# UNIVERSIDAD MAYOR DE SAN ANDRES

**FACULTAD DE CIENCIAS PURAS Y NATURALES**

**CARRERA DE INFORMATICA**


# PROYECTO DE GRADO

## “SISTEMA DE GESTION DE RIESGOS EN ACTIVOS DE INFORMACION”

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMATICA
MENCION: INGENIERIA DE SISTEMAS INFORMATICOS

**POSTULANTE:** Univ. Zulma Jhenny Quispe Mamani

**TUTOR:** Lic. Freddy Miguel Toledo Paz

**REVISOR:** Lic. Hugo Javier Reyes Pacheco

**LA PAZ- BOLIVIA**
**2009**

**DEDICATORIA**

A mis padres, Tomas e Hilda,
mi hermana Magaly y a todas
las personas que confiaron en mí.

## AGRADECIMIENTOS

A Dios por iluminar mi camino y permitirme llegar hasta donde estoy.

A los docentes Lic. Freddy Miguel Toledo Paz por las observaciones que tuvo en el presente proyecto.

Lic. Javier Reyes Pacheco por su paciencia y colaboración.

A todos los docentes que me formaron en mi carrera profesional.

Un agradecimiento especial al Ingeniero Juan Carlos Mendoza por todos los consejos y por permitirme desarrollar el presente proyecto.

A mis padres por su apoyo incondicional, mi hermana por darme su apoyo para seguir adelante.

A todos mis compañeros que me brindaron su apoyo y amistad a lo largo de toda mi carrera universitaria.

# RESUMEN

Los elementos importantes en las empresas con un objetivo claro, son los activos los cuales necesitan tener un mejor control de los mismos.

En este sentido se propone un sistema de información confiable y seguro para gestionar toda la información que se genera sobre los activos existentes dentro de la empresa CRS Bolivia.

La información de los activos esta almacenada en hojas electrónicas, es estructurada y clasificada en archivos por fechas esto siguiendo con las directrices y procesos de la empresa.

El desarrollo del software esta enmarcado en el paradigma orientado a objetos.

La metodología que se utiliza es RUP (Proceso Unificado de Rational) ya que es un proceso de desarrollo de software que se adapta a proyectos de diferente complejidad y tamaño.

Para tener un proceso de análisis y diseño general, se emplea UML (Lenguaje Unificado de Modelado) por ser aceptado por toda la comunidad de desarrollo de software orientado a objetos.

La implementación del sistema se realiza en Visual Basic, reportes Data Report, gestor de base de datos access y Sistema operativo Windows XP.

# ABSTRACT

The important elements in the companies with a clear objective, are the assets which need to have a better control of the same ones.

In this sense he/she intends a system of reliable information and insurance to negotiate the whole information that is generated on the existent assets inside the company CRS Bolivia.

The information of the assets this stored in electronic leaves, it is structured and classified in files by dates this continuing with the guidelines and processes of the company.

The development of the software this framed in the oriented paradigm to objects. The methodology that is used is RUP (I Process Unified of Rational) since it is a process of software development that adapts to projects of different complexity and size.

To have an analysis process and general design, UML is used (Unified Language Modeling) to be accepted by the whole community of development of oriented software to objects.

The implementation of the system is carried out in Visual Basic, reports Data Report, agent of database Access and operative System Windows XP.

# INDICE

## CAPITULO I

## GENERALIDADES



## CAPITULO II

## MARCO TEORICO

## CAPITULO III

## ANALISIS Y DISEÑO



## CAPITULO IV

## SEGURIDAD, CONTROL Y ANALISIS COSTO/BENEFICIO

CAPITULO V

## CONCLUSIONES Y RECOMENDACIONES



## REFERENCIA BIBLIOGRAFICA

## ANEXOS

# CAPITULO I

## GENERALIDADES

# GENERALIDADES

## CAPÌTULO 1

### 1.1 INTRODUCCION

El la actualidad el uso de la tecnología sea convertido en un instrumento de apoyo, estos están ligados a diferentes tipos de riesgos teniendo consecuencias económicas negativas que se pueden dar en caso de ocurrir estos.

Las organizaciones empresariales necesitan garantizar la integridad[1] de sus activos para poder continuar con su actividad productiva aunque se den situaciones desfavorables que dificulten su normal funcionamiento. Esta necesidad impulsa el desarrollo de una gestión de riesgos.

[1] Integridad: Estado de una cosa que mantiene todas sus partes o no ha sufrido alteración.

La Gestión de Riesgos es la planificación efectiva de los recursos necesarios para recuperar el equilibrio financiero y la efectividad operativa y de esta forma, obtener la estabilidad del costo de los riesgos y la minimización de los riesgos de la empresa. Esto con el fin de minimizar los efectos negativos de los riesgos.

En su constante desarrollar, las organizaciones empresariales determinan sus metas que justifican su existencia. Sin embargo, también ellas deben reconocer que la consecución[2] de sus metas está limitada por la presencia de riesgos que, en algunos casos, pueden retardar el cumplimiento de los planes, o bien cambiarlos, pero que en otros pueden significar el desvanecimiento de las organizaciones empresariales.

Justamente el término riesgo es uno de esos que diariamente aparecen cientos de veces y con significados diferentes.

El grado de formalización en el área de gestión de riesgos es bastante deficiente; debido al grado de importancia que se le da debido al método que se utiliza. Lo que condiciona que los nuevos empleados neseciten un largo periodo de tiempo para ambientarse al proceso de trabajo.

Por ello se resalta la importancia de evaluar los niveles de riesgo que pueden ser utilizados cuando se toman decisiones para mejores resultados de efectividad y eficiencia.

El presente proyecto tiene como propósito, realizar un sistema de gestión de riesgos de activos de información, que se centra en gestionar, controlar el manejo de la información y el análisis de riesgos que se centra en controlar sucesos que pueden provocar un cambio no deseado esto con las aplicaciones de estrategias de modo que se pueda evitar o reducir costos que son generados por los riesgos.

[2] Consecución: Acción y efecto de conseguir algo

## 1.2 ANTECEDENTES

El área de gestión de riesgos ha ido creciendo en estos últimos años, dichas investigaciones están orientadas a la continuidad de las organizaciones empresariales e identificar oportunidades y mitigar perdidas. En vista de ello distintos investigadores han realizado aportes a distintos aspectos de gestión de riesgos mismos que se mencionan a continuación.

"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. [Peter Drucker, 2000]

Según Fuertes, "Los riesgos de tecnologías de la información TI, necesitan ser identificados, medidos y gestionados como parte de un único entorno que incorpora todos los riesgos corporativos. Asimismo, dichos riesgos informáticos deben estar supervisados por el equipo de gestión de mayor nivel para conocer y ofrecer pautas que permitan establecer las combinaciones apropiadas de riesgos/recompensas, y con ello conseguir un mayor rendimiento de las inversiones en TI". El nombre con el que se conocen estas acciones para gestionar y equilibrar los riesgos y recompensas en bienes informáticos es Gestión de Riesgos TI.

"La evaluación del riesgos consiste en la identificación y análisis de los factores que podrían afectar la consecución de los objetivos, y, en base a dicho análisis, determinar la forma en que los riesgos deben ser gestionados"[Coso].

Una vez que se han identificado y valorado los riesgos, se debe tomar una decisión respecto a la gestión de estos riesgos. Ésta gestión generalmente es una función de:

- Política de seguridad inicial
- Nivel de seguridad requerido

- Resultados de la evaluación de riesgos
- Legislación, regulaciones y restricciones particulares

Los primeros estudios de gestión de riesgos en organizaciones empresariales se las realiza de acuerdo a la creatividad de cada una la mas común es realizarla en tablas Excel. El control de activos de información se la realiza con una serie de métodos y procedimientos que benefician a las organizaciones empresariales, los resultados obtenidos son interpretados de acuerdo a la experiencia.

Para realizar el control de sus activos y procesos se realizo una tabla en la cual se realiza un inventario de todas las actividades que se desarrolla dentro de la empresa como por ejemplo: análisis de requerimientos, selección y evaluación de proveedores, definición de seguridad y controles internos, administración de contratos con proveedores, pruebas, implementación y capacitación entre otras cosas, ver figura No. 1.

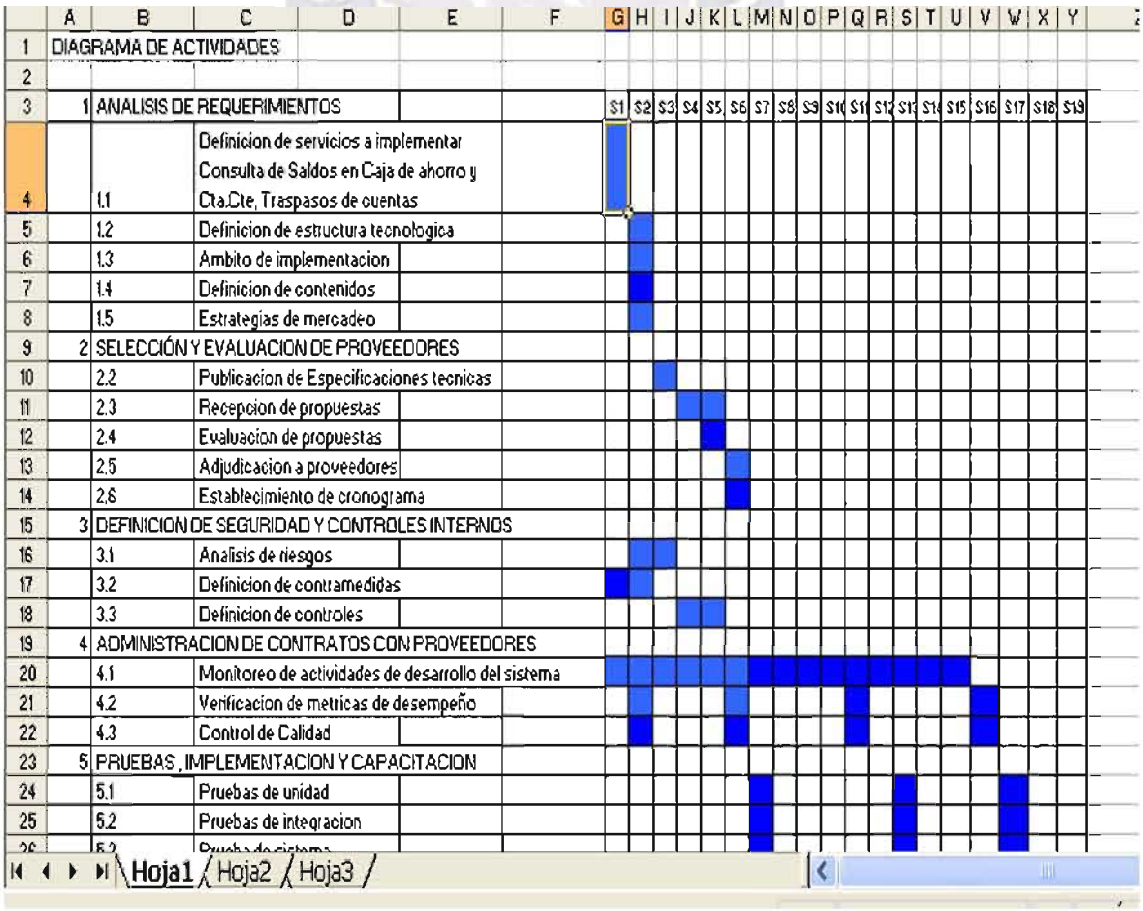
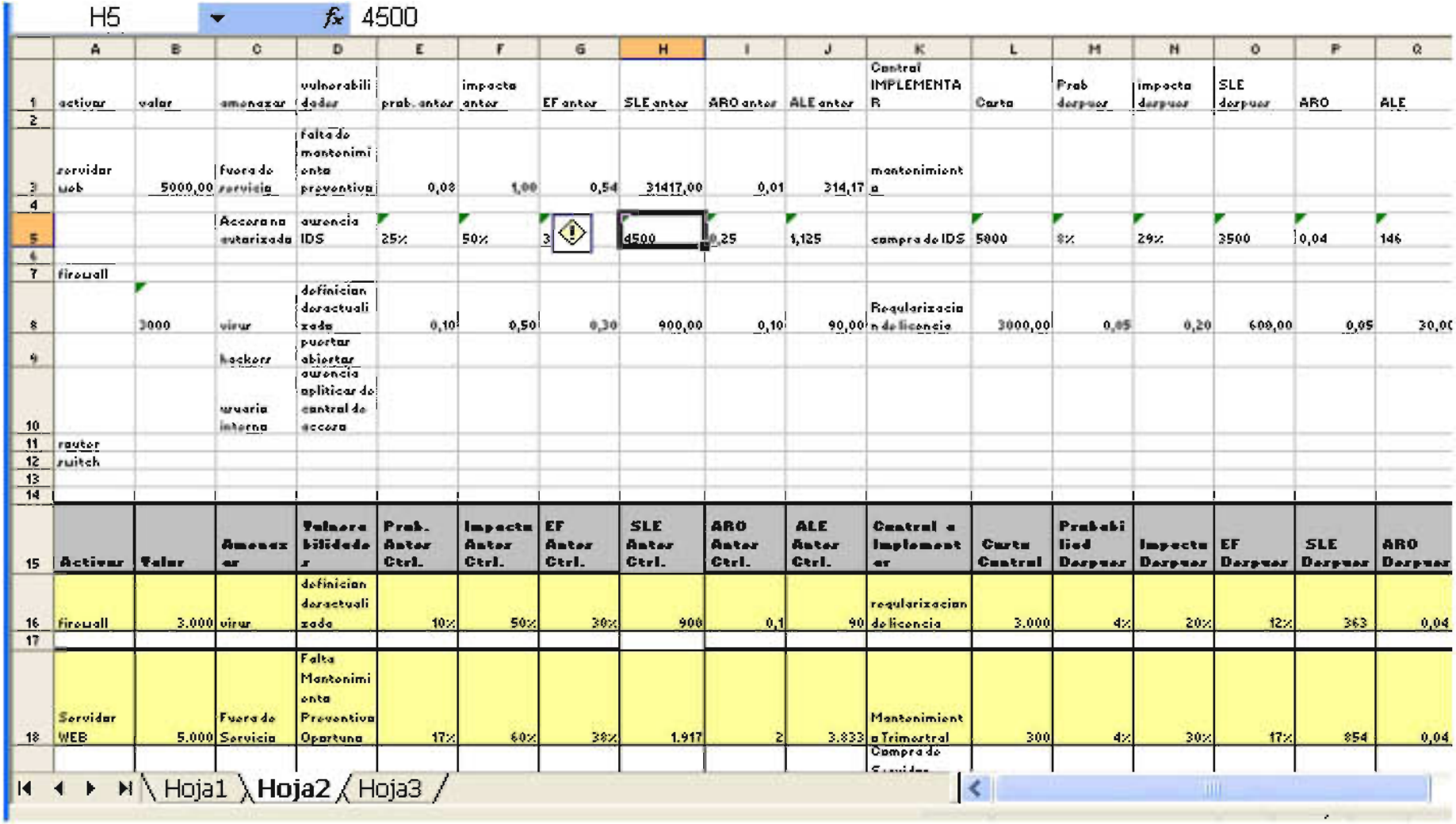



**Figura No. 1** Diagrama de Actividades

[**Fuente:** Organizaciones Empresariales]

En la siguiente tabla realizan un análisis cuantitativo en la cual se realiza un inventario de todos los activos de información, identifican el valor del activo, amenaza a la que esta expuesta, vulnerabilidad con respecto al activo, probabilidad antes del control, impacto antes del control, entre otras cosas y al final se determina si es factible o no, ver figura No. 2.

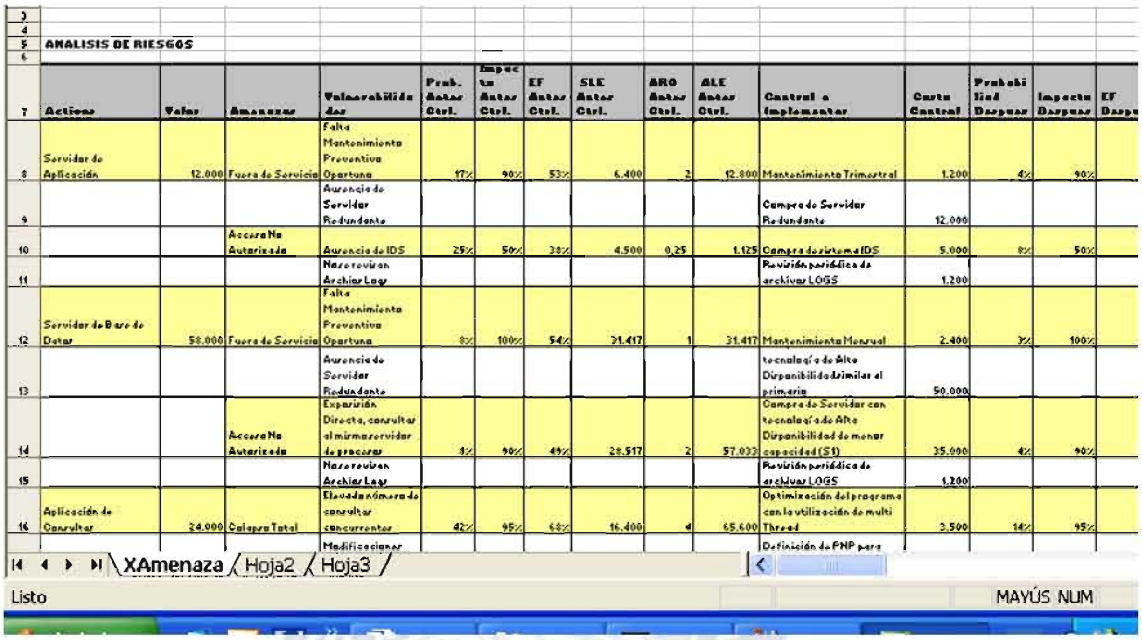


| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | activar | valor | amenazar | vulnerabilidad | prob. antes | impacto antes | EF antes | SLE antes | ARO antes | ALE antes | Control IMPLEMENTAR | Costo | Prob despues | impacto despues | SLE despues | ARO | ALE |
| 2 | | | | | | | | | | | | | | | | | |
| 3 | servidor web | 5000,00 | fuera de servicio | falta de mantenimiento preventivo | 0,08 | 1,00 | 0,54 | 31417,00 | 0,01 | 314,17 | mantenimiento | | | | | | |
| 4 | | | | | | | | | | | | | | | | | |
| 5 | | | Accesso no autorizado | ausencia IDS | 25% | 50% | 3 | d500 | 0,25 | 1,125 | compra de IDS | 5000 | 8% | 29% | 3500 | 0,04 | 146 |
| 6 | | | | | | | | | | | | | | | | | |
| 7 | firewall | | | | | | | | | | | | | | | | |
| 8 | | 3000 | virus | definicion desactualizada | 0,10 | 0,50 | 0,30 | 900,00 | 0,10 | 90,00 | Regularizacion de licencia | 3000,00 | 0,05 | 0,20 | 600,00 | 0,05 | 30,00 |
| 9 | | | hackers | puertas abiertas | | | | | | | | | | | | | |
| 10 | | | usuario interno | ausencia aplitivos de control de acceso | | | | | | | | | | | | | |
| 11 | router | | | | | | | | | | | | | | | | |
| 12 | switch | | | | | | | | | | | | | | | | |
| 13 | | | | | | | | | | | | | | | | | |
| 14 | | | | | | | | | | | | | | | | | |
| 15 | **Activar** | **Valor** | **Amenazar** | **Vulnerabilidades** | **Prob. Antes Ctrl.** | **Impacto Antes Ctrl.** | **EF Antes Ctrl.** | **SLE Antes Ctrl.** | **ARO Antes Ctrl.** | **ALE Antes Ctrl.** | **Control a Implementar** | **Costo Control** | **Probabilidad Despues** | **Impacto Despues** | **EF Despues** | **SLE Despues** | **ARO Despues** |
| 16 | firewall | 3.000 | virus | definicion desactualizado | 10% | 50% | 30% | 900 | 0,1 | 90 | regularizacion de licencia | 3.000 | 4% | 20% | 12% | 363 | 0,04 |
| 17 | | | | | | | | | | | | | | | | | |
| 18 | Servidor WEB | 5.000 | Fuera de Servicio | Falta Mantenimiento Preventivo Oportuno | 17% | 60% | 38% | 1.917 | 2 | 3.833 | Mantenimiento Trimestral | 300 | 4% | 30% | 17% | 854 | 0,04 |
| | | | | | | | | | | | Compra de | | | | | | |

Hoja1 | Hoja2 | Hoja3

**Figura No.2** Análisis Cuantitativo
**[Fuente:** Organizaciones Empresariales]

En esta tabla realizan el análisis de riesgo en la que se tiene un inventario de todos sus activos, amenazas a la que esta expuesta, valor del activo, control de implementación, impacto después del control, etc.



ANALISIS DE RIESGOS

| Activos | Valor | Amenazas | Vulnerabilidades | Prob. Antes Ctrl. | Impacto Antes Ctrl. | EF Antes Ctrl. | SLE Antes Ctrl. | ARO Antes Ctrl. | ALE Antes Ctrl. | Control a implementar | Costo Control | Probabilidad Despues | Impacto Despues | EF Despu |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Servidor de Aplicación | 12.000 | Fuera de Servicio | Falta Mantenimiento Preventivo Oportuno | 17% | 90% | 53% | 6.400 | 2 | 12.800 | Mantenimiento Trimestral | 1.200 | 4% | 90% | |
| | | | Ausencia de Servidor Redundante | | | | | | | Compra de Servidor Redundante | 12.000 | | | |
| | | Acceso No Autorizado | Ausencia de IDS | 25% | 50% | 38% | 4.500 | 0,25 | 1.125 | Compra de sistema IDS | 5.000 | 8% | 50% | |
| | | | No se revisan Archivar Logs | | | | | | | Revisión periódica de archivar LOGS | 1.200 | | | |
| Servidor de Base de Datos | 58.000 | Fuera de Servicio | Falta Mantenimiento Preventivo Oportuno | 8% | 100% | 54% | 31.417 | 1 | 31.417 | Mantenimiento Mensual | 2.400 | 3% | 100% | |
| | | | Ausencia de Servidor Redundante | | | | | | | tecnología de Alta Disponibilidad similar al primario | 50.000 | | | |
| | | Acceso No Autorizado | Exposición Directa, consultar al mismo servidor de procesos | 9% | 90% | 49% | 28.517 | 2 | 57.033 | Compra de Servidor con tecnología de Alta Disponibilidad de menor capacidad (S1) | 25.000 | 4% | 90% | |
| | | | No se revisan Archivar Logs | | | | | | | Revisión periódica de archivar LOGS | 1.200 | | | |
| Aplicación de Consultas | 24.000 | Colapso Total | Elevada número de consultas concurrentes | 42% | 95% | 68% | 16.400 | 4 | 65.600 | Optimización del programa con la utilización de multi Thread | 3.500 | 14% | 95% | |
| | | | Modificaciones | | | | | | | Definición de PNP para | | | | |

XAmenaza / Hoja2 / Hoja3

Listo MAYÚS NUM

**Figura No. 3** Análisis de Riesgos

**[Fuente:** Organizaciones Empresariales]

Estándares que contribuyen a la práctica de seguridad de los activos de información:

COBIT4, para estructurar el análisis de riesgos, COBIT es la gran sombrilla de procesos de tecnología de la información TI, y está alineada completamente con Gobernabilidad de TI, que es de donde a mi criterio debe partir el análisis de riesgo. COBIT no define los riesgos por proceso, pero si tiene herramientas que ayudan a definirlo, y será tarea de cada organización de TI, identificar los riesgos a los procesos de TI o a los objetivos de TI que sean mas relevantes.

