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de activos en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un mecanismo de salvaguarda es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar un mecanismo de salvaguarda haciendo un clic sobre el código de mecanismo de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente al mecanismo de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como mecanismos de salvaguarda existan en la base de datos.

Cambios

Para modificar un mecanismo de salvaguarda, deberán efectuarse los siguientes pasos:
1. Seleccionar un mecanismo de salvaguarda haciendo un clic sobre el código de mecanismo de salvaguarda y luego sobre el botón editar. Automáticamente el mecanismo de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.

El proceso puede repetirse tantas veces como mecanismos de salvaguarda existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Tipos de Funciones de Salvaguarda**

Campos	**Tipo de dato**	**Longitud**
Código del Tipo Función de Salvaguarda	alfanumérico	2
Descripción Tipo de Función de Salvaguarda	alfanumérico	80
Texto libre	alfanumérico	indefinido

Alta

Para dar de alta un tipo de función de salvaguarda damos un clic sobre la opción nuevo, una vez rellenado tanto el código de tipo de función de salvaguarda, descripción de tipo de función de salvaguarda, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta el grupo de activos en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja un tipo de función de salvaguarda, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar un tipo de función de salvaguarda haciendo un clic sobre el código del tipo de función de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente al tipo de función de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cambios

Para modificar un tipo de función de salvaguarda, deberán efectuarse los siguientes pasos:
1. Seleccionar un tipo de función de salvaguarda haciendo un clic sobre el código de tipo de función de salvaguarda y luego sobre el botón editar. Automáticamente el tipo de función de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como grupos de activos existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Funciones de Salvaguarda**

Campos	**Tipo de dato**	**Longitud**
Código de la Función de Salvaguarda	Alfanumérico	3
Descripción de la Función de Salvaguarda	Alfanumérico	80
Código del Tipo Función de Salvaguarda	Alfanumérico	2
Descripción del Tipo de Función de Salvaguarda	Alfanumérico	80
Texto libre	Alfanumérico	indefinido
Código del Mecanismo de Salvaguarda	Alfanumérico	3
Descripción del Mecanismo de Salvaguarda	Alfanumérico	80
Grado de Cumplimentación	Numérico sin decimales	3

Alta

Para dar de alta una función de salvaguarda damos un clic sobre la opción nuevo, una vez rellenado tanto el código de la función de salvaguarda, la descripción de la función de salvaguarda, el código del tipo de la función de salvaguarda, la descripción del tipo de la función de salvaguarda, el código del mecanismo de salvaguarda, la descripción del mecanismo de salvaguarda y el grado de Cumplimentación, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la función de salvaguarda en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja una función de salvaguarda, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar un grupo de activos haciendo un clic sobre el código de función de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente a la función de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como funciones de salvaguarda existan en la base de datos.

Cambios

Para modificar una función de salvaguarda, deberán efectuarse los siguientes pasos:
1. Seleccionar una función de salvaguarda haciendo un clic sobre la función de salvaguarda y luego sobre el botón editar. Automáticamente la función de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como funciones de salvaguarda existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Amenazas**

Campos	Tipo de dato	Longitud
Código de la Amenaza	Alfanumérico	3
Descripción de la Amenaza	Alfanumérico	80
Código del Grupo de Amenazas	Alfanumérico	2
Descripción del Grupo de Amenazas	Alfanumérico	80
Código del Tipo de Amenazas	Alfanumérico	2
Descripción del Tipo de Amenazas	Alfanumérico	80
Texto libre	Alfanumérico	indefinido

Alta

Para dar de alta una amenaza damos un clic sobre la opción nuevo, una vez rellenado tanto el código de amenaza, la descripción de la amenaza, el código del grupo de amenaza, la descripción del grupo de amenaza, el código del tipo de la amenaza, la descripción del tipo de amenaza, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la amenaza en curso dándose de alta automáticamente en la base de datos.

Nota: En esta pantalla no se pueden dar de alta grupos de amenaza, tipos de amenaza. Esa operación se realizará en las pantallas y opciones establecidas para ello.

Baja

Para dar de baja una amenaza, es decir para borrarla de la base de datos debe efectuar lo siguiente: Seleccionar una amenaza haciendo un clic sobre el código de amenaza y luego dar un clic en el botón eliminar. Se borrará la

información referente a la amenaza de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como amenazas existan en la base de datos.

