UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERÍA
MAESTRÍA EN SISTEMAS DE INFORMACIÓN

PROYECTO DE TRABAJO DE GRADO DE MAESTRÍA

MODELO DE MADUREZ PARA LA CALIFICACIÓN Y CUANTIFICACIÓN DEL RIESGO TECNOLÓGICO EN LAS INSTITUCIONES BANCARIAS DE VENEZUELA

PRESENTADO POR
LIC. ANYELIN Y. CALDERON S.
PARA OPTAR AL TÍTULO DE
MAGÍSTER EN SISTEMAS DE INFORMACIÓN

TUTORA:
ING. LOURDES ORTIZ
ASESORA:
LIC. NELLY LUGO

CARACAS, JULIO DE 2011

CARACAS, 18 DE JULIO DE 2011

UNIVERSIDAD CATÓLICA ANDRES BELLO
POSTGRADO EN SISTEMAS DE INFORMACIÓN
LIC. MARIA ESTHER REMEDIOS
PRESENTE.-

CARTA DE APROBACIÓN

Por la presente me permito comunicar que he sido el tutor del Trabajo de Grado de Maestría del estudiante Anyelin Y. Calderon Sequera, cédula de identidad Nro. 13.533.130, quien opta por el título de Magíster en Sistemas de Información, titulado "Modelo de Madurez para la Calificación y Cuantificación del Riesgo Tecnológico en las Instituciones Bancarias de Venezuela".

Asimismo, hago constar que como tutora estoy conforme con el contenido presentado, por lo que cuenta con mi aprobación para ser inscrito como Trabajo de Grado de Maestría.

Sin otro particular al cual hacer referencia, se despide cordialmente,

Ing. Lourdes Ortiz S.
C.I. V-6.976.288

" Que de mis ideales
y experiencias positivas
reciban vida, la familia
y la sociedad,
ellas no solo creen en ti
sino que creen también en mi
como lo haces Tú. "

Gracias Dios porque eres en mí,
Presencia de Vida Perpetua.

Anyelin

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERÍA
MAESTRÍA EN SISTEMAS DE INFORMACIÓN

TRABAJO DE GRADO DE MAESTRÍA

MODELO DE MADUREZ PARA LA CALIFICACIÓN Y CUANTIFICACIÓN DEL RIESGO TECNOLÓGICO EN LAS INSTITUCIONES BANCARIAS DE VENEZUELA

AUTORA: LIC. ANYELIN CALDERÓN
TUTORA: ING. LOURDES ORTIZ
ASESORA: LIC. NELLY LUGO
FECHA: JULIO 2011

RESUMEN

La gestión de riesgos no es algo nuevo, siempre ha sido una parte importante del esfuerzo de los entes reguladores y entidades financieras para evitar el fraude, mantener la integridad de los controles internos y reducir los errores en las operaciones. La presente investigación pretende formular un modelo de madurez apoyado en las metodologías de riesgo y el modelo de madurez CMMI que permita a la Superintendencia de las Instituciones del Sector Bancario la calificación y cuantificación de los riesgos tecnológicos detectados en la supervisión de los entes bajo su regulación, vigilancia y fiscalización; con el objeto de contribuir al buen funcionamiento del sistema bancario nacional. Para su desarrollo se toman como base las mejores prácticas y metodologías en materia de riesgo tecnológico. Este proyecto se enmarca en la modalidad de proyecto factible, con un tipo de investigación de campo y documental. El desarrollo del proyecto consta de las actividades de diagnostico del proceso actual de inspección, investigación documental, formulación del modelo y desarrollo del prototipo.

PALABRAS CLAVE

Riesgo tecnológico, Basilea II, Superintendencia de las Instituciones del Sector Bancario, CMMI. Línea de Investigación Ingeniería de Software, Área de Conocimiento Riesgo Tecnológico.

ÍNDICE GENERAL

Índice General v

Índice de Figuras viii

Índice de Tablas ix

Introducción 1

CAPÍTULO I Planteamiento del Proyecto 4

I.1. Contextualización y Delimitación del Problema 4
I.2. Objetivo General 9
I.3. Objetivos Específicos 9
I.4. Justificación e Importancia de la Investigación 9

CAPÍTULO II Marco Referencial 13

II.1. Antecedentes Históricos de la Sudeban 13
II.2. Concepto 14
II.3. Funciones 14
II.4. Misión 15
II.5. Visión 15
II.6. Mecanismo de Fiscalización y Control 15
II.7. Definición de Modelo 16
II.8. El Modelo de Capacidad y Madurez (CMMI) 17
II.9. Concepto y Principios de CMMI 18
II.10. Niveles de Capacidad 18
II.11. Niveles de Madurez 19
II.12. Representaciones Continua y Escalonada 19
II.13. Áreas de proceso 20
II.14. Estructura del modelo CMMI 20
II.15. Componentes 21
II.16. Productos Típicos 22
II.17. Definición General de Riesgo 23
II.18. Análisis de riesgos 25
II.19. Gestión del Riesgo 25
II.20. Tipo de Riesgo Operacional 26
II.21. Tipo de Riesgo Tecnológico 27
II.22. Fuentes de Riesgo Operativo 27
II.23. ISO TR 13335 Lineamientos para la administración de la seguridad 29
II.24. ISO/IEC 27005:2008 Tecnologías de la información – Técnicas de seguridad – Gestión del Riesgo de Seguridad de la Información. 31
II.25. UNE 71504:2008 Metodología de Análisis y Gestión de Riesgos para los Sistemas de Información 34
II.26. BS 7799-3:2006 Sistemas de Gestión de Seguridad de la Información – Parte 3: Guías para la Gestión de Riesgos de Seguridad de la Información 35
II.27. AS/NZS 4360:2004 Gestión de riesgos 36

II.28. MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información 38
II.29. OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation 39
II.30. CRAMM – CCTA Risk Analysis and Management Method 42
II.31. NIST SP 800-30 Guía de gestión de riesgos para sistemas de tecnología de la información 45
II.32. IRAM – Information Risk Analysis Methodologies 47
II.33. SOMAP – Security Officers Management and Analysis Project 48
II.34. Otros tipos de análisis de riesgo 50
a. Basilea, Comité de Supervisión Bancaria (BCBS) 50
b. Basilea II 51
c. Informe COSO 54
d. COBIT (Objetivos de Control para Tecnología de Información y Tecnologías Afines) 56
II.35. Otras metodologías 59
II.36. Generalidades de las Metodologías de Análisis y Gestión de Riesgos. 60
II.37. Elementos Comunes 60
II.38. Pérdida esperada (Single Loss Expectancy – SLE) 61
II.39. Pérdida anual esperada (Annual Loss Expectancy – ALE) 62
II.40. Cálculo del efecto de las salvaguardas 62
II.41. Relaciones entre los Activos 63
II.42. Métodos Cualitativos 65
II.43. Métodos mixtos 68
II.44. Dimensiones de las Metodologías de Análisis y Gestión de Riesgo 69

CAPÍTULO III Marco Metodológico 74

III.1. Modalidad, Diseño y Tipo de Investigación 74
III.2. Población y Muestra 75
III.3. Definición de las Variables 76
III.4. Técnicas e Instrumentos para la Recolección de Datos 79
III.5. Validez y Confiabilidad del Instrumento 79
III.6. Procedimientos 79

CAPÍTULO IV Desarrollo del Proyecto 82

IV.1. Fase I: Diagnóstico del proceso actual de inspección 82
IV.2. Fase II: Investigación Documental 82
IV.3. Fase III: Formulación del modelo de Riesgo Tecnológico 83
IV.4. Definición de los Requerimientos 83
IV.5. Desarrollo de la Metodología del Modelo de Analisis de Riesgo 85
IV.6. Fase de Planificación 86
a. Actividad A1.1: Determinación del Alcance 86
b. Actividad A1.2: Planificación de la Inspección 87
c. Actividad A1.3: Inicio de la Inspección 88
IV.7. Fase de Aplicación del Análisis de Riesgo 89
a. Actividad A.2.1: Caracterización de los Activos 90
b. Actividad A.2.2: Caracterización de las Amenazas 93
c. Actividad A.2.3: Identificación de Controles 97

d. Actividad A.2.4: Aplicación de la pruebas 100
e. Cálculo del riesgo intrínseco 101
f. Calculo del riesgo efectivo 101
g. Actividad A.2.5: Estimación del Estado del Riesgo 101
h. Actividad A.2.6: Instrucciones 103
IV.8. Desarrollo de Inventarios 103
IV.9. Fase IV: Desarrollo del Prototipo 105
a. Metodología a Utilizar 105
b. Análisis y Especificación del Prototipo 107
c. Actores 108
d. Casos de Uso 109
e. Definición del Esquema Lógico de Datos 110
f. Definición de las Interfaces 111

CAPÍTULO V Conclusiones y Recomendaciones 130

Referencias Bibliográficas 122

Anexo I Áreas de Dominio 125

Anexo II Dimensiones de Seguridad 126

Anexo III Criterios de Valoración 130

Anexo IV Tipos de Activos 132

Anexo V Inventario de Amenazas 136

Anexo VI Inventario de Controles 156

Anexo VII Descripción de Casos de Uso 159

ÍNDICE DE FIGURAS

Figura 1: Mapa de Riesgos 7
Figura 2: Mapa Conceptual del Marco Referencial 12
Figura 3: Representaciones de CMMIM 19
Figura 4: Representación Continúa de CMMI 20
Figura 5: Representación Escalonada de CMMI 21
Figura 6: Procesos de Gestión de Seguridad de la Información (Fuente: ISO/IEC 13335) 30
Figura 7: Proceso de Análisis Detallado de Riesgos (Fuente: ISO/IEC 13335) 31
Figura 8: Proceso de Gestión de riesgos de seguridad de la información de ISO/IEC 27005:2008 33
Figura 9: Modelo UNE 71504 34
Figura 10: Modelo de Procesos de Gestión de Riesgos de BS 7799-3 36
Figura 11: Proceso de Gestión de Riesgos de AS/NZS 4360:2004 37
Figura 12: Modelo MAGERIT 39
Figura 13: Fases del Proceso OCTAVE 41
Figura 14: Modelo de Análisis y Gestión de Riesgos de CRAMM 43
Figura 15: Fases de CRAMM 44
Figura 16: Principales Actividades de Análisis y Gestión CRAMM 44
Figura 17: Proceso de Análisis de Riesgos de NIST SP 800-30 45
Figura 18: Proceso de Gestión de Riesgos de NIST SP 800-30 46
Figura 19: Modelo de Datos de SOMAP (ORIMOR) 49
Figura 20: Estructura de los Componentes de COBIT 58
Figura 21: Fases y Actividades del Proyecto 80
Figura 22: Diagrama del Modelo 85
Figura 23: Valoración de la eficacia de los controles 98
Figura 24: Etapas del Modelo de Prototipado 106
Figura 25: Esquema Lógico de Datos, Modulo de Inventario 110
Figura 26: Esquema Lógico de Datos, Modulo de Activos 110
Figura 27: Esquema Lógico de Datos, Modulo de Valoración 111
Figura 28: Prototipo - Inicio de Sesión 111
Figura 29: Prototipo - Menú Principal 112
Figura 30: Prototipo - Control de Inspecciones 113
Figura 31: Prototipo - Inventario de Tipos de Activos 114
Figura 32: Prototipo - Inventario de Áreas de Dominio 114
Figura 33: Prototipo - Inventario de Amenazas 115
Figura 34: Prototipo - Caracterización de Activos 115
Figura 35: Prototipo - Generación de Informes 116
Figura 36: Descripción de Amenaza (Fuente Magerit - (López F., 2006)) 136

ÍNDICE DE TABLAS

Tabla 1: Matriz de Riesgo 7
Tabla 2: Algunas Áreas de Proceso de CMMI 20
Tabla 3: Procesos de las Metodologías OCTAVE (Fuente Propia)..... 42
Tabla 4: Cálculo Cualitativo del Impacto 67
Tabla 5: Cálculo Cualitativo del Riesgo 67
Tabla 6: Cálculo Cualitativo Mediante la Función Mínimo..... 68
Tabla 7: Cálculo cualitativo Mediante la Función Máximo 68
Tabla 8: Cálculo Cualitativo Mediante la Función Media..... 68
Tabla 9: Principales Metodologías por Tipo de Análisis de Riesgos..... 69
Tabla 10: Origen y Tipo de Análisis de las Metodologías de Análisis y Gestión de Riesgos 70
Tabla 11: Metodologías de Análisis y Gestión de Riesgos por Inventario y Tipos de Riesgo 71
Tabla 12: Metodologías de Análisis y Gestión de Riesgos por Elementos del Modelo 72
Tabla 13: Metodologías de Análisis y Gestión de Riesgos por Objetivos de Seguridad 72
Tabla 14: Clasificación por Cargo GRT..... 75
Tabla 15: Definición de Variables 78
Tabla 16: Áreas de Dominio del Modelo..... 125
Tabla 17: Dimensiones de Seguridad 126
Tabla 18: Criterios de Valoración de Activos 129
Tabla 19: Tabla de Valoración y Criterio de los Activos.....130
Tabla 20: Tipos de Activos 135
Tabla 21: Inventario de Amenazas 152
Tabla 22: Amenazas por Activos de Servicio 152
Tabla 23: Amenazas por Activos de Datos / Información ... .153
Tabla 24: Amenazas por Activos de Aplicaciones ... .153
Tabla 25: Amenazas por Activos de Equipos informáticos 154
Tabla 26: Amenazas por Activos de Redes de Comunicación 154
Tabla 27: Amenazas por Activos de Soportes de Información 155
Tabla 28: Amenazas por Activos de Equipamiento Auxiliar 155
Tabla 29: Amenazas por Activos de Instalaciones.....155
Tabla 30: Amenazas por Activos de Personal 155
Tabla 31: Inventario de Controles 158

INTRODUCCIÓN

La globalización de los servicios financieros, las fusiones, adquisiciones y consolidaciones, junto con la creciente sofisticación de la tecnología financiera están haciendo las actividades bancarias, y en consecuencia, sus perfiles de riesgo, cada vez más complejas. Esto aunado al acelerado crecimiento de la tecnología en los últimos años han generado un creciente número de oportunidades y amenazas.

Un alto nivel de inversión en tecnología, tal cual existe hoy día, produce un efecto multiplicador importante en caso que dichas amenazas se materialicen, dado que las pérdidas posibles se ven incrementadas en igual proporción al aumento de la inversión.

La gestión de riesgos no es algo nuevo, siempre ha sido una parte importante del esfuerzo de los entes reguladores y entidades financieras para evitar el fraude, mantener la integridad de los controles internos y reducir los errores en las operaciones. La presente investigación pretende formular un modelo de madurez apoyado en CMMI, que permita a la Superintendencia de las Instituciones del Sector Bancario la calificación y cuantificación de los riesgos tecnológicos detectados en la supervisión realizada a las instituciones bancarias de Venezuela; con el objeto de contribuir al buen funcionamiento del sistema bancario nacional. Para su desarrollo se consideran las mejores prácticas en materia de riesgo tecnológico considerando para ello Basilea II, COBIT, COSO y otras normativas y documentos descritos en el presente trabajo.

Este documento se enmarca en la modalidad de proyecto factible, con un tipo de investigación de campo y documental. El mismo ha sido dividido en cinco (5) capítulos y siete (7) anexos los cuales se describen a continuación:

Capítulo I: se plantea la problemática de manera descriptiva ubicando la situación objeto de estudio en un contexto que permite comprender su origen y relaciones, se precisa el conjunto de objetivos que orientan las líneas de acción y los límites de estas y se expone la justificación e importancia de la investigación.

Capítulo II: comprende el marco teórico conceptual el cual incluye, el marco organizacional y la definición de términos básicos que serán usados a lo largo del proyecto.

Capítulo III: presenta una descripción del marco metodológico, incluye el tipo o tipos de investigación, las técnicas y los procedimientos que serán utilizados para llevar a cabo el proyecto.

Capítulo IV: en este capítulo se encuentra el desarrollo del proyecto y el desglose de cada una de las fases del mismo, tales como, diagnostico del proceso actual de inspección, investigación documental, formulación del modelo y desarrollo del prototipo.

Capítulo V: muestra las conclusiones y recomendaciones, enunciando los puntos más relevantes del proyecto y realizando sugerencias para trabajos futuros.

Anexo I Áreas de Dominio: listado y descripción de las áreas de negocio incluidas en las inspecciones realizadas a las entidades financieras.

Anexo II Dimensiones de Seguridad: listado de las dimensiones de seguridad que son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas.

Anexo III Criterios de Valoración: valores establecidos para la calificación de los activos y riesgos.

Anexo IV Tipos de Activos: listado de los tipos de activos incluidos en el inventario base de la metodología de análisis de riesgo

Anexo V Inventario de Amenazas: listado de las posibles amenazas que se les pueden presentar a los activos de información.

Anexo VI Inventario de Controles: inventario de controles aplicados a los diversos procesos u activos de información.

Anexo VII Descripción de Casos de Uso: descripción de los casos de usos para la implementación del prototipo.

Capítulo I

Planteamiento del Proyecto

"Los problemas no surgen, no son impersonalmente dados al investigador: sino que el científico individual, con su acervo de conocimiento, su curiosidad, su visión y sus tendencias, registra el problema o incluso lo busca"

Mirian Balestrini Acuña

CAPÍTULO I

PLANTEAMIENTO DEL PROYECTO

En este capítulo se plantea la problemática de manera descriptiva ubicando la situación objeto de estudio en un contexto que permite comprender su origen y relaciones, se precisa el conjunto de objetivos que orientan las líneas de acción y los límites de estas y se expone la justificación e importancia de la investigación.

I.1. CONTEXTUALIZACIÓN Y DELIMITACIÓN DEL PROBLEMA

La Gerencia de Riesgo Tecnológico (en lo sucesivo se denominará GRT), tiene como objetivo establecer las directrices necesarias para que los sujetos sometidos a la supervisión de la Superintendencia de las Instituciones del Sector Bancario[1] implementen un adecuado sistema de control interno asociado al uso de la Tecnología de la Información, así como, en la prestación de servicios financieros automatizados, electrónicos y manejados a través del uso de equipos y sistemas computacionales con el objetivo de mitigar los riesgos existentes en el negocio bancario, asegurando la confiabilidad, integridad y disponibilidad de la información de los usuarios del Sistema Bancario Nacional.

En este sentido, la GRT efectúa visitas de inspección "in-situ" a las instituciones, apoyándose inicialmente en un levantamiento de información para determinar el ambiente de control interno existente, esto es conocer la estructura, los equipos, las aplicaciones, el esquema de telecomunicaciones y los mecanismos de seguridad instalados en estas instituciones financieras. Cabe destacar que la citada información es obtenida de los "cuestionarios de tecnología de la información". En este instrumento se obtiene datos de once (11) áreas de control entre las que se mencionan: planeación y estrategia de los recursos de información, operación de los sistemas de información, proveedores externos, seguridad de la información, continuidad del negocio,

---

[1] Superintendencia de las Instituciones del Sector Bancario en lo sucesivo Sudeban, es un organismo autónomo, de carácter técnico y especializado, con personalidad jurídica y patrimonio propio e independiente del Fisco Nacional que tiene como función principal supervisar, controlar y vigilar las instituciones financieras establecido en la Ley General de Bancos y Otras Instituciones Financieras.

mantenimiento e implantación de los sistemas, bases de datos, soporte a la red, hardware, software y banca electrónica.

Una vez analizada la información de los cuestionarios o los papeles de trabajo de las inspecciones anteriores, los auditores del área de GRT proceden a realizar la planificación de la visita in-situ a la entidad financiera, con el fin de realizar el diagnostico y análisis de riesgos.

El auditor una vez en las instalaciones de los bancos, enfoca su trabajo en la evaluación de los controles internos aplicados en las áreas mencionadas anteriormente, también se orienta en obtener evidencias que avalen la inexistencia de la calidad de los sistemas de información empleados por el bancos para identificar, evaluar, monitorear, controlar y mitigar el riesgo tecnológico que es uno de los componentes principales del riesgo operacional, el cual se define como "riesgo de pérdidas debido a fallas o inadecuados procesos, personal y sistemas internos o bien a causa de acontecimientos externos[2]".

En el citado son revisados aspectos como:

- La infraestructura tecnológica que soporta las operaciones de un banco, así como su mantenimiento,
- las políticas y procedimientos establecidos para el manejo de las relaciones con proveedores, incluyendo los contratos, acuerdos y niveles de servicios;
- la estructura organizacional y funcional de la unidad de tecnología y su interrelación con el resto del Banco;
- la alineación de la tecnología con la estrategia del negocio, planes de contingencia y continuidad de negocios que involucran la infraestructura de tecnología (sistemas, aplicaciones, computadores, comunicación), las pruebas de estos planes y su efectiva retroalimentación;

---

[2] Definición extraída del documento: "Practicas sanas para la Administración y Supervisión del Riesgo Operacional" del Comité de Basilea (Febrero de 2003).

- los procesos para la gestión de calidad de los datos, los cuales involucran controles internos que se establecen desde las aplicaciones o sistemas, cuando nacen o se generan los datos y la estructura que los contienen (bases de datos, archivos);
- los aspectos de seguridad física, seguridad lógica y de redes, las políticas y procedimientos para esta gestión, así como, el perfil del personal que maneja los citados procesos. En cuanto a la seguridad física, se hace mayor énfasis en las características y adecuaciones de las instalaciones donde se encuentra la plataforma tecnológica o centros de procesamiento de datos principales o contingentes,
- la administración del riesgo tecnológico el cual demanda el establecimiento de políticas, procesos y procedimientos para la evaluación de la infraestructura, los sistemas o aplicaciones que atienden las operaciones del banco;
- la supervisión de la banca electrónica la cual está determinada por los canales electrónicos a través de los cuales el Banco brinda el servicio a sus clientes.

Para una evaluación eficiente de los controles internos, los auditores se apoyan en programas de trabajos de elaboración propia los cuales están basados en las mejores prácticas existentes tales como: los Objetivos de Control para tecnología de información y tecnologías afines (COBIT), Control Interno Informe COSO, Basilea II, la Organización de Estándares Internacionales (ISO) y en la "Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras."

El proceso de visita "in-situ", culmina una vez que se han evaluado los controles internos correspondientes a cada área y recolectado las evidencias que soportan los hallazgos encontrados.

Finalmente, los riesgos y controles identificados en la inspección son analizados y plasmados en una matriz de riesgo, podemos observar el formato de la matriz en la tabla 1.