La primera fuente para que una organización identifique sus necesidades de seguridad es la valoración de sus riesgos. La forma de abordar esta valoración es mediante la realización de un análisis de riesgos formal y metodológico [Según la norma UNE/ISO 17799].

Las organizaciones, disponen de controles y medidas de seguridad (salvaguardas) que actúan sobre las vulnerabilidades y amenazas disminuyendo los niveles de riesgo [norma UNE/ISO 17799].

Código de práctica para la administración de la seguridad de la información: esta parte brinda recomendaciones para la gestión de la seguridad de la información que han de ser aplicadas por los responsables de iniciar, implementar o mantener la seguridad en sus organizaciones. [Norma ISO 17000].

## 1.3 PLANTEAMIENTO DEL PROBLEMA

El objeto de estudio es el de determinar si la gestión de riesgos tiene alguna influencia importante dentro de las organizaciones empresariales esto con la evaluación de los factores de riesgo que se suscitan dentro de ella así como: amenazas, vulnerabilidades, probabilidad de ocurrencia, etc.

Se realizo un diagnóstico previo en el que se identificó, deficiencias en el actual manejo y disposición de los activos de información y distintos problemas asociados:

- Carencia de elementos de observación en las organizaciones empresariales, seguimiento, supervisión y responsables de los activos de información.
- Dificultades en el proceso de obtener información del registro de los activos de información y sus responsables.
- Discontinuidad en el trabajo.
- El problema radica en la falta de información sobre los riesgos a que esta expuesto la empresa.
- No cuenta con herramientas de gestión de riesgos para mejorar las expectativas contempladas.
- No cuenta con la información oportuna para la toma de desiciones.
- Carencia de mecanismos de control en la organización.

La gestión de riesgos no esta implementada dentro de muchas empresas: la Gerencia de Riesgos combina los recursos financieros, humanos, materiales y técnicos de la empresa, para identificar y evaluar los riesgos potenciales y decidir como manejarlos con una combinación óptima de costo – efectividad.[3] La Gerencia de Riesgos se ha convertido en una función estratégica esencial de la dirección corporativa moderna, y no una mera decisión comercial o productiva.[4]

A la vista de informes de las organizaciones empresariales, se pueden detectar métodos, departamentos, sistemas, personas que pueden originar o participar en los acontecimientos con resultados negativos. Las informaciones que con más frecuencias proporcionan indicios o avances de actuaciones peligrosas son: apuntes contables, informes del personal, documentos legales, memorias y proyectos de obras e instalaciones, servicios, representaciones y otros; informes jurídicos, inventario de edificio, instalaciones, maquinaria y mercancías, patentes y tecnología propia y adquiridas. Pero la ausencia de información sobre los activos de información dificultan el manejo y control de estos lo que provoca la discontinuidad de las organizaciones empresariales.

En este contexto se plantea la siguiente problemática:

¿Los riesgos se pueden mitigar por medio de salvaguardas o contramedidas para proteger los activos de información?

## 1.4 OBJETIVOS

### *1.4.1 Objetivo General*

Implementar un Sistema de Gestión de Riesgos en Activos de Información el cual permitirá gestionar y controlar el manejo de la

[3] Tomado de la Intervención del Dr. Ramón Rodríguez Carrera, "Situación actual y perspectivas de la Administración de Riesgos en Cuba", en el 1er Seminario Nacional sobre Administración de Riesgos, Mayo 1998.
[4] Tomado del 1er Seminario Nacional sobre Administración de Riesgos, "El Role del Gerente de Riesgos en una organización", Mayo 1998.

información sobre los activos de información, coadyuvando en la buena toma de decisiones.

### *1.4.2 Objetivos Específicos*

- Mejorar el manejo y control de los activos de información.
- Construir una base de datos para el registro de la información de los activos de información.
- Generar informes que muestren el estado de los activos de información y sus responsables.
- Diseñar y desarrollar las interfaces que faciliten la operabilidad del sistema.
- Capacitar al personal sobre el manejo del nuevo sistema.
- Realizar la baja de los activos de información.
- Realizar el análisis cualitativo y cuantitativo de los activos de información el cual permitirá identificar los activos más significantes, amenazas más relevantes.
- Estimar los riesgos según una escala simple de valores.

## 1.5. JUSTIFICACION

### 1.5.*1 Justificación Económica*

En cuanto a la situación económica el proyecto plantea un sistema que reduzca los gastos económicos que se contemplan por las fallas de seguridad en los activos de información, puesto que le permitirá tomar decisiones en el momento oportuno, esto con la automatización se reducirá el tiempo y esfuerzo laboral, reduciendo costos económicos.

### *1.5.2 Justificación Social*

El proyecto será de beneficio para la gerencia o personal interesado, debido a que este le colaborara en el desempeño de sus tareas, con el registro y control de la información de los activos de información.

### *1.5.3 Justificación Técnica*

Técnicamente se cuenta con equipos de computación y ambiente de trabajo que son necesarios para realizar el desarrollo e implementación del presente proyecto y se cuenta con el apoyo necesario, también en su desarrollo se utilizan herramientas y metodologías para el análisis y diseño de sistemas.

### *1.5.4 Justificación Teórica*

De acuerdo a los antecedentes mencionados anteriormente, la gestión de riesgos hace posible el manejo y control de los activos de información. Desarrollar un sistema con estas características para contribuir a la experiencia sobre seguridad de los activos de información. Usando la siguiente metodología: Magerit Version2 que es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Pilar Basic el cual realiza el análisis y gestión de riesgos y el estándar ISO 17000 el cual es un código de practica para la administración de la seguridad de la información.

## 1.6 METODOLOGIA Y HERRAMIENTAS

### *1.6.1 Metodología*

Para el desarrollo del proyecto se utilizará una metodología orientada a objetos, específicamente la metodología RUP (Rational Unified Process), ya que es un proceso de desarrollo de software que se adapta a proyectos de diferente complejidad y tamaño, y por ajustarse a las necesidades del presente proyecto.

Para el modelado de análisis y diseño se utiliza UML (Unified Modeling Languaje) ya que permite modelar, construir y documentar los elementos que forman parte del sistema.

### *1.6.2 Herramientas*

- Para el desarrollo del proyecto se usara como plataforma el Sistema Operativo Windows XP o 2000.
- Las interfaces graficas se realizaran con Visual Basic.

- Para la elaboración de reportes se usará Datareport.
- Como motor de base de datos, se hará uso de Access.

## 1.7 ALCANCES Y APORTES

### 1.7.1 Límites y Alcances

#### *1.7.1.1 Límites*

El presente proyecto abarcará la gestión de riesgos en activos de información, tomando en cuenta el control y manejo de información de los activos de información con los que cuenta las organizaciones empresariales.

#### *1.7.1.2 Alcances*

El Sistema de Gestión de Riesgos en Activos de Información esta orientado a:

- Registro de activos de información, el cual se realizara en forma dinámica tomando en cuenta la información necesaria para realizar el registro.
- Reporte de los activos de información, el cual proporcionara la información necesaria.
- Realizará un análisis de riesgo que proporcionara información sobre el tratamiento de los riesgos.
- Realizará la baja de los activos de información.

### 1.7.2 Aportes

En términos de la utilidad el proyecto permitirá optimizar la gestión de riesgos de los activos de información en los siguientes aspectos:

- Los procesos manuales se automatizaran, la información coadyuvara al manejo de toda la información sobre los activos de información y el suministro de la información para la toma de decisiones.

- Sistema de autenticación de usuarios autorizados para el manejo del sistema en el aspecto administrativo.

Proveerá información de todo lo concerniente a activos de información, consecuentemente desempeña un papel muy importante en el proceso de continuidad de las organizaciones empresariales.

# CAPÌTULO II

## MARCO TEÓRICO

# MARCO TEORICO

# CAPITULO II

## 2.1. CONCEPTOS DE GESTIÓN DEL RIESGO

### 2.1.1. Definición de Riesgo

Es la probabilidad que una amenaza aproveche una vulnerabilidad. Como el riesgo constituye una falta de conocimiento sobre los futuros acontecimientos se puede definir como el efecto acumulativo que estos acontecimientos adversos podrían tener sobre los objetivos de la actividad planificada. También puede hablarse de riesgo cuando la consecuencia sea

positiva para la marcha de la organización algunos autores llaman a este caso oportunidad.

### 2.1.2. Definición de Vulnerabilidad

Son las inseguridades que posee el activo tanto por problemas tecnológicos, como problemas de procedimientos. Está demostrado que la gran mayoría de pérdidas de activos son por falta de procedimientos o desconocimiento.

### 2.1.3. Definición Amenaza

Todo aquello que pueda provocar un daño a nuestro activo.

### 2.1.4. Definición de Activo

Recurso, producto, proceso, dato, todo aquello que tenga un valor para el negocio de la compañía [tomado de: www.puntonetsoluciones.com.ar].

### 2.1.5. Definición de Gestión de Riesgos

La gestión de riesgos es el conjunto de elementos, medidas y herramientas dirigidas a la intervención de la amenaza o la vulnerabilidad, con el fin de disminuir o mitigar los riesgos existentes. La gestión de riesgos es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir. La Gestión del Riesgo conlleva la identificación, el análisis, el control y la minimización de la pérdida asociada a un evento determinado [www.aduana.cl/prontus_aduana sertvicio nacional de aduanas –gestión de riesgos-chile].

## 2.2. CLASIFICACION DE LOS RIESGOS

**2.2.1. Riesgos Financieros:** El riesgo financiero envuelve la relación entre una organización y una ventaja que puede ser perdida o perjudicada. De este modo el riesgo financiero envuelve 3 elementos:

- La organización que esta expuesta a pérdidas
- Los elementos que conforman las causas de pérdidas financieras
- Un peligro que puede causar la pérdida (amenaza a riesgo).

**2.2.2. Riesgos Dinámicos:** Son el resultado de cambios en la economía que surgen de los tipos de factores.

**2.2.3. Riesgos Estáticos:** Estos riesgos surgen de otras causas distintas a los cambios de la economía tales como: deshonestidad o fallas humanas.

**2.2.4. Riesgo Especulativo:** Describe una situación que espera una posibilidad de pérdida o ganancia. Un buen ejemplo es una situación aventurada o del azar.

**2.2.5. Riesgo Puro:** Designa aquellas situaciones que solamente generan o bien pérdida o ganancia, un ejemplo es la posibilidad de pérdida en la compra de un bien (automóviles, casas, etc.).

## 2.3. RIESGOS EN ACTIVOS DE INFORMACION

Los principales riesgos informáticos de los negocios son los siguientes:

**2.3.1. Riesgos de Integridad:** Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización.

**2.3.2. Administración de Cambios:** Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con

la administración inadecuada de procesos de cambios organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.

**2.3.3. Información:** Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos.

**2.3.4. Riesgos de Relación:** Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (Información y datos correctos de una persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

**2.3.5. Riesgos de Acceso:** Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información.

**2.3.6. Administración de la Información:** El mecanismo provee a los usuarios acceso a la información específica del entorno.

**2.3.7. Entorno de Procesamiento:** Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.

**2.3.8. Redes:** En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.

**2.3.9. Nivel Físico:** Protección física de dispositivos y un apropiado acceso a ellos.

**2.3.10. Riesgos de Utilidad:** Estos riesgos se enfocan en tres diferentes niveles de riesgo:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
- Backups y planes de contingencia controlan desastres en el procesamiento de la información.

**2.3.11. Riesgos en la Infraestructura:** Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.

**2.3.12. Administración de Seguridad:** Los procesos en esta área aseguran que la organización está adecuadamente direccionada a establecer, mantener y monitorizar un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de fraudes a niveles aceptables.

**2.3.13. Riesgos de Seguridad General:** Los estándar [5]IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

- Riesgos de choque de eléctrico: Niveles altos de voltaje.
- Riesgos de incendio: Inflamabilidad de materiales.
- Riesgos de niveles inadecuados de energía eléctrica.
- Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
- Riesgos mecánicos: Inestabilidad de las piezas eléctricas.

## 2.4. ELEMENTOS DE GESTION DE RIESGOS

[5] Estándar de la Comisión Electrónica Internacional (IEC)- en inglés, él cual es utilizado para tecnología informática y equipos eléctricos.

La función de la gestión de riesgos es identificar, estudiar y eliminar las fuentes de los eventos perjudiciales antes de que empiecen a amenazar los procesos informáticos. La gestión de riesgos se divide generalmente en:

**2.4.1. Estimación de Riesgos:** La estimación de riesgos describe cómo estudiar los riesgos dentro de la planeación general del entorno informático.

**2.4.2. Identificación de Riesgos:** En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático.

**2.4.3. Análisis de Riesgos:** Una vez que se hayan identificado los riesgos en la planificación, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

**2.4.4. Exposición a Riesgos:** Una actividad útil y necesaria en el análisis de riesgos es determinar su nivel de exposición en cada uno de los procesos en que se hayan identificado.

**2.4.5. Priorización de Riesgos:** En este paso de la estimación de riesgos, se estiman su prioridad de forma que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización (elementos de alto riesgo y pequeños riesgos), estos últimos no deben ser de gran preocupación, pues lo verdaderamente crítico se puede dejar en un segundo plano.

## 2.5. TECNICAS DE PROCEDIMIENTOS PARA ADMINISTRAR RIESGOS

**2.5.1. Evitar Riesgos:** Un riesgo es evitado cuando en la organización no se acepta. Esta técnica puede ser más negativa que positiva. Si el evitar riesgos fuera usado excesivamente el negocio sería privado de muchas oportunidades de ganancia (por ejemplo: arriesgarse a hacer una inversión) y probablemente no alcanzaría sus objetivos.

**2.5.2. Reducción de Riesgos:** Los riegos pueden ser reducidos, por ejemplo con: programas de seguridad, guardias de seguridad, alarmas y estimación de futuras pérdidas con la asesoría de personas expertas.

**2.5.3. Conservación de Riesgos:** Es quizás el más común de los métodos para enfrentar los riesgos, pues muchas veces una acción positiva no es transferirlo.

## 2.6. POLITICAS EN LA ADMINISTRACION DE RIESGOS

Una política es una guía general de acción, este es un plan estándar de la organización que traduce los objetivos en guías más específicas. Para determinar las políticas en la administración de riesgos para una organización en particular se tienen en cuenta decisiones que pueden ser hechas solamente por la gerencia de la organización. En el diseño de políticas de administración de riesgos, algunos factores son necesarios para tomar decisiones, que son:

**2.6.1. Los objetivos básicos del programa de gestión de riesgos:** El principal objetivo es preservar la eficiencia operativa de la organización. Este objetivo implica evitar las perdidas financieras causadas por desastres que impidan las funciones básicas de la organización.

**2.6.2. Consolidación del programa de retención**: Cuando la política de gestión de riesgos especifica un máximo nivel de retención (delineamiento de exposiciones o pérdidas que no serán retenidas), se tiene un razonable direccionamiento de consolidación de pérdidas retenidas, permitiendo gran flexibilidad en las decisiones de control.

## 2.7. ANALISIS DE RIESGOS

El objetivo general del análisis de riesgos es identificar sus causas potenciales, en la figura No. 3 se aprecia por ejemplo, los principales riesgos que amenazan el entorno informático. Esta identificación se realiza en una determinada área para que se pueda tener información suficiente al respecto, optando así por un

adecuado diseño e implantación de mecanismos de control; a fin de minimizar los efectos de eventos no deseados, en los diferentes puntos de análisis.
Además el análisis de riesgos cumple los siguientes objetivos:

- Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.
- Llevar a cabo un minucioso análisis de los riesgos y debilidades.
- Identificar, definir y revisar los controles de seguridad.
- Determinar si es necesario incrementar las medidas de seguridad.
- Cuando se identifican los riesgos, los perímetros de seguridad y los sitios de mayor peligro, se pueden hacer el mantenimiento más fácilmente [Tomado de: Monografías.com].

Hardware

Organización

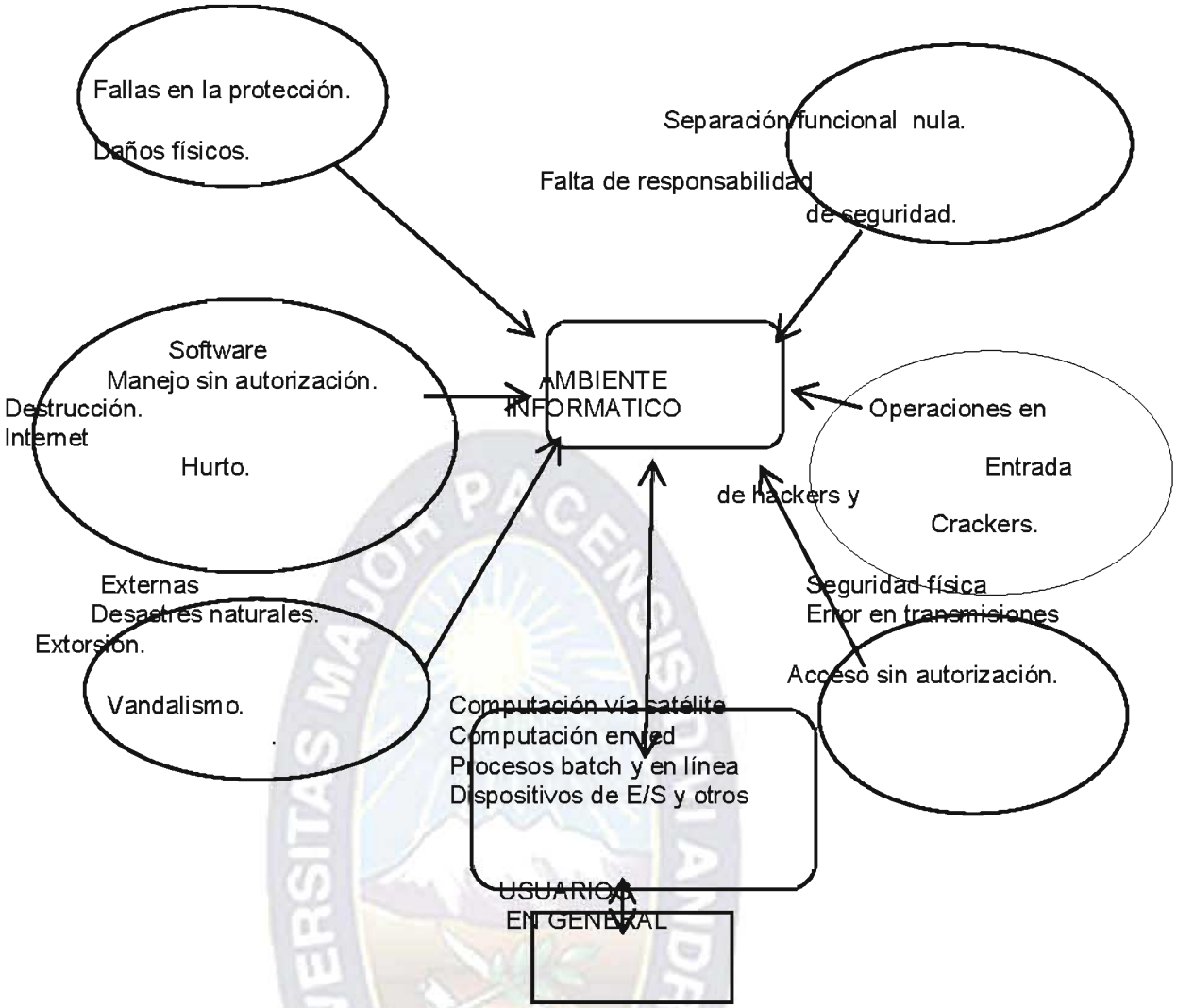



**Figura No. 3** Principales amenazas que afectan el ambiente informático

**[Fuente:** monografías.com]

Antes de realizar el análisis de riesgos hay que tener en cuenta los siguientes aspectos:

- Se debe tener en cuenta las políticas y las necesidades de la organización así como la colaboración con todas las partes que la conforman y que intervienen en los procesos básicos.
- Debe tenerse en cuenta los nuevos avances tecnológicos y la astucia de intrusos expertos.
- El comité o la junta directiva de toda organización debe incluir en sus planes y presupuesto los gastos necesarios para el desarrollo de programas de seguridad, así como tener en cuenta que esta parte es fundamental de todo proceso de desarrollo de la empresa, especificar

los niveles de seguridad y las responsabilidades de las personas relacionadas, las cuales son complemento crucial para el buen funcionamiento de todo programa de seguridad.

# CAPITULO III

## ANALISIS Y DISEÑO

# ANALISIS Y DISEÑO

## CAPITULO III

En este capitulo el análisis y diseño del sistema se explicara de forma clara, concisa y comprensible, diseñado para el usuario final esto le lograra con la captura de aspectos del mundo real, utilizando métodos de recopilación de datos como la metodología RUP y procesos básicos que realizan los usuarios de forma manual.

### 3.1 MODELADO DE NEGOCIO

Dentro de este punto se identificara los distintos procesos o el ámbito de trabajo, lo que vendría a ser el como se esta realizando la gestión de riesgos dentro de la organización o empresa para esto será representando por el diagrama de casos de uso general.