Cambios

Para modificar una amenaza, deberán efectuarse los siguientes pasos:
1. Seleccionar una amenaza haciendo un clic sobre el código de amenaza y luego sobre el botón editar. Automáticamente la amenaza aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como amenazas existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Amenaza por Función de Salvaguarda**

Código de la amenaza	Alfanumérico	3
Descripción de la función	Alfanumérico	80

de salvaguarda		
Porcentaje de reducción de vulnerabilidad	Numérico sin decimales	3
Porcentaje de reducción de impacto	Numérico sin decimales	3

Alta

Para dar de alta una amenaza por función de salvaguarda damos un clic sobre la opción nuevo, una vez rellenado tanto el código de la amenaza, la función de salvaguarda, el porcentaje de reducción de vulnerabilidad, porcentaje de reducción del impacto, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la amenaza por función de salvaguarda en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja una amenaza por función de salvaguarda, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar una amenaza por función de salvaguarda haciendo un clic sobre el código de la amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente a la amenaza por función de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como amenazas por función de salvaguarda existan.

Cambios

Para modificar una amenaza por función de salvaguarda, deberán efectuarse los siguientes pasos:

1. Seleccionar una amenaza por función de salvaguarda haciendo un clic sobre el código de amenaza y luego sobre el botón editar. Automáticamente la amenaza por función de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como amenazas por función de salvaguarda existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Amenazas por Activo**

Descripción de la amenaza	Alfanumérico	80	
Descripción del activo	Alfanumérico	80	
Vulnerabilidad	Alfanumérico	3	Solo puede ser q esta relacionado MF: muy frecuente F: frecuente FN: frecuencia normal PF: poco

			frecuente MPF: muy poco frecuente
Degradación	Alfanumérico sin decimales	3	

Alta

Para dar de alta una amenaza por activo damos un clic sobre la opción nuevo, se nos presenta una ventana donde tenemos diferentes combos que nos muestran la descripción de las amenazas, activos, vulnerabilidad y degradación existentes, una vez seleccionados los datos que deseamos, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la amenaza por activo en curso dándose de alta automáticamente en la base de datos. El código de grupo de amenaza será presentado automáticamente en la ventana principal

Baja

Para dar de baja una amenaza por activo, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar una amenaza por activo haciendo un clic sobre el código de grupo de amenaza y luego dar un clic en el botón eliminar. Se borrará la información referente a la amenaza por activo de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como amenazas por activo existan en la base de datos.

Cambios

Para modificar una amenaza por activo, deberán efectuarse los siguientes pasos:

1. Seleccionar una amenaza por activo haciendo un clic sobre el código de grupo de amenaza y luego sobre el botón editar. Automáticamente el la amenaza por activo aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como amenazas por activos existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Funciones por Mecanismos de Salvaguarda**

Funciones de Salvaguarda	Alfanumérico	80
Mecanismos de Salvaguarda	Alfanumérico	80
Grado de Cumplimiento	Alfanumérico	80

Alta

Para dar de alta una función por mecanismo de salvaguarda damos un clic sobre la opción nuevo, se nos presenta una ventana donde tenemos diferentes combos que nos muestran la descripción de la función de salvaguarda, los mecanismos de salvaguarda y el grado de cumplimiento, una vez

seleccionados los datos que deseamos, el usuario puede grabar los datos en la base de datos haciendo un clic sobre el botón grabar situado en la parte inferior de la pantalla. Si el usuario pulsa este botón significará que se acepta la función por mecanismo de salvaguarda en curso dándose de alta automáticamente en la base de datos.

Baja

Para dar de baja una función por mecanismo de salvaguarda, es decir para borrarlo de la base de datos debe efectuar lo siguiente: Seleccionar una función por mecanismo de salvaguarda haciendo un clic sobre la función de salvaguarda y luego dar un clic en el botón eliminar. Se borrará la información referente a la función por mecanismo de salvaguarda de la base de datos, con lo que también desaparecerá de la pantalla.
El proceso puede repetirse tantas veces como funciones por mecanismo de salvaguarda existan en la base de datos.

Cambios

Para modificar una función por mecanismo de salvaguarda, deberán efectuarse los siguientes pasos:
1. Seleccionar una función por mecanismo de salvaguarda haciendo un clic sobre la función por mecanismo de salvaguarda y luego sobre el botón editar. Automáticamente la función por mecanismo de salvaguarda aparecerá en la ventana de edición.
2. Realizar las modificaciones.
3. Hacer un clic sobre el botón grabar, situado en la parte inferior derecha de la pantalla. Si los datos han sido modificados, se grabarán en la base de datos, actuando como si de un alta se tratase.
El proceso puede repetirse tantas veces como funciones por mecanismo de salvaguarda existan en la base de datos.

Cancelar

Este botón se encuentra en cada una de las ventanas sirve para cancelar cualquier operación que no estemos seguros de realizar.