AREA DE CONTINUIDAD DEL NEGOCIO				
NO.	RIESGO(S) IMPACTO(S)	CONTROL(ES) EXISTENTE(S)	PRUEBA (S) /OBSERVACIÓN(ES)	INSTRUCCIÓN (ES)/ RECOMENDACIÓN (ES)
01	**Riesgo:** Posibilidad de paralización parcial o total de las operaciones en caso de presentarse fallas, inconvenientes o eventualidades que cause interrupción en los sistemas de información. Calificación del Riesgo: Alto **Impacto(s):** . Pérdida de información crítica del negocio afectando la continuidad de las operaciones financieras y bancarias.	Existencia del documento denominado Plan de Contingencias del Centro de Cómputo. Diseño: Preventivo Tipo: Manual / Automático Frecuencia: Eventual	**Prueba:** Se revisó el contenido del documento denominado "Plan de Contingencias del Centro de Cómputo", a fin de validar su uso y aplicabilidad. **Observaciones:** . El documento "Plan de Contingencias Tecnológicas", se encuentra desactualizado, debido a que el mismo hace referencia al documento "Plan de Tecnológica", el cual está en desuso.	7.7 Adecuar el "Plan de Contingencias del Centro de Cómputo" a la actual infraestructura tecnológica, recursos y procedimientos establecidos por la...Institución Financiera. 7.8 Garantizar que la totalidad de las transacciones puedan ser restauradas y/o recuperadas en un tiempo oportuno en caso de ocurrir una contingencia mayor.

Tabla 1: Matriz de Riesgo

Una vez, culminado las matrices, incorporando identificación de impactos e instrucciones, se enumeran los riesgos (Ver Figura 1) y se procede a construir el mapa de riesgos, que consiste en una combinación de medición y priorización del riesgo y en la graficación de los mismos en un plano cartesiano, donde (Ver figura 2):

- el eje X representa la probabilidad de ocurrencia y,
- el eje Y el impacto que tendría el riesgo identificado sobre el negocio bancario.

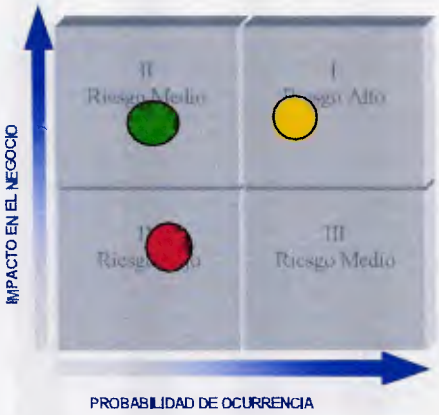


Figura 1: Mapa de Riesgos

Por otra parte, en la calificación del riesgo se emplean (rojo = alto, amarillo = medio, verde=bajo) y la incorporación en los cuadrantes (ver círculos figura 2) es realizada en función de la experiencia de los auditores, así como, de sus supervisores; este proceso ocasiona problemas como:

- Ponderación del riesgo a criterio de cada Auditor lo cual eleva la subjetividad en la designación realizada.
- Posibles errores de inferencia.
- No existe una calificación y cuantificación precisa, la colocación en el mapa de los riesgos podría ser subjetivo.
- Dado que la matriz de riesgo (figura 1) debe suministrarse a los bancos a través de soporte documental (archivo Word), existe el riesgo de extravió o pérdida del documento, así como, su dilación en la entrega al organismo. Por otra parte, los riesgos asociados a la divulgación de información confidencial son elevados.
- Inexistencia de una base de datos de conocimiento con los riesgos, resaltando que, los archivos electrónicos existentes quedan a disposición de los auditores o en disco compactos (CD) o cualquier otro medio sin mecanismos de encriptación o cifrado de datos.
- No existen mecanismos que permitan obtener información estadística de los riesgos e indicadores en tiempo real, debido a que la información se encuentra en forma documental lo cual dificulta la búsqueda.
- Inexistencia de un sistema de ratings, el cual permita conocer por medio de indicadores el estado actual del sistema financiero en materia de riesgo tecnológico.

Por las razones anteriormente expuestas, esta investigación está orientada a la formulación de un Modelo de Madurez para la Cuantificación y Calificación del Riesgo Tecnológico en las Instituciones Bancarias de Venezuela, con el fin de apoyar en los procesos de toma de decisiones, mediante la generación de información oportuna, integra y confiable.

I.2. Objetivo General

Formular un modelo de madurez para la calificación y cuantificación del riesgo tecnológico en las Instituciones Bancarias de Venezuela.

I.3. Objetivos Específicos

- Efectuar un diagnóstico del proceso actual de inspección y obtención del nivel de riesgo tecnológico.
- Examinar las metodologías y mejores prácticas en materia de calificación y cuantificación del riesgo tecnológico.
- Diseñar el modelo de madurez para calificar y cuantificar el riesgo tecnológico en las instituciones bancarias de Venezuela.
- Vincular el modelo propuesto con un prototipo de software.

I.4. Justificación e Importancia de la Investigación

La supervisión de las entidades financieras constituye una actividad de notable trascendencia social, dado el interés público que se trata de proteger; el buen funcionamiento del sistema financiero nacional, su eficiencia y estabilidad y la sostenibilidad del sistema económico de la nación.

Un modelo eficaz de regulación y supervisión bancaria promueve la fluidez de los mecanismos de intermediación financiera, generando un entorno de confianza en las instituciones por parte de los ahorristas.

El negocio bancario está basado en la confianza de los depositantes, que necesitan un entorno institucional apropiado, incluyendo un sistema de supervisión bien organizado, para suplir en parte, su falta de capacidad e información para medir con precisión el riesgo en que incurren, específicamente el tecnológico ya que el 80% de sus operaciones están soportadas en la tecnología.

A su vez, mediante la supervisión del sistema se favorece a la eficiencia del sistema bancario a través de las obligaciones e incentivos que se prevén para la adopción por las entidades de crédito de sistemas integrales y prudentes, de gestión de riesgos, del fomento de la competencia y del impulso de prácticas apropiadas de trasparencia con la clientela y con los mercados en general.

Por último, el objetivo de estabilidad, que es básico, consiste, por un lado, en minimizar la importancia y el coste de las crisis bancarias y, por otro, en evitar que el denominado <<riesgo de sistema>> desencadene sus efectos.

En definitiva, la incorporación de un modelo que califique y cuantifique los riesgos de las instituciones redunda en beneficios como:

- Uso eficiente de los recursos de fiscalización, hacia las entidades más riesgosas.
- Alineación con los modelos de supervisión internacionales como Basilea II.
- Apoya los procesos de toma de decisiones en la GRT y por ende permite el suministro de información confiable y oportuna a las autoridades competentes del Organismo y del Estado.
- Disminución de costos operativos (papelería, archivos y horas hombre).
- Reducción del riesgo reputacional al ofrecer elevados niveles de seguridad y confidencialidad en la información manejada por la SUDEBAN.
- Control de los lapsos establecidos por el Organismo para la entrega de la información por parte de las Instituciones.
- Generación de reportes que faciliten la determinación de los principales riesgos tecnológicos de los entes supervisados.

Por último, existe un aporte significativo para la Universidad Católica Andrés Bello ya que el tema ha sido poco desarrollado y representa un pilar fundamental en el conocimiento del análisis de riesgo tecnológico y auditoría de sistema.

Capítulo II

Marco Referencial

"La mayoría de las ideas fundamentales de la ciencia son esencialmente sencillas y, por regla general pueden ser expresadas en un lenguaje comprensible para todos"

Albert Einstein

CAPÍTULO II

MARCO REFERENCIAL

Incluye la definición de términos básicos que serán usados a lo largo del proyecto. A continuación se presenta un mapa con una síntesis de todos los contenidos que se han de considerar en este capítulo.

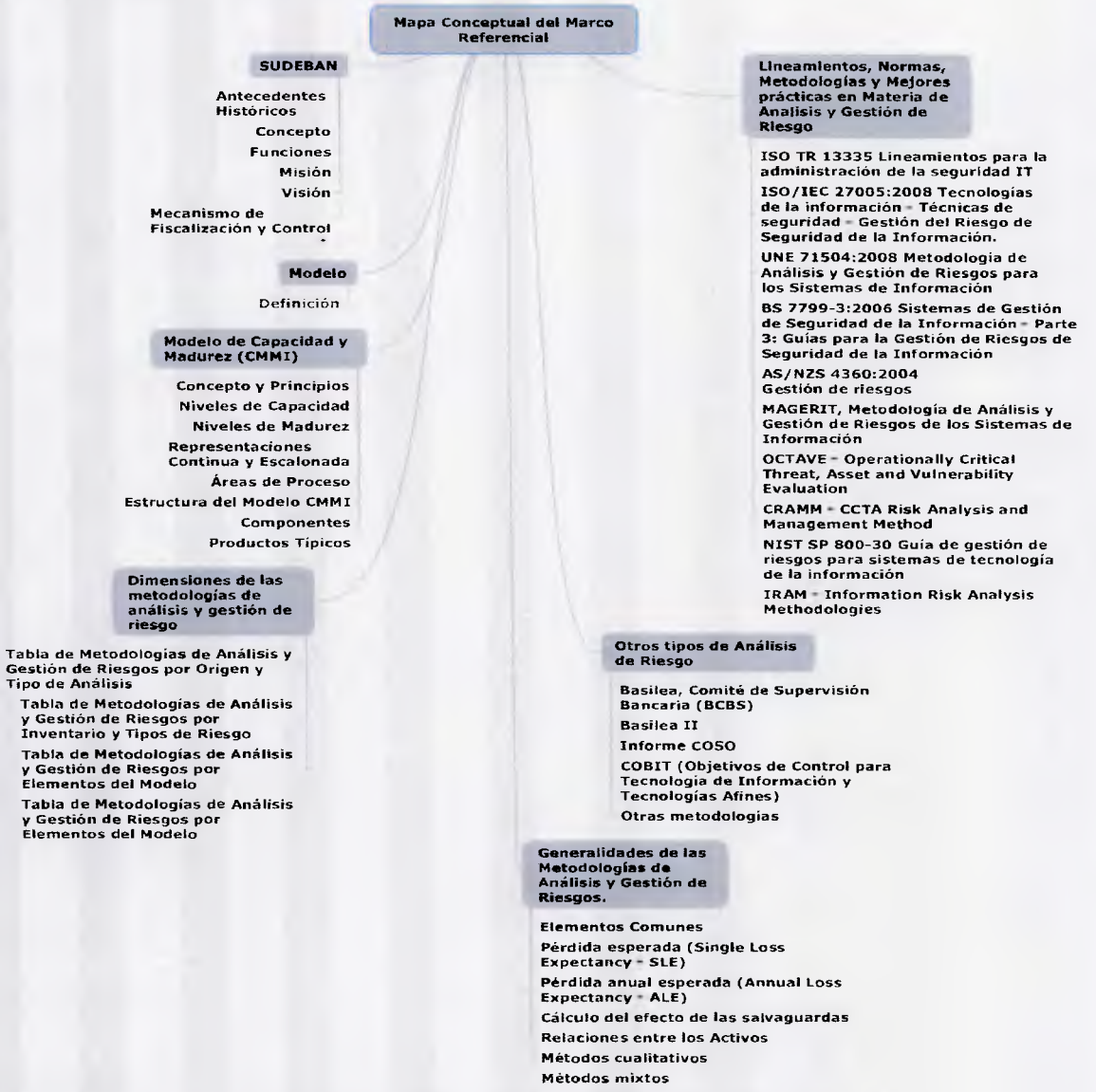


Figura 2: Mapa Conceptual del Marco Referencial

Para entrar en contexto iniciamos el marco referencial conociendo un poco a la institución objeto de estudio de esta tesis, denominada Superintendencia de las Instituciones del Sector Bancario (SUDEBAN).

II.1.Antecedentes Históricos de la Sudeban

La Superintendencia de las Instituciones del Sector Bancario (SUDEBAN), fue creada por la Ley de Bancos del 24 de enero de 1940. Con su creación se sustituyó a la Fiscalía General del Ministerio de Fomento a cuyo cargo habían estado las funciones de vigilancia y revisión de la actividad bancaria. Es así como nace el Ente que vino a fiscalizar, inspeccionar y vigilar a la banca, casas de cambio y demás instituciones de carácter financiero. Posteriormente, se incluyeron visitas a las oficinas bancarias ubicadas en el interior del país.

Con el propósito de unificar las operaciones bancarias se elaboró un instructivo que permitiría estandarizar la presentación de los resultados de la banca. Entre los años 1949 y 1958 se produjo la mayor apertura de agencias bancarias en la historia financiera venezolana, con la que se incrementó el número de visitas de inspección a sesenta y cuatro por año, detectándose para ese momento como principal inconveniente el incumplimiento fiel del encaje legal mínimo exigido por el Banco Central de Venezuela. Al finalizar la dictadura en Venezuela, se produjeron hechos que alteraron el desarrollo del sistema financiero, de allí que la labor de la SUDEBAN fue determinante para encaminar hacia un buen destino la banca.

Por otro lado, la reforma parcial que recibió la Ley de Bancos en febrero de 1988, le otorgó a la SUDEBAN potestad exclusiva en la práctica de medidas de intervención, en caso de ser detectadas irregularidades en el manejo de alguna entidad bancaria. Esto a raíz de la crisis financiera de 1994 donde las medidas adoptadas no llegaron al fondo de la solución de los problemas que colapsaron el sistema financiero y los organismos de vigilancia y control no escaparon de esa realidad. Allí quedó evidenciada la debilidad estructural y funcional de la SUDEBAN de esa década, que a pesar de los esfuerzos realizados no pudo evitar el fatal desenlace del cierre de varias instituciones financieras. Después de normalizada la crisis bancaria se realizó una profunda reestructuración de la SUDEBAN con relación a los aspectos tecnológicos, una mejor

planificación de las inspecciones y mejor capacitación del recurso humano. También se ejecutaron medidas de carácter externo como la implementación de regulaciones para las fusiones bancarias, constitución de provisiones bancarias, normativas para presentar y registrar las informaciones financieras, supervisión preventiva, mecanización de la información, entre otros aspectos. El 11 de noviembre de 2010 según Gaceta Oficial Nº 39.491 se aprobó la reforma parcial a la Ley General de Bancos que contempla la creación de un fondo para financiar proyectos comunales, y otro para proteger a los usuarios de posibles quiebras, así como, otros artículos relacionados con la banca.

II.2.CONCEPTO

La SUDEBAN, es un organismo autónomo de carácter técnico y especializado que tiene como función principal supervisar, controlar y vigilar a las instituciones financieras regidas por la Ley General de Bancos, a objeto de determinar la correcta realización de sus actividades, con el fin de evitar crisis bancarias y permitir el sano y eficiente funcionamiento del Sistema Financiero Venezolano.

II.3.FUNCIONES

Entre las funciones se pueden mencionar las siguientes:

- Asegurar que los bancos, entidades de ahorro y préstamo e instituciones financieras tengan sistemas y procedimientos adecuados para vigilar y controlar sus actividades a escala nacional e internacional, si fuese el caso.
- Obtener información sobre el grupo financiero a través de inspecciones regulares, estados financieros auditados y otros informes, sobre las transacciones y relaciones entre las empresas del grupo financiero.
- Recibir estados financieros consolidados a nivel nacional e internacional, si fuese el caso, o información comparable que permita el análisis de la situación del grupo financiero en forma consolidada.
- Evaluar los indicadores financieros de la institución y del grupo.

- Obtener información sobre la respectiva estructura accionaría, incluyendo los datos que permitan determinar con precisión la identidad de las personas naturales, propietarias finales de las acciones o de las compañías que las detentan.
- Obtener la información necesaria, mediante inspecciones in situ o extra situ, a los fines de verificar que las agencias, sucursales, oficinas, filiales y afiliadas en el exterior, de bancos o instituciones financieras venezolanos, cumplen con las regulaciones y disposiciones aplicables del lugar donde funcionan. Asegurar que los bancos, entidades de ahorro y préstamo, instituciones financieras y demás empresas sujetas a este Decreto Ley, tengan sistemas y procedimientos adecuados para evitar que sean utilizados para legitimar capitales provenientes de actividades ilícitas.

II.4.MISIÓN

Es una institución conformada por un talento humano comprometido con la supervisión y regulación del Sistema Bancario y Otras Instituciones Financieras, a través de la aplicación de las mejores prácticas nacionales e internacionales, que contribuyan con la estabilidad del Sistema y el desarrollo nacional

II.5.VISIÓN

Ser modelo de institución pública inspiradora de confianza y credibilidad, de reconocido prestigio nacional e internacional

II.6. MECANISMO DE FISCALIZACIÓN Y CONTROL

Los mecanismos de fiscalización y control de los que dispone la SUDEBAN pueden agruparse en:

- Controles previos, relativos a la autorización de promoción y funcionamiento de instituciones financieras, conocido también como la promoción, que inicia la idea de constitución de una entidad financiera y la autorización del inicio de sus operaciones.

- Controles regulares, ejercidos a través de la fiscalización, inspección y control de los bancos y demás instituciones financieras, con el objeto de determinar su sujeción a las disposiciones legales y reglamentarias que las rigen. Estos los realiza la SUDEBAN y se dividen en Supervisión y Control de Campo y Supervisión y Control a Distancia.
- Controles excepcionales, conocido también como control directo o examen *in-situ*, estos se efectúa a través de las inspecciones que se realizan en la sede u otras oficinas de los propios institutos. Estas visitas de inspección son de dos clases:
- Inspecciones Especiales, son aquellas que se realizan a fin de constatar, verificar o examinar algún aspecto en particular de las operaciones del instituto, Inspecciones Ordinarias, son aquellas que se efectúan regularmente, según lo establecido en la Ley, de acuerdo a una planificación de programas de inspección ordinarios en base a las metas anuales.

II.7.DEFINICIÓN DE MODELO

¿Cómo se puede estudiar y entender algo tan formidablemente complejo como es la biosfera o una selva tropical o el clima?. Es necesario usar simplificaciones que tengan en cuenta sólo las propiedades más importantes y básicas. Estas versiones simplificadas de la realidad se llaman modelos, para poder crear un modelo necesitamos comprender su definición, así como, los modelos existentes en la actualidad para los sistemas de información.

Los modelos se utilizan con muchos propósitos, pero básicamente para "captar y enumerar exhaustivamente los requisitos y el dominio del conocimiento, de forma que todos los implicados puedan entenderlos y estar de acuerdo con ellos" (Rumbaugh, 2000).

En un modelo se definen las fases y tareas esenciales para el desarrollo de sistemas. Sirve para planear, ejecutar y controlar un proyecto de desarrollo de software.

Un modelo puede ser tan sencillo como una simple explicación con palabras de lo fundamental de una realidad. A este tipo se le suele llamar modelo verbal.

En otros modelos usamos diagramas en los que se dibujan de una forma simplificada los componentes del sistema señalando con flechas las acciones de unos sobre otros, estos son modelos gráficos. Algunos pueden ser muy esquemáticos, pero cuando en cada flecha se indica el tipo de acción que tiene lugar y se señalan diferentes compartimentos y tipos de interacción, pueden llegar a ser muy complicados.

En los modelos numéricos se usan magnitudes y ecuaciones matemáticas para describir con exactitud los distintos componentes del sistema y las relaciones entre ellos.

El desarrollo de los ordenadores ha hecho posible manejar una gran cantidad de datos y por eso ahora se usan, cada vez más, modelos computacionales, en los que con programas de ordenador se imita el funcionamiento de sistemas complejos.

II.8.El Modelo de Capacidad y Madurez (CMMI)

A finales de los 90 algunas organizaciones llevaban a cabo planes de calidad que integraban de forma simultánea varios modelos de madurez de capacidad (CMM).

Para facilitar la incorporación de varios CMM's, el instituto federal estadounidense de investigación y desarrollo (SEI) desarrolla y publica en 2001 el modelo CMMI que integra:

- El Modelo de Madurez de la Capacidad para el desarrollo de Software (CMM-SW).
- Modelo de Madurez de Capacidades en la Ingeniería de Sistemas (SE-CMM).
- El Modelo de Madurez de Capacidades para el Desarrollo Integrado de Productos (IPD-CMM).

CMMI está registrado en la Oficina de Patentes y Marcas de EE.UU. por la Universidad Carnegie Mellon.

II.9.Concepto y Principios de CMMI

Según el SEI en su documento CMMI para desarrollo (University, 2006) se asienta en el mismo principio expuesto para CMM: La calidad de un producto o de un sistema es en su mayor parte consecuencia de la calidad de los procesos empleados en su desarrollo y mantenimiento.

- Madurez: Atributo de las organizaciones que desarrollan o mantienen los sistemas de software. En la medida que éstas llevan a cabo su trabajo siguiendo procesos, y en la que éstos se encuentran homogéneamente implantados, definidos con mayor o menor rigor; conocidos y ejecutados por todos los equipos de la empresa; y medidos y mejorados de forma constante, las organizaciones serán más o menos "maduras".
- Capacidad: Atributo de los procesos. El nivel de capacidad de un proceso indica si sólo se ejecuta, o si también se planifica se encuentra organizativa y formalmente definido, se mide y se mejora de forma sistemática.

II.10.Niveles de Capacidad

Los 6 niveles definidos en CMMI para medir la capacidad de los procesos son:

- Incompleto: El proceso no se realiza, o no se consiguen sus objetivos.
- Ejecutado: El proceso se ejecuta y se logra su objetivo.
- Gestionado: Además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos.
- Definido: Además de ser un proceso "gestionado" se ajusta a la política de procesos que existe en la organización, alineada con las directivas de la empresa.
- Cuantitativamente gestionado: Además de ser un proceso definido se controla utilizando técnicas cuantitativas.

- Optimizado: Además de ser un proceso cuantitativamente gestionado, de forma sistemática se revisa y modifica para adaptarlo a los objetivos del negocio.

II.11.NIVELES DE MADUREZ

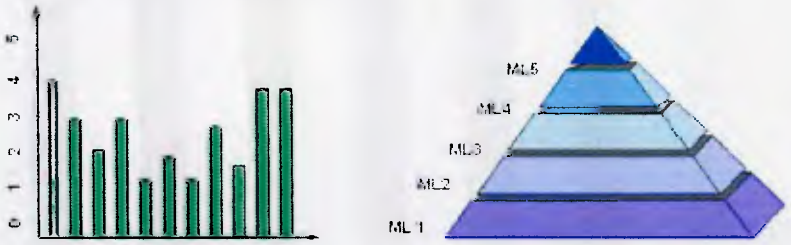
Son los mismos 5 que los descritos en el modelo SW-CMM:

- Nivel 1: Inicial
- Nivel 2: Gestionado
- Nivel 3: Definido
- Nivel 4: Gestionado cuantitativamente
- Nivel 5: Optimizado

II.12.REPRESENTACIONES CONTINUA Y ESCALONADA

Los modelos de calidad que centran su foco en la madurez de la organización, presentan un modelo de mejora y evaluación "escalonado". Los que enfocan las actividades de mejora y evaluación en la capacidad de los diferentes procesos presentan un modelo "continuo". CMMI nació integrando tres modelos diferentes, con representaciones diferentes:

- CMM-SW: representación escalonada.
- SE-CMM: representación continúa.
- IPD-CMM: modelo mixto.