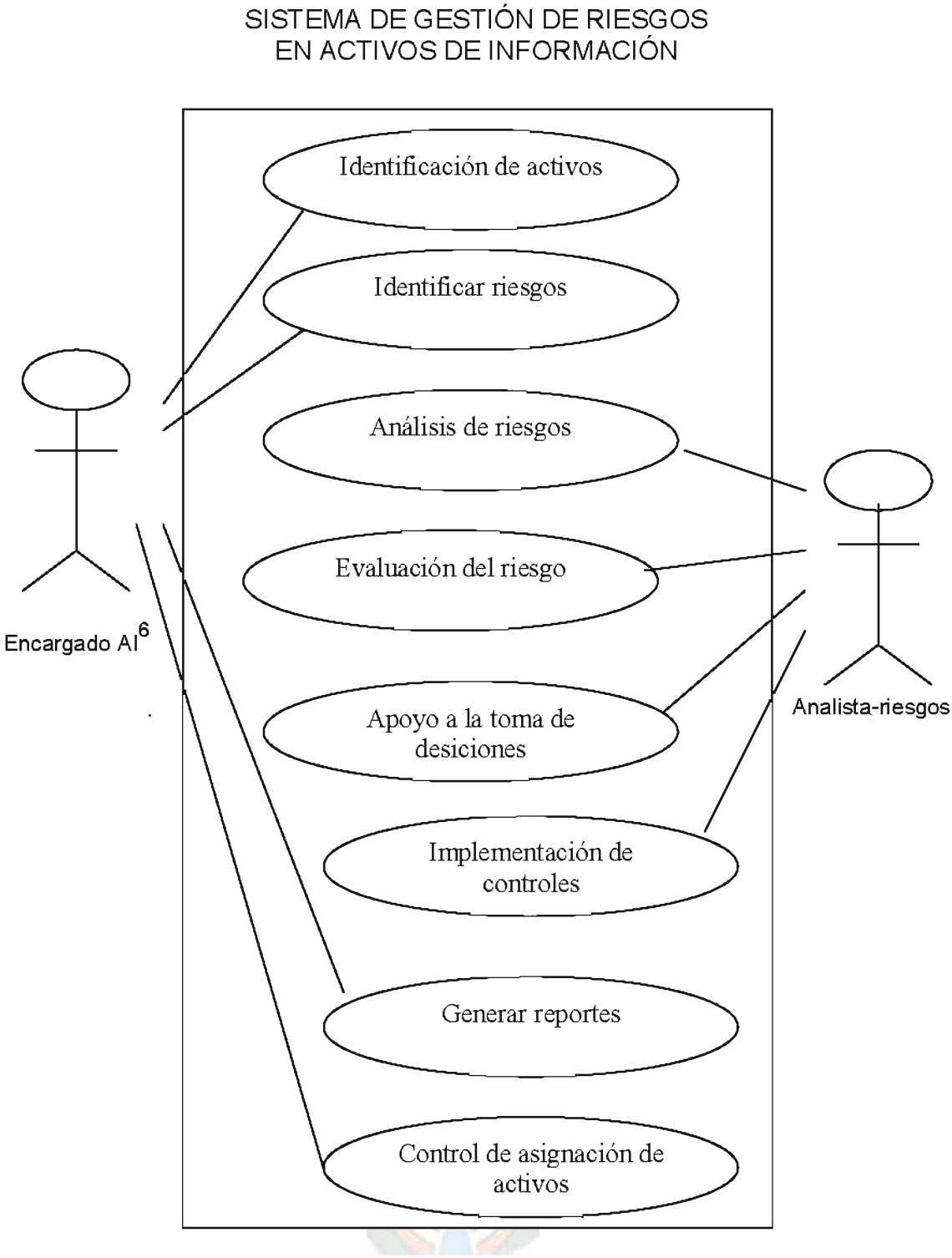



**Figura 3.1.1** DIAGRAMA DE CASOS DE USO (alto nivel)
**Fuente:** Elaboración propia

[6] AI: Activo de Información

**Tabla 1** CASO DE USO EN FORMATO DE ALTO NIVEL

| | | |
|---|---|---|
| ***CASO DE USO*** | ***:*** | ***IDENTIFICAR ACTIVO*** |
| **ACTORES** | : | Encargado de AI |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Identificar y registrar los activos adquiridos |

| | | |
|---|---|---|
| ***CASO DE USO*** | ***:*** | ***IDENTIFICAR RIESGOS*** |
| **ACTORES** | : | Encargado de AI |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Identificar y registrar los riesgos reales y percibidos. |

| | | |
|---|---|---|
| ***CASO DE USO*** | ***:*** | ***ANALISIS DE RIESGOS*** |
| **ACTORES** | : | Analista-riesgos |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Se determina la probabilidad e impacto asignadas a cada riesgo. |

| | | |
|---|---|---|
| ***CASO DE USO*** | ***:*** | ***EVALUACIÓN DEL RIESGO*** |
| **ACTORES** | : | Analista-riesgos |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Muestra las consecuencias de las amenazas sobre los activos. |

| *CASO DE USO* | : | *APOYO A LA TOMA DE DESICIONES* |
|---|---|---|
| **ACTORES** | : | Analista-riesgos |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Identificar y evaluar las soluciones de control mediante un proceso de análisis coste-beneficio. |

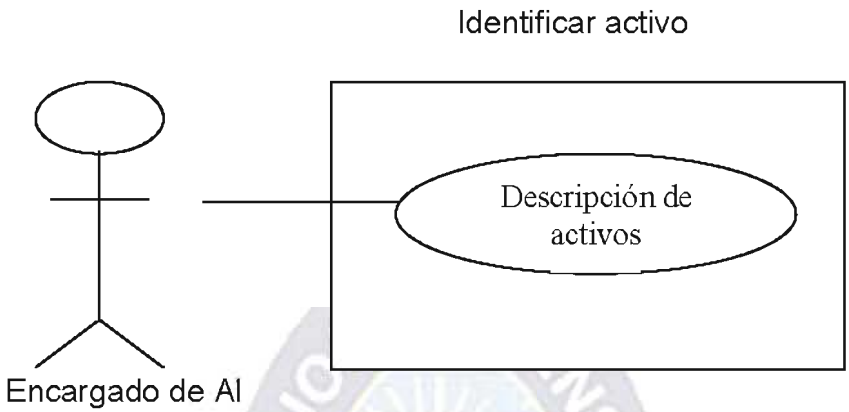
| *CASO DE USO* | | *IMPLEMENTACION DE CONTROLES* |
|---|---|---|
| **ACTORES** | : | Encargado de AI |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Implementar y poner en funcionamiento las soluciones con el fin de reducir el riesgo en las empresas. |

| *CASO DE USO* | : | *GENERAR REPORTE* |
|---|---|---|
| **ACTORES** | : | Encargado de AI |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Generar reportes para que el usuario final se informe a cerca de todo el proceso de gestión de riesgos. |

| *CASO DE USO* | : | *CONTROL DE ASIGNACION DE ACTIVOS* |
|---|---|---|
| **ACTORES** | : | Encargado de AI |
| **TIPO** | : | Primario |
| **DESCRIPCION** | : | Llevar un control de los responsables de los activos. |

**Fuente:** Elaboración Propia

**Figura 3.2** DIAGRAMA DE CASOS DE USO DE NIVEL EXPANDIDO (bajo nivel)



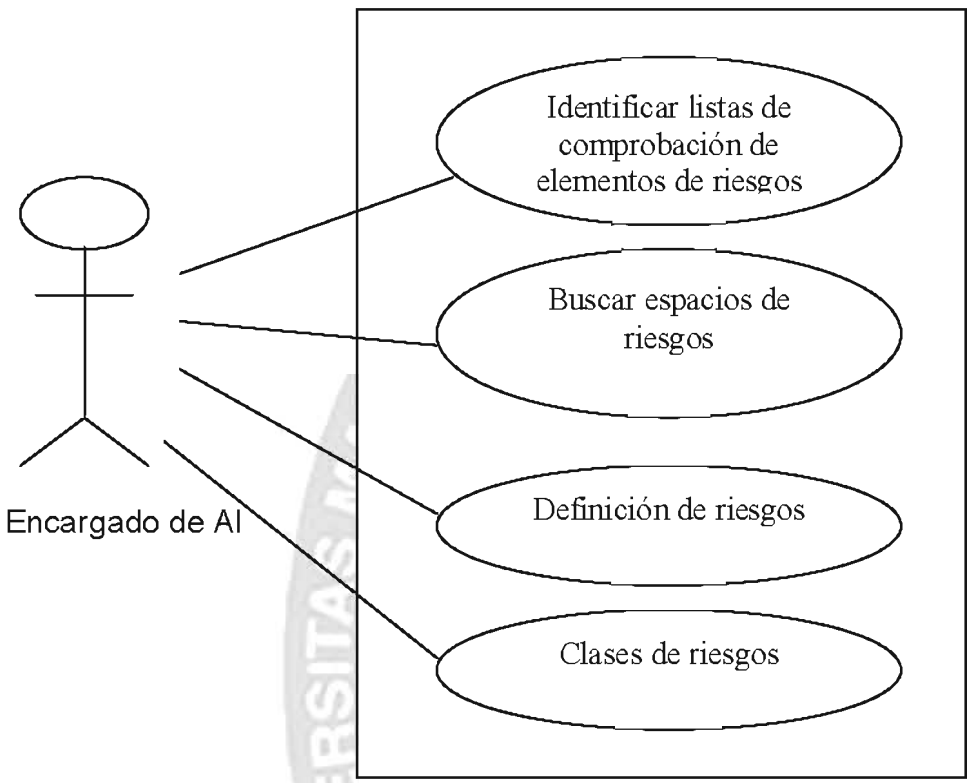

**Fuente:** Elaboración propia

**Tabla 2.** Caso de uso de expandido Identificar Activo

| *CASO DE USO* | *IDENTIFICAR ACTIVO* |
|---|---|
| **ACTORES** | Encargado de AI |
| **PROPOSITO** | Capturar los activos y sus características singulares |
| **RESUMEN** | Se pide que identifique los activos por ser elementos básicos para el análisis de riesgos sometidos a amenazas y protegidos por salvaguardas. |
| **TIPO** | Primario |

**Fuente:** Elaboración propia

**Figura 3.3** Diagrama de casos de uso identificar riesgos



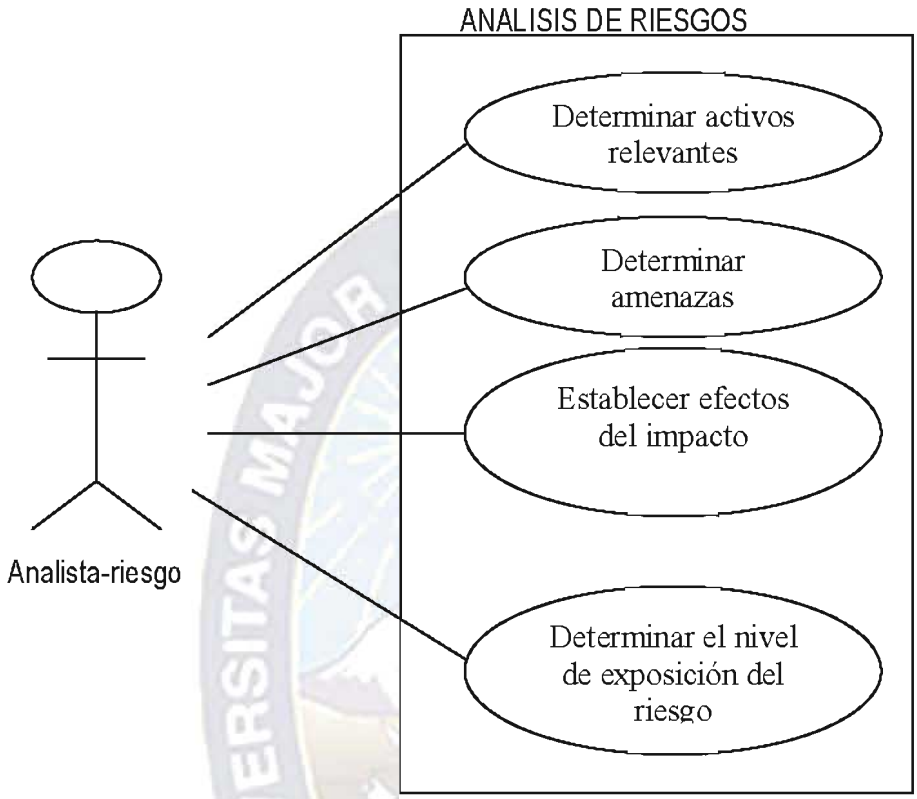

**Fuente:** Elaboración propia

**Tabla 3.** Caso de uso de expandido Identificar los riesgos

| ***CASO DE USO*** | ***IDENTIFICAR RIESGOS*** |
|---|---|
| ***ACTORES*** | Encargado de AI |
| ***PROPOSITO*** | Identificar y registrar los riesgos reales que serán evaluados y administrados durante la revisión. |
| ***RESUMEN*** | Es un proceso de reflexión a través de diferentes técnicas para establecer que cosas, elementos o circunstancias son riesgos. |
| ***TIPO*** | Primario |

**Fuente:** Elaboración propia

**Figura 3.4** Diagrama de casos de uso de Análisis de Riesgos



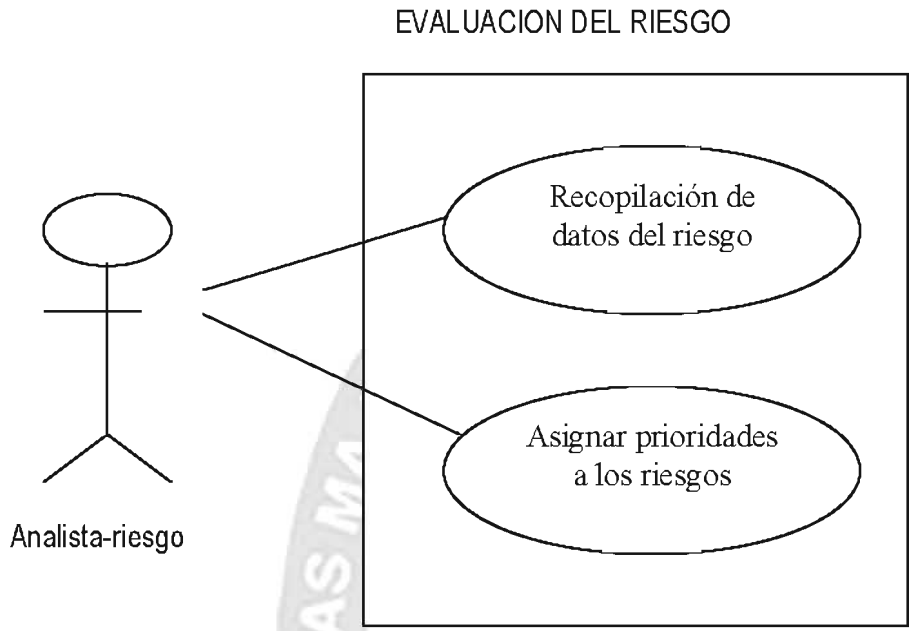

**Fuente:** Elaboración propia

**Tabla 4.** Caso de uso de uso expandido Análisis de Riesgos

| ***CASO DE USO*** | ***ANALISIS DE RIESGOS*** |
|---|---|
| ***ACTORES*** | Analista-riesgos |
| ***PROPOSITO*** | Analizar los riesgos para determinar así su impacto tomando así posibles alternativas de solución. |
| ***RESUMEN*** | Es el proceso de examinar los riesgos en detalle para determinar su extensión, sus interrelaciones y su importancia. |
| ***TIPO*** | Primario |

**Fuente:** Elaboración propia

**Figura 3.5** Diagrama de casos de uso Evolución del riesgo



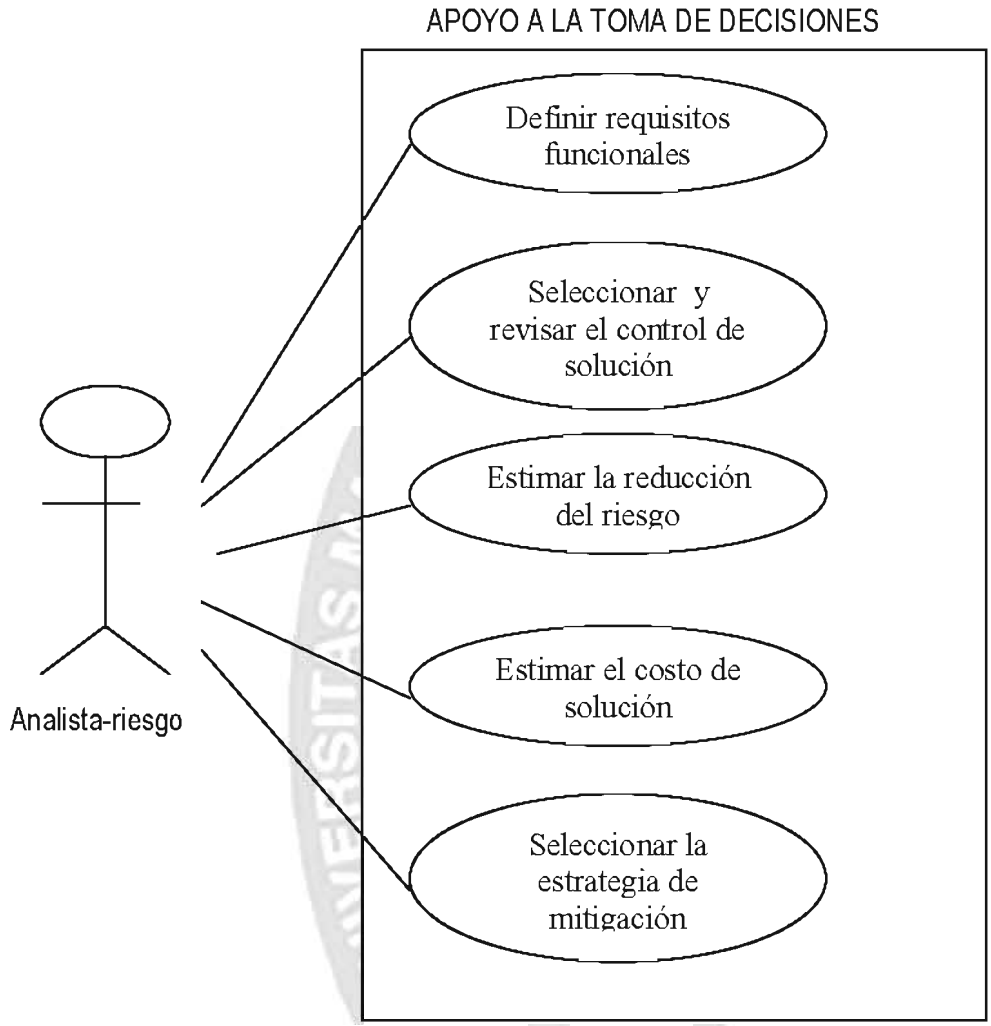

**Fuente:** Elaboración propia

**Tabla 5.** Caso de uso expandido Evaluación del riesgo

| ***CASO DE USO*** | ***EVALUACION DE RIESGOS*** |
|---|---|
| ***ACTORES*** | Analista-riesgos |
| ***PROPOSITO*** | Identificar y asignar prioridades a los riesgos para la empresa. |
| ***RESUMEN*** | Establecer una lista de prioridades de los riesgos |
| ***TIPO*** | Primario |

**Fuente:** Elaboración propia

**Figura 3.6** Diagrama de casos de uso Apoyo a la toma de decisiones



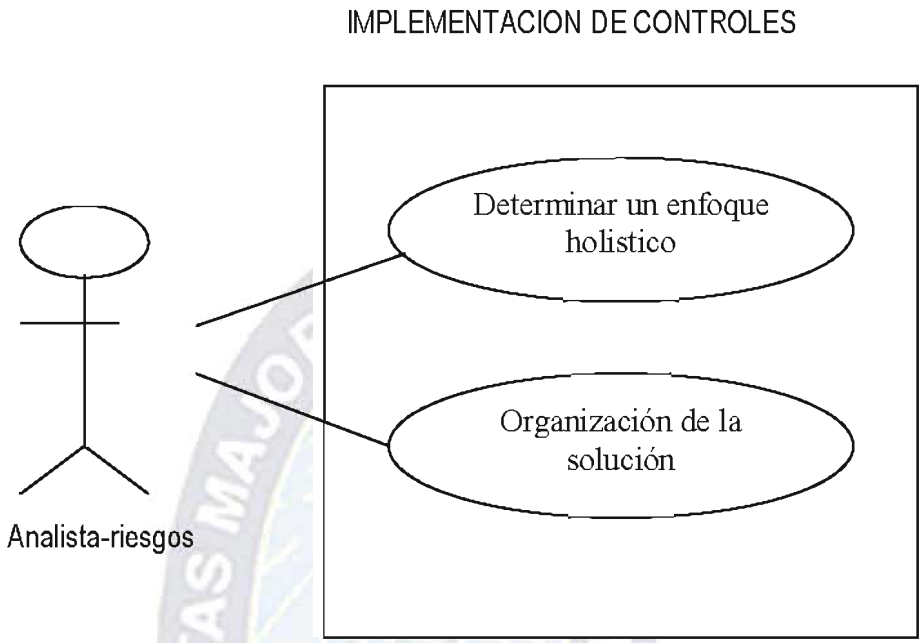

**Fuente:** Elaboración propia

**Tabla 6.** Caso de uso expandido Apoyo a la toma de decisiones

| ***CASO DE USO*** | ***APOYO A LA TOMA DE DECISIONES*** |
|---|---|
| ***ACTORES*** | Analista-riesgos |
| ***PROPOSITO*** | Identificar y evaluar las soluciones de control |
| ***RESUMEN*** | Emplear métricas de riesgos para precisar los objetivos específicos |
| ***TIPO*** | Primario |

**Fuente:** Elaboración propia

**Figura 3.7** Diagrama de casos de uso Implementación de Controles




**Fuente:** Elaboración propia

**Tabla 7.** Caso de uso expandido Implementación de controles

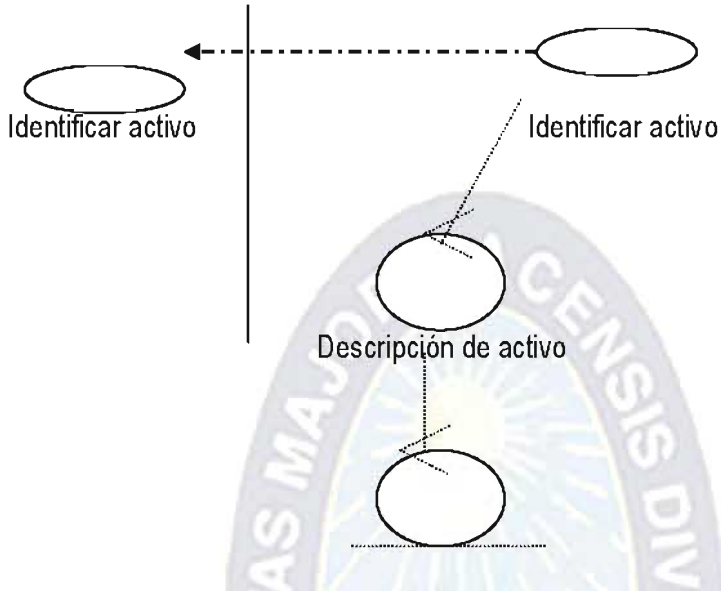
| ***CASO DE USO*** | ***IMPLEMENTACION DE CONTROLES*** |
|---|---|
| ***ACTORES*** | Analista-riesgos |
| ***PROPOSITO*** | Implementar y poner en funcionamiento las soluciones con el fin de reducir el riesgo para la empresa. |
| ***RESUMEN*** | Crear y ejecutar planes en función de la lista de solución de control para mitigar los riesgos identificados en la fase de evaluación del riesgo |
| ***TIPO*** | Primario |