Salir

Este botón nos permite salir de la ventana en la que estamos trabajando y nos regresa a la ventana principal

- **Eliminar Información**

Esta opción elimina todos los datos contenidos en la base de datos.

- **Parámetros**

Como ya se ha visto en el caso de valoración de activos, degradación, vulnerabilidad su aplicación suele ser difícil al valorarlos desde un punto de vista económico. Generalmente es más fácil, adjudicarle según el grado de importancia de los servicios que suministra. Debido a que MAGERIT, cuando realiza el proceso de análisis y gestión de riesgos, se basa en factores económicos, en estos casos de valoración no económica, se perdería la posibilidad de realizar la valoración de riesgos (siempre en función del valor económico del activo amenazado). Por ello se estima conveniente realizar una asociación entre los valores de escala y un equivalente económico. Una vez que se han tecleado los distintos valores y el botón aceptar esta información pasará a la base de datos de parámetros en la tabla de valores de escala . El tamaño máximo de la información no deberá exceder de 9 dígitos.

3. CHINCHON

- **Copiar Datos**

Esta opción nos permite copiar los datos ingresados en el Ris2k al Chinchon para que en base a esos mismos datos realice los cálculos.

- **Datos Chinchon**

Dentro de esta opción tenemos los datos que debemos ingresar para que el chinchon realice los cálculos.

Es necesario indicar que los datos que se ingresaran son los mismos que se ingresa para el Ris2k: parámetros, grupo de activos, activos, árbol de activos, funciones de salvaguarda, mecanismos de salvaguarda, funciones por mecanismos de salvaguarda, grupos de amenazas, tipos de amenazas, amenazas, amenazas por función de salvaguarda, amenaza por activos y eliminar información es necesario indicar que Chinchon para realizar el cálculo no necesita de los tipos de función de salvaguarda.
El ingreso de los datos se los realiza de la misma forma que para el Ris2k .

4. Análisis

El menú de Análisis comprende los procesos que permiten gestionar las relaciones entre los componentes del riesgo descritos en la Captura de Datos, además de proporcionar los primeros resultados en cuanto a nivel del riesgo efectivo. Dentro de la opción análisis tenemos las opciones de calculo para el Ris2k y Chinchon

- **Ris2k**

Dentro de esta opción tenemos: la opción Nuevo, riesgo efectivo, riesgo simulado.

Nuevo
Nos borra cálculos anteriores es indispensable utilizar esta opción antes de realizar cualquier cálculo para que los datos no sean alterados.

Riesgo Efectivo

Se calcula el riesgo efectivo, para lo cual hay que considerar la efectividad de las funciones de salvaguarda, obtenida por la implementación de los mecanismos que se han detectado como existentes. Una vez conocida la efectividad de las funciones se evalúa su capacidad para disminuir el riesgo y se aplica a los activos amenazados.

Riesgo Simulado

En este proceso, se cálcula el riesgo de simulación, para lo cual hay que considerar la efectividad de las funciones de salvaguarda, obtenida por la implementación de los mecanismos que se han seleccionado para la simulación. Una vez conocida la efectividad de las funciones se evalúa su capacidad para disminuir el riesgo y se aplica a los activos amenazados.

En la pantalla aparecerá una relación de los mecanismos (código y descripción). A través de una serie de columnas MAGERIT informa sobre qué mecanismos existen y cuáles han sido propuestos. Al mismo tiempo se ofrece la posibilidad de seleccionar aquellos mecanismos que se van a utilizar para la simulación, es decir para calcular el riesgo de simulación. Opcionalmente es posible añadir a la selección los mecanismos complementarios y descartar los mecanismos excluyentes.

Una vez seleccionados los mecanismos para la simulación se puede proceder a calcular el riesgo de simulación haciendo un clic sobre el botón Riesgo Simulación que aparece en la parte inferior derecha de la pantalla.

- **Chinchon**

Dentro de esta opción tenemos: Nuevo y Riesgo Efectivo

Nuevo

Nos borra cálculos anteriores es indispensable utilizar esta opción antes de realizar cualquier cálculo para que los datos no sean alterados.

Riesgo Efectivo

Valor del riesgo si se aplican las salvaguardas existentes. Toma en consideración la disminución del impacto y la disminución de la vulnerabilidad.

5. GRÁFICAMENTE

Aquí se nos presenta dos opciones de graficación estadística así tenemos: grafico del riesgo por amenaza y grafico del riesgo por activo.

Grafico del Riesgo por Amenaza

Esta opción nos representa gráficamente los niveles de riesgo en cuanto a las amenazas existentes.

Grafico del Riesgo por Activo

Esta opción nos representa gráficamente le nivel de riesgo que corre cada uno de los activos ingresados.