CONTINUA **ESCALONADA**

Figura 3: Representaciones de CMMIM

II.13.ÁREAS DE PROCESO

CMMI identifica 25 áreas de procesos (22 en la versión que no integra IPD). Vistas desde la representación continua del modelo, se agrupan en 4 categorías según su finalidad: Gestión de proyectos, Ingeniería, Gestión de procesos y Soporte a las otras categorías.

Vistas desde la representación escalonada, se clasifican en los 5 niveles de madurez. Al nivel de madurez pertenecen las áreas de proceso cuyos objetivos debe lograr la organización para alcanzarlo, niveles 3, 4 y 5.

Áreas de Proceso	Categoría	Nivel de madurez
Análisis y resolución de problemas	Soporte	5, 3
Gestión integral de proyecto	G. Proyectos	3
Gestión de equipos	G. Proyectos	3
Medición y análisis	Soporte	2
Planificación de proyecto	G. Proyecto	2
Gestión cuantitativa de proyectos	G. Proyectos	4
Gestión de riesgos	G. Proyectos	3
Gestión y acuerdo con proveedores	G. Proyectos	2

Tabla 2: Algunas Áreas de Proceso de CMMI

II.14.ESTRUCTURA DEL MODELO CMMI

Representación continúa:

Figura 4: Representación Continúa de CMMI

Representación escalonada:

Figura 5: Representación Escalonada de CMMI

II.15.COMPONENTES

- Área de proceso: Conjunto de prácticas relacionadas que son ejecutadas de forma conjunta para conseguir un conjunto de objetivos
- Objetivo genérico: Los objetivos genéricos asociados a un nivel de capacidad establecen lo que una organización debe alcanzar en ese nivel de capacidad. El logro de cada uno de esos objetivos en un área de proceso significa mejorar el control en la ejecución del área de proceso
- Objetivo específico: Los objetivos específicos se aplican a una única área de proceso y localizan las particularidades que describen que se debe implementar para satisfacer el propósito del área de proceso.
- Práctica genérica: Una práctica genérica se aplica a cualquier área de proceso porque puede mejorar el funcionamiento y el control de cualquier proceso.

- Práctica específica: Una práctica específica es una actividad que se considera importante en la realización del objetivo específico al cual está asociado. Las prácticas específicas describen las actividades esperadas para lograr la meta específica de un área de proceso.
- Los Componentes Informativos son: propósito, notas introductorias, referencias, nombres, tablas de relaciones práctica – objetivo y prácticas

II.16.Productos Típicos

- Sub-prácticas: Una sub-practica es una descripción detallada que sirve como guía para la interpretación de una práctica genérica o especifica.
- Ampliaciones de la disciplina: contienen información relevante de una disciplina particular y relacionada con una práctica específica
- Elaboraciones de prácticas genéricas: Una elaboración de una práctica genérica es una guía de cómo la practica genérica debe aplicarse al área de proceso

En otro orden de ideas, un banco es un tipo especial de empresa, que capta dinero del público, estos recursos del exterior, conjuntamente con los recursos propios de la entidad son transferidos en forma de préstamos, a terceros, que pagan intereses por el uso del dinero. Así, usualmente los recursos con los que un banco genera sus ingresos son, en parte propios (patrimonio o capital), y mayoritariamente ajenos (depósitos del público). Por ello, dado que la mayoría del dinero que un banco administra no le pertenece, la gestión bancaria requiere un proceso constante de evaluación y medición de los riesgos a los que se exponen los recursos de los depositantes en las operaciones de la entidad.

Estos riesgos, en conjunto, se denominan *riesgo bancario* y su administración suele ser regulada por los organismos supervisores de la banca (SUDEBAN) en cada país individual. Una preocupación básica de estos organismos es asegurar que cada entidad bancaria pueda devolver los depósitos del público, lo que requiere de un nivel

adecuado de capital para que, en caso de una pérdida, ésta se cubra con recursos propios y no con dinero del público. En la siguiente sección se dará a conocer un poco la definición general de riesgo, así como, los elementos involucrados en su calificación y cuantificación, para luego definir el riesgo tecnológico, en el cual nos enfocaremos el resto de la trabajo.

II.17.DEFINICIÓN GENERAL DE RIESGO

Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva dos tipos de consecuencias: ganancias o pérdidas.

En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo el riesgo de perder datos debido a rotura de disco, virus informáticos, etc.).

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico (ISO, 1996) como:

"La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándole perdidas o daños".

En la definición anterior se pueden identificar varios elementos que se deben comprender adecuadamente para poder comprender integralmente el concepto de riesgo.

Estos elementos son: probabilidad, amenazas, vulnerabilidades, activos e impactos. A continuación se analiza cada uno de ellos:

Probabilidad: establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción paliativa, o sea, debe considerarse en cada caso qué posibilidades existen que la amenaza se presente independientemente del hecho que sea o no contrarrestada.

Existen amenazas, como por ejemplo incendios, para las cuales hay información suficiente (series históricas, compañías de seguros y otros datos) para establecer con

razonable objetividad su probabilidad de ocurrencia. Otras amenazas presentan mayor dificultad en establecer cuantitativamente la probabilidad. Por ejemplo, el acceso no autorizado a datos; dónde se hacen estimaciones sobre la base de experiencias. Siguiendo con el ejemplo, para el personal interno del Centro de Cómputos (CPD), la probabilidad puede ser el 70%, para el personal de la organización, externo al CPD, del 45%, y para personas de fuera, el 80% (a través de acceso por Internet).

Amenazas: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

Las amenazas pueden ser de carácter físico o lógico, como ser una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

Vulnerabilidades: son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a esos activos a ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.

Estas vulnerabilidades son de naturaleza variada. A modo de ejemplo se citan las siguientes: "falta de conocimiento del usuario, tecnología inadecuadamente probada ("testeada"), transmisión por redes públicas, etc."

Una vulnerabilidad común es contar con antivirus no actualizado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado la amenaza (virus) si bien potencialmente seguiría existiendo no podría materializarse.

Activos: Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplos típicos son los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

Impactos: las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

II.18.ANÁLISIS DE RIESGOS

Todas las Organizaciones, ya sean públicas o privadas, formales o informales, se crean y mantienen con unos objetivos determinados (Lybrand, 1997).

El universo formado por todos los posibles eventos que pueden afectar de forma negativa al cumplimiento de los objetivos establecidos puede considerarse infinito. Estos eventos pueden tener origen interno o externo, ser fortuitos o intencionados y tener naturalezas absolutamente dispares: riesgo financiero, operativo, tecnológico, de mercado, legal, de seguridad de la información, etc.

De la misma forma, el universo formado por todas las medidas de protección contra dichos eventos es inabarcable por razones de coste. Para gestionar esta complejidad es necesario definir un procedimiento que permita identificar aquellos riesgos que deben tenerse en consideración en contraposición con aquellos que, por su baja probabilidad de ocurrencia, por su bajo impacto o por la dificultad o coste de su mitigación, deberán ser asumidos por la Organización.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta la Dirección (López F., 2006).

II.19.GESTIÓN DEL RIESGO

Por "Gestión de Riesgos" se entiende en general el proceso consistente en identificar acontecimientos posibles, cuya materialización afectará al logro de los objetivos y la aplicación de las medidas destinadas a reducir la probabilidad o el impacto de esos acontecimientos. Un factor fundamental para la Gestión de Riesgos es la eficacia de los controles institucionales internos.

Entre las principales definiciones se pueden resaltar las del Project Management Institute (Duncan, 1996):

- "es el proceso por el que los factores de riesgo se identifican sistemáticamente y se evalúan sus propiedades.
- es una metodología sistemática y formal que se concentra en identificar y controlar áreas de eventos que tienen la capacidad de provocar un cambio no deseado.
- es el contexto de un proyecto, es el arte y ciencia de identificar, analizar y responder a los factores de riesgo a lo largo de la vida del proyecto y en el mejor cumplimiento de sus objetivos."

En el año 1985, el Comité COSO (Lybrand, 1997) publicó un nuevo Marco de Gestión Integral de Riesgo "COSO" Enterprise Risk Management - Integrated Framework cuya definición fue:

> *"Gestión de Riesgos es un proceso efectuado por el directorio, la administración superior y otros miembros de la organización, basado en la estrategia y a lo largo de la empresa, diseñado para identificar potenciales eventos que puedan afectar a la entidad y administrar el riesgo dentro de los rangos de aversión al riesgo aceptado por la entidad, para proveer una razonable seguridad en el logro de sus objetivos".*

II.20. Tipo de Riesgo Operacional

Una definición para riesgo operacional se plasmó en el Segundo Documento Consultivo (Comité de Basilea, 2003) el cual lo define como:

> *"el riesgo de sufrir pérdidas debido a la inadecuación o a fallos en los procesos, personal y sistemas internos o bien por causa de eventos externos. Lo que incluye el riesgo legal pero excluye a los riesgos reputacional, estratégico y sistémico".*

Uno de los mayores avances que se consiguió al consensuar una definición para riesgo operacional es que a partir de ella se puedo establecer una clasificación y determinación de los principales factores y eventos de pérdida. Dicha clasificación se compone de tres niveles, que permiten complementar y delimitar un concepto que en sí resultaba algo ambiguo.

En el primer nivel se encuentran:

- Fraude interno y externo.
- Relaciones laborales y seguridad en el puesto de trabajo.
- Incidencias en el negocio y fallos en los sistemas.
- Daños a activos materiales.
- Clientes, productos y prácticas empresariales.
- Ejecución, entrega y gestión de procesos.

El segundo nivel proporciona una apertura más detallada al nivel anterior, mediante 20 categorías.

Por último, el tercer nivel ejemplifica las actividades principales y más comunes asociadas a cada categoría del segundo nivel.

II.21.Tipo de Riesgo Tecnológico

Según la (Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras, 2007) se define como:

> *"la posible pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en los equipos, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios o financieros con los clientes."*

II.22.Fuentes de Riesgo Operativo

Procesos Internos: Posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, o con políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la

información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y presupuestos planeados.

Personas: Posibilidad de pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores. Se puede también incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación.

Tecnología de Información: Posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

Las instituciones pueden considerar de incluir en ésta área, los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas TI, a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología y fallas para alinear la TI con los objetivos de negocio, con entre otros aspectos. Otros riesgos incluyen la falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio. (ASBA, 2010)

Para llevar a cabo el proceso de análisis y gestión del riesgo, existen diversos lineamientos, normas y metodologías para el análisis y la gestión de riesgo que son utilizadas, en esta sección vamos a mencionar algunas de la más importante y explicar brevemente en qué consisten:

II.23.ISO TR 13335 LINEAMIENTOS PARA LA ADMINISTRACIÓN DE LA SEGURIDAD

ISO/IEC TR 13335 es un compendio de 5 documentos que de forma práctica aborda la seguridad de las Tecnologías de la Información y orienta sobre los aspectos de su gestión. Estos documentos son:

Parte 1: Conceptos y modelos para la seguridad TI, publicado en 2004 (ISO, International Organitation Standards, 2004).

Parte 2: Planificación y gestión de la seguridad de las Tecnologías de la Información, publicada en 1997, ha quedado obsoleta por la publicación de la última versión de la parte 1.

Parte 3: Técnicas para la gestión de la seguridad de las Tecnologías de la Información, publicada en 1998, ha quedado obsoleta por la publicación de la norma ISO/IEC 27005:2008.

Parte 4: Selección de salvaguardas, publicada en 2000, ha quedado obsoleta por la publicación de la norma ISO/IEC 27005:2008.

Parte 5: Salvaguardas para conexiones externas, publicada en 2001, ha quedado obsoleta por la publicación de la norma ISO/IEC 18028-1:2006.

Su objetivo es el de describir y recomendar métodos para una exitosa administración de la seguridad IT Dicho proceso de las técnicas de administración se basan en la parte 1 y 2 de la norma de acuerdo al siguiente ciclo realimentado:

- Objetivos, estrategia y políticas de seguridad
- Estrategia corporativa de análisis de riesgos
- Enfoque combinado, que incluye análisis profundos de riesgos, selección de salvaguardias, aceptación de riesgos, políticas y planeamientos de seguridad
- Implementación del plan de seguridad
- Seguimiento, incluye, el mantenimiento, mejoramiento, manejo de incidentes, etc

El modelo de procesos propuesto por el informe técnico ISO/IEC 13335 para la gestión de la Seguridad de la Información se resume en el siguiente gráfico:

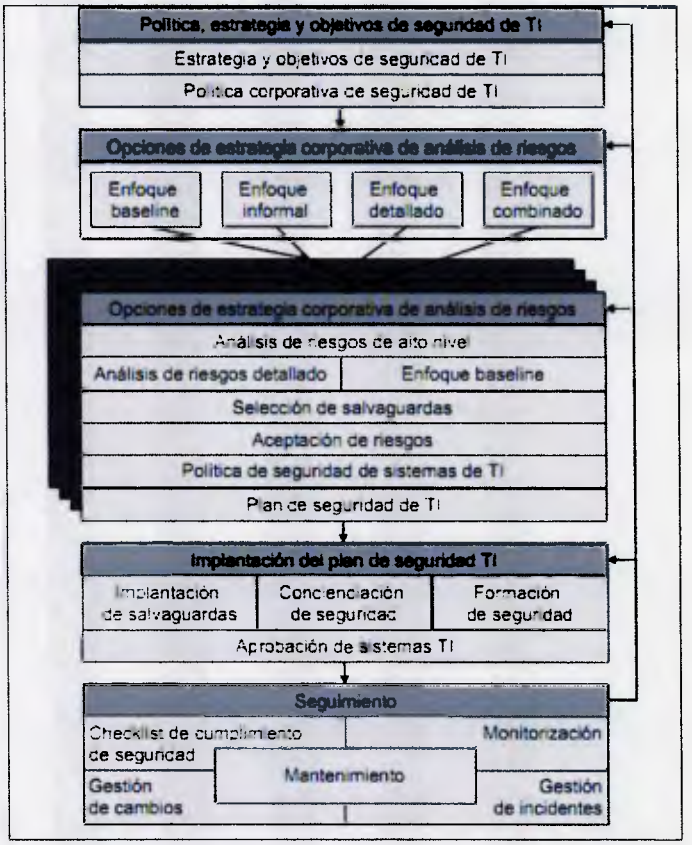


Figura 6: Procesos de Gestión de Seguridad de la Información

(Fuente: ISO/IEC 13335)

Como parte del proceso de gestión de seguridad de la información se incluye el proceso de análisis detallado de riesgos, que se describe en el siguiente gráfico:

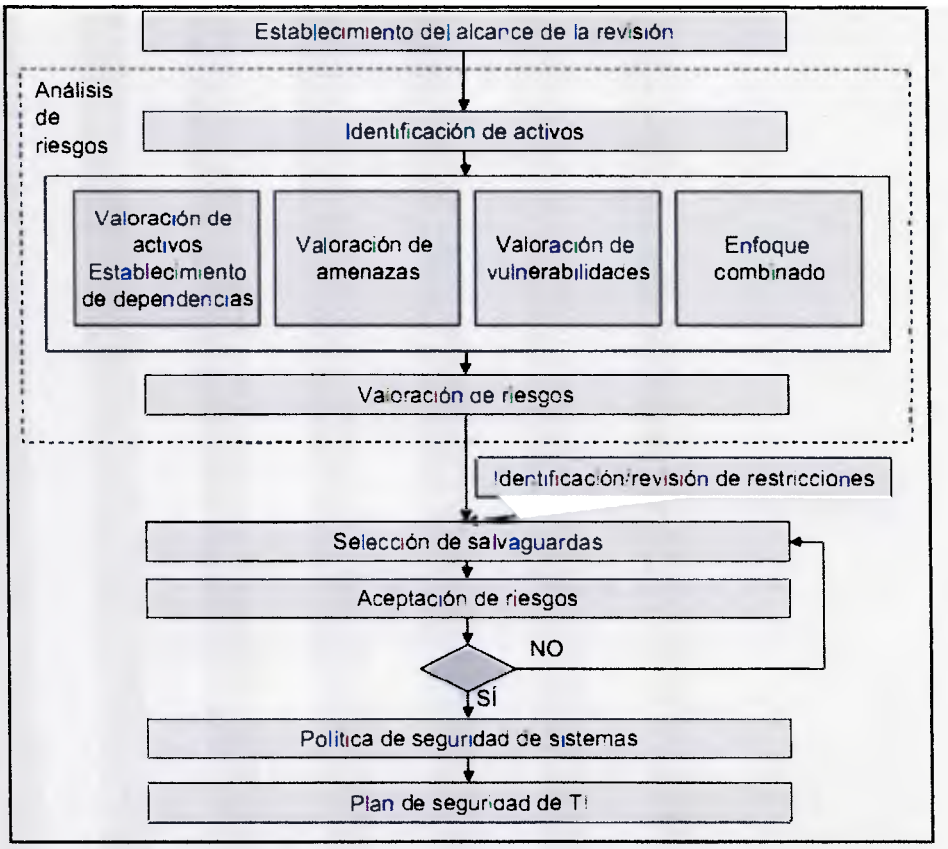


Figura 7: Proceso de Análisis Detallado de Riesgos (Fuente: ISO/IEC 13335)

II.24.ISO/IEC 27005:2008 TI– TÉCNICAS DE SEGURIDAD – GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.

La norma ISO/IEC 27005:2008 (ISO, International Organitation Standards, 2008) forma parte de la familia ISO 27000 dedicada a la seguridad de la información. Sirve de complemento a las dos primeras normas de la familia ISO/IEC 27001:2005 e ISO/IEC 27002:2005 que definen la necesidad de elaborar un análisis de riesgos pero no especifican directrices para ello.

Está basada en los informes técnicos ISO/IEC TR 13335-3:1998 (ISO, International Organization Standards, 1997) e ISO/IEC TR 13335-4:2000 (ISO, International

Organization Standards, 2000), descritos en el apartado anterior, que quedaron obsoletos desde su publicación. También está basada en la norma BS 7799-3:2006.

El proceso de gestión de riesgos se describe en las siguientes 6 cláusulas (ISO, International Organitation Standards, 2008):

Cláusula 1: Establecimiento del contexto, en la que se definen los objetivos, el alcance y la organización para todo el proceso.

Cláusula 2: Valoración de riesgos, en la que se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos. Se divide en tres apartados:

- Identificación de riesgos, que consiste en determinar qué puede provocar pérdidas a la Organización.
- Estimación de riesgos, que consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, teniendo en cuenta los activos, las amenazas y las salvaguardas.
- Evaluación de riesgos, que consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

Cláusula 3: Tratamiento de riesgos, en la que se define la estrategia para tratar cada uno de los riesgos valorados: reducción, aceptación, evitación o transferencia.

Cláusula 4: Aceptación de riesgos, en la que se determinan los riesgos que se decide aceptar, y la justificación correspondiente a cada riesgo aceptado.

Cláusula 5: Comunicación de riesgos, en la que todos los grupos de interés intercambian información sobre los riesgos.

Cláusula 6: Monitorización y revisión de riesgos, en la que el análisis de riesgos se actualiza con todos los cambios internos o externos que afectan a la valoración de los riesgos.

El proceso de gestión de riesgos definido por la norma ISO/IEC 27005:2008 puede resumirse en el siguiente gráfico:

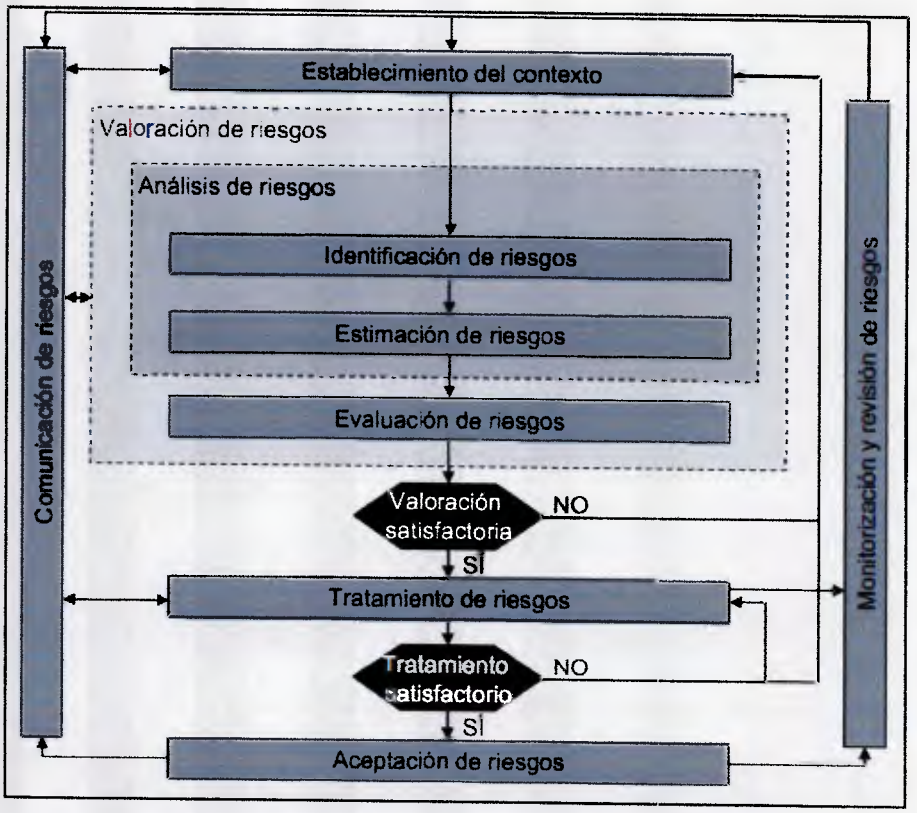


Figura 8: Proceso de Gestión de riesgos de seguridad de la información de ISO/IEC 27005:2008

II.25.UNE 71504:2008 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Desarrollada por el comité técnico AEN/CTN 71 Tecnología de la información, de AENOR. El cual define las siguientes fases principales y actividades en el presente grafico:

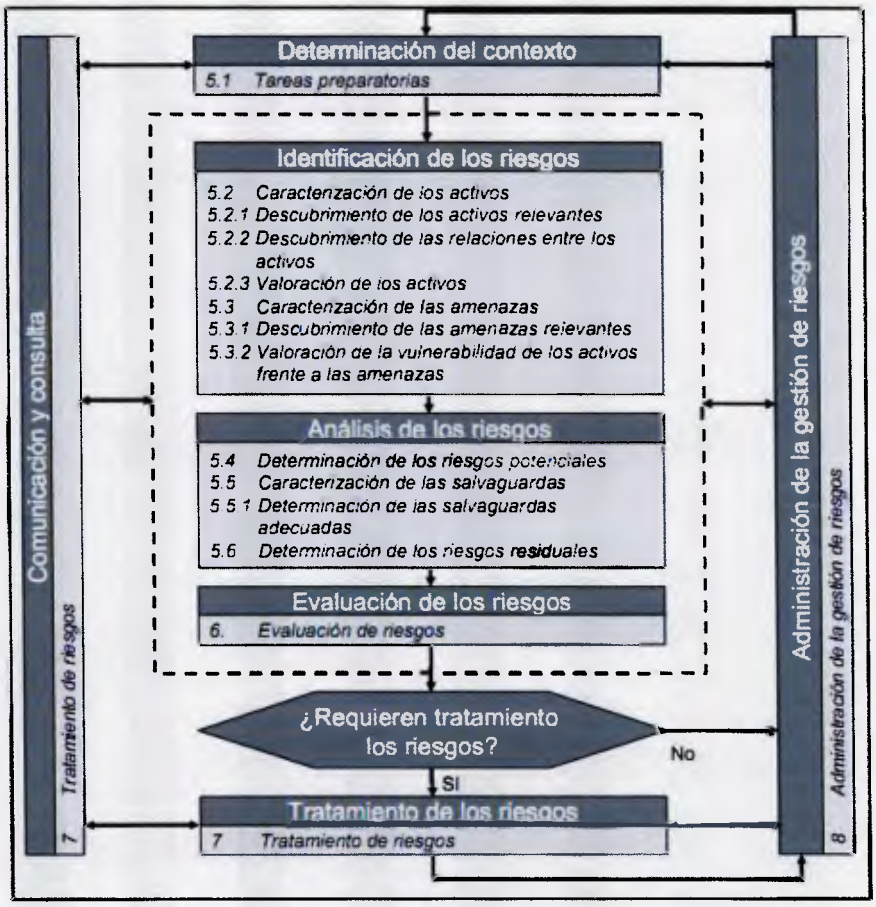


Figura 9: Modelo UNE 71504

II.26.BS 7799-3:2006 Sistemas de Gestión de Seguridad de la Información – Parte 3: Guías para la Gestión de Riesgos de Seguridad de la Información

Se definió para soportar la implantación de Sistemas de Gestión de Seguridad de la Información basados en el estándar ISO/IEC 27001:2005.