**Fuente:** Elaboración propia

## 3.2 MODELO DE ANALISIS

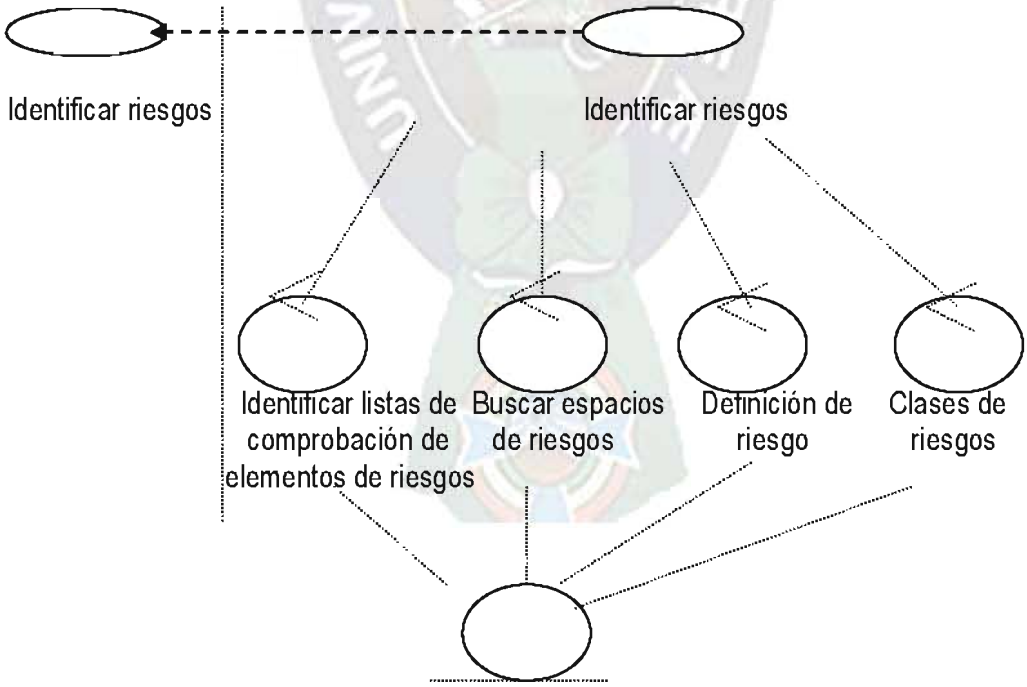
En el modelo de análisis se reflejan los diagramas de casos de uso

**Figura 3.8** Diagrama de Análisis Identificar activo



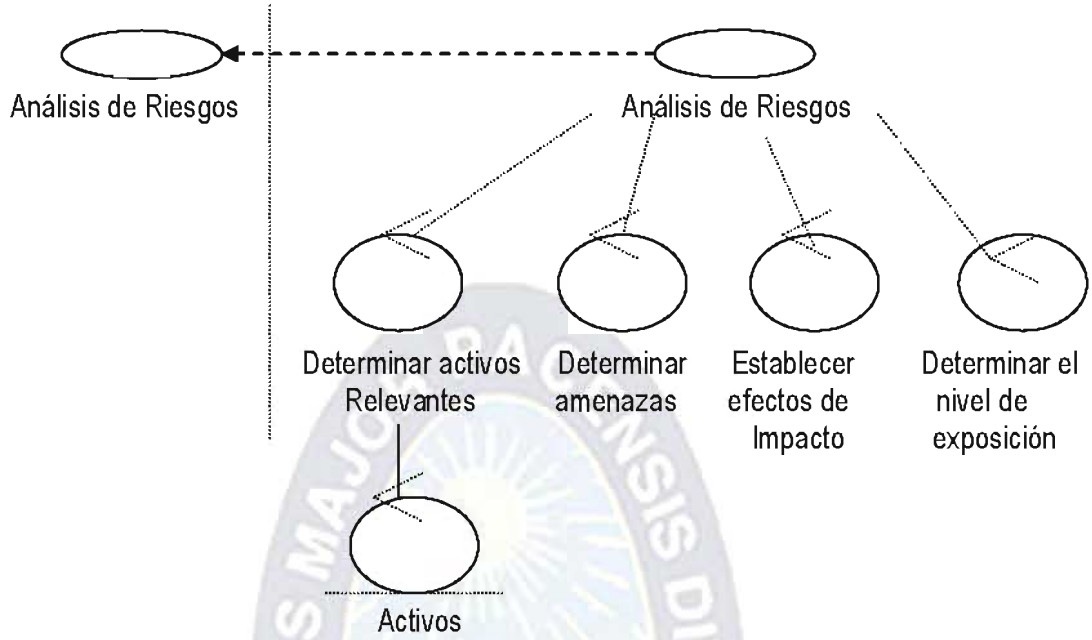

**Fuente:** Elaboración propia

**Figura 3.9** Diagrama de Análisis para identificar los riesgos



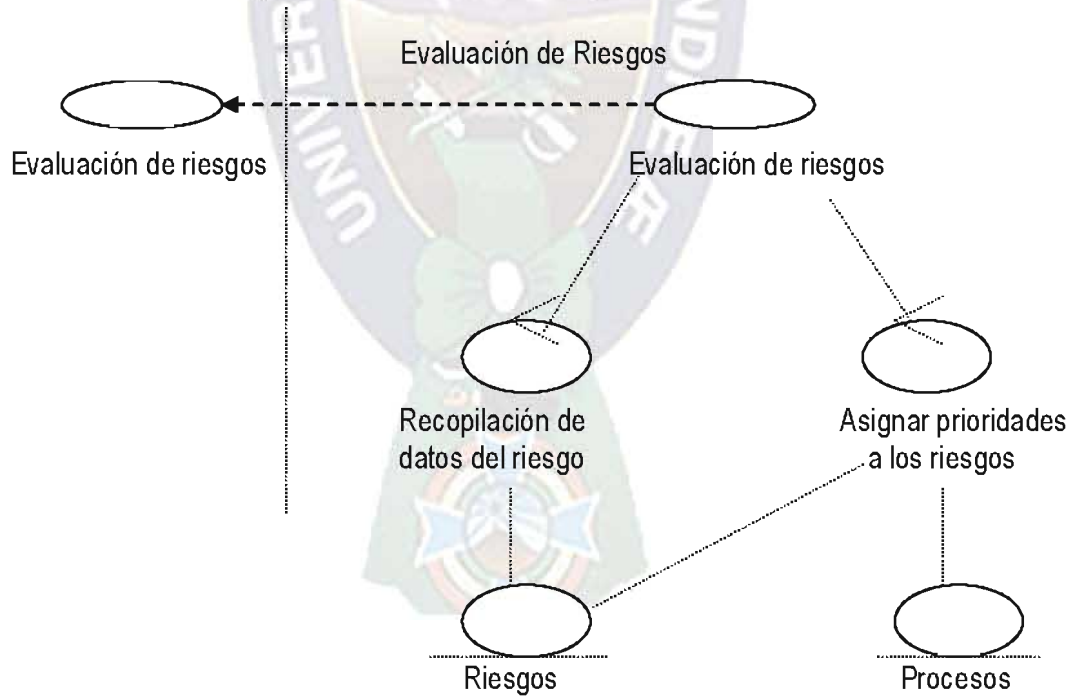

**Fuente:** Elaboración propia

**Figura 3.10** Diagrama de Análisis para Análisis de Riesgos



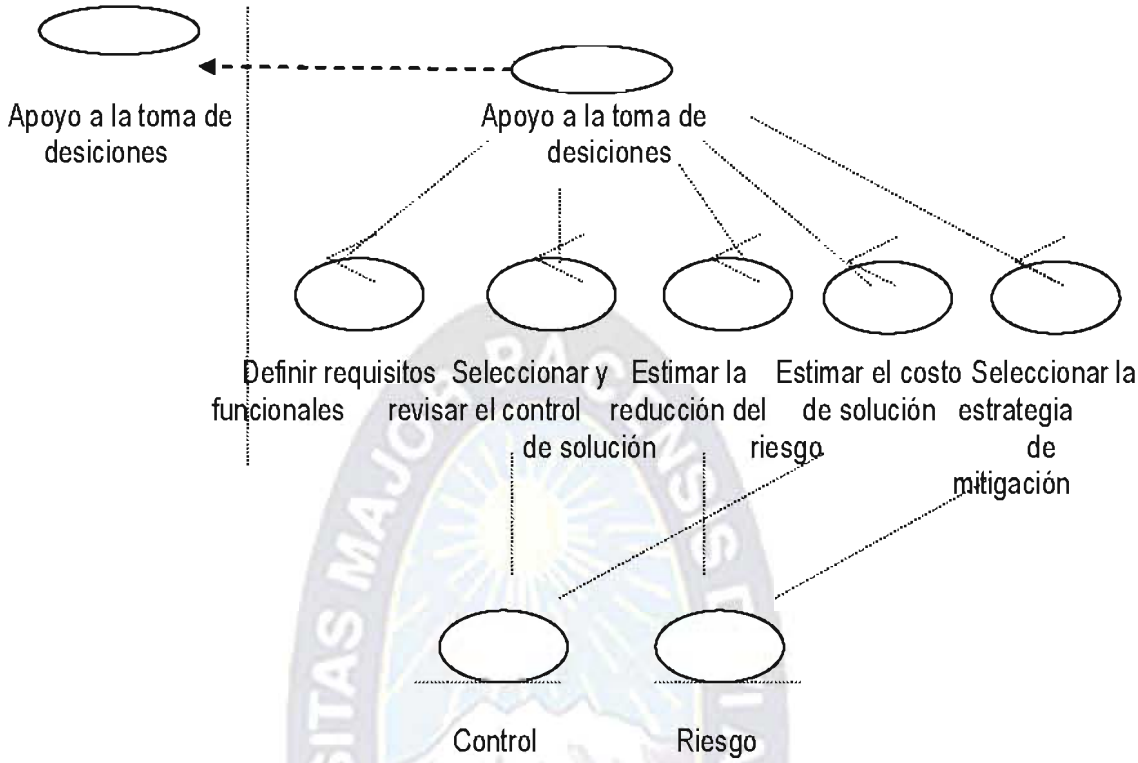

**Fuente:** Elaboración propia

**Figura 3.11** Diagrama de Análisis para Evaluación del Riesgo



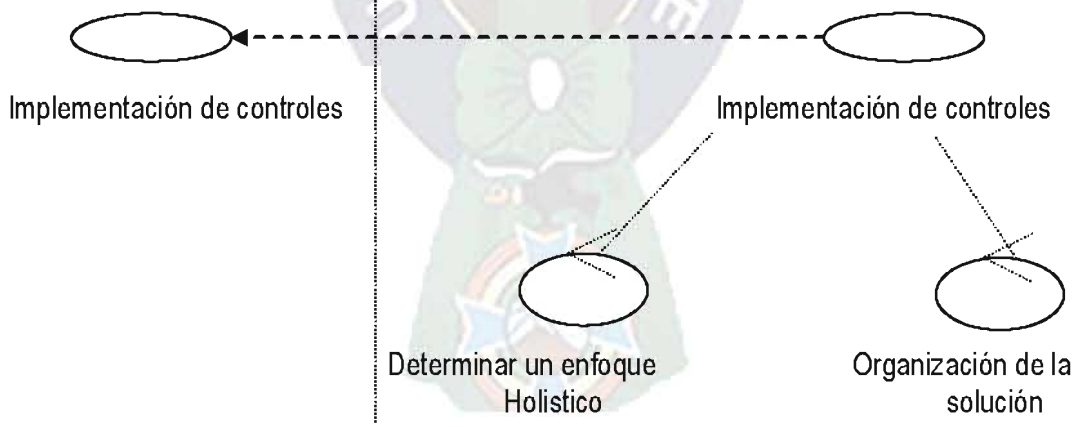

**Fuente:** Elaboración propia

**Figura 3.12** Diagrama de Análisis para Apoyo a la Toma de desiciones



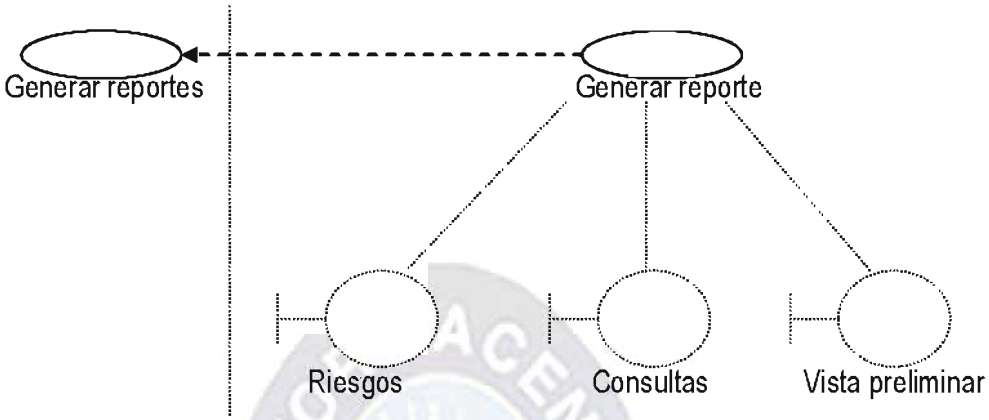

**Fuente:** Elaboración propia

**Figura 3.13** Diagrama de Análisis Implementación de Controles




**Fuente:** Elaboración propia

**Figura 3.14** Diagrama de Análisis para Generar reportes

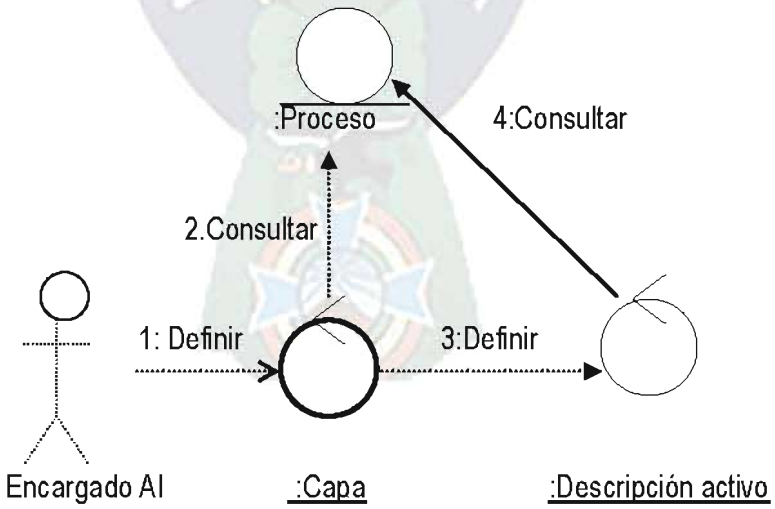



**Fuente:** Elaboración propia

## 3.3 DIAGRAMA DE COLABORACION

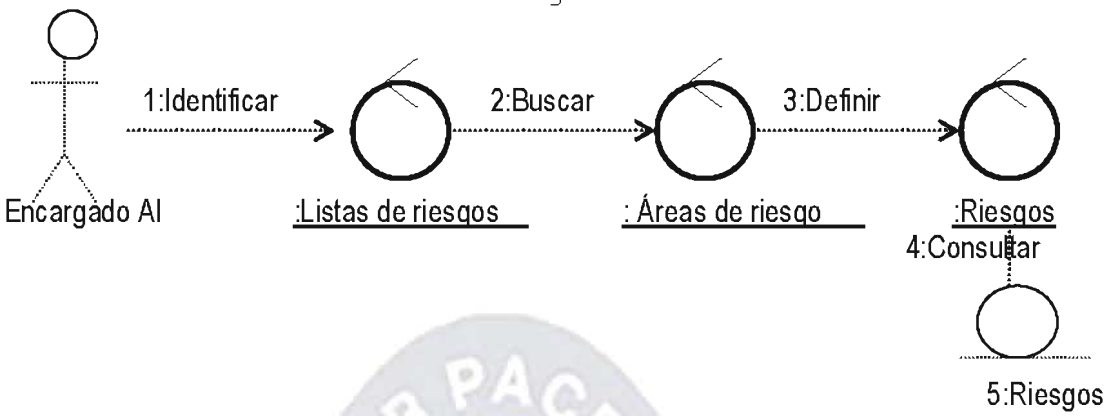
Los diagramas de colaboración destacan el contexto y organización general de los objetos que interactúan de acuerdo al espacio.

**Figura 3.15** Diagrama de Colaboración para Identificar activo



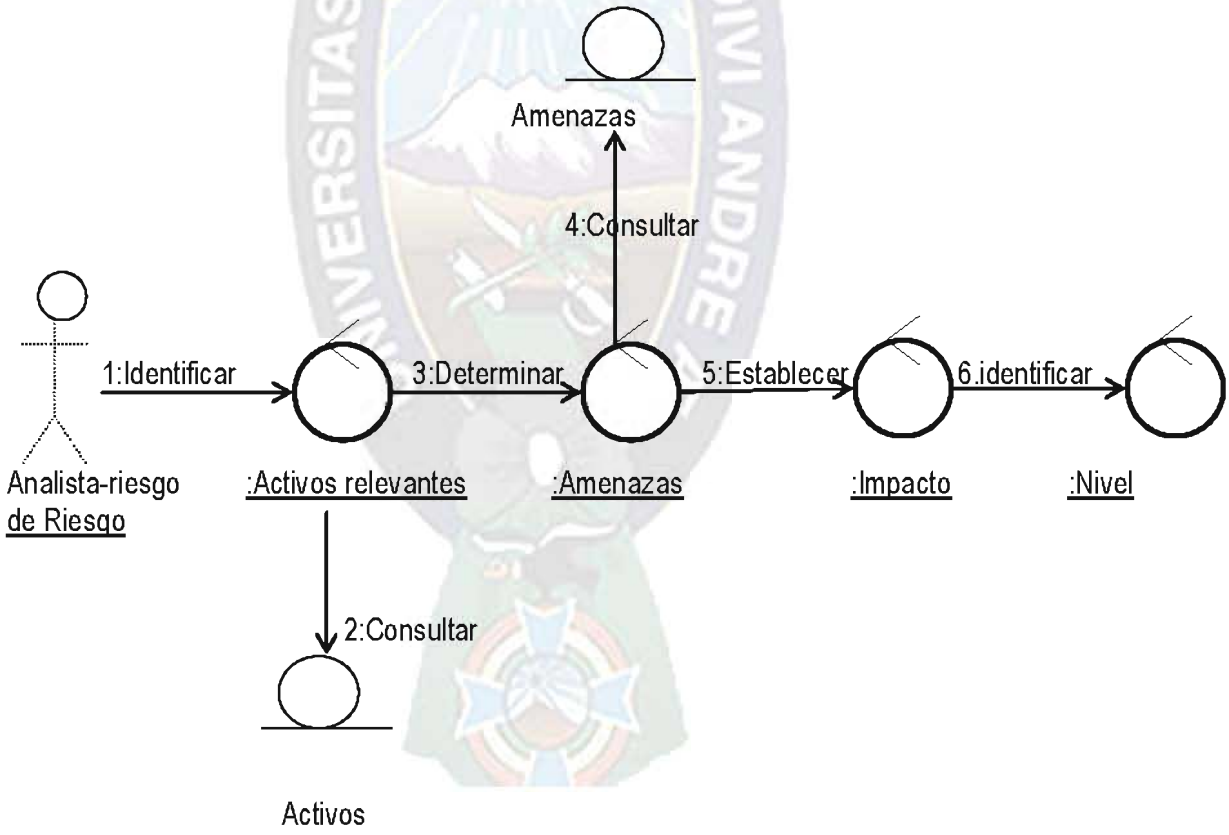

**Fuente:** Elaboración Propia

**Figura 3.16** Diagrama de Colaboración para Identificar Riesgos



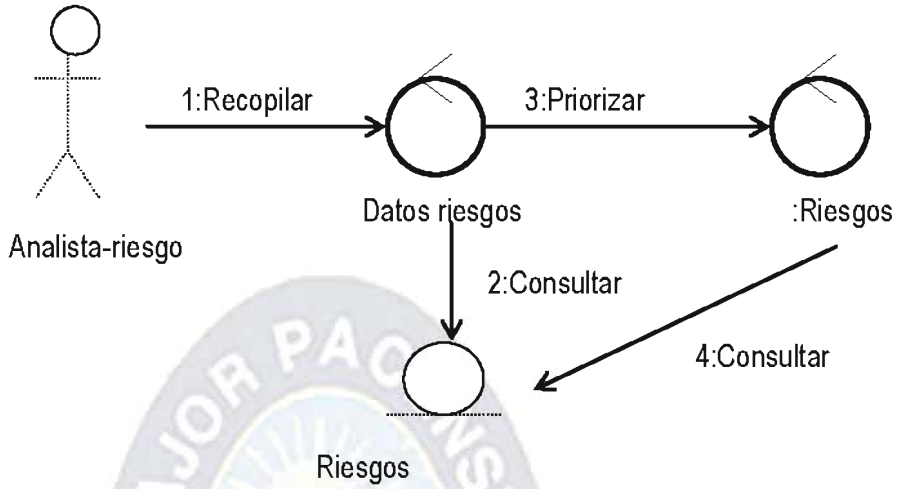

**Fuente:** Elaboración Propia

**Figura 3.17** Diagrama de Colaboración para Análisis de Riesgo



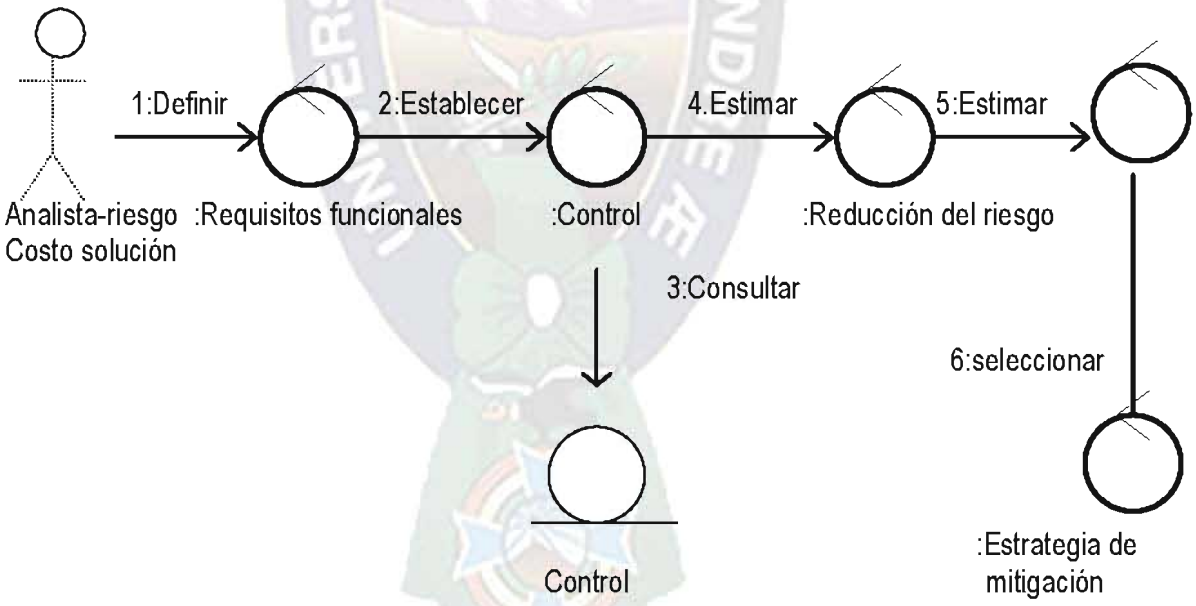

**Fuente:** Elaboración Propia

**Figura 3.18** Diagrama de colaboración para Evaluación del Riesgo



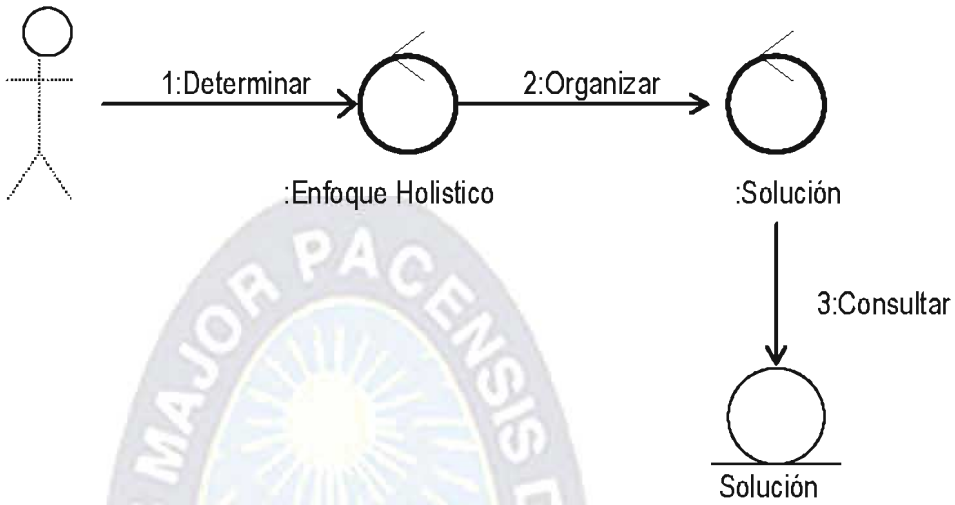

**Fuente:** Elaboración Propia

**Figura 3.19** Diagrama de Colaboración Apoyo a la Toma de Desiciones



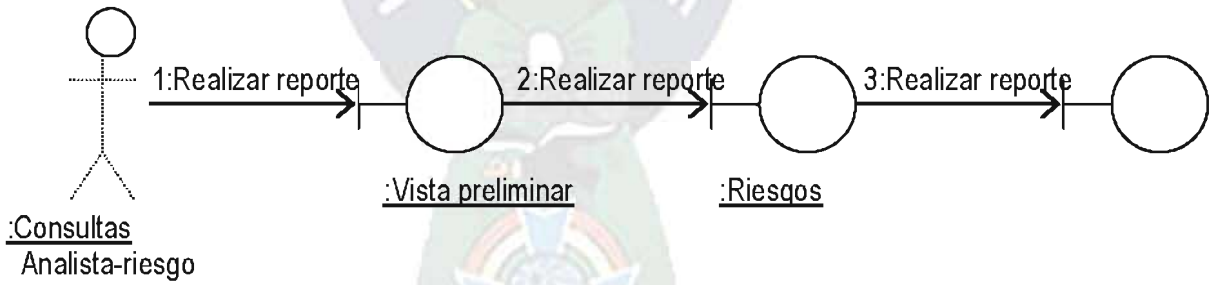

**Fuente:** Elaboración Propia

**Figura 3.20** Diagrama de Colaboración Implementación de controles




**Fuente:** Elaboración Propia

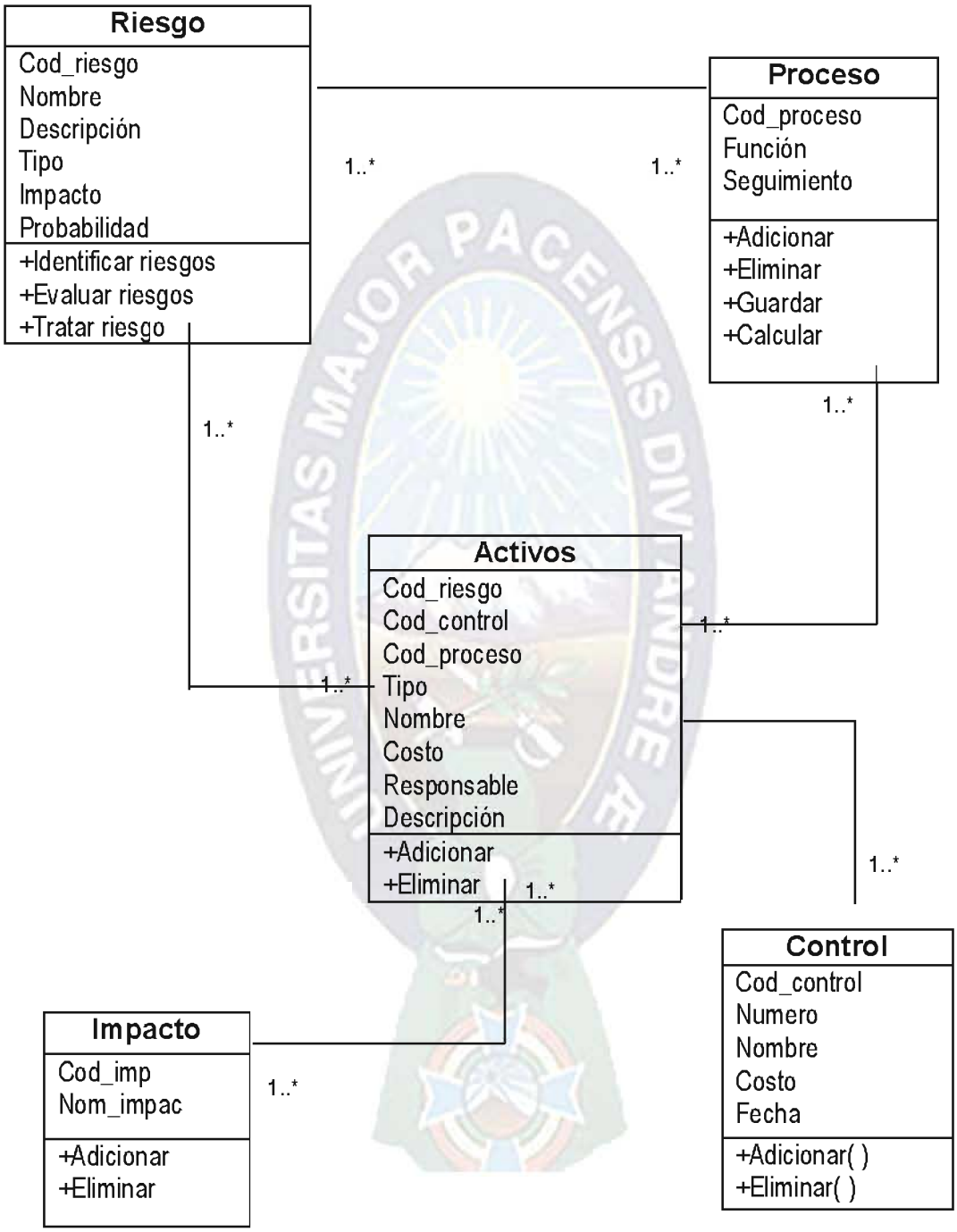
**Figura 3.21** Diagrama de Colaboración para Generar Reportes




**Fuente:** Elaboración Propia

## 3.4 DIAGRAMA DE CLASES

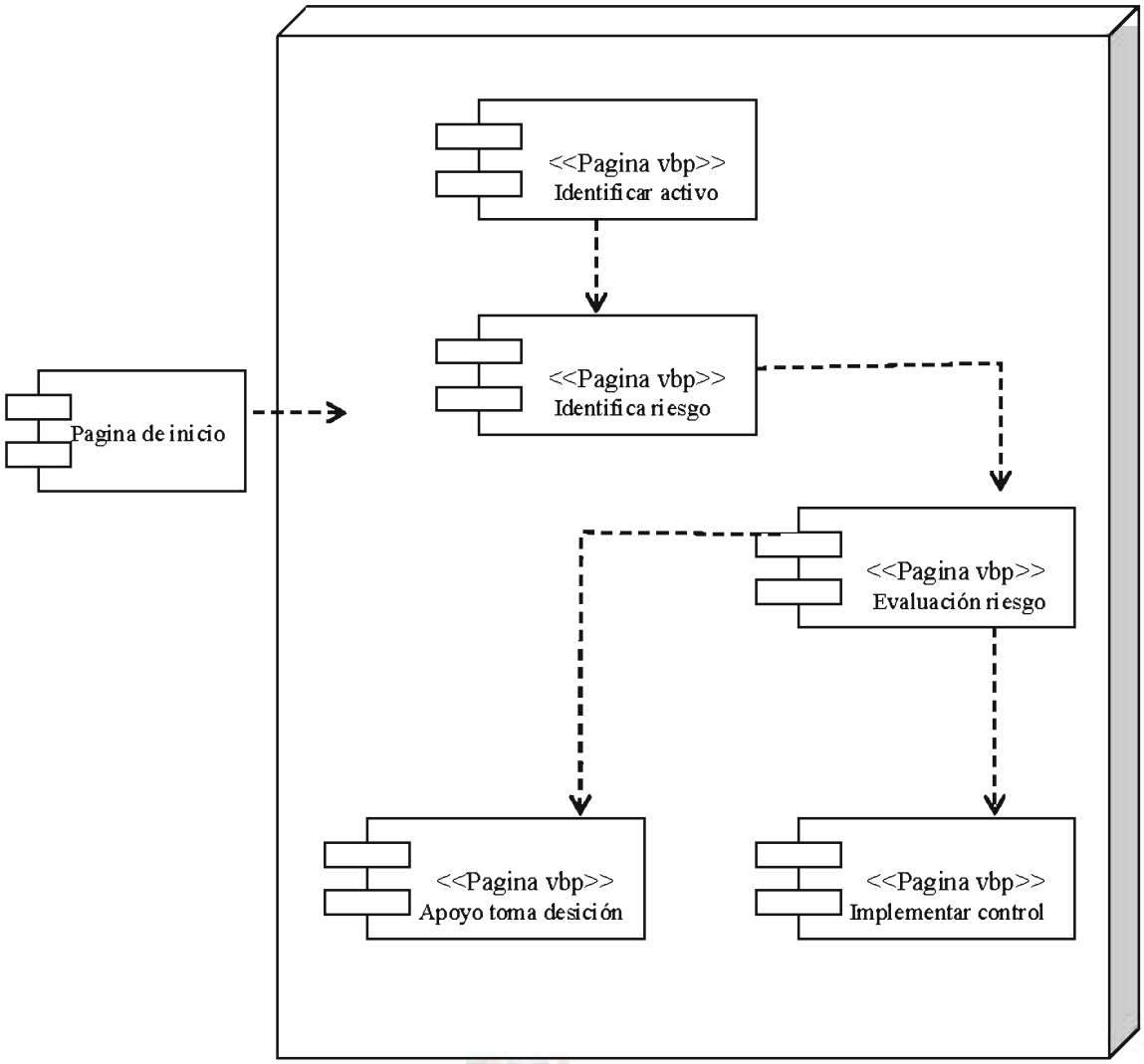
**Figura 3.22** Diagrama de Clases




**Fuente:** Elaboración propia

### 3.5 DIAGRAMA DE COMPONENTES

El diagrama de componentes contiene obviamente, componentes, interfaces y relaciones todo esto desde un punto de vista estático.




**Fuente:** Elaboración Propia

# CAPITULO IV

## SEGURIDAD, CONTROL Y ANALISIS COSTO/BENEFICIO

# SEGURIDAD, CONTROL Y ANALISIS COSTO/BENEFICIO

## CAPITULO IV

Es importante resaltar la constante evolución de las amenazas de seguridad llevando consigo un número cada vez mayor de desafíos para las empresas u organizaciones ya que el avance de la informática es vertiginoso y el empleo de las TICs[7] en el contexto actual no puede estar alejado del avance informático y sus influencias en el desarrollo de las empresas.

[7]Tecnologías de Información y Comunicación

Es por esto que la Seguridad protege una amplia gama de amenazas, con el fin de garantizar la continuidad comercial, minimizar el daño y maximizar el retorno sobre las inversiones y las oportunidades.

## 4.1 IDENTIFICACION Y AUTENTICACION

La autenticación es empleada en la mayoría de los sistemas, puede tomarse en dos contextos diferentes: autenticación de usuarios y autenticación de datos. En nuestro caso autenticación de usuario que es el proceso de determinar si una persona esta autorizada para llevar a cabo una acción dada.

La identificación y autenticación es considerada una de las primeras líneas de defensa para la mayoría de las aplicaciones esto con el objetivo de impedir el acceso no autorizado a la información contenida en los sistemas de información. En conclusión la autenticación de una persona a menudo consiste en verificar su identidad. La autenticación depende de uno o varios factores.

El "Sistema de Gestión de Riesgos en Activos de Información" realiza la **Identificación** usando como método la **Autenticación** se da cuando se establece un intercambio de información, y el sistema realiza una verificación sobre esta identificación de manera irrefutable.

Existen tres sistemas de identificación de usuarios, las cuales pueden ser utilizadas individualmente o combinadas:

1. La **autentificación mediante contraseña** es el sistema más común, usadas para el acceso a recursos informáticos, generalmente con un nombre de usuario asociado, y los PINs o NIPs[8] , etc.

2. La **autentificación mediante dispositivo** sólo reconocerá al usuario mientras mantenga introducida una "llave", normalmente una tarjeta con chip.

[8] Número de Identificación Personal

3. Los **dispositivos biométricos** son un caso especial del anterior, en los que la "llave" es una parte del cuerpo del usuario, huella dactilar, voz, pupila o iris.
El principal elemento necesario y suficiente para la autenticación de un usuario es la existencia de un identificador único que identifique al usuario de forma única en relación con otros usuarios. Los identificadores de los usuarios pueden haber muchas formas siendo la más usual la sucesión de caracteres conocida usualmente como password.

El paso normal de autenticación del sistema consta de los siguientes pasos:

1. El usuario solicita acceso al sistema
2. El sistema le solicita al usuario que inserte su contraseña o se identifique.
3. El usuario realiza su identificación.
4. El sistema valida según sus reglas los datos aportados por el usuario y verificar si son validos para dar acceso al sistema o no.

Cualquier sistema de identificación ha de poseer unas determinadas características para ser viable:

- Ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros).
- Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).
- Soportar con éxito cierto tipo de ataques.
- Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen.

La **Autenticación** o **autentificación**[9], en términos de seguridad de redes de datos, se puede considerar uno de los tres pasos fundamentales (AAA). Cada uno de ellos es, de forma ordenada:

[9] Con este mismo sentido se ha creado modernamente el verbo *autentificar*, que se considera también válido; Diccionario panhispánico de dudas, autenticar

1. **Autenticación** En la seguridad de ordenador, la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.

2. **Autorización** Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.

3. **Auditoria** Mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no.

El problema de la autorización a menudo, es idéntico a la de autenticación. Sin embargo, el uso más exacto describe la autenticación como el proceso de verificar la identidad de una persona, mientras la autorización es el proceso de verificación que una persona conocida tiene la autoridad para realizar una cierta operación. La autenticación, por lo tanto, debe preceder la autorización. Para distinguir la autenticación de la autorización de término estrechamente relacionada, existen unas notaciones de taquigrafía que son:

- A1 para la autenticación y
- A2 para la autorización, que de vez en cuando son usadas.

## 4.2 CRIPTOGRAFIA

La criptografía, es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y asegurar que la información que se envía es auténtica y que el remitente sea realmente quien dice ser.

La criptografía proviene del griego (*krypto* – oculto) y (*graphos* – escribir) literalmente "escritura oculta". El mensaje enviado, habitualmente denominado **criptograma** (Ver figura 4.1)

Información segura

Persona autorizada

Figura 4.1

La finalidad de la criptografía[10] es, en primer lugar, garantizar el secreto en la comunicación y en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado no haya sido modificado. Y así hacer cumplir el objetivo de la administración de la seguridad de la información que implica: "mantener la integridad, autenticidad, privacidad….." y hacer cumplir con el **No repudio**, siendo este una propiedad de que un receptor sea capaz de probar que el emisor de alguna información realmente la envió, aun cuando el emisor pudiera negar posteriormente haber enviado dicha información.

El sistema contiene información encriptada que solo puede ser vista por el administrador o por el operador del sistema, de esa forma garantizar el secreto de la información, es decir en el momento en que un usuario solicita un ingreso al sistema el password del mismo es encriptado, asegurando de que la información transmitida es autentica.

## 4.3 CRIPTOGRAFIA SIMETRICA

[10] En la Jerga de la criptografía, la información original que debe protegerse se denomina *texto en claro*. El *cifrado* es el proceso de convertir el *texto plano* en un galimatías ilegible, denominado *texto cifrado* o *criptograma*.

Continuando con la seguridad del sistema, este contiene criptografía simétrica. En términos informáticos la criptografía simétrica se basa en que emplea la misma clave para encriptar que para desencriptar, y entonces se habla de algoritmo de cifrado simétrico. La clave debe ser conocida tanto por el emisor como el receptor del mensaje y ambos deben mantenerla en estricto secreto, ya que si se conoce peligraría el contenido del mensaje. (Ver Figura 4.2)

El esquema básico de los algoritmos de clave simétrica es:

**MENSAJE + CLAVE = CÓDIGO (encriptación)**

**CÓDIGO + CLAVE = MENSAJE (desencriptación)**

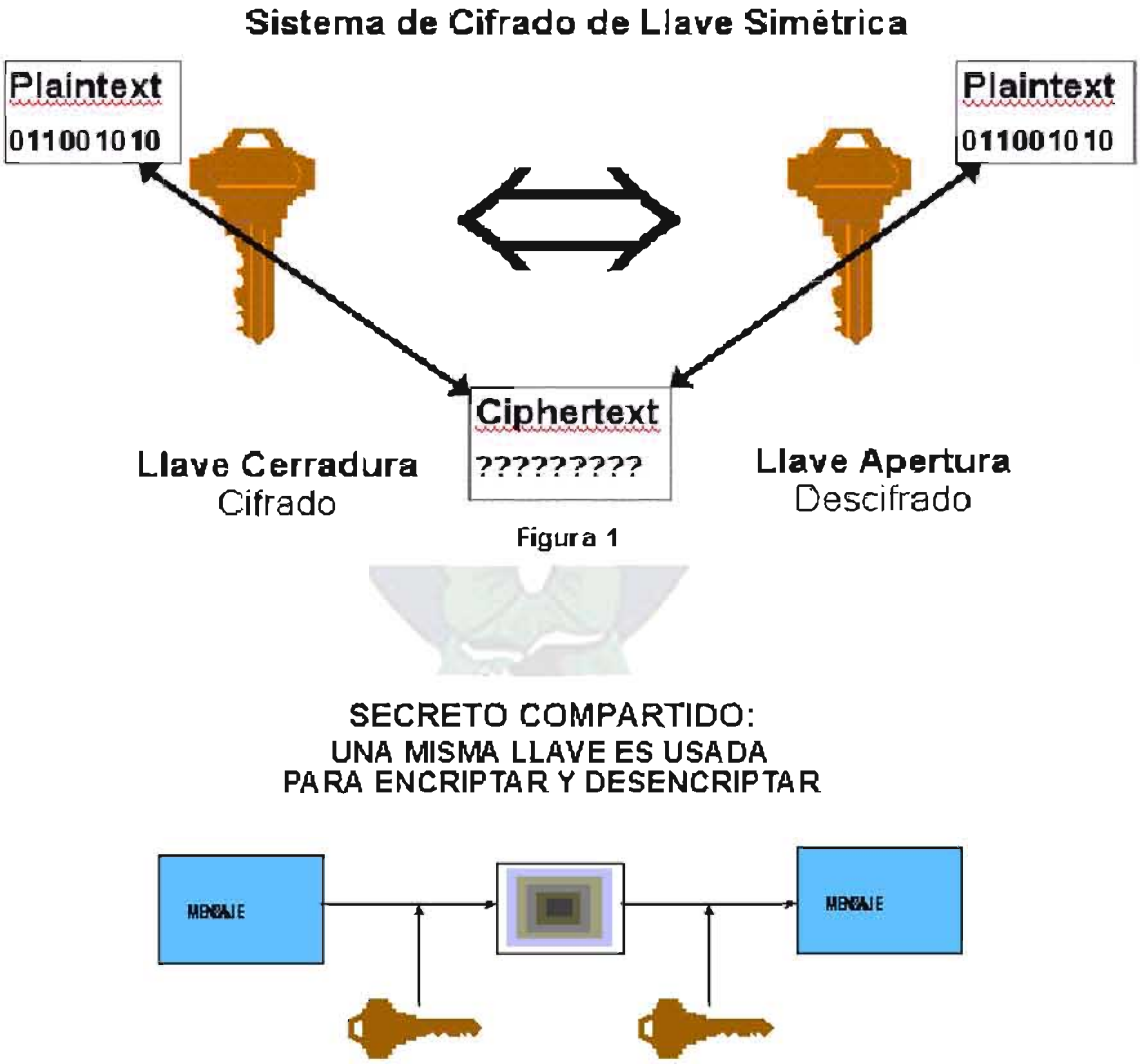



Figura 4.2

**Fuente:** [WWW. INEI Metodologías Informáticas · Seguridad en Internet.mht.html]

Con la criptografía simétrica, se remite el uso de una llave para encriptar el mensaje, entonces envía el mensaje encriptado al receptor. El receptor usa la misma llave para desencriptar el mensaje. Se debe tener una cifra y una llave, que puede cambiar, para ocultar el mensaje. Cuando se toma la cifra y aplica la llave a un mensaje, se puede crear o destrabar el mensaje. Aquí hay algunos ejemplos simples:

| El Mensaje | Cifra | LLave | Texto Cifrado |
|---|---|---|---|
| *Nosotros estamos seguros* | *Sustitución del texto* | *A=B* | *Xf bsf tbgf* |
| *Nosotros estamos seguros* | *Palabras ajenas* | *Cada 3ra palabra* | *Que si nosotros sabemos que estamos realmente muy seguros de comer?* |

**Ventaja:**

En aplicaciones donde existe un número limitado de usuarios y un gran volumen de información, la criptografía de llave simétrica es efectiva.

## 4.4 FUNCIONES RESUMEN (HASH)

Para identificar el mensaje propiamente dicho se utilizan las llamadas funciones resumen (en inglés, *hash*)[11]. El resultado de aplicar una función resumen a un texto es un número grande, el número resumen, que tiene las siguientes características:

- Todos los números resumen generados con un mismo método tienen el mismo tamaño sea cual sea el texto utilizado como base.
- Dado un texto base, es fácil y rápido (para un ordenador) calcular su número resumen.
- Es imposible reconstruir el texto base a partir del número resumen.
- Es imposible que dos textos base diferentes tengan el mismo número resumen.

[11] El término hash proviene, aparentemente, de la analogía con el significado estándar (en inglés) de dicha palabra en el mundo real: picar y mezclar.

En informática hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una *función hash* o *algoritmo hash*. Un **hash** es el resultado de dicha función o algoritmo.

Hash es una función que te permite comprobar la contraseña de un usuario contra una base de datos sin necesidad de conocerla.