Los principales procesos de análisis de riesgos que define son:

Análisis de riesgos:	Evaluación de riesgos:
Identificación de activos Identificación de requerimientos legales y de negocio relevantes para los activos identificados. Valoración de los activos teniendo en cuenta los requerimientos identificados y el impacto resultante de la pérdida de confidencialidad, integridad o disponibilidad. Identificación de amenazas y vulnerabilidades relevantes para los activos identificados. Valoración de la posibilidad de que ocurran las amenazas y vulnerabilidades.	Calculo de riesgos Evaluación de los riesgos teniendo en cuenta una escala de riesgos. Tratamiento de riesgos y decisiones de la dirección o Determinación de la estrategia de gestión de los riesgos: Reducir, Aceptar, Transferir y Evitar. Evaluación del riesgo residual Definición del plan de tratamiento de riesgos Actividades de gestión continuo del riesgo: Mantenimiento y monitorización. Revisiones de la dirección. Revisiones y reevaluaciones de riesgos. Auditorías. Controles de documentación. Acciones correctivas y preventivas. Reportes y comunicaciones

Los procesos propuestos para la gestión del riesgo definen un ciclo iterativo que se puede comprobar en el siguiente diagrama (BSI – British Standards Institution, 2006):

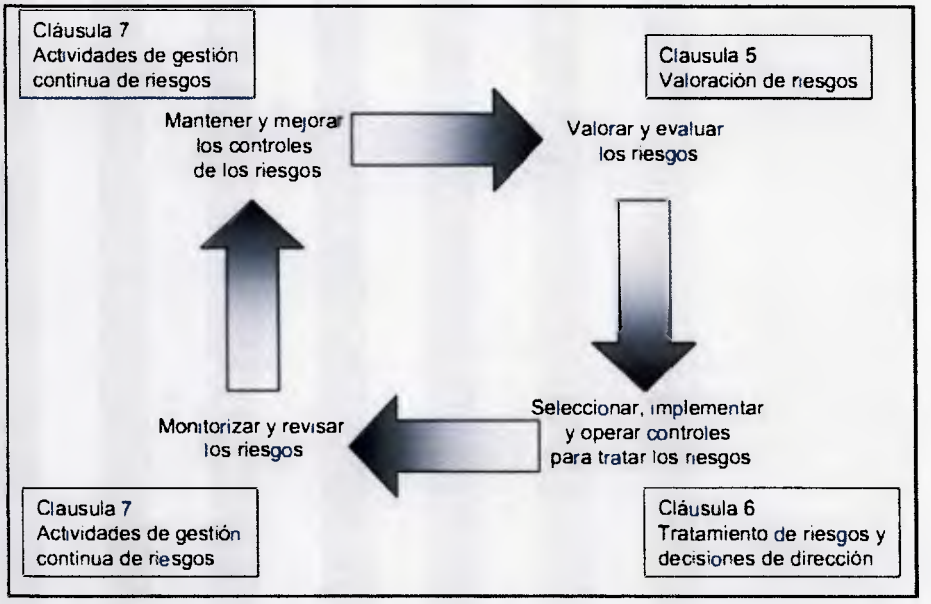


Figura 10: Modelo de Procesos de Gestión de Riesgos de BS 7799-3

II.27.AS/NZS 4360:2004 GESTIÓN DE RIESGOS

En el momento de la publicación de las normas ISO/IEC 27001:2005 e ISO/IEC 27002:2005 la norma AS/NZS 4360:2004 era la única norma internacional publicada para la realización de análisis de riesgos de seguridad de la información (si no se considera el informe técnico ISO/IEC TR 13335-3 y ISO13335-4, que no tenía rango de norma, y los diversos modelos y metodologías existentes que no estaban respaldados por organizaciones de estandarización y normalización), y por ello, hasta la publicación de las normas BS 7799-3:2006 e ISO/IEC 27005:2008 fue la norma dominante a nivel internacional soportando la implantación de Sistemas de Gestión de Seguridad de la Información.

El proceso de gestión de riesgos propuesto por la norma AS/NZS 4360:2004 puede resumirse en el siguiente esquema (AS/NZS – Australian Standards / New Zealand Standards, 2008)

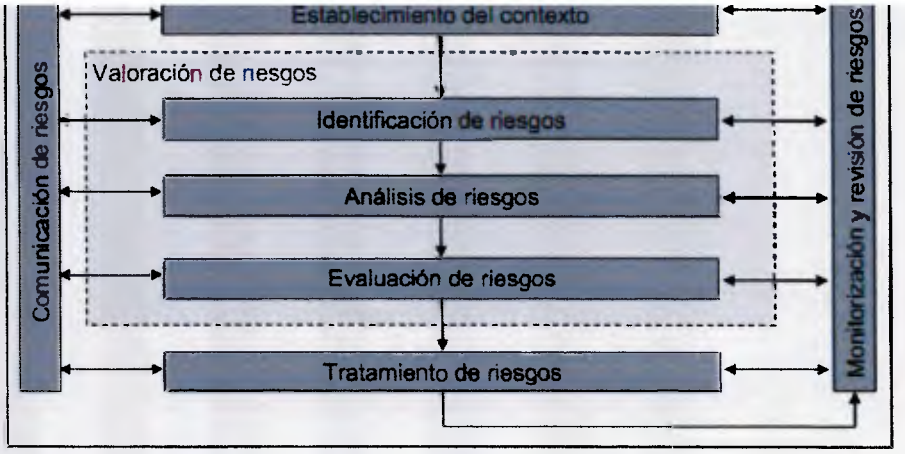


Figura 11: Proceso de Gestión de Riesgos de AS/NZS 4360:2004

Los principales aspectos considerados por la norma AS/NZS 4360:2004 son:

Establecimiento del contexto:	-Definición de objetivos -Identificación de grupos de interés -Definición de criterios para el análisis de riesgos -Definición de elementos clave
Valoración de riesgos	-Identificación de riesgos -¿Qué puede ocurrir? -¿Cómo puede ocurrir? -Revisar controles -Posibilidades -Consecuencias -Nivel de riesgo -Evaluación de los riesgos -Evaluar los riesgos -Priorizar los riesgos
Tratamiento de los riesgos	-Identificar opciones (reducción, aceptación, traspaso, evitación) -Seleccionar las mejores estrategias -Desarrollar planes de tratamiento de riesgos -Implementar los planes

II.28.MAGERIT, METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

La metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica, y publicada por el Ministerio de Administraciones Pública. (López F., 2006)

La primera versión se publicó en 1997 y la versión vigente en la actualidad es la versión 2.0, publicada en 2006.

Se trata de una metodología abierta, de uso muy extendido en el ámbito español, y de uso obligatorio por parte de la Administración Pública Española.

Dispone de una herramienta de soporte, PILAR II (Proceso Informático-Lógico para el Análisis y la gestión de Riesgos), de uso gratuito para la Administración Pública española y comercial para organizaciones privadas.

La metodología consta de tres volúmenes:

- Volumen I – Método, es el volumen principal en el que se explica detalladamente la metodología.
- Volumen II – Catálogo de elementos, complementa el volumen principal proporcionando diversos inventarios de utilidad en la aplicación de la metodología. Los inventarios que incluye son:
  - Tipos de activos
  - Dimensiones y criterios de valoración
  - Amenazas
  - Salvaguardas
- Volumen III – Guía de técnicas, complementa el volumen principal proporcionando una introducción de algunas de técnicas a utilizar en las distintas fases del análisis de riesgos. Las técnicas que recoge son:

Técnicas específicas para el análisis de riesgos: análisis mediante tablas, análisis algorítmico y arboles de ataque

Técnicas generales: análisis coste-beneficio, diagramas de flujo de datos (DFD), diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo: entrevistas, reuniones y presentaciones y valoración Delphi.

La metodología MAGERIT se puede resumir gráficamente de la siguiente figura:

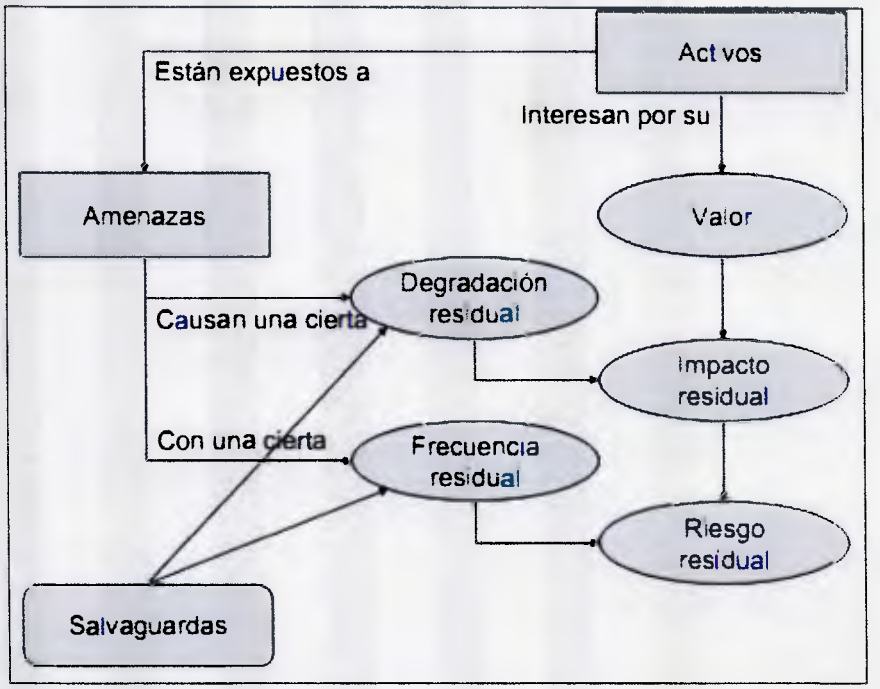


Figura 12: Modelo MAGERIT

II.29.OCTAVE – OPERATIONALLY CRITICAL THREAT, ASSET AND VULNERABILITY EVALUATION

OCTAVE es un modelo para la creación de metodologías de análisis de riesgos desarrollado por la Universidad de Carnegie Mellon. (Christopher J. Alberts, OCTAVE).

El núcleo centro de OCTAVE es un conjunto de criterios (principios, atributos y resultados) a partir de los cuales se pueden desarrollar diversas metodologías.

Cualquier metodología que aplique los criterios puede considerarse compatible con el modelo OCTAVE. Las tres metodologías publicadas a la fecha de este documento por el Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon son:

- OCTAVE. La metodología original, definida para grandes organizaciones.
- OCTAVE-S. Metodología definida para pequeñas organizaciones.
- OCTAVE Allegro. Metodología definida para analizar riesgos con un mayor enfoque en los activos de información, en oposición al enfoque en los recursos de información.

Los criterios que forman el núcleo de OCTAVE son:

Principios de los que se derivan atributos:	
La metodología debe ser auto-dirigida	RA.1 Equipo de análisis RA.2 Capacidades del equipo de análisis
Las medidas deben ser adaptables a las necesidades	RA.3 Catálogo de prácticas RA.4 Perfil genérico de amenazas RA.5 Catálogo de vulnerabilidades
El proceso debe ser definido	RA.6 Actividades de evaluación definida RA.7 Documentación de los resultados de la evaluación RA.8 Alcance de la evaluación El proceso debe ser continuo RA.9 Próximos pasos RA.3 Catálogo de prácticas RA.10 Enfoque en riesgos
El proceso debe centrarse en un reducido número de riesgos críticos	RA.8 Alcance de la evaluación RA.11 Actividades enfocadas
Gestión integrada:	RA.12 Aspectos organizativos y tecnológicos RA.13 Participación de negocio y de áreas tecnológicas RA.14 Participación de la alta dirección
Comunicación abierta	RA.15 Enfoque colaborativo
Perspectiva global	RA.12 Aspectos organizativos y tecnológicos RA.13 Participación de negocio y de áreas tecnológicas
Equipo de trabajo	RA.1 Equipo de análisis RA.2 Capacidades del equipo de análisis RA.13 Participación de negocio y de áreas tecnológicas RA.15 Enfoque colaborativo

El resultados de las distintas fases son:

Fase 1: **Visión organizativa**	RO1.1 Activos críticos RO1.2 Requerimientos de seguridad para los activos críticos RO1.3 Amenazas sobre los activos críticos RO1.4 Prácticas de seguridad actuales RO1.5 Vulnerabilidades organizativas actuales
Fase 2: **Visión tecnológica**	RO2.1 Componentes clave RO2.2 Vulnerabilidades tecnológicas actuales
Fase 3: **Estrategia y desarrollo del plan**	RO3.1 Riesgos sobre activos críticos RO3.2 Medidas contra los riesgos RO3.3 Estrategia de protección RO3.4 Planes de mitigación del riesgo

También podemos resumir las fases del proceso OCTAVE en el siguiente gráfico:

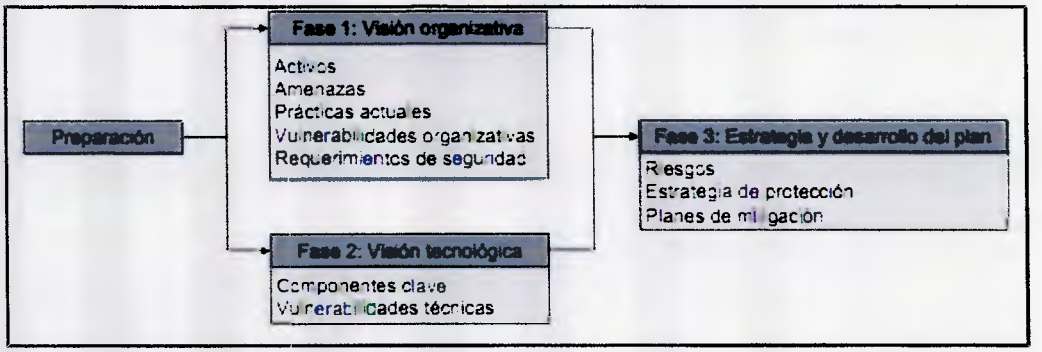


Figura 13: Fases del Proceso OCTAVE

Para cada metodología se define un conjunto de procesos diferente adaptado a las necesidades particulares, siempre cumpliendo todos los criterios. Los procesos de cada una de las metodologías los podemos ver en la siguiente tabla:

OCTAVE	Fase 1 Visión organizativa	Identificar conocimiento de la alta dirección Identificar conocimiento de la dirección de áreas operativas Identificar conocimiento del personal de áreas operativas y de TI Crear perfiles de amenazas
	Fase 2: Visión tecnológica	Identificar componentes clave Evaluar componentes seleccionados
	Fase 3: Estrategia y desarrollo del plan	Analizar los riesgos Diseñar la estrategia de protección
	Fase 1	Identificar información organizativa

OCTAVE-S	Visión organizativa	Crear perfiles de amenazas
	Fase 2: Visión tecnológica	Examinar la infraestructura tecnológica relacionada con los activos críticos
	Fase 3: Estrategia y desarrollo del plan	Analizar los riesgos Diseñar la estrategia de protección y planes de mitigación
OCTAVE Allegro	Fase 1: Establecer dirección	Establecer criterios de valoración de riesgos
	Fase 2 Perfilar activos	Desarrollar perfiles de activos de información Identificar recursos de información
	Fase 3 Identificar amenazas	Identificar áreas de interés para el análisis Identificar escenarios de amenazas
	Fase 4 Identificar y mitigar riesgos	Identificar riesgos Analizar riesgos Seleccionar enfoque de mitigación

Tabla 3: Procesos de las Metodologías OCTAVE (Fuente Propia)

II.30.CRAMM – CCTA RISK ANALYSIS AND MANAGEMENT METHOD

CRAMM es una metodología de análisis de riesgos desarrollada en Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Comenzó a desarrollarse en la década de 1980 y actualmente está en su versión 5.1. Es el método de análisis de riesgos preferente en Organismos de la Administración Pública británica (Telecommunications Agency, 2003).

Pese a tratarse de una iniciativa del Sector Público, el mantenimiento y la gestión de la metodología lo realiza una empresa privada de consultoría, Insight Consulting, actualmente integrada en Siemens.

El modelo de análisis y gestión de riesgos de CRAMM puede resumirse en el siguiente gráfico:

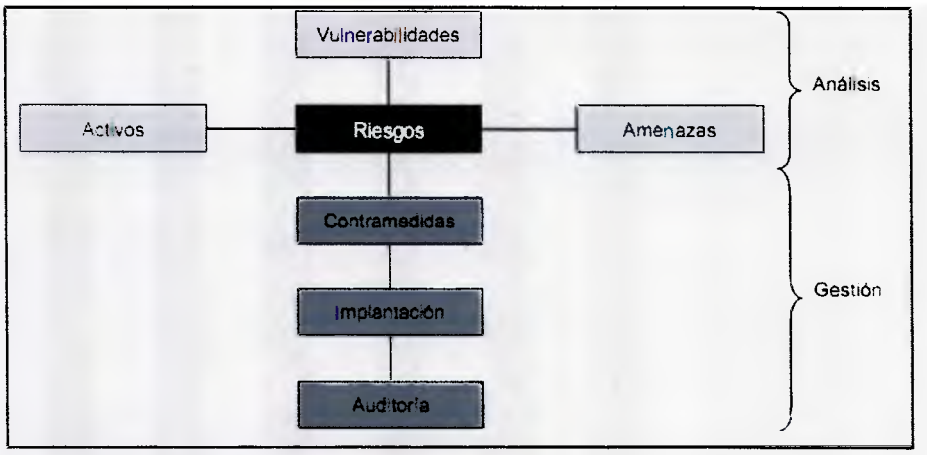


Figura 14: Modelo de Análisis y Gestión de Riesgos de CRAMM

Uno de los aspectos principales de CRAMM es el soporte que proporciona la herramienta informática que la soporta, con una base de datos de:

- Más de 400 tipos de activos
- Más de 25 tipos de impacto
- 38 tipos de amenaza
- 7 tipos de medida del riesgo
- Más de 3.500 salvaguardas.
- Actualmente CRAMM soporta tres tipos de revisiones:
- CRAMM Express
- CRAMM Expert
- BS7799

Adicionalmente existen variantes para la gestión de riesgos en proyectos de desarrollo, con una interfaz al ciclo de vida estándar utilizado por la Administración Pública británica: SSADM (Structured System Analysis and Design Method).