**Función:**

```
Function HashPassword(ByVal vsUserId As String, ByVal vsPassword As String) As
Double

Const uHASH_DEPTH = 6
Static k(uHASH_DEPTH) As Integer
Dim S As String
Dim I As Integer
Dim J As Integer
Dim k1 As Integer
Dim N As Integer
Dim fHash As Double
Dim fTemp As Double

‘ Si la contraseña está en blanco,
‘ el valor de hash sigue siendo cero.
‘ Por lo tanto significa “sin contraseña”.
fHash = 0#

If vsPassword <> “” Then
‘ Si incluyes el nombre del usuario como parte del hash,
‘ dos usuarios con la misma contraseña no tendrán el mismo
‘ valor de hash:
S = vsPassword & vsUserId
’s = UCase$(s) ‘ Activa esta linea para convertir a mayúsculas
N = Len(S)

k(1) = Asc(Mid$(S, 1, 1))
For J = 2 To uHASH_DEPTH
k1 = 1 + (k(J - 1) Mod N)
k(J) = Asc(Mid$(S, k1, 1))

If k(J) = k(J - 1) Then

k(J) = k(J) + 1
End If
Next J
```

```
For I = 1 To N
fTemp = I
For J = 1 To uHASH_DEPTH
k1 = 1 + ((I + k(J)) Mod N)
fTemp = fTemp * Asc(Mid$(S, k1, 1))
Next J

fHash = fHash + fTemp
Next I
End If

HashPassword = fHash
End Function
```

Una **función de hash** es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo). Varían en los conjuntos de partida y de llegada y en cómo afectan a la salida similitudes o patrones de la entrada.

Es posible que existan claves resultantes iguales para objetos diferentes, ya que el rango de posibles claves es mucho menor que el de posibles objetos a resumir.

Son usadas en múltiples aplicaciones, como los arrays asociativos, criptografía, procesamiento de datos y firmas digitales, entre otros. Una buena función de *hash* es una que experimenta pocas **colisiones** en el conjunto esperado de entrada; es decir que se podrán identificar unívocamente las entradas (ver función inyectiva).

Muchos sistemas relacionados con la seguridad informática usan funciones o tablas hash.

## 4.6 SEGURIDAD Y CONTROL DEL SISTEMA

En cuanto a seguridad el "Sistema de Gestión de Riesgos en Activos de Información" posee la propiedad de identificación y autenticación de usuarios. El sistema de autenticación es un proceso de seguridad que asegura de que el usuario que esta realizando la solicitud de ingreso al sistema sea quien dice ser, realizando una validación de datos. En caso de que el sistema valide los

datos como verdaderos, se le dará el acceso al sistema en calidad de administrador u operador.

La siguiente figura 4.3 nos muestra un diagrama, el cual nos describe los pasos de ingreso al sistema, solicitándonos un **password** permitiéndonos acceder a todo el entorno de la aplicación desarrollada.

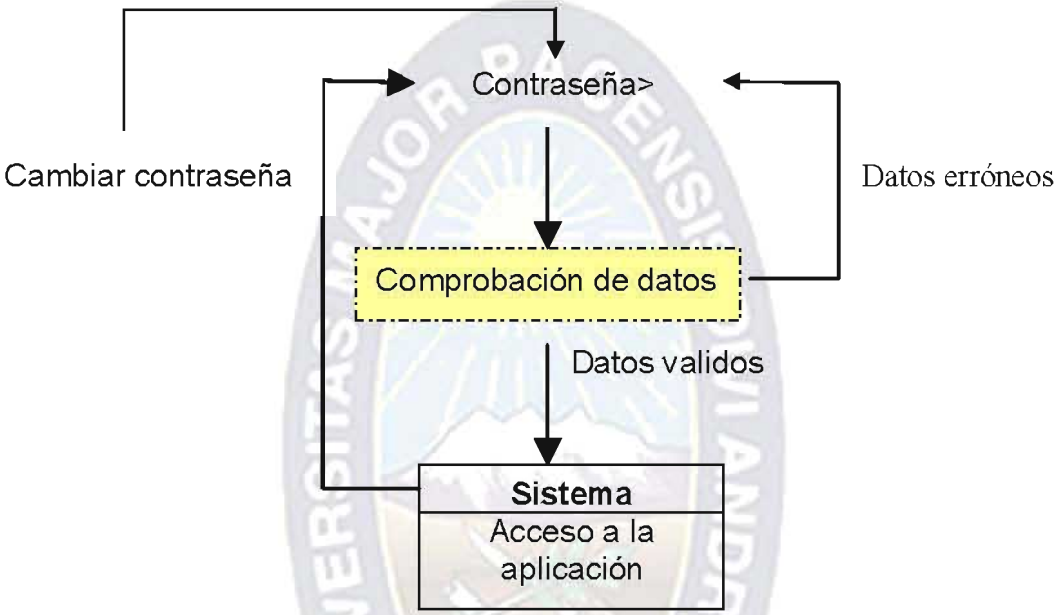



Figura 4.3

Los datos introducidos por el usuario son enviados a la página dibujada con línea segmentada, esta es la que se encarga de hacer la verificación de los datos. Según la respuesta de verificación el sistema nos da acceso o no, en caso de ser validos los datos nos redirecciona a la primera pantalla de la aplicación, Si no satisface dicha comprobación (el usuario no se ha autenticado correctamente) y los datos son erróneos, el sistema no devuelve un mensaje error que dice "la contraseña es incorrecta intente de nuevo" y nos devuelve a la interfaz de Login para volver a intentar ingresar al sistema.

## 4.7 ANALISIS COSTO-BENEFICIO DEL SISTEMA

La técnica de Análisis de Costo / Beneficio, tiene como objetivo fundamental proporcionar una medida de la rentabilidad del proyecto, mediante la

comparación de los costos previstos con los beneficios esperados en la realización del mismo.

Esta técnica se debe utilizar al comparar proyectos para la toma de decisiones. Así esta perspectiva orienta a la ejecución de medidas de seguridad solo en los escenarios en que el análisis costo-beneficio se justifique.
La utilidad de la presente técnica es la siguiente:

- Para valorar la necesidad y oportunidad de la realización de un proyecto.
- Para seleccionar la alternativa más beneficiosa de un proyecto.
- Para estimar adecuadamente los recursos económicos necesarios, en el plazo de realización de un proyecto.

### 4.7.1 ANALISIS DE COSTOS ANTES DE IMPLEMENTACION

En este punto se realizara un análisis de costos previo a la implementación del sistema:

- Un evaluador de riesgos realiza un análisis en 50 horas, esto tiene un costo de 3000 Bs. El trabajo lo realizan entre dos personas lo que implicaría un costo total del análisis de riesgos de 6000 Bs. Los beneficios adquiridos por el actual control no es tan eficaz como se podría esperar que sea, los datos se resumen en la siguiente tabla:

| Nro. Evaluadores | Horas de trabajo | Costo | Beneficio | Costo/beneficio | Deseable Si o No |
|---|---|---|---|---|---|
| **Evaluador 1** | 50/2 | 3500 Bs. | 50% | 3500 Bs./50 % | **No** |
| **Evaluador 2** | 50/2 | 3500 Bs. | 50% | 3500 Bs./50 % | **No** |
| **Total** | **50** | **7000 Bs.** | **50%** | **3500 Bs./50%** | **No** |

**Fuente:** Elaboración Propia

- Considerando que al año se realiza 8 análisis de riesgos en relación a los activos de información, entonces tenemos un gasto anual de:

| Descripción | Numero de análisis de riesgos por año | Costo de análisis | Costo total de análisis por año |
|---|---|---|---|
| Análisis de riesgos | 8 | 7000 Bs. | 56000 |

**Fuente:** Elaboración propia

### 4.7.2 ANALISIS DE COSTOS DESPUES DE LA IMPLEMENTACION

El análisis de costos después de implementación de la aplicación se la describe de la siguiente manera:

- Con la implementación del sistema se ha logrado un ahorro en tiempo de un 30%. Esto vendría ha ser en términos de tiempo un ahorro de 15 horas. Entonces un análisis de riesgos se lo realizaría en 35 horas. Y no solo se logra un ahorro en términos de tiempo si no que de la mano viene lo que es una reducción en los gastos económicos.

- Sin la implementación del sistema el sueldo era de 7000 Bs. por 50 horas, horas en que se realizaba un análisis de riesgos. Con la implementación del nuevo sistema el sueldo es de 5000 Bs. por análisis, teniendo un ahorro en gastos económicos de 2000 Bs. Los se resumen en la siguiente tabla:

| Nro. Evaluadores | Horas de trabajo | Costo | Beneficio | Costo/beneficio | Deseable Si o No |
|---|---|---|---|---|---|
| **Evaluador 1** | 35/2 | 2500 Bs. | 85% | 2500 Bs./85 % | **SI** |
| **Evaluador 2** | 35/2 | 2500 Bs. | 85% | 2500 Bs./85 % | **SI** |
| **Total** | **35** | **5000 Bs.** | **85%** | **5000 Bs./85%** | **SI** |

**Fuente:** Elaboración Propia

- Considerando que anualmente se realiza 8 análisis de riesgos tenemos un gasto económico de:

| Descripción | Numero de análisis de riesgos por año | Costo de análisis | Costo total de análisis por año |
|---|---|---|---|
| Análisis de riesgos | 8 | 5000 Bs. | 40000 |

### 4.7.3 ANALISIS COSTO/BENEFICIO

Después de realiza el análisis de costo con respecto al antes y después de la implementación de la aplicación, obtenemos una comparación de precios, en el cual se ve el beneficio de la implementación, en donde se ve claramente un ahorro de 2000 Bs. por año, veamos en detalle en la siguiente tabla:

| Descripción | Costo total del análisis de riesgos | Costo total por año |
|---|---|---|
| Análisis sin aplicación | 7000 Bs. | 56000 Bs. |
| Análisis con aplicación | 5000 Bs. | 40000 Bs. |
| **Costo total de ahorro después de la implementación de la aplicación** | **2000** | **16000 Bs.** |

**Fuente:** Elaboración Propia

Esta estimación de costos se la realizo tomando los siguientes criterios de valoración:

La aplicación se diseño en el lenguaje de programación Visual Basic, con una base de datos Access y con el sistema operativo Windows XP.

Con respecto al lenguaje de programación Visual Basic:

- Su tiempo de respuesta es rápido
- La programación no es complicada
- Posee una plataforma estable y segura
- Es gratuito
- Su interfaz es amigable
- No tiene restricción en cuanto a plataformas.

Se eligió la base de datos Access por que:

- Es fácil de usar
- Captura y presenta los datos de manera eficiente
- Tiene una interfaz amigable
- Su tiempo de respuesta es rápido
- Es gratuito

Con todo esto se concluye que la implementación del sistema se encuentra claramente justificada en todos sus ámbitos, ya que facilitara el trabajo de gestión de riesgos, dándose también una reducción en cuanto a gastos económicos y tiempo de trabajo que pueden ser empleados en otras actividades en beneficio de la organización.

## 4.8 CONTROL DE CALIDAD DEL SISTEMA

### 4.8.1 Introducción

A continuación se describe los factores de calidad con el objeto de evaluar la calidad del sistema. En cuanto a calidad no es necesariamente llegar al objetivo perfecto mas por el contrario es la necesidad y suficiencia para cada contexto de uso en el momento de manejo de los usuarios, se tomo los siguientes criterios de calidad.

- Confiabilidad
- Funcionalidad
- Mantenibilidad
- Portabilidad
- Usabilidad

Estos criterios de calidad están basados en el estándar ISO/IEC 9126 que establece un estándar internacional para la evaluación de la calidad de productos de software, en el cual se establecen las características de calidad para productos de software. Cada una de las cuales se detalla a través de un conjunto de subcaracteristicas que permiten profundizar en la evaluación de la calidad de productos de software y se encuentran desarrollados a continuación.

### 4.8.2 Confiabilidad

La confiabilidad de un sistema es un elemento importante en su calidad general. Para determinar la confiabilidad se toma en cuenta la las fallas que se

producen en el sistema en un tiempo determinado. Primeramente se considera la confiabilidad de cada modulo independiente.

Para esto se necesita encontrar el "modelo del sistema" mediante funciones de transferencia el cual nos permite delimitar el comportamiento del mismo en cada uno de sus módulos.

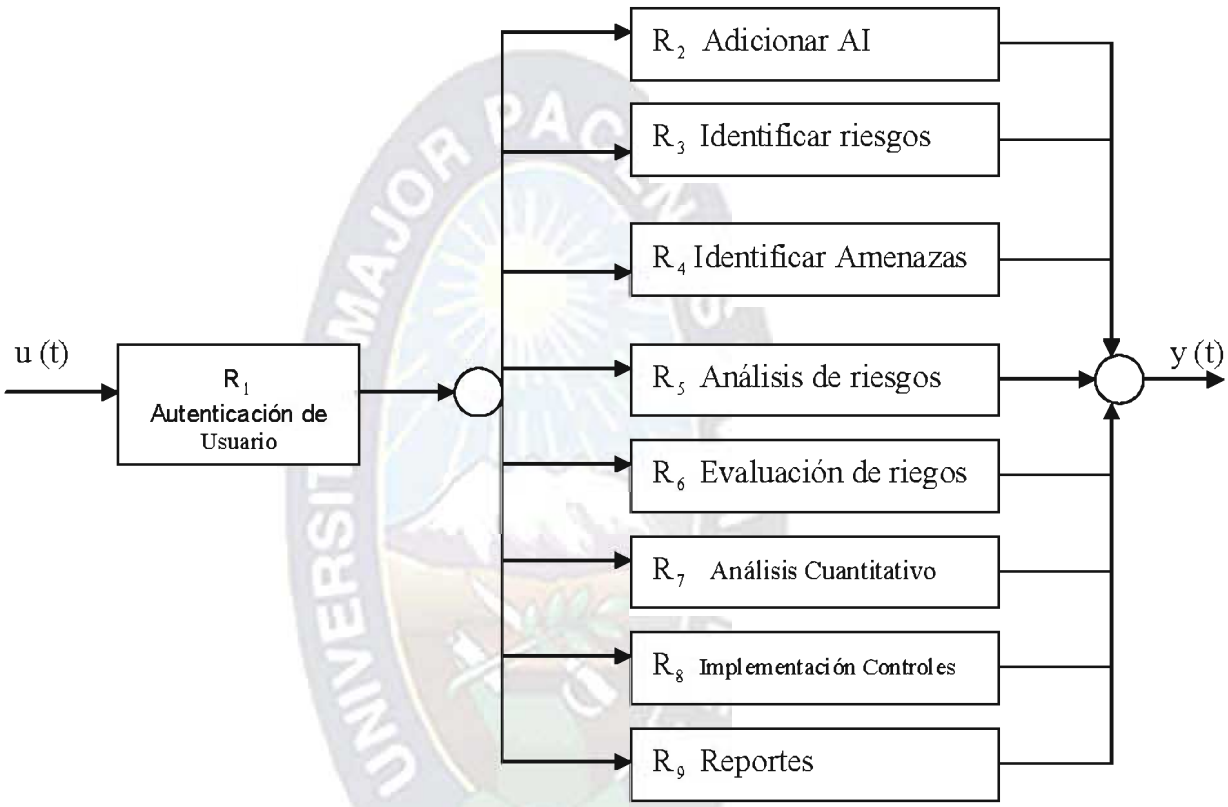



**Figura 5.1** Modelo del Sistema GRAI
**Fuente:** Elaboración propia

Tomando en cuenta la siguiente relación: $R(t) = e^{-\lambda t}$

Se realiza el cálculo de la confiabilidad de cada modulo del sistema:

| | Módulos | λ | T | R(T) |
|---|---|---|---|---|
| 1 | Autenticación del usuario | 0.03 | 2 horas | 0.94 |
| 2 | Adicionar AI | 0.03 | 5 horas | 0.86 |
| 3 | Identificar riesgos | 0.04 | 3 horas | 0.85 |
| 4 | Identificar Amenazas | 0.04 | 1 horas | 0.96 |

| | | | | |
|---|---|---|---|---|
| **5** | Análisis de riesgos | 0.05 | 5 horas | 0.90 |
| **6** | Evaluación de riegos | 0.07 | 2 horas | 0.86 |
| **7** | Análisis Cuantitativo | 0.06 | 1 hora | 0.94 |
| **8** | Implementación de controles | 0.03 | 1 hora | 0.97 |
| **9** | Reportes | 0.02 | 3 horas | 0.94 |

El modelo del sistema nos muestra una conexión compuesta donde se tiene inicialmente una conexión en serie y posteriormente una conexión en paralelo. Por lo tanto realizando los cálculos correspondientes tenemos:

$$R = R_1 * R_s$$

en donde: $R_1 = R_1 = 0.94$

$R_s = 1- \{[1-R_2 (T)]*.....*[1-R_s (T)]\}$

$R_s = 1- (0.14)*(0.15)*(0.04)*(0.10)*(0.14)*(0.06)*(0.03)*(0.06)$

$R_s = 0.9999999987$

$R = [(0.94) * (0.9999999987)]= 0.94$

$\%R = 94\%$

De acuerdo con el resultado obtenido podemos decir que el "Sistema de Gestión de Riesgos en Activos de Información" , presenta una confiabilidad del 94%, entonces se puede afirmar que es un sistema confiable.

### 4.8.3 Funcionalidad

Las métricas del software orientadas a la función utilizan una medida de funcionalidad entregada por la aplicación. La funcionalidad se valora evaluando el conjunto de características y capacidades del sistema.

Para determinar la funcionalidad del sistema mediante la métrica del punto función, se debe determinar cinco características de dominio de información y se proporciona las cuentas en la posición apropiada a la tabla. Los valores de los dominios de información se definen de la siguiente forma:

- Numero de entradas de usuario
- Numero de salidas de usuario
- Numero de peticiones de usuario
- Numero de archivos
- Numero de interfaces externas

A continuación se realiza el conteo de los parámetros mencionados

| | |
|---|---|
| Entradas de usuario | 3 |
| Salidas de usuario | 9 |
| Peticiones de usuario | 8 |
| Archivos | 1 |
| Interfaces externas | 0 |

**Tabla 5.1** Conteo de parámetros de Punto Función

Una vez que se ha recopilado los datos se le asocia un valor de complejidad que se muestra en la siguiente tabla:

| Parametros de Medición | Cuenta | Factor de ponderación Simple | Medio | Complejo | |
|---|---|---|---|---|---|
| Numero de entradas de usuario | 3 | 3 | 4 | 6 | 12 |
| Numero de salidas de usuario | 9 | 4 | 5 | 7 | 45 |
| Numero de peticiones de usuario | 8 | 3 | 4 | 6 | 32 |
| Numero de archivos | 1 | 7 | 10 | 15 | 10 |
| Numero de interfaces externas | 0 | 5 | 7 | 10 | 0 |
| Cuenta Total | | | | | 99 |

**Tabla 5.2** Calculo de Punto de Función

A continuación se obtiene los "valores de ajuste de la complejidad" según las respuestas a las siguientes preguntas.

| | Factor | No Importante 0 | Incidental 1 | Moderado 2 | Medio 3 | Significativo 4 | Esencial 5 |
|---|---|---|---|---|---|---|---|
| 1 | ¿Requiere el sistema copias de seguridad y de recuperación fiable? | | | | | | X |
| 2 | ¿Se requiere comunicación de datos? | | | | | X | |
| 3 | ¿Existen funciones de procesamiento distribuido? | X | | | | | |
| 4 | ¿Es critico el rendimiento? | | | | | X | |
| 5 | ¿Se ejecutara el el sistema en un entorno operativo existente y fuertemente utilizado? | | | | | X | |
| 6 | ¿Requiere el sistema entrada de datos interactiva? | | | | | X | |
| 7 | ¿Requiere la entrada de datos interactiva, que las transacciones de entrada se lleven a cabo sobre multiples pantallas u operaciones? | | | | | X | |
| 8 | ¿Se actualizan los archivos maestros de forma interactiva? | | | | | X | |
| 9 | ¿Son complejas las entradas, las salidas, los archivos o las peticiones? | | | X | | | |
| 10 | ¿Es complejo el procesamiento interno? | | | X | | | |
| 11 | ¿Se ha diseñado el codigo para ser reutilizable? | | | | | X | |
| 12 | ¿Están incluidas en el diseño la conversión y la instalación? | X | | | | | |
| 13 | ¿Se ha diseñado el sistema para soportar multiples instalaciones en diferentes organizaciones? | | X | | | | |
| 14 | ¿Se ha diseñado la aplicación para facilitar los cambios y para ser facilmente utilizada por el usuario? | | | | | | X |

Entonces:

$$\sum F_i = F_1 + F_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + F_{14}$$

$$\sum F_i = 5 + 4 + 0 + 4 + 4 + 4 + 4 + 4 + 2 + 2 + 4 + 0 + 1 + 5$$

$$\sum F_i = 43$$

Reemplazando en la relación siguiente:

$$PF = Cuenta\_Total * [ X + Min ( Y ) * \sum F_i ]$$

X: confiabilidad del sistema, es igual a la confiabilidad hallada anteriormente

X = 0.94

Min (Y): error mínimo aceptable

Min (Y) = 0.01

Cuenta_total = 99

$\sum F_i = 43$

Reemplazando en la formula de PF se tiene:

$$PF = 99*[0.94 + 0.01 * 0.43]$$

$$PF = 136$$

Este PF supone 136 líneas de código

Si se considera la $\sum F_i = 70$, considerando el 100%, reemplazando en la relación anterior se tiene:

$$PF_{max} = 136 * [0.94 + 0.01 * 70]$$

$$PF_{max} = 223$$

Por lo tanto la funcionalidad esta dado por:

$$Funcionalidad = PF / PF_{max} = 136 / 223$$

$$Funcionalidad = 0.61$$

$$\%Funcionalidad = 0.61 * 100 = 61\%$$

Esto nos indica una funcionalidad en el sistema del 61%.

### 4.8.4 Mantenibilidad

Para la facilidad de mantenimiento se utiliza la métrica de Índice de Madurez del Sistema (IMS) que fue sugerida por el estándar IEEE 982.1-1998 que proporciona una indicación de estabilidad de un producto de software (basada en los cambios que ocurren en cada versión del producto). El índice de madurez del software se calcula de la siguiente manera:

$$IMS = [M_T - (F_a + F_c + F_d)/ M_T]$$

Donde se determina la siguiente información:

$M_T$ = 4 módulos actuales

$F_a$ = 0 módulos que se han añadido

$F_c$ = 1 modulo en la versión actual que se han añadido

$F_d$ = 0 módulos en la versión anterior que se han borrado en la versión actual

La formula se la aplico consecutivamente en el sistema dando como resultado:

$M_T = 4$ $F_a = 0$ $F_c = 1$ $F_d = 0$

Reemplazando en la formula de IMS se tiene:

$$IMS = (4- (1 + 0 + 0)) / 4$$
$$IMS = 0.75$$

La estabilidad del software se acerca a 1 vemos que el producto es estable.

### 4.8.5 Portabilidad

La portabilidad del software se enfoca en tres aspectos: Hardware de la PC, Sistema Operativo y Software de la aplicación.

| | |
|---|---|
| Hardware de la PC | Pentium IV o superior<br>Velocidad 1 GHz o más<br>Memoria RAM 256 MB o más<br>Disco duro 40 GB o más |
| Sistema Operativo | Microsoft Windows:<br>Win 2000, Win 2003, Win XP |
| Software de aplicación | Visual basic 6.0 visual basic 2005 |

Por lo mencionado anteriormente el software de "Sistema de Gestión de Riesgos en Activos de Información", es portable en sus diferentes entornos tanto en hardware y software por lo tanto se puede considerar una portabilidad del 100%.

### 4.8.6 USABILIDAD

El estándar ISO 9126, puntualiza la usabilidad como "La capacidad del software de ser comprendido, aprendido, usado y de ser atractivo para el usuario, en condiciones especificas de uso".

Entre los atributos que se relacionan con el esfuerzo necesitado para el uso y en la valoración individual de tal uso por el conjunto de usuarios están los siguientes:

- Operatividad
- Comprensión
- Aprendizaje

Es dificultoso en si conocer exactamente la usabilidad que tiene una aplicación, esto por ser un atributo muy subjetivo. La aplicación de cuestionarios es una de las formas de conocer el grado de usabilidad que tiene una aplicación, estos van dirigidos al personal de la empresa que utilizaran la aplicación.

| PREGUNTA | RESPUESTAS |
|---|---|
| 1. ¿Las respuestas del sistema son las solicitadas? | 100% |
| 2. ¿Las operaciones del sistema son entendibles? | 88% |
| 3. ¿Las respuestas del sistema son rápidas? | 85% |
| 4. ¿La información que da el sistema son completas? | 100% |
| 5. ¿Se aprendió a usar el sistema con rapidez? | 90% |
| **USABILIDAD** | 93% |

**Fuente:** Elaboración Propia

# CAPITULO V

## CONCLUSIONES Y RECOMENDACIONES

# CONCLUSIONES Y RECOMENDACIONES

# CAPITULO V

## 5.1 CONCLUSIONES

Al haber concluido con el proyecto de grado se han realizado todas las actividades y los objetivos que se plantearon en un principio a las conclusiones que se llegaron son las siguientes:

- ✓ El "Sistema de Gestión de Riesgos en Activos de Información" , llego a su conclusión de forma satisfactoria, efectuándose todos los requisitos especificados en la etapa de análisis, dando lugar al cumplimiento de su objetivo principal.

- ✓ Se desarrollo el "Sistema de Gestión de riesgos en Activos de Información" el cual realiza un análisis de riesgo de forma cualitativa y cuantitativa, esto evaluando, tratando y realizando controles sobre los mismos.

- ✓ Al obtener con el producto final, el "Sistema de Gestión de Riesgos en Activos de Información" se logro construir una base de datos con toda la información para el usuario, el cual logra cumplir con uno de los objetivos específicos.

- ✓ Se puede llegar afirmar que la implementaron del presente sistema, ayudo a mejorar el desempeño de la administración de los activos de información.

- ✓ En cuanto a los mecanismos de seguridad y control del sistema se implemento un modulo de autenticación y control del ingreso de usuarios.

- ✓ De este modo se concluye que todos los objetivos indicados al inicio del proyecto han sido cumplidos en su totalidad.

## 5.2 Recomendaciones

Las recomendaciones que se logran dar a partir del manejo del sistema son:

- ✓ Se recomienda la integración del sistema con otros sistemas que maneja la empresa en el área de seguridad con el fin de centralizar la toda la información.

- ✓ Concienciar a los administradores de activos de información a emplear el uso del sistema sin prejuicios o temores.

- ✓ Concienciar a los usuarios de los activos de información sobre la importancia que tienen estos dentro de la empresa.

- ✓ Se recomienda realizar el mantenimiento preventivo como correctivo para el buen manejo del sistema.

# REFERENCIA BIBLIOGRAFICA


- [Aud2008a]: AUDITORIA de Riesgos Tecnológicos [en línea]. [Consulta: 02-mayo-2008 13:22]. Disponible en: <http://www.ey.com/global/content.nsf/South_America_S/Servicios_-_Auditoria_-_Riesgo_Tecnologico>

- [Aud2008b]: AUDITORIA de Riesgos Financieros [en línea]. [Consulta: 08-mayo-2008 14:12]. Disponible en: <http://www.ey.com/global/content.nsf/South_America_S/Servicios_-_Auditoria_-_Riesgos_financieros>

- [Mendez, 2008]: MENDEZ, Barco Andrés. Guía de Seguridad de las TIC [en línea]. [Consulta: 19-mayo-2008 20:58].

- [Evaluación, 2007]EVALUACIÓN y gestión del riesgo para Pymes [en línea]. 2007 [Consulta.06-mayo-2008]. Disponible en:<http:// www.sequ-info.com.ar>

- [Feria, 2008]: FERIA, Domínguez José Manuel. Gestión de Riesgos [en línea]. [Consulta:05-mayo-2008 21:27]. Disponible en:< http:/tecnologia\Gestión de Riesgos.htm>
- [Gestión, 2008]: GESTIÓN de riesgos en ingeniería del software [en línea]. [Consulta: 05-mayo-2008 21:27]. Disponible en: <http://www.um.es/docencia/barzana/IAGP/IAGP.html>

- [Juan, 2008]: JUAN, Fuente Aquilino Adolfo CUEVA Lovelle Juan Manuel. Proyectos de Informática [en línea]. [Consulta: 05-mayo-2008 21:23]. Disponible en: <http:/www.proyectos.v2006.c7.v2.pdf>

- [Modelo de Entidades de Magerit, 2006]: MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas [en línea]. Madrid, 2006 [Consulta: 02-mayo-2008]. Disponible en: < http://www.MAGERIT Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.htm>

- [Med, 2007]:MEDICION de riesgos tecnológicos: un enfoque practico [en línea]. En: VIII Conferencia Anual de la asociación Española de métricas de sistemas informáticos, 1 de octubre 2007[en línea]. [Consulta: 29-abril-2008]. Disponible en: <http:/www.everis_metricas_riesgos.pdf>

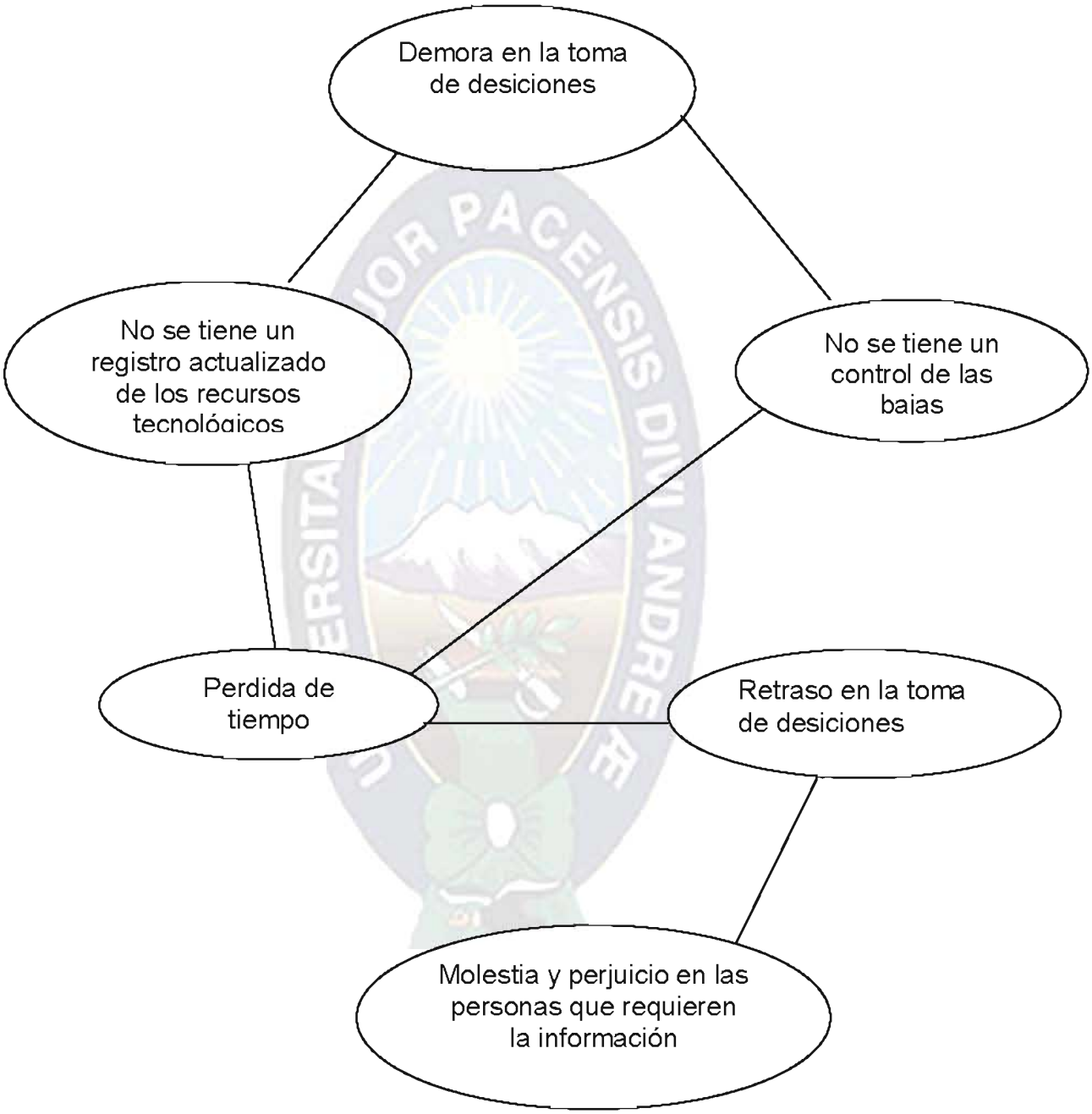
- [Serrano, 2006]: SERRANO, Jorge A. Gestión de Riesgos y la Auditoria de Sistemas [en línea]. En: Conferencia OLACEFS, Santiago de Chile junio 2006. [Consulta: 02-mayo-2008 13.33]. Disponible en: <http://www.gestion de riesgos y la auditoria de sistemas.pdf>
- [Wikilearning, 2008]: WIKILEARNING. Gestión de Riesgos en Ingeniería del Software [en línea]. [Consulta: 19-mayo-2008 20:27]. Disponible en:

<http://www.wikilearning.com/curso_gratis/gestion_de_riesgos_en_ingenieria_del_software-reduccion_supervision_y_gestion_del_riesgo/3620-13

# ANEXOS

# ANEXO A

## Árbol de problemas



# ANEXO B

# ISO 17000

## ¿Que es seguridad de la información?

La información es un recurso que, el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La seguridad de la información se define aquí como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ellas.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

## Clasificación y control de Activos

- **Responsabilidad por rendición de cuentas de los activos**
  Objetivo: mantener una adecuada protección de los activos de la organización.

  Se debe rendir cuentas por todos los recursos de información importantes y se debe designar un propietario para cada uno de ellos.
  La rendición de cuentas por los activos ayuda garantizar que se mantenga una adecuada protección.

- **Inventario de activos**

  Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos, y también pueden ser necesarios para otros propósitos de la empresa, como los relacionados con la sanidad y seguridad, seguros o finanzas (administración de recursos). El proceso de compilación de un inventario de activos es un aspecto importante de la administración de riesgos. Una organización debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la organización puede entonces, asignar niveles de protección proporcionales al valor e importancia de los activos. Se debe elaborar y mantener un inventario de activos importantes asociados a cada sistema de información. Cada activo debe de ser claramente identificado su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo (importante cuando se emprende una recuperación posterior a una perdida o daño).

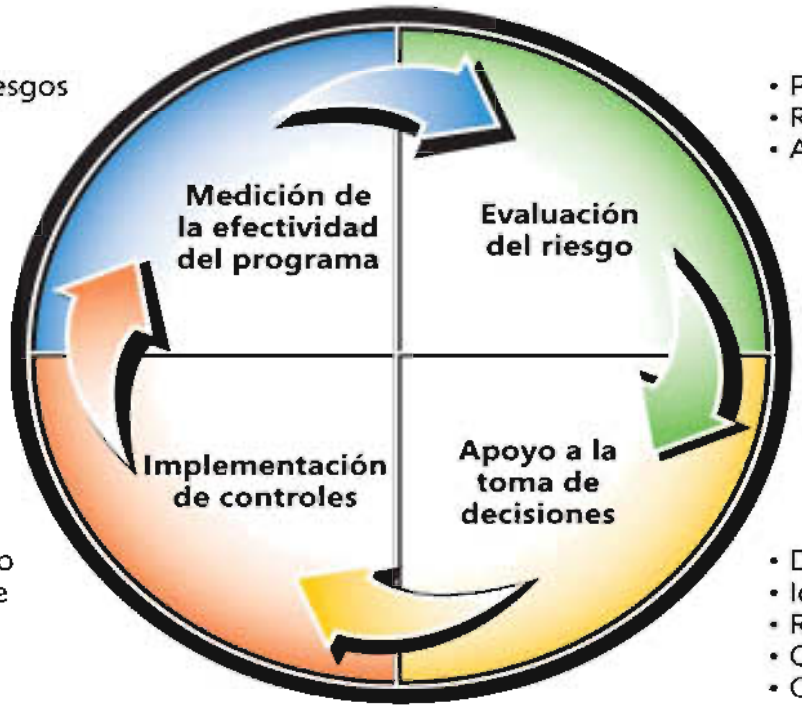
  Ejemplos de activos asociados a sistemas de información son los siguientes:

  - **Recursos de información:** base de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, dispocisiones relativas a sistemas de emergencia para la reposición de información perdida.
  - **Recursos de software:** software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
  - **Activos físicos:** equipamiento informático, equipos de comunicación, medios magnéticos, otros equipos técnicos, mobiliario, lugares de emplazamiento.
  - **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales, por ej. Calefacción, iluminación, energía eléctrica, aire acondicionado.

## ANEXO C

## PROCESO DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE MICROSOFT

- Desarrollar el cálculo de riesgos de seguridad
- Medir la efectividad del control




- Planear la recopilación de datos de riesgo
- Recopilar datos de riesgo
- Asignar prioridades a los riesgos

- Buscar un enfoque holístico
- Organizar las soluciones de control

- Definir los requisitos funcionales
- Identificar las soluciones de control
- Revisar la solución según los requisitos
- Calcular la reducción del riesgo
- Calcular el costo de la solución
- Seleccionar la estrategia de mitigación de riesgos

## ANEXO D
## GESTION DE RIESGOS MICROSOFT

En el proceso de administración de riesgos de seguridad de Microsoft se describe la fase de evaluación de riesgo como una actividad programada dentro del proceso de administración de riesgos. La fase de evaluación de riesgos define los pasos para identificar y asignar prioridades a los escenarios de riesgos conocidos para la organización. El resultado es una lista de riesgos con prioridades tanto en el nivel de resumen como en el de detalle. La evaluación de riesgos programada también proporciona los datos para las fases restantes del programa de administración de riesgos. Aunque la evaluación de riesgos programada ofrece un gran valor, los riesgos para la empresa cambian y evolucionan continuamente como una parte normal del negocio. Por lo tanto, el equipo de administración de riesgos de seguridad necesita un proceso definido para identificar y analizar los riesgos independientemente de la fase del ciclo de administración de riesgos. Esperar a que se analicen los riesgos hasta la próxima tanda programada de evaluación de riesgos no constituye una práctica lógica.

La necesidad inmediata por comprender el riesgo se puede producir en cualquier momento. Por ejemplo, puede resultar evidente que hay falta de consenso sobre el nivel de riesgo en torno a una amenaza potencial o que no se ha comprendido bien. Cuando esto sucede, los distintos participantes pueden ofrecer opiniones y soluciones de mitigación contradictorias. El equipo de administración de riesgos de seguridad tiene que documentar una posición acerca del riesgo y contribuir en el proceso de apoyo a la toma de decisiones, similar al programa de administración de riesgos formal. Es probable que se solicite al equipo de administración de riesgos de seguridad que cree requisitos funcionales para un determinado escenario que no puede, ni debe, derivarse sin comprender todos los elementos de riesgo. Esto indica que se precisa una evaluación de riesgos inmediata y ad hoc. Hay que tener precaución con las evaluaciones de riesgos que intentan realizar un uso incorrecto del proceso de evaluación de riesgos como un medio para justificar soluciones o implementaciones preconcebidas. La evaluación de riesgos debe dar como

resultado una declaración imparcial acerca de los riesgos reales asociados a un determinado problema.

En el proceso de administración de riesgos de seguridad de Microsoft se han evaluado varios escenarios de riesgos y, a continuación, se les han asignado prioridades. En la evaluación de riesgos ad hoc, los riesgos se analizan caso por caso. Una evaluación de riesgos ad hoc se centra en un solo problema de riesgo; por ejemplo, "¿cuáles son los riesgos asociados al proporcionar a los invitados de la empresa acceso inalámbrico a la red?" o "¿qué riesgos se corren al permitir que los dispositivos móviles se conecten a los recursos empresariales?". La evaluación de riesgos ad hoc utiliza la metodología descrita en el proceso; sin embargo, no es obligatorio establecer prioridades para el riesgo y la solución frente a otros riesgos de la empresa. Una asignación de prioridades formal sólo puede ser necesaria si la solución de mitigación es costosa. Con frecuencia, una comparación con riesgos similares proporciona suficiente perspectiva con el fin de establecer prioridades para la evaluación de riesgos ad hoc. Evidentemente, los resultados ad hoc se incorporarán en el proceso formal según resulte adecuado.

La plantilla de discusión de riesgos incluida en la sección Herramientas de esta guía también se puede utilizar para las evaluaciones de riesgos ad hoc. No obstante, es posible que la recopilación de datos sólo requiera investigación en vez de una reunión de los participantes. El equipo de administración de riesgos de seguridad tiene que responder a las preguntas clave de la plantilla, pero las respuestas se pueden hallar en el propio equipo. Por ejemplo, si el equipo intenta comprender los riesgos asociados a los dispositivos móviles, la investigación de la frecuencia de pérdida de dispositivos puede constituir una información necesaria. Esta información también se puede obtener mediante una investigación externa o a través de los equipos de TI responsables del área de servicio.

La evaluación de riesgos ad hoc se puede comunicar en un documento estructurado con las siguientes secciones:

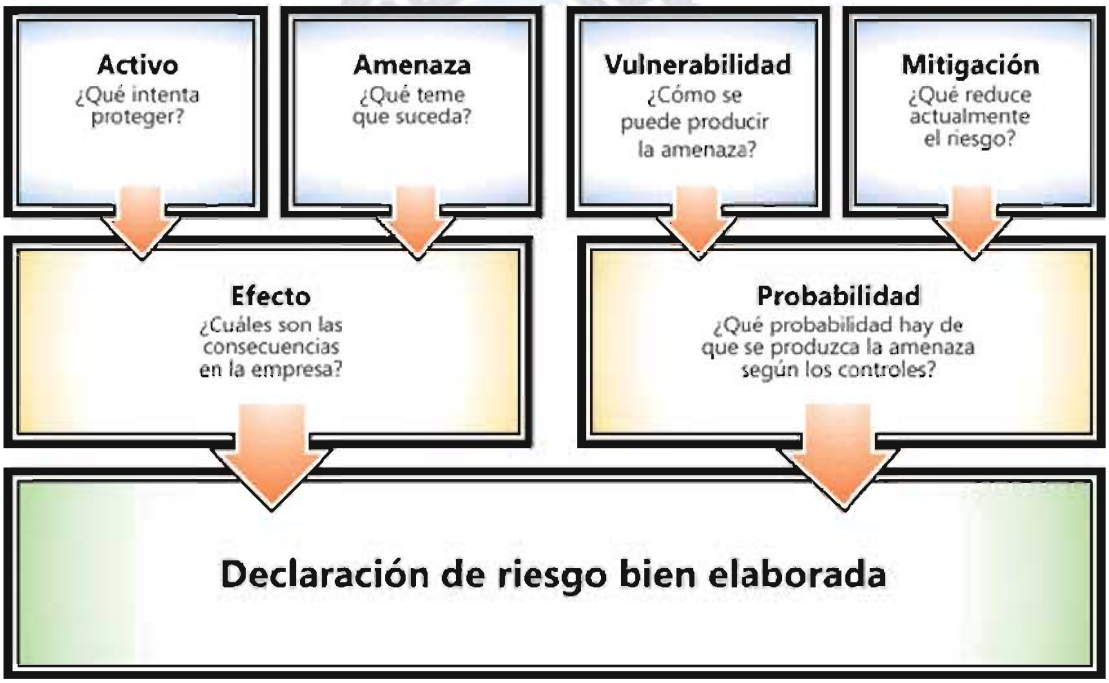
- Resumen ejecutivo. Este resumen debe incluir toda la evaluación y se debe poder extraer de la evaluación de riesgos como un documento independiente.
- Lista de supuestos relativos al alcance y los objetivos de la evaluación de riesgos ad hoc.
- Una descripción del activo que se protegerá y su valor para la empresa.
- Una declaración adecuada, según lo descrito en el proceso de administración de riesgos de seguridad de Microsoft, que responda a las siguientes preguntas:

    - ¿Qué se desea evitar que le suceda al activo?
    - ¿Cómo se puede producir la pérdida o exposición?
    - ¿Cuál es el alcance de la exposición potencial para el activo?
    - ¿Qué se está haciendo en la actualidad para minimizar la probabilidad de que se produzca el riesgo o para reducir el impacto si fallan las medidas de protección?
    - ¿Cuál es el riesgo global? Incluya una afirmación como "Hay una alta probabilidad de que el ataque consiga poner en peligro la integridad de los activos digitales de valor medio, lo que representa un riesgo alto para la organización".
    - ¿Cuáles son las acciones que podrían reducir la probabilidad en el futuro?
    - ¿Cuál es el riesgo global si se implementan los controles posibles?

Una sola evaluación de riesgos puede contener varios escenarios de amenaza. En el ejemplo de una solución de acceso inalámbrico para invitados, un escenario puede ser el riesgo de que un invitado ataque a otro; un segundo escenario puede ser un ataque externo a uno de los invitados; un tercer escenario puede ser un invitado que haga un uso incorrecto del acceso para realizar un ataque a través de Internet. Debe desarrollar una declaración de riesgo para todos los escenarios aplicables.

Cuando se comprenden los riesgos, puede ser suficiente con comunicarlos. También es posible que el resultado deseado sea una declaración de los requisitos funcionales del equipo de administración de riesgos de seguridad. Si se generan requisitos funcionales, se deben asignar a los riesgos específicos a los que se dirigen. Un documento de evaluación de riesgos con requisitos de seguridad funcionales constituye una herramienta eficaz para que la empresa comprenda el riesgo y decida la mejor solución de mitigación.