La metodología CRAMM define tres fases para la realización del análisis de riesgos, las cuales podemos observar en la siguiente tabla:

Fase 1: Establecimiento de objetivos de seguridad	-Definir el alcance del estudio. -Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación. -Identificar y evaluar los activos físicos que forman parte del sistema. -Identificar y evaluar los activos de software que forman parte del sistema.
Fase 2: Evaluación de riesgos	-Identificar y valorar el tipo y nivel de las amenazas que pueden afectar al sistema. -Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas. -Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.
Fase 3: Identificación y selección de contramedidas	-Los principales productos de la metodología CRAMM son: -Documento de inicio del proyecto -Informes de análisis de riesgos -Informes de gestión de riesgos, basados en una base de datos de más de 3.500 salvaguardas técnicas y organizativas. -Plan de implantación

Figura 15: Fases de CRAMM

Las principales actividades del proceso de análisis y gestión de riesgos de CRAMM se resumen en el siguiente gráfico:

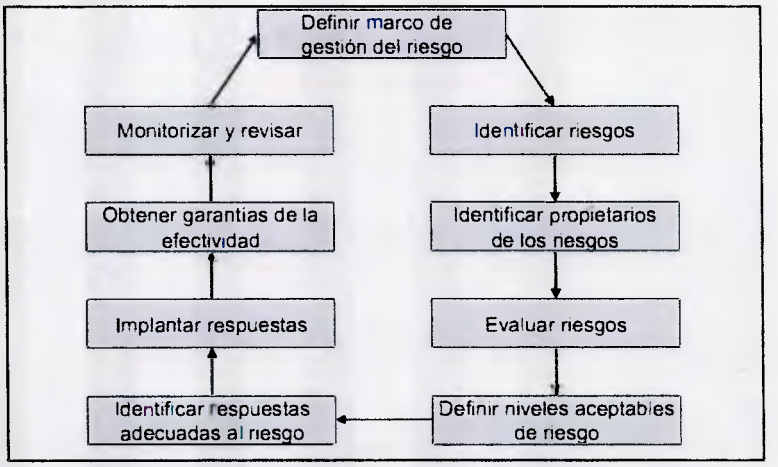


Figura 16: Principales Actividades de Análisis y Gestión CRAMM

II.31.NIST SP 800-30 GUÍA DE GESTIÓN DE RIESGOS PARA SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN

El NIST (National Institute of Standards and Technology) ha dedicado una serie de publicaciones especiales, la SP 800 a la seguridad de la información. Esta serie incluye una metodología para el análisis y gestión de riesgos de seguridad de la información, alineada y complementaria con el resto de documentos de la serie. El proceso de análisis de riesgos definido en la metodología NIST SP 800-30 puede resumirse en el siguiente gráfico (Stoneburner G., 2002):

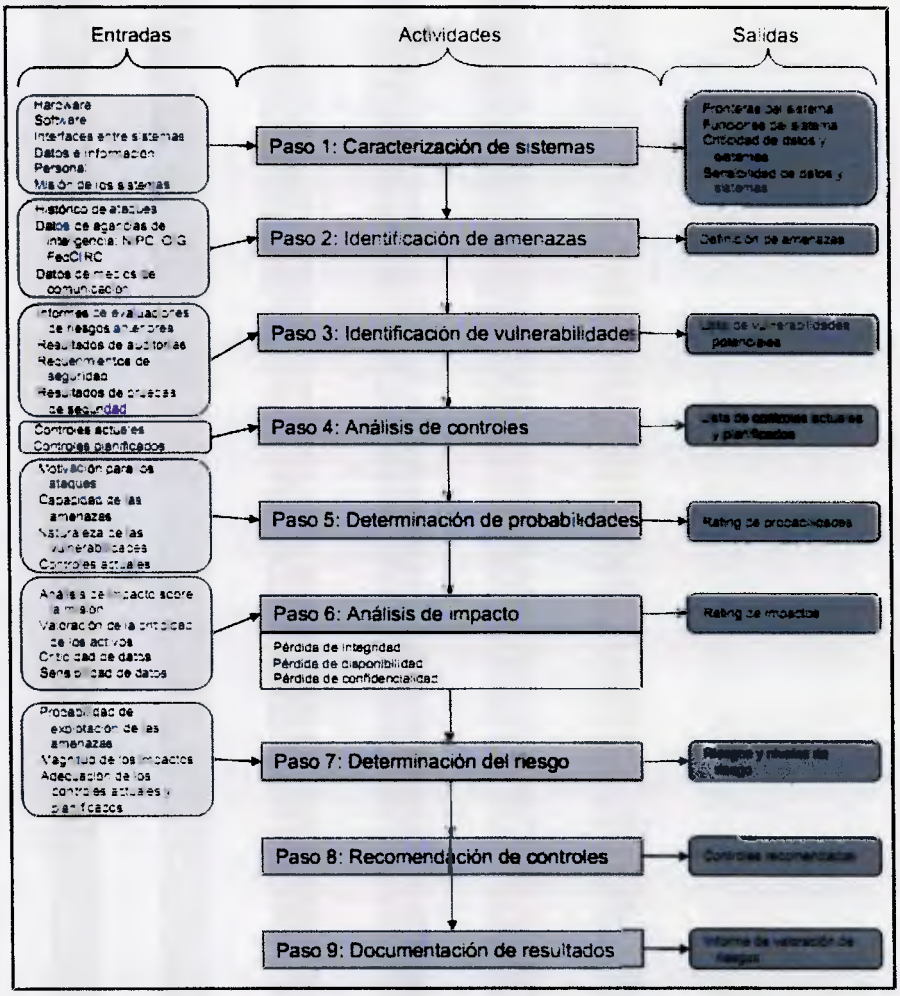


Figura 17: Proceso de Análisis de Riesgos de NIST SP 800-30

El proceso de gestión de riesgos definido en la metodología NIST SP 800-30 puede resumirse en el siguiente gráfico:

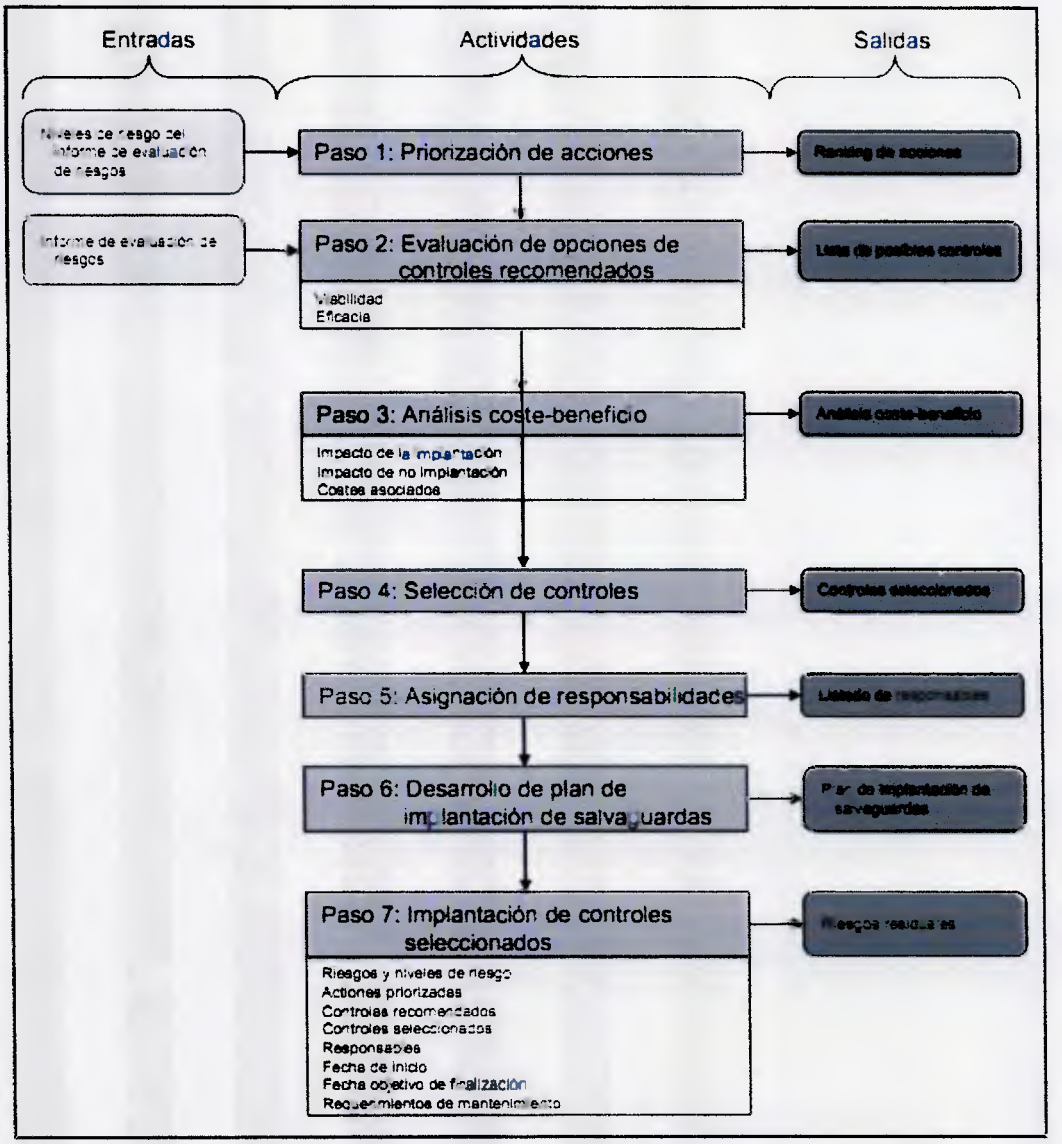


Figura 18: Proceso de Gestión de Riesgos de NIST SP 800-30

II.32.IRAM – INFORMATION RISK ANALYSIS METHODOLOGIES

El ISF es una organización sin ánimo de lucro de ámbito internacional que desarrolla de forma colaborativa recomendaciones y herramientas de seguridad para sus miembros. Entre las principales preocupaciones del ISF se encuentra el análisis y la gestión de riesgos, y por ello ha desarrollado y publicado diversas metodologías y modelos de análisis de riesgos a lo largo del tiempo (ISF – Information Security Forum, 2006)

- SPRINT (Simplified Process for Risk Identification): Análisis de riesgos para una aplicación informática importante pero no crítica.
- SARA (Simple to Apply Risk Analysis): Análisis de riesgos para una aplicación informática crítica.
- FIRM (Fundamental Information Risk Management): Evaluar riesgos en un entorno heterogéneo dentro de un ciclo regular de monitorización.

La metodología actual de análisis y gestión de riesgos del ISF es IRAM, y está alineada con el resto de proyectos del ISF, y en particular con:

Estudio bienal de amenazas de seguridad (ISF Information Security Status Survey) (ISF – Information Security Forum, 2006)

Manual de buenas prácticas de seguridad de la información (The Standard of Good Practice for Information Security), que incluye un inventario de más de 3.200 salvaguardas. (ISF – Information Security Forum, 2007)

IRAM consta de tres fases principales:

Fase 1:	Análisis de impacto sobre el negocio (BIA): Soportada por la herramienta BIA Assistant.
Fase 2:	Evaluación de amenazas y vulnerabilidades: Soportada por la herramienta T&VA Assistant.
Fase 3:	Selección de controles: Soportada por la herramienta CS Assistant.

Las tres herramientas han sido migradas del entorno microinformático original a un entorno web en una nueva herramienta integrada: IRAM Risk Analyst Workbench.

II.33.SOMAP – SECURITY OFFICERS MANAGEMENT AND ANALYSIS PROJECT

El Security Officers Management and Analysis Project (SOMAP) es una organización sin ánimo de lucro cuyo objetivo es desarrollar proyectos Open Source relacionados con la gestión de la seguridad de la información. (SOMAP – Security Officers Management & Análisis Project, 2006).

Actualmente, SOMAP tiene en marcha cuatro proyectos:

Open Governance, Risk & Compliance Maturity Management Methodology (OGRCM3) se centra en desarrollar una metodología para la medición y la gestión de riesgos. Está publicada la versión 1.0, que considera un proceso cíclico de cuatro fases:

- Alcance de cumplimiento
- Gestión y categorización de activos
- Medición y documentación del cumplimiento
- Evaluación y reporte
- Open Risk Model Repository (ORIMOR) se centra en desarrollar una base de datos que soporte el marco de referencia y la herramienta. Dispone de un repositorio de:
- Tipos de activos y dependencias entre ellos
- Vulnerabilidades
- Salvaguardas
- Relación entre activos, vulnerabilidades y salvaguardas.
- Relación entre vulnerabilidades y salvaguardas
- Cuestionarios

Está prevista la publicación periódica de informes con el contenido de la base de datos para su uso independiente de la herramienta de gestión (ver ORICO)

Algunas características relevantes de la herramienta son:

Uso de identificadores UUID (Universally Unique Identifier) según los estándares ISO/IEC 11578:1996 y DCE 1.1, para facilitar las actualizaciones y migraciones y el soporte multilenguaje.

La base de datos presente ser multilenguaje, considerando inicialmente el inglés y el alemán.

Uso de Open Source Vulnerability DataBase (OSVDB) para mantener actualizada permanentemente la base de datos.

Open Risk & Compliance Framework and Tool (ORICO) se centra en desarrollar un marco de referencia y una herramienta de soporte del modelo.

Actualmente se han publicado versiones beta, pero aún no se ha publicado ninguna versión estable.

El modelo de datos actual de ORIMOR es el siguiente:

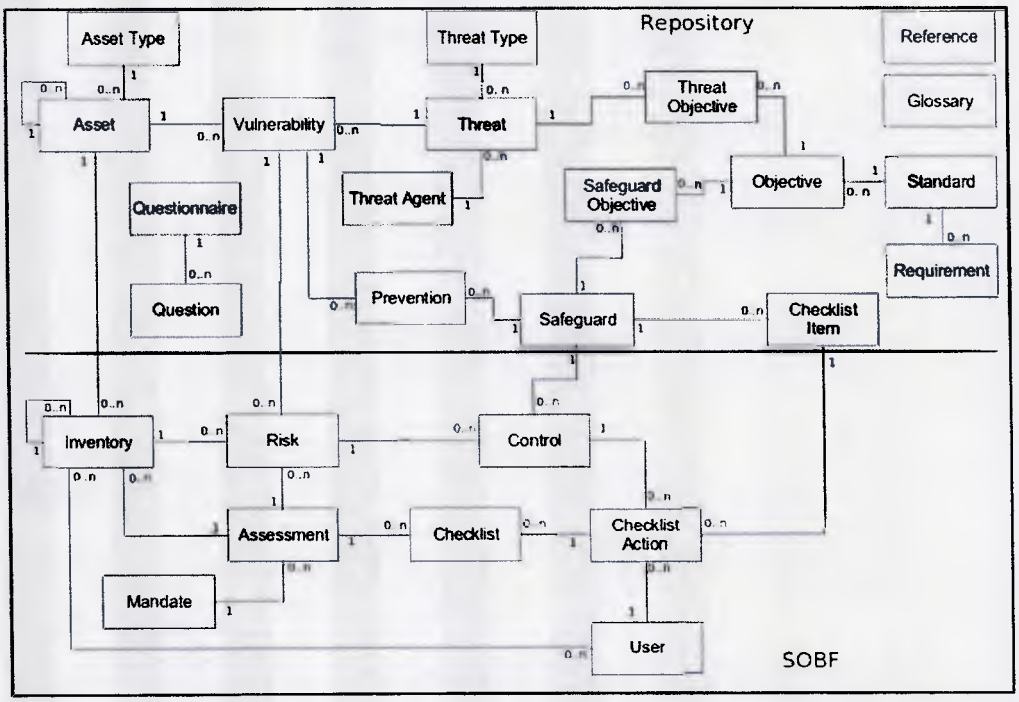


Figura 19: Modelo de Datos de SOMAP (ORIMOR)

II.34.OTROS TIPOS DE ANÁLISIS DE RIESGO

a) BASILEA, COMITÉ DE SUPERVISIÓN BANCARIA (BCBS)

El Comité de Supervisión Bancaria de Basilea (BCBS, por su nombre en inglés) fue creado a fines de 1974 por los países del Grupo de los Diez, y su denominación hasta 1990 fue la de Comité de Regulaciones y Prácticas Supervisoras Bancarias.

La finalidad de su creación fue la de coordinar la supervisión de los bancos internacionalmente activos. Se reúne trimestralmente y tiene cerca de 25 grupos de trabajo y fuerzas de tarea ("task forces") que se reúnen regularmente.

Los miembros del Comité son los siguientes países: Bélgica, Canadá, Francia, Alemania, Italia, Japón, Luxemburgo, Holanda, España, Suecia, Suiza, Reino Unido y los Estados Unidos de América. Lo componen altos representantes de los bancos centrales de los países, así como de la autoridad con responsabilidades formales de la supervisión prudencial de los negocios de los bancos, en donde no opera como tal el respectivo banco central.

El Comité tiene su secretaría en el Banco de Pagos Internacionales (BIS, por su nombre inglés), no es un organismo internacional, ni tiene personería jurídica propia, ni posee poderes formales de ningún tipo. Sus recomendaciones son aprobadas por los gobernadores presentes en el Banco Internacional de Pagos, y no tienen el carácter de norma internacional.

No obstante, las recomendaciones del Comité han tenido una influencia considerable en los países no miembros, por razón de la calidad de las propuestas y los análisis y la corriente de exigir a todos los países del mundo el

cumplimiento de códigos y estándares internacionalmente aprobados en muchas áreas de la vida económica (a través del FMI [3] y del Banco Mundial).

b) BASILEA II

Según (Soley & Rahnema, 2004) "es una normativa bancaria cuyo objetivo es mejorar la estabilidad, el funcionamiento y la trasparencia informativa de las entidades crediticias".

Basilea II está compuesta de tres pilares:

- Pilar 1 - Requerimientos mínimos de capital: contempla los riesgos de crédito, de mercado y operativo.
- Pilar 2 - El proceso de examen supervisor: contempla el proceso de evaluación de riesgos, de la suficiencia del capital y del entorno del control; riesgo de liquidez.
- Pilar 3 - La disciplina de mercado: define los requisitos de divulgación de información sobre el capital y la gestión de riesgos al mercado.

Los tres pilares se complementan y refuerzan mutuamente. Basilea II propone una nueva metodología y múltiples opciones para medir el riesgo de crédito. El documento propone dos alternativas para medir el riesgo crediticio de las entidades: una de carácter estándar y otra basada en la calificación interna (acronimo en ingles, Internal Rating-Based Approach, IRB-Approach).

La idea básica de Basilea es que los tres pilares deben funcionar conjuntamente, que no es posible basarse únicamente en uno o dos de ellos, sin tener presente el tercero. Las entidades tienen que tener un nivel mínimo de recursos propios (capital) calculados de acuerdo con el contenido del pilar 1; las autoridades supervisoras deben asegurarse de que, además, las entidades

[3] Fondo Monetario Internacional o FMI (en inglés: International Monetary Fund, IMF) fue creado en 1945, con el objetivo principal de promover políticas cambiarias sostenibles a nivel internacional, facilitar el comercio internacional y reducir la pobreza.

disponen de unos sistemas internos adecuados para calcular el "capital económico" necesario en relación con sus riesgos, independientemente del "nivel legal exigido", y deben ser capaces de analizar el perfil de riesgos de cada entidad, con la finalidad de conocer si el nivel de solvencia es el adecuado; éste es el Pilar 2. Finalmente, bancos y supervisores deben dar suficiente información al mercado para asegurar la disciplina emanante del mismo (Pilar 3), reforzando de esta manera los dos pilares anteriores.

(Soley & Rahnema, 2004) expresan lo siguiente de los pilares:

Pilar I: Requerimientos mínimos de capital

El nuevo acuerdo establece una metodología novedosa y múltiples opciones para medir el *riesgo de crédito*.

Existen dos enfoques diferentes para el cálculo de los requerimientos mínimos de recursos propios en Basilea II:

- Un enfoque estándar similar al actual con algunas modificaciones.
- Otro basado en "ratings internos".

El comité de Basilea propone un nuevo enfoque estandarizado para la ponderación del riesgo, basado en evaluaciones externas, teniendo en cuenta la calidad y la metodología de este tipo de fuente. Es decir, mantiene el sistema actual con algunas variaciones: el Comité propone por ejemplo, que para las empresas, se mantenga la ponderación general del 100 por 100, aunque puede aplicarse un porcentaje del 20 por 100 para aquellas corporaciones con un "rating internos". De AAA/AA- y un porcentaje del 150 por 100 con un ratings por debajo de B-. Lo que realmente es novedad en Basilea II es la aplicación de "rating internos" por parte de las entidades crediticias.

Para el tratamiento de otros riesgos tales como; el Riesgo Operacional es lo suficientemente importante para cuantificarlo e incorporarlo a los requerimientos de Recursos Propios.

A efectos del cálculo, la normativa de Basilea II (Comité de Basilea, 2003) propone tres métodos del más sencillo al más complejo para que las entidades se adecuen según su negocio y volumen:

- "Básico": Se calcula aplicando un coeficiente del 15 por 100 al margen ordinario de la entidad crediticia.
- "Estándar": División de la actividad de la entidad entre ocho líneas de negocios a cada una de las cuales asigna un coeficiente según desglose adjunto. El cálculo aplica cada coeficiente al margen ordinario de cada línea de negocio.
- "Avanzado": (Advanced Management Approach): El más complejo, que tiene en cuenta un conjunto cuantitativo y cualitativo de datos estadísticos en concepto de pérdidas operacionales esperadas y no esperadas de la entidad y que también incluye una gestión proactiva de los riesgos operacionales identificados. Por este método avanzado la entidad conseguirá también un menor consumo de recursos propios.

Pilar II: Revisión supervisora

El comité establece que el objetivo de los organismos supervisores al revisar el cumplimiento de los requerimientos mínimos de recursos propios es asegurar que las entidades bancarias dispongan de unos recursos propios consistentes con un perfil de riesgo y permitir detectar a tiempo situaciones que requieran una intervención. Para ello da unos poderes amplios a las autoridades bancarias.

El Comité ha identificado cuatro principios claves que se pueden resumir así:

Principio 1:	Los bancos deben tener un proceso que mida la suficiencia de su capital total en relación a su perfil de riesgo y una estrategia para mantener sus recursos propios a niveles adecuados.
Principio 2:	los supervisores deben examinar y evaluar las estrategia y valoraciones internas de la suficiencia de capital de los bancos, así como su capacidad para vigilar y asegurar la aplicación de los coeficientes de capital de supervisión. Los supervisores deben intervenir si no están satisfechos con el resultado de este proceso.

Principio 3:	Los supervisores deben esperar que los bancos operen por encima de los coeficientes mínimos de capital regulador y tener la capacidad de exigir a los bancos que los mantengan por encima de ese mínimo.
Principio 4:	Los supervisores deben procurar intervenir lo antes posible para evitar que el capital descienda por debajo de los niveles mínimos necesarios para cubrir las características de riesgo de un banco y exigir una acción correctiva inmediata cuando el capital no esté en el nivel requerido.

Pilar III: Informe al mercado

El Comité opina que una divulgación completa es esencial para que los participantes del mercado comprendan la relación entre el perfil de riesgo y el capital de una institución.

Por ello, la norma Basilea II (Comité de Basilea, 2003) hace especial referencia a que las entidades deben informar periódicamente de su estructura de recursos propios, de la suficiencia de los mismos y de la exposición al riesgo, así como de su sistema de gestión y evaluación por cuanto el dinamismo de los mercados puede cambiar el perfil de riesgo de las entidades.

c) INFORME COSO

El mencionado informe (Coopers & Lybrand, 1997) es un manual de control interno que publica el Instituto de Auditores Internos de España en colaboración con la empresa de auditoría Coopers & Lybrand. Se trata de un trabajo que encomendó el Instituto Americano de Contadores Públicos, la Asociación Americana de Contabilidad, el Instituto de Auditores Internos que agrupa a alrededor de cincuenta mil miembros y opera en aproximadamente cincuenta países, el Instituto de Administración y Contabilidad y el Instituto de Ejecutivos Financieros.

La Finalidad del Informe COSO es establecer una definición común de control interno que responda a las necesidades de las distintas partes. Así como, facilitar un modelo en base al cual las empresas y otras entidades, cualquiera sea su tamaño y naturaleza, puedan evaluar sus sistema de control interno.

El Control Interno es un proceso efectuado por el directorio, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un

grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones
- Fiabilidad de la información financiera
- Cumplimiento de la leyes y normas aplicables

La definición anterior refleja ciertos conceptos fundamentales:

- El control interno es un proceso. Es un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- El control interno lo llevan a cabo las personas.
- No se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización.
- El control interno sólo puede aportar un grado de seguridad razonable, no la seguridad total a la dirección y al directorio.
- El control interno está pensado para facilitar la consecución de objetivos.

La estructura del control interno, propuesta por el modelo COSO, identifica cinco componentes interrelacionados:

- Ambiente de Control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Monitoreo

d) COBIT (Objetivos de Control para Tecnología de Información y Tecnologías Afines)

El COBIT definido (COBIT, 1998), es una herramienta de gobierno de las Tecnologías de la Información que ha cambiado de igual forma que lo ha hecho el trabajo de los profesionales de TI. La Asociación de Auditoría y Control para Sistemas de Información (ISACF), organización creadora de esta norma COBIT así como sus patrocinadores, han diseñado este producto principalmente como una fuente de instrucción para los profesionales dedicados a las actividades de control. La definición que ofrece el sumario ejecutivo del COBIT es la siguiente:

"COBIT busca, desarrolla, publica y promueve un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores".

Dicho de una forma menos formal, señalaremos que COBIT ayuda a salvar las brechas existentes entre los riesgos de negocio, necesidades de control y aspectos técnicos. Además, proporciona "prácticas sanas" a través de un marco referencial (Framework) de dominios y procesos, y presenta actividades en una estructura manejable y lógica. Las "prácticas sanas" del COBIT representan el consenso de los expertos (ayudarán a los profesionales a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo que serán juzgados si las cosas salen mal).

El tema principal que trata el COBIT es la orientación a negocios. Éste, está diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. De forma creciente, las prácticas de negocio comprenden la completa autorización de los procesos propios de negocio, con lo que poseen una total responsabilidad para todos los aspectos de dichos procesos.

La norma COBIT, proporciona una herramienta para los procesos propios de negocio que facilitan la descarga de esta responsabilidad. La norma parte con una simple y pragmática premisa: *En orden de proporcionar la información que*

la organización necesita para llevar a cabo sus objetivos, los requisitos de las tecnologías de la información necesitan ser gestionados por un conjunto de procesos agrupados de forma natural.

El desarrollo de COBIT ha resultado en la publicación de:

- un Resumen Ejecutivo el cual consiste en un Síntesis Ejecutiva (que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT) y el Marco Referencial (el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de TI);
- el Marco Referencial que describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de TI que son impactados en forma primaria por cada objetivo de control;
- Objetivos de Control, los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de TI;
- Guías de Auditoría, las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o una recomendaciones de mejoramiento;
- un Conjunto de Herramientas de Implementación, proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

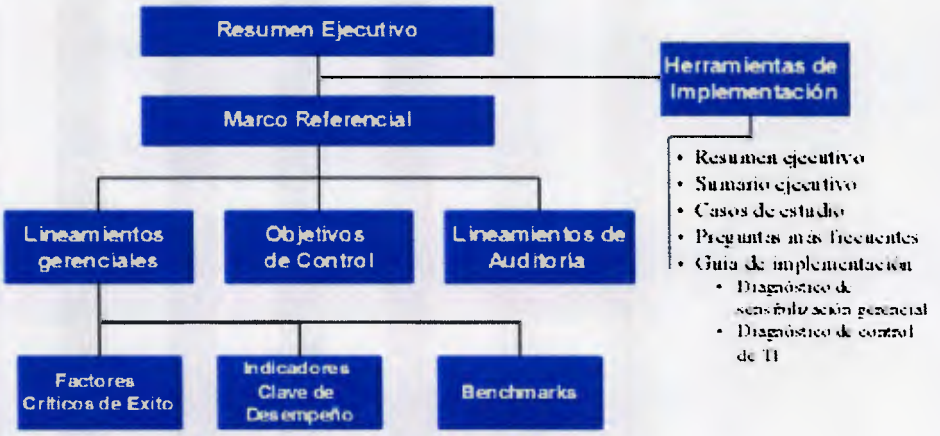


Figura 20: Estructura de los Componentes de COBIT

COBIT está diseñado para ser utilizado por tres audiencias distintas:

- Administración: Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.
- Usuarios: Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.
- Auditores de sistemas de información: Para dar soporte a las opiniones mostradas a la administración sobre los controles internos.

Además de responder a las necesidades de la audiencia inmediata de la Alta Gerencia, a los auditores y a los profesionales dedicados al control y seguridad, COBIT puede ser utilizado dentro de las empresas por el propietario de procesos de negocio en su responsabilidad de control sobre los aspectos de información del proceso, y por todos aquéllos responsables de TI en la empresa.

II.35. OTRAS METODOLOGÍAS

Adicionalmente a las metodologías descritas, existen otras que no se han analizado en detalle porque se han considerado de menor relevancia en el ámbito actual. Algunas de las metodologías descartadas por estos motivos han sido las siguientes:

- CORAS – COnstruct a platform for Risk Analysis of Security critical systems
- FAIR – Factor Analysis of Information Risk · FRAP/FRAAP (Facilitated Risk Analysis –and Assessment - Process),
- FRAP/FRAAP (Facilitated Risk Analysis –and Assessment - Process), metodología simplificada para el análisis de riesgos cualitativo basada en la realización de ejercicios de brainstorming por parte de un grupo de participantes de distintos perfiles complementarios. Su principal característica es la rapidez con la que puede aplicarse. Desarrollada por Peltier Associates.
- PARA (Practical Application of Risk Analysis)
- Austrian IT Security Handbook (sólo disponible en alemán)
- Dutch A&K Analysis (sólo disponible en holandés)
- Ebios (Expression des Besoins et Identification des Objectifs de Sécurité), publicada por la Administración Pública francesa. Incorpora una herramienta de soporte.
- IT-Grundschutz (IT Baseline Protection Manual), publicada por la Administración Pública alemana. Soportado por la herramienta GSTool.
- Mehari, publicada por el Club Francés de Seguridad de la Información.
- ARiES (Aerospace Risk Evaluation System)
- STIR (Simple Technique for Illustrating Risk)

- CORA (Cost-Of-Risk Analysis)
- ISRAM (Information Security Risk Analysis Method)

II.36. Generalidades de las Metodologías de Análisis y Gestión de Riesgos.

A pesar de que existe un elevado número de metodologías de análisis de riesgos, que se describen en esta sección, existe un modelo y unos principios básicos comunes a todas ellas que se describen a continuación.

La base sobre la que se apoyan las metodologías actuales de análisis de riesgo es el cálculo de probabilidades, según la secuencia que se describe a continuación.

II.37. Elementos Comunes

Las metodologías de análisis y gestión de riesgos parten de la necesidad de identificar formalmente los elementos a proteger. Estos elementos se recogen en un inventario de *activos* de información, considerando como tales aquellos elementos que tienen valor para la Organización. (López F., Amutio. M. 2006)

Los activos deben valorarse en función de un conjunto de requerimientos. Estos requerimientos varían entre las diferentes metodologías, si bien existe consenso sobre tres de ellas: confidencialidad, integridad y disponibilidad. Esto significa que para cada activo de información debe valorarse de forma independiente el costo que tendría para la Organización una pérdida total de su confidencialidad, de su integridad y de su disponibilidad, así como de los otros requerimientos de seguridad que se consideren en cada caso. (López F., Amutio. M. 2006)

Una vez identificados los activos, deben identificarse las *amenazas* que pueden causar pérdidas sobre estos activos, teniendo en cuenta los diferentes requerimientos de seguridad. Algunas metodologías especifican un elemento intermedio, las *vulnerabilidades*, consideradas como las debilidades que hacen que un determinado activo pueda ser vulnerable a una determinada amenaza. (Christopher J. Alberts, OCTAVE-S Implementation Guide)

Identificadas las amenazas, debe identificarse las *salvaguardas* que permiten proteger a los activos de las diferentes amenazas. (Telecommunications Agency, 2003).

La cuantificación de los distintos elementos que forman parte del modelo de análisis de riesgos se aborda en los siguientes apartados.

II.38. PÉRDIDA ESPERADA (SINGLE LOSS EXPECTANCY – SLE)

Considerando un único activo de información (A), un único requerimiento de seguridad (R) y una única amenaza (T) se puede estimar la pérdida económica esperada en caso de que la amenaza se realice. (Hansche S., 2004) (Harris, 2006)

Generalmente, la pérdida esperada no se representa en términos absolutos, sino como un porcentaje de degradación referido al valor total del activo para el requerimiento considerado. De esta forma, se puede considerar:

$$SLE(A, R, T) = Valor(A, R) \times Degradación(A, R, T)$$

Dado que la valoración se realiza generalmente respecto a diferentes requerimientos de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, etc.), la pérdida total debida a la realización de una amenaza sobre un activo se calculará como la suma de las pérdidas en cada requerimiento:

$$SLE(A, T) = \sum_{R} SLE(A, R, T) = \sum_{R} Valor(A, R) \times Degradación(A, R, T)$$

Dado que existen diversos activos a los que puede afectar la amenaza considerada, la pérdida esperada total es la suma de la pérdida provocada en cada uno de los activos:

$$SLE(T) = \sum_{A} SLE(A, T) = \sum_{A} \sum_{R} Valor(A, R) \times Degradación(A, R, T)$$

II.39. PÉRDIDA ANUAL ESPERADA (ANNUAL LOSS EXPECTANCY – ALE)

Una vez conocida la pérdida provocada por la realización de cada amenaza, en caso de que ocurra, se debe considerar la probabilidad de que la amenaza se realice efectivamente en el periodo de un año. La pérdida anual esperada provocada por una amenaza puede definirse, por tanto, como (Hansche S., Guide to the CISSP Exam., 2004):

$$ALE(T) = P(T) \times SLE(T) = P(T) \times \sum_{A} \sum_{R} Valor(A, R) \times Degradación(A, R, T)$$

La pérdida anual esperada teniendo en cuenta todas las amenazas puede definirse, por tanto, como:

$$ALE = \sum_{T} P(T) \times SLE(T) =$$
$$= \sum_{T} \left(P(T) \times \sum_{A} \sum_{R} Valor(A, R) \times Degradación(A, R, T) \right)$$

El concepto de riesgo intrínseco se asocia habitualmente a la pérdida anual estimada, y se representa de forma equivalente como:

$$\text{Riesgo intrínseco} = \text{Frecuencia} \times \text{Impacto} =$$
$$= \text{Frecuencia} \times \text{Valor} \times \text{Degradación} = ALE$$

II.40. CÁLCULO DEL EFECTO DE LAS SALVAGUARDAS

Las salvaguardas (S) implantadas permiten reducir la frecuencia de ocurrencia de las amenazas o la degradación causada por ellas en caso de realizarse (Hansche S., Guide to the CISSP Exam., 2004) (López F., 2006).

Teniendo en cuenta la reducción de la frecuencia, se puede considerar P(S) la probabilidad de que una salvaguarda sea eficaz en la prevención de la ocurrencia de una amenaza determinada. Por tanto, puede considerarse que:

$$P(A/S_i) = P(A) \times (1 - P(S_i))$$

Dado el conjunto de salvaguardas implantadas, la probabilidad de ocurrencia puede calcularse como:

$$P(A/S) = P(A) \times \prod_{S} (1 - P(S))$$

Siendo P(S) la probabilidad de que la salvaguarda S sea eficaz mitigando la amenaza A. Considerando el concepto de frecuencia en lugar del de probabilidad, la frecuencia anual de ocurrencia se puede calcular como:

$$ARO' = ARO \times \prod_{S} (1 - P(S))$$

De forma análoga, se puede calcular la degradación una vez aplicadas las salvaguardas:

$$\text{Degradación}(A, R, T)' = \text{Degradación}(A, R, T) \times \prod_{S} (1 - I(S))$$

Donde I(S) es la reducción del impacto provocado por la acción de la salvaguarda S.

Por tanto, el cálculo del riesgo residual puede definirse como:

$$ALE = \sum_{T} \left[ARO(T) \times \prod_{S} (1 - P(S)) \times \sum_{A} \sum_{R} \text{Valor}(A, R) \times \text{Degradación}(A, R, T) \times \prod_{S} (1 - I(S)) \right]$$

Debido al elevado coste computacional de estos cálculos, algunas metodologías simplifican el cálculo definiendo un porcentaje fijo de reducción de la probabilidad y de la degradación para cada salvaguarda implantada. De esta forma:

$$ARO'' = ARO \times \sum_{T} \Delta P$$

$$\text{Degradación}(A, R, T)' = \text{Degradación}(A, R, T) \times \sum_{T} \Delta I$$

II.41. RELACIONES ENTRE LOS ACTIVOS

Los activos de información tienen relaciones de dependencia que afectan adicionalmente al cálculo de los riesgos. Para simplificar la notación, no se

tendrán en cuenta en este apartado los distintos requerimientos considerados en el análisis de riesgos (López F., 2006).

Dados dos activos A y B, de forma que el activo A depende del activo B, el valor del activo B (para cada uno de los requerimientos de seguridad considerados), a efectos del análisis de riesgos, puede incrementarse con el valor del activo A, debido a que la realización de una amenaza sobre el activo B no sólo provocará la degradación correspondiente del activo B, sino también una degradación proporcional en el activo A. Esto se conoce como Valor acumulado.

$$\text{Valor acumulado}(B) = \text{Valor}(B) + \text{Valor}(A)$$

Considerando adicionalmente que la dependencia entre los activos puede no ser total, sino estar expresada en forma de un porcentaje, queda:

$$\text{Valor acumulado}(B) = \text{Valor}(B) + \text{Valor}(A) \times \text{Dependencia}(A, B)$$

En caso de realizarse una amenaza T sobre el activo B, las pérdidas podrían estimarse como el impacto sobre B más el impacto sobre A soportado por B:

$$SLE'(B) = SLE(B) + SLE(A)$$

$$\begin{aligned} \mathbf{SLE'(B)} = \; & \text{Valor}(B) \times \text{Impacto}(B, T) + \\ & + \text{Dependencia}(A, B) \times \mathbf{Valor(A)} \times \text{Impacto}(B, T) \end{aligned}$$

$$SLE'(B) = (\text{Valor}(B) + \text{Dependencia}(A, B) \times \text{Valor}(A)) \times \text{Impacto}(B, T)$$

El riesgo total de B puede estimarse como la suma entre el riesgo propio de B más el riesgo de A soportado por B:

$$\begin{aligned} \text{Riesgo}(B) = \; & (\text{Valor}(B) + \text{Dependencia}(A, B) \times \text{Valor}(A)) \times \\ & \times \text{Impacto}(B, T) \times P(B, T) \end{aligned}$$

De forma análoga, dado el mismo caso de dos activos A y B, siendo A dependiente de B en cierto porcentaje, y dada una determinada amenaza T, el efecto de la realización de la amenaza sobre el activo A debe tener en cuenta

también la dependencia del activo B. De esta forma, se puede considerar el cálculo del riesgo total sobre A como el riesgo intrínseco más el riesgo repercutido por B:

$$\text{Riesgo}(A) = \text{Riesgo}(A) + \text{Riesgo Repercutido}(B)$$

$$\begin{aligned}\text{Riesgo}(A) = \; & P(A,T) \times \text{Valor}(A) \times \text{Impacto}(A,T) + \\ & + \text{Dependencia}(A,B) \times P(B,T) \times \text{Valor}(A) \times \text{Impacto}(B,T)\end{aligned}$$

$$\begin{aligned}\text{Riesgo}(A) = \; & \text{Valor}(A) \times (P(A,T) \times \text{Impacto}(A,T) + \\ & + \text{Dependencia}(A,B) \times P(B,T) \times \text{Impacto}(B,T))\end{aligned}$$

El cálculo de los distintos parámetros acumulados o repercutidos cobra interés especialmente en la obtención de resultados parciales del análisis, teniendo en cuenta sólo un determinado activo o una determinada amenaza.

II.42. MÉTODOS CUALITATIVOS

Los conceptos desarrollados hasta ahora muestran los principios básicos para un análisis de riesgos cuantitativo, basado en el cálculo de pérdidas en términos monetarios.

La valoración de los diferentes requerimientos de seguridad puede realizarse de forma cuantitativa o cualitativa [ISC2.04] [MAGE06]:

La valoración cuantitativa supone establecer un valor numérico para cada uno de los requerimientos de seguridad. Este valor se calcula en términos de las pérdidas esperadas en caso de incumplimiento de dicho requerimiento. Los principales conceptos de pérdidas a tener en cuenta en una valoración cuantitativa incluyen los siguientes:

- Coste de reposición de los activos y recursos de información perdidos: adquisición, instalación, recuperación, etc.
- Coste de mano de obra invertida en recuperar y/o reponer los activos y recursos de información.

- Lucro cesante debido a la pérdida de ingresos provocada por la parada degradación del funcionamiento de los diferentes procesos afectados.
- Capacidad de operar, debido a la pérdida de confianza de los clientes y proveedores, que se traduce en una pérdida de actividad o en peores condiciones económicas.
- Sanciones y penalizaciones por incumplimiento de la ley u obligaciones contractuales.
- Daños medioambientales.
- Daños reputacionales: percepción del mercado, pérdida de clientes, dificultad para acceder al crédito, coste de las campañas de marketing necesarias para recuperar la reputación perdida, etc.
- Valor de los secretos desvelados: secreto industrial, secreto comercial, etc.

La valoración cualitativa supone asignar un valor de una escala definida para cada uno de los requerimientos de seguridad. Este valor se calcula en base a un conjunto de características que define cada una de las categorías de la escala, basadas en las descritas para la valoración cuantitativa.

La valoración cuantitativa es más precisa, pero supone un mayor esfuerzo y dificultad, por la necesidad de valorar los distintos conceptos de pérdida en términos generalmente económicos.

Debido a la dificultad y el coste de realizar un análisis cuantitativo, muchas metodologías de análisis de riesgos han desarrollado enfoques cuantitativos, que permiten ubicar el riesgo en una escala de órdenes de magnitud. Este análisis se conoce como análisis cualitativo.

Los principios del análisis cualitativo son los mismos que los del análisis cuantitativo, sustituyendo los cálculos aritméticos por la aplicación de tablas. De esta forma, considerando que el valor de los activos y la degradación causada

por una determinada amenaza están valorados en una escala de tres niveles (Alto, Medio, Bajo), y dado que:

Impacto = Valor x Degradación

Se puede estimar el orden de magnitud del impacto utilizando la siguiente tabla:

Impacto		Degradación		
		Baja	Media	Alta
Valor	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto

Tabla 4: Cálculo Cualitativo del Impacto

De forma análoga al impacto, el riesgo puede definirse como:

Riesgo = Frecuencia x Impacto

Y puede calcularse con la siguiente tabla:

Riesgo		Impacto		
		Bajo	Medio	Alto
Probabilidad	Baja	Bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Alto

Tabla 5: Cálculo Cualitativo del Riesgo

La elaboración de las tablas puede variar en función de las diferentes metodologías o necesidades de cada análisis. A continuación se muestran dos ejemplos de tablas utilizando las funciones máximo, mínimo y media:

Mínimo		Parámetro 2		
		Bajo	**Medio**	**Alto**
Parámetro 1	**Bajo**	Bajo	Bajo	Bajo
	Medio	Bajo	Medio	Medio
	Alto	Bajo	Medio	Alto

Tabla 6: Cálculo Cualitativo Mediante la Función Mínimo

Máximo		Parámetro 2		
		Bajo	**Medio**	**Alto**
Parámetro 1	**Bajo**	Bajo	Medio	Alto
	Medio	Medio	Medio	Alto
	Alto	Alto	Alto	Alto

Tabla 7: Cálculo cualitativo Mediante la Función Máximo

Media		Parámetro 2		
		Bajo	**Medio**	**Alto**
Parámetro 1	**Bajo**	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto

Tabla 8: Cálculo Cualitativo Mediante la Función Media

II.43. MÉTODOS MIXTOS

Debido a que los métodos cuantitativos y cualitativos tienen ventajas e inconvenientes, existen alternativas para combinar ambos métodos de forma que se obtengan las mayores ventajas de cada uno. Esos métodos que presentan algunas características de los métodos cuantitativos y otras características de los métodos cualitativos se denominan métodos mixtos [ISC2.04].

II.44. DIMENSIONES DE LAS METODOLOGÍAS DE ANÁLISIS Y GESTIÓN DE RIESGO

Por la gran dimensión de riesgos que existen en las diferentes áreas de negocio, se desarrollan diferentes métodos para realizar una eficaz gestión y análisis de riesgos, podemos observar un resumen de las principales metodologías clasificadas por nombre, descripción y tipo de análisis (cualitativo, cuantitativo y mixto) en la siguiente tabla:

Leyenda: ● Completo ◕ Amplio ◑ Satisfactorio ◔ Pobre ○ No tiene

Nombre - Año - País	Origen				
	Descripción	Organización	Tipo de Análisis		
			Cuant.	Cualt.	Mixto
ISO TR 13335:1997 Internacional Suiza	Tecnología de la información – Guías para la gestión de la seguridad de las TI Gestión de Riesgo de Seguridad de Información	ISO	◑	●	◑
ISO 27005:2008 Suiza	Tecnologías de la información – Gestión de Riesgo de Seguridad de Información	ISO	◑	●	◑
UNE 71504:2008 España	Metodología de análisis y gestión de riesgos para los sistemas de información	AENOR	◔	◔	○
MAGERIT 2006 España	Metodología de Análisis y Gestión de Riesgos de IT	Ministerio de Administraciones Públicas	◑	●	◑
BS 7799-3:2006 Reino Unido	Sistemas de Gestión de Seguridad de la Información – Parte 3: Guías para la gestión de riesgos de seguridad de la información	BSI	●	●	●

Tabla 9: Principales Metodologías por Tipo de Análisis de Riesgos

Nombre - Año - País	Origen				
	Descripción	Organización	Tipo de Análisis		
			Cuant.	Cualt.	Mixto
AS/NZS 4360:2004 Australia / Nueva Zelanda	Gestión de riesgos	AS/NZS	●	●	○
OCTAVE 2001 - 2007 EEUU	Operationally Critical Threat, Asset and Vulnerability Evaluation	Universidad de Carnegie Mellon	◑	◑	◑
CRAMM 2003 Reino Unido	CCTA Risk Analysis and Management Method	CCTA - Central Computing and Telecommunications Agency23	●	●	○
NIST SP 800 – 30 2002 EEUU	Guía de gestión de riesgos para sistemas de tecnología de información	NIST - National Institute of Standards and Technology	●	●	○
SOMAP Beta Suiza	Security Officers Management & Analysis Project	SOMAP.org Internacional	●	●	○
FAIR 2005 EEUU	Factor Analysis of Information Risk	Risk Management Insight	●	●	●

Tabla 10:Origen y Tipo de Análisis de las Metodologías de Análisis y Gestión de Riesgos

También se puede clasificar a las metodologías por el tipo de riesgo (Intrínseco, Efectivo y Residual) y su inventario (Tipo de Recurso, Vulnerabilidad, Amenaza y Salvaguarda):

Nombre	Inventarios				Tipo de Riesgo		
	TR	V	A	S	Intr.	Efec.	Resi.
ISO TR 13335:1997	○	●	●	●	○	●	◔
ISO 27005:2008	●	●	●	●	○	●	◔
UNE 71504:2008	○	○	○	○	●	●	◔
MAGERIT	●	○	●	◕	●	●	○
BS 7799-3:2006	●	●	●	●	○	●	◔
AS/NZS 4360:2004	○	○	◑	◑	○	●	◔
OCTAVE 2001	●	●	●	●	○	●	◔
CRAMM	●	●	●	●	●	●	○
NIST SP 800 – 30	●	●	●	●	○	●	◔
SOMAP	●	●	●	●	○	●	◔
FAIR	○	○	●	●	○	●	○

Tabla 11:Metodologías de Análisis y Gestión de Riesgos por Inventario y Tipos de Riesgo

A continuación una clasificación por los elementos del modelo (Proceso, Activos, Recursos, Dependencias, Vulnerabilidades, Amenazas y Salvaguardas):

Nombre	Elementos del Modelo						
	P	A	R	D	V	A	S
ISO TR 13335:1997	○	◑	●	◑	●	●	●
ISO 27005:2008	○	●	●	●	●	●	●
UNE 71504:2008	○	●	○	●	○	●	●
MAGERIT	○	●	○	●	○	●	●
BS 7799-3:2006	●	●	●	●	●	●	●
AS/NZS 4360:2004	●	●	●	●	●	●	●

Nombre	Elementos del Modelo						
	P	A	R	D	V	A	S
OCTAVE 2001	●	●	●	●	●	●	●
CRAMM	○	●	○	●	●	●	●
NIST SP 800 – 30	○	○	●	○	●	●	●
SOMAP	○	○	●	●	●	●	●
FAIR	○	◑	●	○	●	●	●

Tabla 12:Metodologías de Análisis y Gestión de Riesgos por Elementos del Modelo

La siguiente es una clasificación por los objetivos de seguridad (Confidencialidad, Integridad, Disponibilidad, Autenticidad, Trazabilidad y Otros:

Nombre	Objetivos de Seguridad					
	C	I	D	A	T	O
ISO TR 13335:1997	●	●	●	●	●	Fiabilidad
ISO 27005:2008	●	●	●	●	●	Fiabilidad
UNE 71504:2008	●	●	●	◑	◑	◑
MAGERIT	●	●	●	●	●	○
BS 7799-3:2006	●	●	●	○	○	○
AS/NZS 4360:2004	●	●	●	○	○	○
OCTAVE 2001	●	●	●	○	○	○
CRAMM	●	●	●	○	○	○
NIST SP 800 – 30	●	●	●	○	○	○
IRAM	●	●	●	○	○	○
CORAS	◔	◔	◔	◔	◔	◔
SOMAP	●	●	●	●	●	●
FAIR	●	●	●	○	○	Mal Uso Divulgación

Tabla 13:Metodologías de Análisis y Gestión de Riesgos por Objetivos de Seguridad

Capítulo III

Marco Metodológico

"Es importante aprender métodos y técnicas de investigación, pero sin caer en un fetichismo metodológico. Un método no es una receta mágica. Más bien es como una caja de herramientas, en la que se toma la que sirve para cada caso y para cada momento"

Ander-Egg

CAPÍTULO III

MARCO METODOLÓGICO

Una vez revisada las bases teóricas y los antecedentes se procede en este capítulo a describir los métodos, técnicas y procedimientos aplicados del cómo se realiza la investigación, además se mencionan las razones de selección de la modalidad y tipo de investigación.