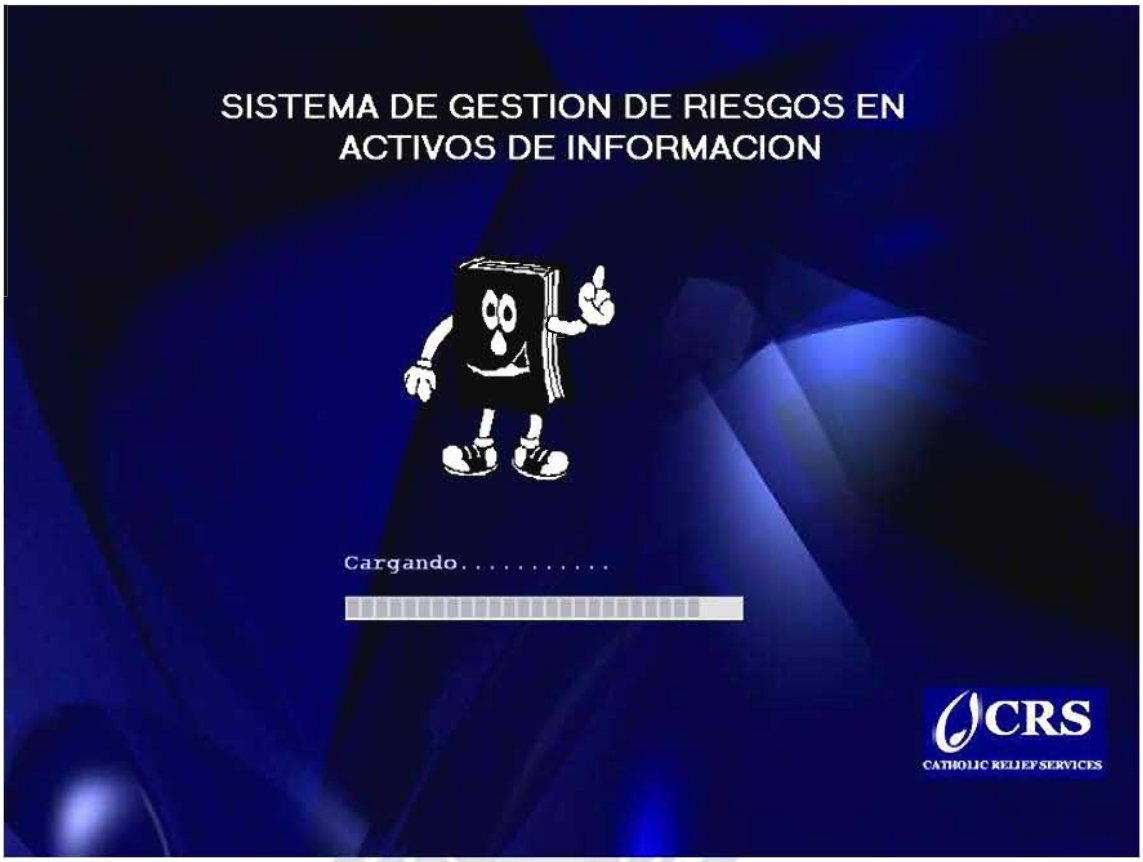
## COMPONENTES DE LA DECLARACIÓN DE RIESGO BIEN ELABORADA



# ANEXO E

# PANTALLAS DE LA INTERFAZ DEL USUARIO

**Figura A.1** Pantalla de Bienvenida al sistema




**Fuente:** Elaboración Propia

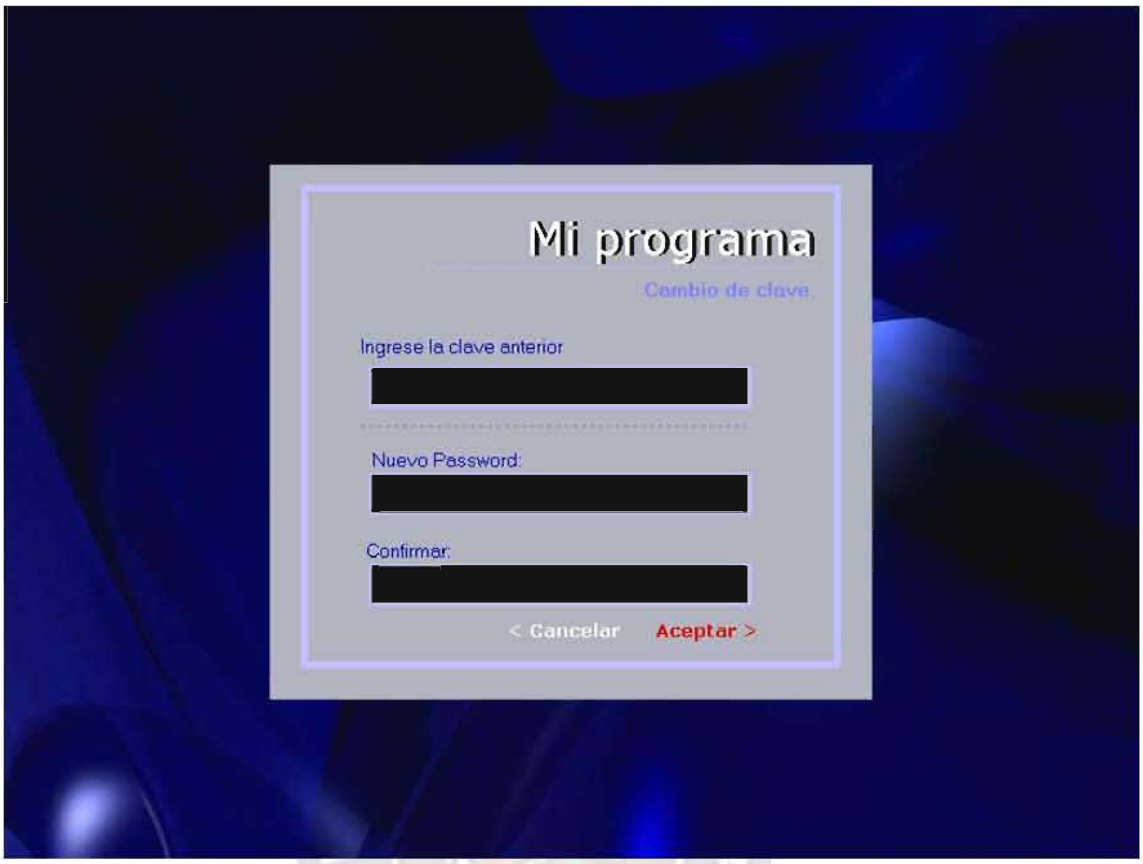
**Figura A.2** Pantalla de acceso al sistema


La pantalla de la figura A.2 muestra la pagina de acceso al Sistema de Gestión de Riesgos en activos de información, en la que el usuario de be ingresar su password. Si presionamos la opción cambiar password nos muestra la siguiente pantalla.

La pantalla A.2 muestra la pagina principal del sistema

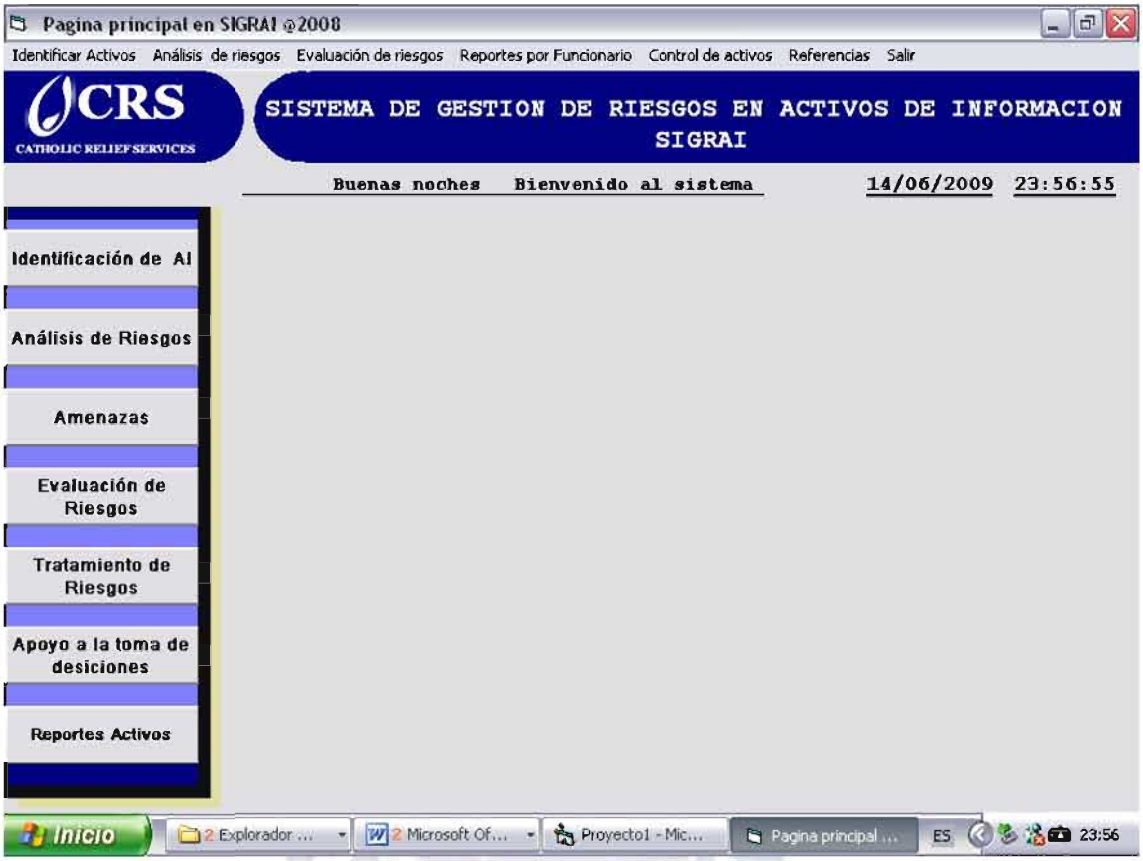
**Fuente:** Elaboración Propia

**Figura A.3** Pantalla de cambio de password



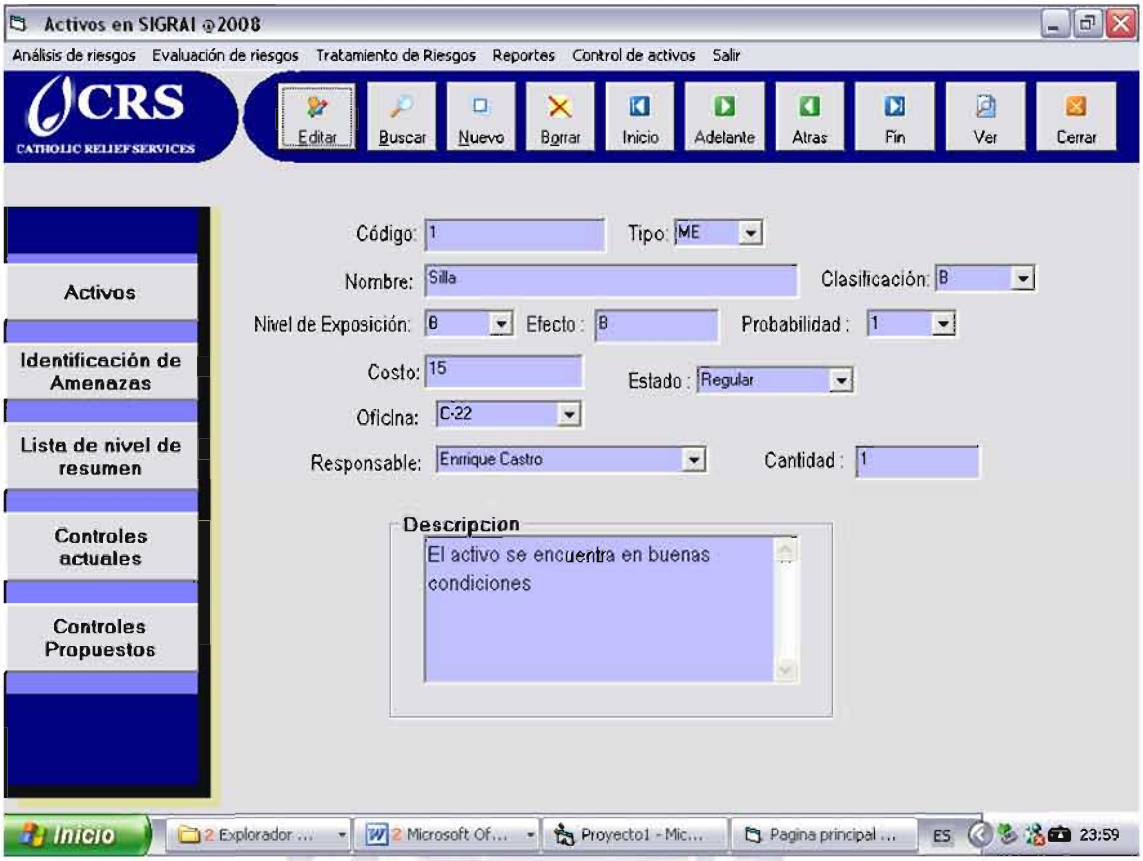

**Fuente:** Elaboración Propia

**Figura A.4** Pantalla principal del sistema



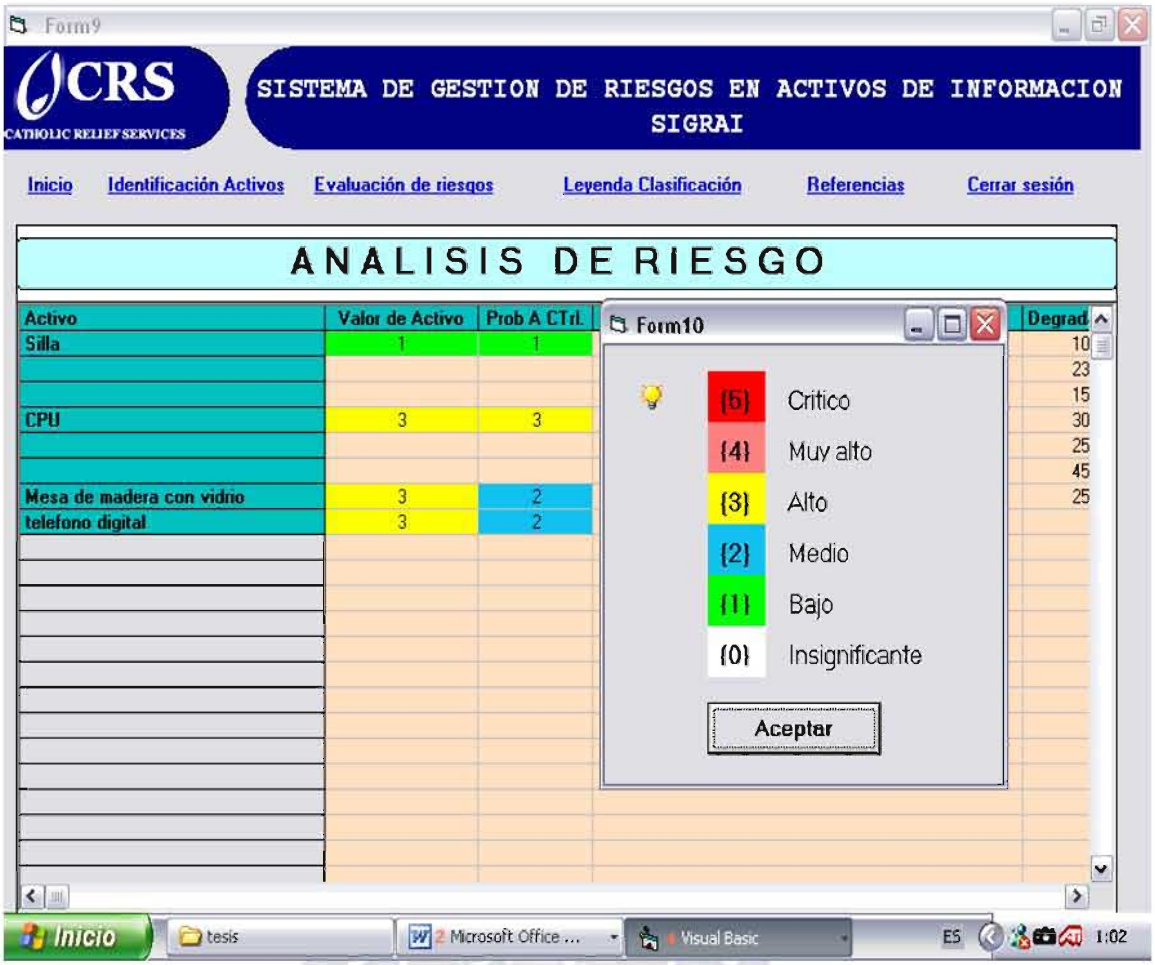

**Fuente:** Elaboración Propia

**Figura A.5** Pantalla de identificación de activos




**Fuente:** Elaboración Propia

**Figura A.6** Pantalla Análisis de riesgos

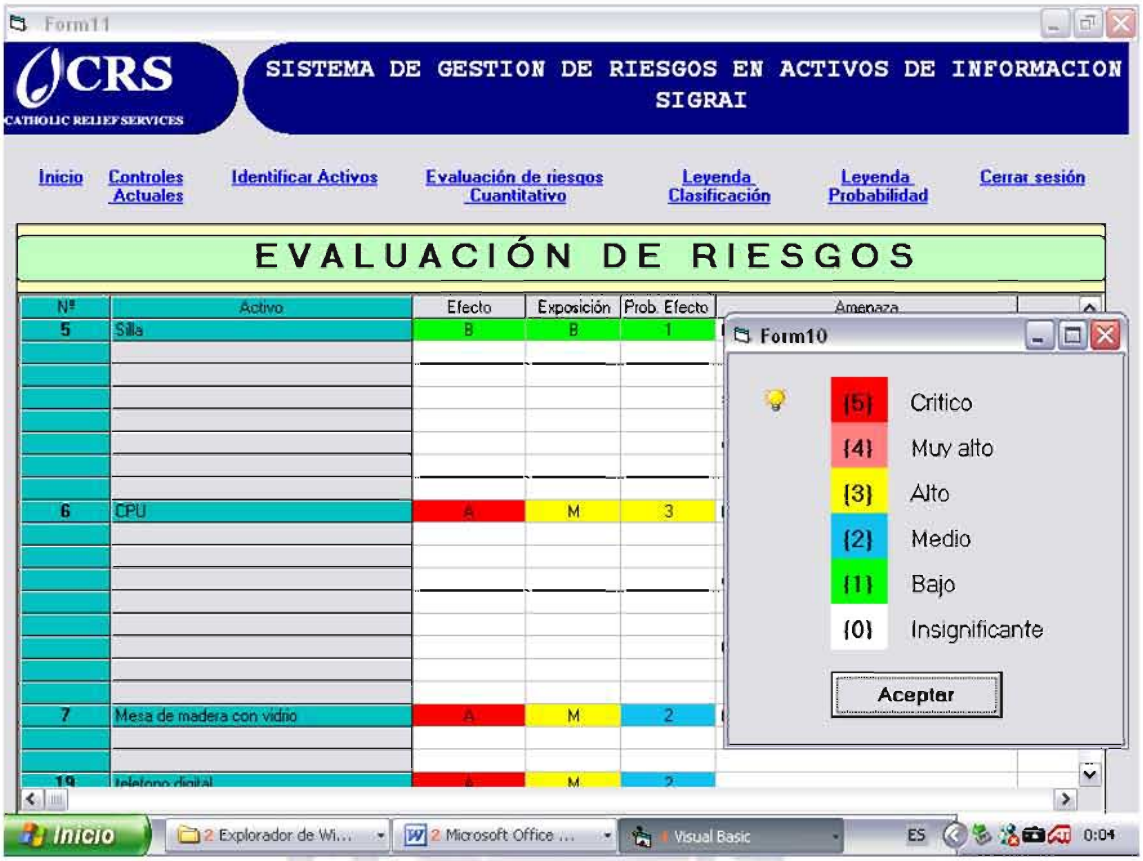



**Fuente:** Elaboración propia

**Figura A.7** Figura fuentes de amenazas

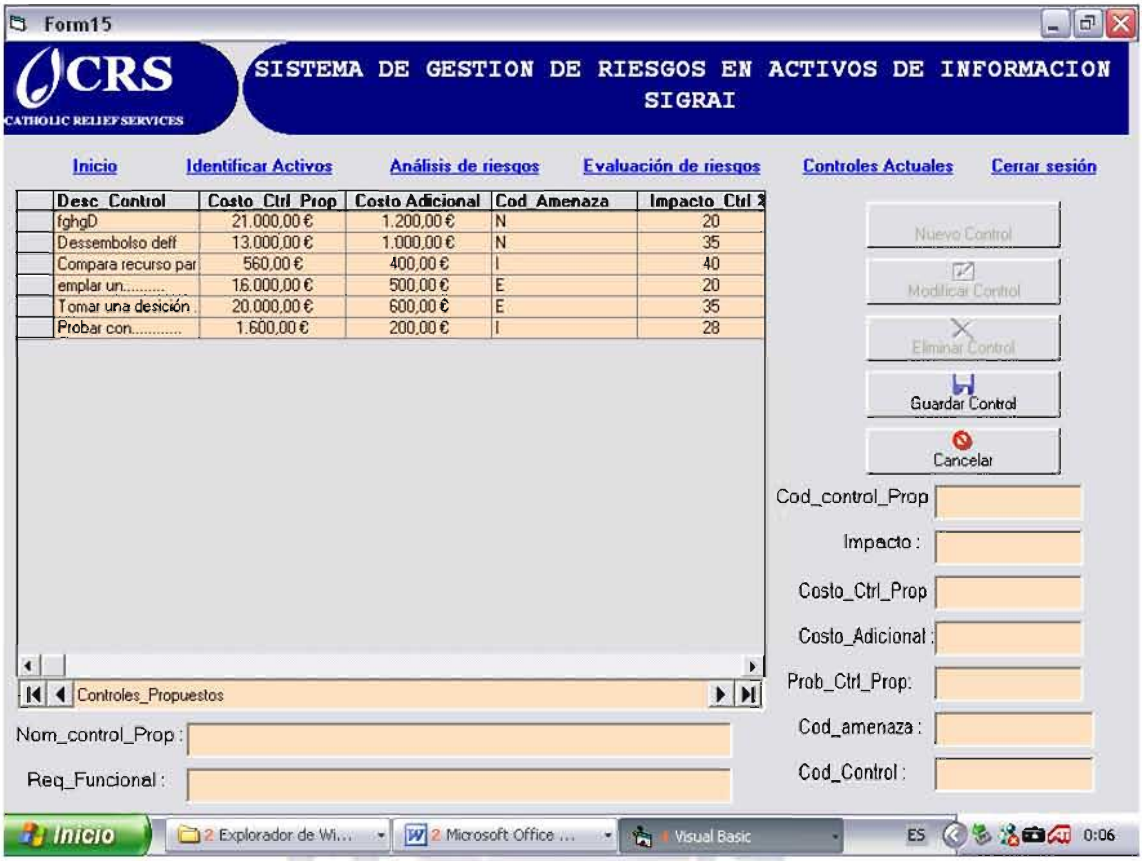

**Fuente:** Elaboración Propia

**Figura A.8** Pantalla Evaluación de riesgos




**Fuente:** Elaboración Propia

**Figura A.9** Pantalla controles propuestos




**Fuente:** Elaboración Propia

**Figura A.10** Pantalla Generación de Reportes


**Fuente:** Elaboración Propia