III.1.MODALIDAD, DISEÑO Y TIPO DE INVESTIGACIÓN

Este trabajo se enmarcara en la modalidad de Proyecto Factible que según el Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Experimental Libertador (UPEL, 2005):

> *"El Proyecto Factible consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El Proyecto debe tener apoyo en una investigación de tipo documental, de campo o un diseño que incluya ambas modalidades. (p. 16)."*

Aunque el método científico es uno, existen diversas formas de identificar su práctica o aplicación en la investigación. De modo que la investigación se puede clasificar de diversas maneras. Una de las formas más común de clasificar las investigaciones es aquella que las divide en exploratorias, descriptivas, correlaciónales y experimentales. Hay autores que la clasifica en cuatro tipos: básica, aplicada, documental, de campo o mixta. Para el presente estudio se ubicó el tipo de investigación en:

De Campo, porque los datos de interés serán recogidos en forma directa de la realidad de la SUDEBAN; partiendo la investigación desde datos primarios y originales. Según Cazares y otros (Cazares, 1991) la definen como:

> *"Aquella en que el mismo objeto de estudio sirve como fuente de información para el investigador. Consiste en la observación, directa y en vivo, de cosas, comportamiento de personas, circunstancias en que ocurren ciertos hechos; por ese motivo la naturaleza de las fuentes determina la*

manera de obtener los datos. Las técnicas usualmente utilizadas en el trabajo de campo para el acopio de material son: la encuesta, la entrevista, la grabación, la filmación, la fotografía, etc."

Documental, debido a que se han encontrado pocas evidencias de trabajos que apoyen la investigación, de acuerdo con Cazares y otros (Cazares, 1991),

> *"La investigación documental depende fundamentalmente de la información que se recoge o consulta en documentos, entendiéndose este término, en sentido amplio, como todo material de índole permanente, es decir, al que se puede acudir como fuente o referencia en cualquier momento o lugar, sin que se altere su naturaleza o sentido, para que aporte información o rinda cuentas de una realidad o acontecimiento."*

En cuanto al diseño de la investigación se centra en un diseño no experimental. Según Sampieri y otros (Roberto, Carlos, & Pilar, 1991) describen el diseño no experimental como: "aquel en que no se construye ninguna situación, sino que se observan situaciones ya existentes, no provocado intencionalmente por el investigador (p. 189)".

III.2. POBLACIÓN Y MUESTRA

De acuerdo a (Morles; 1994), la población o universo se refiere,

> *"al conjunto real por el cual serán válidas las conclusiones que se obtengan; a los elementos o unidades (personas, instituciones o cosas) a las cuales se refiere la investigación." (p. 17)*

Para efectos de este estudio se considera como población al personal de la Gerencia de Riesgo Tecnológico de la Superintendencia de las Instituciones del Sector Bancario conformado por 38 funcionarios, que se encuentran clasificados por cargos y un promedio de experiencia de la siguiente forma:

Cargo	Cantidad	Años de Experiencia
Gerente y Coordinador	2	16
Especialistas	4	10
Analistas III	8	6
Analistas I y II	11	4
Asistentes	3	2

Tabla 14: Clasificación por Cargo GRT

La investigación se realizo en la Gerencia de Riesgo Tecnológico de la empresa, se selecciono como muestra a los gerentes, coordinadores, especialistas y analistas III debido a sus años de experiencia y conocimientos en el área, esto con el propósito de recolectar la información necesaria a través de las entrevistas abiertas.

III.3. DEFINICIÓN DE LAS VARIABLES

Las variables a continuación forman los elementos comunes y los fundamentos teóricos de las metodologías mencionadas en el capitulo anterior, el sistema de variables de la investigación consiste en una serie de características, definidas de manera operacional.

Variable	Conceptualización	Dimensión	Indicador
Modelo de Riesgo Tecnológico	Proceso que indica los pasos a seguir para el análisis y gestión del riesgo tecnológico.	Fases del modelo	1-Definición de políticas y normas 2 -Definición de alcance de las áreas 3 -Análisis de riesgos 4 –Gestión del riesgo 5 -Selección de las instrucciones o recomendaciones
Madurez	Atributo que hace referencia a las instituciones que desarrollan o mantienen sistemas de software, siguiendo procesos de los cuales pueden estar definidos, implantados y medidos.	Nivel de madurez de la entidades	1= Inicial 2 = Gestionado 3 = Definido 4=Gestionado Cuantitativamente 5 =Optimizado
Capacidad	Atributo de los procesos, indica si solo se ejecuta, o si también se planifica, se encuentra formalmente definido y se mide y mejora de forma sistemática.	Nivel de capacidad de los procesos	0= Incompleto 1= Ejecutado 2= Gestionado 3= Definido 4=Cuantitativamente Gestionado 5= Optimizado
Dominio	Es la limitación de las áreas de control con el fin de alcanzar unos objetivos específicos.	Nombre de las áreas de control	Planeación Estratégica. Operaciones SI Proveedores Externos. Seguridad de la Inf. Continuidad del Negocio. Mantenimiento e Implantación de los SI. Base de Datos Soporte de Red Banca Electrónica

Variable	Conceptualización	Dimensión	Indicador
Activo	Recursos que posee o usa la organización, ubicados en las áreas de control evaluadas, necesarios para que las Entidades funcionen correctamente y alcancen los objetivos propuestos por la alta gerencia.	Equipamiento y Suministros Personal Edificación y Mobiliario Hardware Software Comunicaciones Datos Soporte Funciones de la Organización	10= El valor más alto, el daño más alto 7-9= el valor más grande / el daño más grave que suele darse en servicios civiles o de la administración pública 5-6= cuando las consecuencias no afectan a otras organizaciones externas 1-3= consecuencias limitadas, de carácter interno 0= insignificante - puede ser obviado a todos los efectos prácticos
Amenaza	Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o perdidas inmateriales en sus activos.	Causas de la Amenaza	No Humana Humanas Involuntarias Humanas Intencionales con presencia física Humanas Intencionales con origen remoto
Vulnerabilidades	Es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.	Distancia entre la amenaza (potencial) y su materialización como agresión real sobre el activo. Frecuencia histórica.	Probabilidad de Ocurrencia
Impactos	Es la materialización de una amenaza sobre un activo.	Gravedad Intrínseca del resultado.	Muy bajo (<1) Bajo (<10) Medio (<100) Alto (<1000) Muy Alto (>1000)

Variable	Conceptualización	Dimensión	Indicador
Controles	Permiten proteger a los activos de la diferentes amenazas.	Efectividad del Control	Sin efecto (0%) Poca efectividad (1%) Efectivo (4%) Muy Efectivo (10%)
Riesgo	Posibilidad que se produzca un impacto en un activo asociado a un proceso que afecta a la organización.	Estimación del riesgo También se estima el : Riesgo calculado intrínseco, antes de aplicar acciones. Riesgo calculado residual, se da tras aplicar acciones correctivas.	Cuantitativamente: Muy bajo (<0,5) Bajo (<5) Medio (<50) Alto (<500) Muy Alto (>1000) Cualitativamente: Sabiendo el impacto de una amenaza y su probabilidad, se estima el riesgo como impacto * frecuencia La frecuencia se expresada como: MF: muy frecuente (a diario) F: frecuente (mensual) FN: frecuencia normal (anual) PF: poco frecuente (cada varios años) Cualitativamente se aplica un modelo de cálculo sobre los activos.
Instrucciones o Recomendaciones	Conjunto de sugerencias o acciones a aplicar para mitigar el riesgo apoyado en las mejores prácticas.	Norma que apoya la instrucción	Se clasifica como: Controlar Compartir Eliminar Aceptar Se describe la norma a aplicar.

Tabla 15:Definición de Variables

III.4. Técnicas e Instrumentos para la Recolección de Datos

Para efectuar el proceso de recolección de datos, en esta investigación se procederá a seleccionar la técnica de la entrevista y consulta en documentos, entendiéndose este término último, en sentido amplio, como todo material de índole permanente, es decir, al que se puede acudir como fuente o referencia en cualquier momento o lugar, sin que se altere su naturaleza o sentido, para que aporte información o rinda cuentas de una realidad o acontecimiento.

III.5. Validez y Confiabilidad del Instrumento

Sierra y Álvarez (Álvarez, 1998) afirman:

> *"La validez es una condición necesaria de todo diseño de investigación y significa que dicho diseño permite detectar la relación real que pretendemos analizar y la confiabilidad es el grado con el que se obtiene resultados similares en distintas aplicaciones. (p.22). "*

Por ente la validez del instrumento se realiza mediante la definición conceptual y operacional de las variables, esta investigación se realiza a través del juicio de expertos, para ello se les realizó una serie de entrevistas, así como, la presentación de la investigación y variables para su conformidad. Todo el proceso de desarrollo del modelo fue elaborado en conjunto con los expertos y las mejores prácticas en materia de riesgo tecnológico.

III.6. Procedimientos

Según (UPEL, 2005), el proyecto factible como Trabajo de Grado implica el cumplimiento de las siguientes etapas generales:

> *".... diagnóstico, planteamiento y fundamentación teórica de la propuesta; procedimiento metodológico, actividades y recursos necesarios para su ejecución; análisis y conclusiones sobre la viabilidad y realización del proyecto; y en caso de su desarrollo, la ejecución de la propuesta y la evaluación tanto del proceso como de sus resultados. Los Trabajos de Grado, de Especialización y Maestría (...) pueden llegar hasta la etapa de las conclusiones sobre su viabilidad, o pueden consistir en la ejecución y evaluación de proyectos factibles presentados y aprobados por otros estudiantes (...) Las Tesis Doctorales deberán cubrir todas las etapas señaladas en el numeral anterior (p. 16)".*

Con el fin de dar cumplimiento al desarrollo de este proyecto se ha organizado el procedimiento en cuatro (4) fases que se describen en el siguiente gráfico:

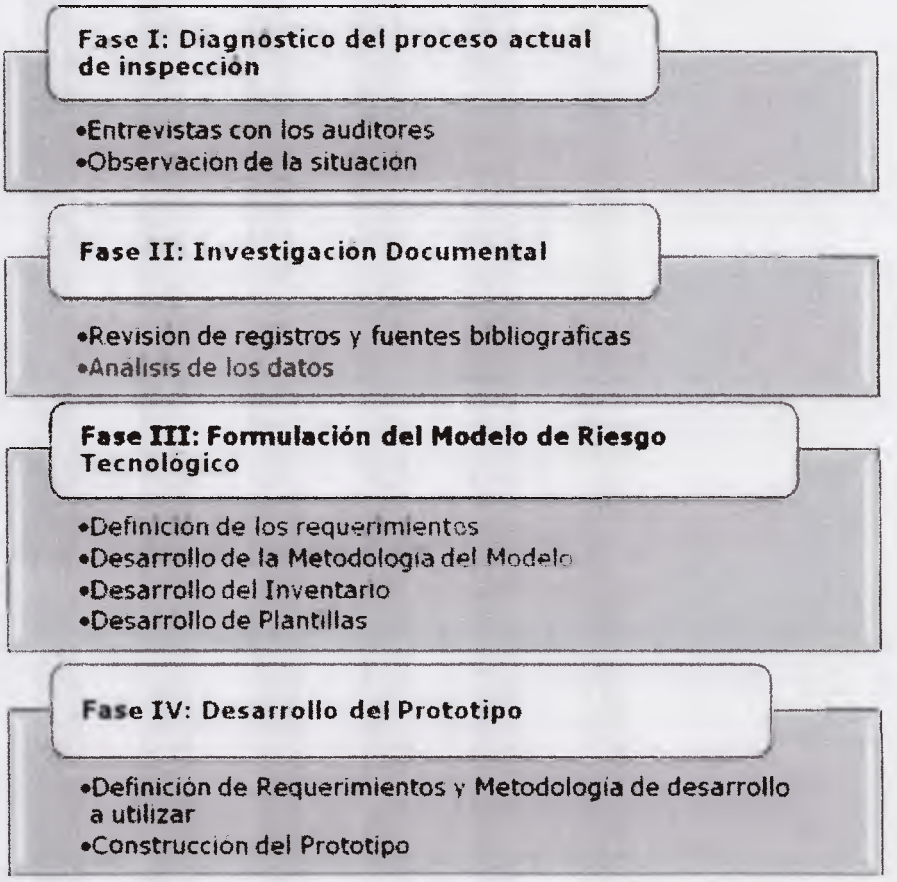


Figura 21: Fases y Actividades del Proyecto

Capítulo IV

Desarrollo del Proyecto

"En días de permanente cambio como los de hoy, el mañana será para los que sigan aprendiendo."

Lao Tse

CAPÍTULO IV

DESARROLLO DEL PROYECTO

Este capítulo comprende el desarrollo del proyecto y el desglose de las fases y sus actividades, tales como, diagnostico del proceso actual de inspección, investigación documental, formulación del modelo y desarrollo del prototipo.

IV.1. FASE I: DIAGNÓSTICO DEL PROCESO ACTUAL DE INSPECCIÓN

En esta fase se realizaron entrevistas con el coordinador y los especialistas del área de riesgo tecnológico, permitiendo describir y entender el proceso actual de inspección tecnológica realizado a las entidades bancarias, esta información se detalla en el capítulo I de este proyecto denominado Planteamiento del Problema.

IV.2. FASE II: INVESTIGACIÓN DOCUMENTAL

La investigación efectuada es de tipo documental, la cual se apoya en documentos de cualquier especie tales como, las obtenidas a través de fuentes bibliográficas, hemerográficas o archivísticas; la primera se basa en la consulta de libros, la segunda en artículos o ensayos de revistas y periódicos, y la tercera en documentos que se encuentran en archivos como cartas oficios, circulares, expedientes, informes, etcétera. La metodología utilizada una vez seleccionado el tema y definida la problemática, fue el acopio de bibliografía básica sobre el tema, elaboración de fichas bibliografías, lectura rápida del material, delimitación del tema, elaboración del esquema de trabajo, ampliación y lectura minuciosa de la bibliografía y finalmente la elaboración del contenido. El resultado de esta fase se encuentra en el capítulo II de este documento y en las referencias bibliográficas.

IV.3. Fase III: Formulación del modelo de Riesgo Tecnológico

Una vez definido el problema y realizado la investigación documental, la siguiente etapa consiste en formular un modelo para el análisis de riesgo, mediante la construcción de un metodología que represente la solución del problema planteado.

Los modelos son representaciones idealizadas de la realidad. Los modelos tienen muchas ventajas sobre una descripción verbal del problema, una ventaja obvia es que el modelo describe un problema en forma mucho más concisa.

En esta etapa se utiliza como insumo el contenido de las dimensiones de las metodologías de análisis y gestión de riesgo disponible y descritas en las tablas empleadas en el capítulo II. En los siguientes apartados podremos verificar las actividades de esta fase.

IV.4. Definición de los Requerimientos

Teniendo en cuenta las distintas metodologías disponibles para hacer el análisis de riesgos, se decidió desarrollar una metodología adaptada específicamente a las necesidades de la Organización.

Las características deseables en la metodología a desarrollar son los siguientes:

- Basada en estándares y mejores prácticas, para aprovechar el conocimiento y herramientas aplicadas, a fin de determinar la que mejor satisface sus necesidades.
- Sencillez y facilidad de uso, tanto en el momento de la primera implantación como en el mantenimiento.
- Modular y adaptable, que pueda adecuarse a diferentes entornos y áreas de negocio.
- Enfocada a los procesos de negocio y de soporte de la Organización.
- Objetiva, los resultados no deben depender de quién aplique la metodología ni de cómo lo haga.

Dadas las características deseables para la metodología, se han desarrollado unos principios para su desarrollo:

- Metodología mixta, con entrada de datos cualitativa, para facilitar la comunicación entre las distintas partes que deben participar en el análisis y métodos de cálculo cuantitativos para aprovechar la mayor eficiencia computacional y mayor precisión en los resultados.
- Utilización de principios, estándares y metodologías en los aspectos que se deban tratar y no cubran métodos implementados en el análisis de riesgos.
- Eliminación de los elementos que aporten menor valor en la consecución de los objetivos, en aras de mayor facilidad de uso y claridad.
- Que disponga de diversos inventarios de tipos de activos, amenazas y controles, de modo que se pueda utilizar con sencillez y que se pueda adaptar fácilmente a distintas necesidades y objetivos del análisis.
- Que disponga de una herramienta de soporte específica que facilite la entrada de datos y la realización de los cálculos.
- Que disponga de todos los elementos habituales que permiten dotar de objetividad al proceso: acuerdo entre varios expertos, definición de varios objetivos de valoración y proporcionar ejemplos con valores de referencia reales.
- Apoyo en las diferentes normativas utilizadas por la Gerencia de Riesgo Tecnológico de la Sudeban.

IV.5. Desarrollo de la Metodología del Modelo de Analisis de Riesgo

Para definir la presente metodología se ha considerado un conjunto de modelos identificados en el capítulo II que forma la base de todas las metodologías estándar de análisis de riesgos, y se han seleccionado las diferentes alternativas disponibles para la definición del modelo teniendo en cuenta los principios descritos.

Podemos resumir el modelo general de la metodología en el siguiente diagrama:

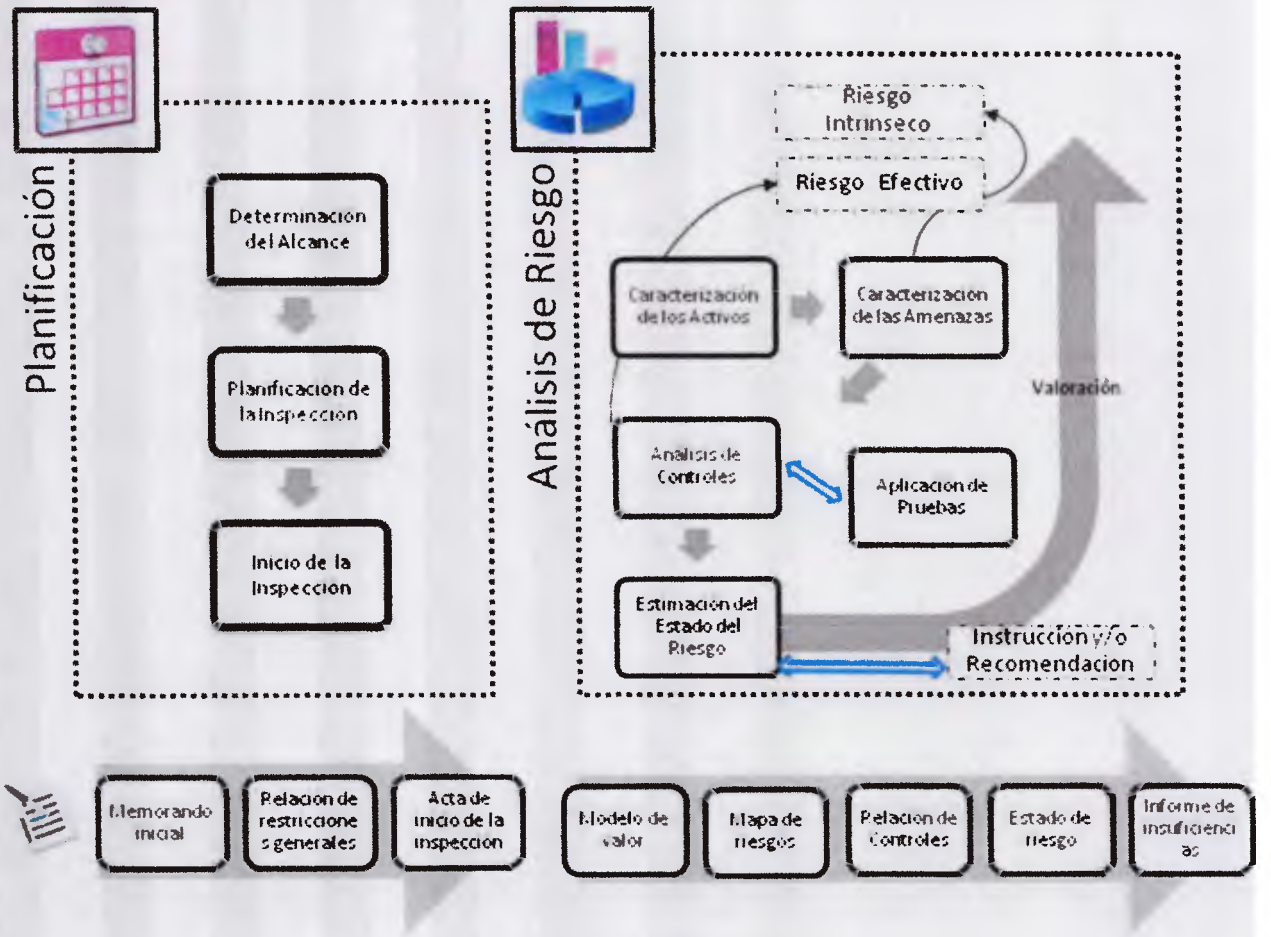


Figura 22: Diagrama del Modelo

En primer lugar, el modelo se divide en dos grandes procesos, desglosados cada uno en una serie de actividades y estas, a su vez, en tareas con el grado de detalle oportuno, los siguientes procesos son:

- Planificación, este proceso establece las consideraciones necesarias para arrancar la inspección, se revisan los antecedentes, se definen los objetivos, alcance y áreas de dominio (ver Anexo I) y se planifican los recursos materiales, financieros y humanos.
- Análisis de Riesgos, que comprende la obtención de información referente a los procesos, activos, recursos, vulnerabilidades, amenazas y controles, para luego estimar el impacto y el riesgo.

Estos dos procesos son secuenciales. El proceso de Planificación es claramente el iniciador del proceso y debe formar parte del proceso de análisis de riesgos. A lo largo de estos procesos se genera una serie de documentos de interés general los cuales se detallan en cada una de las actividades.

IV.6. Fase de Planificación

El objetivo principal de esta fase es establecer el marco general de referencia para toda la inspección, así como, crear las condiciones humanas, materiales y inancieras para el buen desarrollo de la misma. Este proceso se desarrolla por medio de las siguientes actividades y tareas:

a)Actividad A1.1: Determinación del Alcance

En esta actividad se definen los objetivos finales de la inspección, sus áreas de dominio, sus límites y los procesos de negocios. Se realiza una primera identificación del entorno y de las restricciones generales a considerar. El resultado de esta actividad es una planificación detallada de las áreas que serán evaluadas, los recursos que las evaluarán y el alcance del trabajos que efectuarán en cada ámbito definido.

Las tareas asociadas a la actividad son:

T1.1.1	Evaluación de los Antecedentes
T1.1.2	Determinación del alcance y objetivos.

T1.1.3	Inventario de las áreas de dominio.
T1.1.4	Documentación breve de los objetivos de cada una de las áreas de negocio.
T1.1.5	Identificación del entorno (revisión del cuestionario)
T1.1.6	Identificar las relaciones existentes entre los distintos procesos: dependencia, secuencia, etc.
T1.1.7	Desarrollo de análisis de los riesgos detectados en inspecciones anteriores, que permita descartar aquellos procesos que no resulten de interés para las fases posteriores (antecedentes).

Productos de Entrada

- Recopilación y análisis de la documentación asociada a las Instituciones Financieras.

Productos de Salida

- Memorando detallando de las áreas de dominio, objetivos, antecedentes y alcance de la inspección.
- Oficio y Credencial de apertura de la inspección.
- Acta de inicio de la inspección

Técnicas, prácticas y pautas

- Reuniones de trabajo con el coordinador y gerente de riesgo, gerencias e inspección para la discusión del alcance.
- Revisión documental.

b) ACTIVIDAD A1.2: PLANIFICACIÓN DE LA INSPECCIÓN

Se determinan las cargas de trabajo que supone la realización de la inspección. Se elabora el plan de trabajo para la realización de la inspección. En esta actividad se determinan los auditores que participarán en el proceso y se estructuran los diferentes grupos y comités para llevar a cabo la inspección.

El resultado de esta actividad está constituido por:

- un plan de trabajo para la inspección (cronograma de actividades)

Las tareas asociadas a la actividad son:

T1.2.1:	Evaluar cargas
T1.2.2:	Organizar a los auditores por áreas de dominio
T1.2.3:	Planificar el trabajo a realizar

Productos de entrada

- Resultados de la tarea T1.1.1, Determinación de las áreas de dominio y límites
- Resultados de la tarea T1.1.3, Determinación de los objetivos
- Esquema de las relaciones de las unidades del dominio con el entorno

Productos de salida

- Cronograma de actividades

Técnicas, prácticas y pautas

- Reuniones
- Memorándum de Planificación.
- Diagrama de Gantt

c)ACTIVIDAD A1.3: INICIO DE LA INSPECCIÓN

Se adaptan los formatos y cuestionarios para la recopilación de información adaptándolos a la inspección presente. También se realizará la carga inicial de datos en la herramienta propuesta.

El resultado de esta actividad está constituido por:

- Los planes de reuniones
- Programas de trabajo

Las tareas asociadas son:

T1.3.1:	Realizar o ajustar programas de trabajo
T1.3.3:	Incluir los datos iniciales en el sistema propuesto

Productos de entrada

- Resultados de la actividad A1.1, A.1.2

Productos de salida

- Programa de trabajo adaptado a la inspección

Técnicas, prácticas y pautas

- Planificación de la inspección

IV.7. Fase de Análisis de Riesgo

Este proceso es el núcleo central de la metodología propuesta y su correcta aplicación condiciona la validez y utilidad de toda la inspección. La identificación y estimación de los activos y de las posibles amenazas que les acechan representa una tarea compleja.

Este proceso tiene los siguientes objetivos:

- Levantar un modelo de valor de los dominios establecidos, identificando y valorando los activos relevantes.
- Levantar un mapa de riesgos de la inspección, identificando y valorando las amenazas sobre aquellos activos.
- Obtener un conocimiento de la situación actual de los controles.
- Evaluar el posible impacto sobre las áreas en estudio, tanto el impacto intrínseco (sin controles), como el impacto efectivo (incluyendo el efecto de los controles implementados).
- Evaluar el riesgo, tanto el riesgo intrínseco (sin controles), como el riesgo efectivo (incluyendo el efecto de los controles).
- Generar el informe que muestra las áreas de dominio con mayor impacto y/o riesgo.

El punto de partida de este proceso es la documentación del proceso de planificación, referente a los objetivos de la inspección, alcance y plan de trabajo. Este proceso se desarrolla por medio de las siguientes actividades y tareas:

a) ACTIVIDAD A.2.1: CARACTERIZACIÓN DE LOS ACTIVOS

Una vez identificadas las áreas de dominio o negocio y los procesos críticos para el mismo, se deben identificar los activos de los recursos de información relevantes involucrados en cada proceso, para ello se considera que un:

- activo es toda aquella información que tiene valor para la Organización en la medida en que le permite el cumplimiento de sus objetivos, y un,
- recurso de información es cualquier elemento que se emplea en el manejo de los activos de información.

Las tareas asociadas son:

T2.1.1:	Identificación de los activos y recursos de información
T2.1.2:	Dependencias entre activos y recursos de información
T2.1.3:	Valoración de los activos

En la Tarea T2.1.1 se pretende identificar los activos relevantes dentro de las áreas de dominio establecidas en el alcance. Los activos de información son intangibles, es decir, la tarea no consiste en identificar aplicaciones, archivos o bases de datos sino la información que se utiliza en el proceso desde un punto de vista conceptual y que es vital y necesaria para los procesos críticos del negocio.

Para cada activo de información identificado se debe registrar, la siguiente información:

- Nombre y código del activo de información.
- Clasificación del activo de información.
- Descripción del contenido del activo de información.
- Tipo (o tipos) que caracterizan el activo.
- Unidad y persona responsable.
- Valoración del activo bajo la dimensión de valoración de seguridad.
- Otras características específicas del tipo de activo.
- Cantidad de activos

Debido a que los recursos de información no tienen valor por sí mismos, sino sólo, en la medida en que permiten el manejo de los activos de información, tienen un valor intrínseco para la Organización, por ende los recursos de información no se valoran.

Para facilitar la identificación de los recursos de información se considera necesario disponer de un inventario, que se ha elaborado en base al inventario empleado en la metodología MAGERIT (López F., 2006), el cual se encuentra detallado en el anexo I. Este inventario puede modificarse para adaptarlo a las necesidades específicas de cada análisis de riesgos.

Con respecto a la tarea T2.1.2 es importante el concepto de "dependencias entre activos" o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. En la valoración de los activos es necesario entrevistar a diferentes personas dentro de la Organización, para lo cual es conviene registrar la siguiente información:

- dimensiones en las que el activo es relevante (ver "Apéndice I")
- estimación de la valoración en cada dimensión
- explicación de la valoración
- entrevistas realizadas de las que se han deducido las anteriores estimaciones.

En aras de asegurar la adaptabilidad, la metodología dispone de un inventario de recursos de información y un conjunto de dimensiones de valoración las cuales pueden ser ampliadas, y son detalladas en el Apéndice I Y II.

La identificación de las relaciones de dependencia entre activos y recursos de información es clave en la aplicación de la metodología, puesto que la asignación de valor a los recursos de información no se realiza directamente, sino a través de los activos de información que soportan, y, de forma inversa, los activos de información al

ser conceptuales, no tienen amenazas sino a través de los recursos de información que los procesan.

Debido a que se desprecia el valor intrínseco de los recursos de información y que las dependencias son totales, la creación de una jerarquía de dependencias entre recursos de información no aporta información adicional. Por ello, no se consideran dependencias entre los diferentes recursos de información, sino que todos los recursos soportan directamente sus activos.

La metodología propuesta no define una escala determinada a utilizar en la valoración, recomendándose usar escalas de entre 3 y 10 valores, en función de las necesidades de cada análisis de riesgos. La escala por defecto tiene 5 niveles y está recogida en el anexo II de este documento.

Productos de entrada

- Inventarios de datos manejados por la Organización
- Procesos de negocio
- Diagramas de flujo de datos
- Inventarios de equipamiento lógico y físico
- Cuestionario electrónico de tecnología y sistemas (Cetys)

Productos de salida

- Informe de los activos componentes del dominio y sus agrupaciones.
- Definición de las relación entre los activos.

Técnicas, prácticas y pautas

- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas y Reuniones

b) ACTIVIDAD A.2.2: CARACTERIZACIÓN DE LAS AMENAZAS

Una amenaza es cualquier causa potencial, ya sea intencional o fortuita, de un daño a un recurso de información, y, por extensión, a los activos de información que dicho recurso soporta (ISO, International Organization Standards, 2004).

Esta actividad suele realizarse de forma concurrente con la actividad de caracterización de los activos dado que los responsables a entrevistar son los mismos.

Esta actividad consta de dos tareas:

T2.2.1:	Identificación de las amenazas
T2.2.2:	Valoración de las amenazas

En la tarea T2.2.1 se identifican las amenazas significativas sobre los activos identificados, tomando en consideración:

- el tipo de activo
- las dimensiones en que el activo es valioso
- la experiencia de la Organización

Para cada amenaza sobre los activos conviene registrar la siguiente información:

- tipología de la amenaza
- explicación del efecto de la amenaza
- resultado de las entrevistas realizadas en las que se ha deducido la anterior estimación
- antecedentes, si los hubiera, bien en la propia Organización, o en otras organizaciones que se haya considerado relevantes

Para la tarea T2.2.2, valoración de las amenazas es necesario estimar un ratio anual de ocurrencia y un porcentaje de degradación para cada uno de las dimensiones de seguridad definidas. (López F., 2006).

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- degradación: cuán perjudicado resultaría el activo
- frecuencia: cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. y se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde.

En el caso de amenazas fortuitas, algunos de los principales factores que pueden considerarse para estimar la frecuencia incluyen:

- Información histórica de la realización de las amenazas en el entorno analizado. Por ejemplo, estudio de la climatología y de las catástrofes naturales ocurridas en el entorno de un CPD.
- Exposición de los activos a cada amenaza.
- Cambios en la estructura organizativa o tecnológica de la Organización.
- Externalización de procesos, puede incrementar la frecuencia de incidentes fortuitos de seguridad, debidos a la compartición de recursos con otras organizaciones que puedan ser atacadas o por la realización de amenazas sobre los contratistas.

Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

En el caso de las amenazas intencionadas, algunos de los principales factores que pueden considerarse para la estimación de la frecuencia incluyen:

- Beneficio que un potencial atacante puede esperar de la realización del ataque. Si los potenciales atacantes pueden esperar un beneficio elevado de sus ataques, estos se producirán con mayor frecuencia.

- Dificultad que un potencial atacante percibe de la realización del ataque, y conocimientos y material necesarios para su ejecución.
- Existencia de motivaciones no económicas para la realización de sabotajes: conflictividad laboral, relaciones agresivas con competidores, proveedores o clientes, etc. El sabotaje se producirá con mayor frecuencia cuanto mayor sea el número de motivaciones para realizarlo.
- Relevancia de la Organización. Si una Organización tiene una especial exposición al público, por su elevado número de empleados, de clientes, o por su actividad comercial y de marketing, el número de potenciales atacantes que pueden planear un ataque se incrementa, y con ello la frecuencia de los ataques.
- Volumen de tratamiento de información relacionada con terceros.
- Conocimiento de la estructura organizativa y tecnológica de la Organización.
- La información disponible por parte de terceros o de la opinión pública sobre la Organización puede utilizarse para realizar ataques.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos:

100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

La estimación del impacto de las amenazas sobre los distintos requerimientos de seguridad de los recursos de información se expresa en porcentajes de degradación. La estimación de estos porcentajes se realiza en función de diversos factores. Algunos de los principales factores a considerar al realizar las estimaciones son:

- Capacidad de la amenaza de afectar a todo el recurso o sólo a una parte del mismo.
- Si la amenaza afecta a partes claves o a partes accesorias del recurso de información. Si la amenaza, una vez realizada, afecta de forma puntual o de forma permanente al recurso.

La metodología proporciona un inventario clasificado de amenazas basado en la Metodología MAGERIT (López F., 2006) que puede consultarse en el anexo III. Este inventario incluye unos valores de referencia de la frecuencia y el impacto de cada amenaza sobre cada uno de los tipos de recurso de información definido que no se han incluido en el documento debido a su elevado volumen.

En función de los objetivos definidos para el análisis de riesgos el inventario de amenazas puede ajustarse a los requerimientos específicos o sustituirse por otro que se adapte mejor a ellos.

Los valores de referencia propuestos pueden aceptarse para la realización de un análisis de riesgos rápido y menos preciso o pueden ajustarse en función de cada uno de los recursos de información identificado, para realizar un análisis de riesgos más laborioso y preciso.

Productos de Entrada

- Resultados de la actividad A2.1, Caracterización de los activos

Productos de Salida

- Relación de amenazas posibles
- Mapa de riesgos: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos

Técnicas, prácticas y pautas

- Catálogos de amenazas
- Entrevistas, reuniones y técnicas de elaboración de informes
- Valoración Delphi

c) ACTIVIDAD A.2.3: IDENTIFICACIÓN DE CONTROLES

Los controles son las medidas establecidas por la Organización para mitigar sus riesgos. Los controles pueden reducir la probabilidad de éxito de una amenaza reduciendo, por tanto, su frecuencia y/o reducir el impacto en caso de producirse (López F., 2006). La eficacia de un control para una determinada amenaza y recurso de información se mide en el porcentaje de reducción de la probabilidad y el impacto de la ocurrencia.

Esta actividad consta de dos tareas:

T2.3.1	Identificación de las controles existentes
T2.3.2	Valoración de los controles existentes

La metodología propuesta incluye un inventario de controles obtenido del código de buenas prácticas ISO/IEC 27002:2007 [ISO27002.05], según se recoge en el Anexo VI. En función de los objetivos definidos para el análisis de riesgos, el inventario de controles puede ajustarse a los requerimientos específicos o sustituirse por otro que se considere más adecuado, por ejemplo las diversas normativas utilizadas por la Gerencia de Riesgo Tecnológico.

De la misma forma que se estableció una valoración por defecto de las distintas amenazas, se ha definido una valoración por defecto de la efectividad de cada uno de los controles para cada tipo de recurso y amenaza, considerando la reducción de la probabilidad y la reducción del impacto para cada uno de los requerimientos de seguridad. Esta tabla no se ha incluido en este documento debido a su volumen: al aplicar la combinatoria entre amenazas y controles se obtiene una tabla de cerca de 8.000 registros, en este sentido solo se exponen algunos de ellos en el anexo VI para que se hagan una idea de su contenido.

Debido a que no existe ninguna fuente de datos fiable sobre la eficacia de los controles para mitigar las distintas amenazas, se ha realizado un análisis cualitativo para realizar dicha valoración sobre una escala de 4 valores:

- **Sin efecto** → El control no tiene ningún impacto sobre la amenaza.

- **Poca efectividad** → El control tiene un impacto indirecto o general sobre la amenaza.
- **Efectivo** → El control reduce la frecuencia o el impacto de la amenaza de forma significativa.
- **Muy efectivo** → Control específicamente diseñado para mitigar la amenaza.

Se ha asignado un valor numérico a cada nivel de la escala para permitir el uso de los cálculos cuantitativos. La asignación se ha realizado considerando los siguientes criterios:

- Escala de tipo exponencial, que permita diferenciar los controles muy efectivos del efecto de los controles menos efectivas.
- La aplicación de todos los controles supone una mitigación superior al 99% del riesgo. Debido al método de cálculo utilizado en la estimación del riesgo efectivo, no es posible reducir el riesgo hasta cero.

	Eficacia de los controles
Sin efecto	0%
Poca efectividad	1%
Efectivo	4%
Muy efectivo	10%

Figura 23: Valoración de la eficacia de los controles

Por otra parte, el grado de implantación de los controles puede variar en función de las distintas áreas de la Organización o entornos tecnológicos, por lo que la efectividad de cada control se condiciona, adicionalmente, a su grado de implantación en el entorno analizado. La implantación de los controles se representa por un porcentaje.

La determinación del porcentaje de implantación de los controles se realiza teniendo en cuenta los siguientes criterios:

- **Calidad del diseño del control**: identificar si existen limitaciones en su aplicación o circunstancias en que el funcionamiento pueda no ser adecuado para el control de las amenazas.
- **Alcance de la implantación**: recursos de información cubiertos y no cubiertos por el control.
- **Nivel de madurez de la implantación**, define en qué medida se puede confiar en el funcionamiento adecuado del control según sus especificaciones. En la determinación del nivel de madurez se considera el modelo CMMI (Capability Maturity Model), que define los siguientes niveles de madurez aplicables a cualquier proceso o control:
  - **Nivel 0 (Inexistente):** El control no se ha implantado.
  - **Nivel 1 (Inicial):** La implantación del control depende de la iniciativa de personas individuales, por lo que no se puede garantizar su aplicación de forma consistente ni en todos los casos.
  - **Nivel 2 (Repetible):** El control se aplica de forma generalizada debido al conocimiento de todos los interesados de su necesidad y de su funcionamiento, pero no se ha llevado a cabo una formalización que asegure la aplicación de forma consistente ni que la aplicación de la medida se mantendrá a lo largo del tiempo al cambiar las personas responsables.
  - **Nivel 3 (Formalizado):** La aplicación del control está formalmente documentada en políticas, procedimientos, guías, estándares, cuadernos de carga, definiciones de puestos, etc. Esta formalización asegura que la salvaguarda se aplicará de forma generalizada y consistente y se mantendrá independientemente de las personas responsables.
  - **Nivel 4 (Gestionado):** La aplicación del control se monitoriza y se revisa periódicamente. Esta monitorización y revisión permite

detectar cualquier desviación en la aplicación de la salvaguarda, garantizando su funcionamiento permanente.

- **Nivel 5 (Optimizado):** La monitorización y la revisión del control se utiliza para introducir mejoras que permitan aumentar la eficacia a lo largo del tiempo.

Productos de entrada

- Inventario de procedimientos operativos
- Inventario de productos y/o desarrollos hardware o software de soporte a la seguridad de los sistemas
- Acuerdos de externalización de servicios
- Inventario de Controles
- Normativas de Tecnología

Productos de salida

- Relación de controles

Técnicas, prácticas y pautas

- Entrevistas y reuniones

d) ACTIVIDAD A.2.4: APLICACIÓN DE LA PRUEBAS

En esta actividad la tarea principal es seleccionar y documentan las diversas pruebas que se deben aplicar a los controles identificados para verificar su correcta aplicación en las diversas áreas de dominio.

Para cada prueba se debe documentar lo siguiente:

- Número de prueba
- Nombre de la prueba
- Descripción detallada
- Número de control sobre el cual se aplica la prueba

- Tipo de Control al que pertenece la prueba

e)CÁLCULO DEL RIESGO INTRÍNSECO

Se considera que el riesgo intrínseco es la pérdida anual esperada considerando que no existe ningún control que proteja los recursos de información de sus amenazas (López F., 2006).

f)CALCULO DEL RIESGO EFECTIVO

Se considera que el riesgo efectivo es la pérdida anual esperada considerando el efecto de los controles actualmente implantados para proteger a los recursos de información de sus amenazas. (López F., 2006)

g)ACTIVIDAD A.2.5: ESTIMACIÓN DEL ESTADO DEL RIESGO

En esta actividad se combinan los descubrimientos de las actividades anteriores (A2.1, A2.2 y A2.3) para derivar estimaciones del estado del riesgo de la Organización.

Esta actividad consta de tres tareas:

T2.5.1	Estimación del impacto
T2.5.2	Estimación del riesgo
T2.5.3	Interpretación de los resultados

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

En la tarea T2.4.1 se estima el impacto al que están expuestos los activos de la organización identificados en las áreas de dominio:

- el impacto intrínseco, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no los controles actualmente desplegados
- el impacto efectivo, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de los controles actualmente desplegados.

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

En la tarea T2.4.2 se estima el riesgo al que están sometidos los activos de la organización identificados en las áreas de control.

Finalmente, se interpretan los resultados anteriores del impacto y del riesgo, se establecen relaciones de prioridad por activos o grupos de activos, bien por orden de impacto o por orden de riesgo y se genera el informe final.

Productos de entrada

- Resultados de la actividad A2.1, Caracterización de los activos
- Resultados de la actividad A2.2, Caracterización de las amenazas
- Resultados de la actividad A2.3, Análisis de los Controles

Productos de salida

- Informe de impacto intrínseco por activo
- Informe de impacto efectivo por activo
- **Estado de riesgo**: informe resumen del impacto y riesgo intrínseco o efectivo a que está sometido cada activo del dominio
- **Informe de insuficiencias**: informe que destaca las incoherencias entre los controles que se necesitan y las que existen y las divergencias entre la magnitud del riesgo y la eficacia actual del control.

Técnicas, prácticas y pautas

- Análisis mediante tablas
- Análisis algorítmico

h)Actividad A.2.6: Instrucciones

Se encuentran enmarcadas en el cumplimiento de la normativa legal vigente establecida por el Organismo supervisor, regulador y fiscalizador en este caso la Sudeban. Para esta actividad se deben identificar los siguientes datos para generar los resultados:

- Código y nombre de la inspección
- Identificador del riesgo
- Código de la instrucción
- Descripción de la instrucción

IV.8. Desarrollo de Inventarios

Para facilitar la aplicación de la metodología en casos reales, se han identificado e incluido diversos inventarios de elementos. La función de estos inventarios es asegurar que todos los elementos relevantes para el análisis se tienen en consideración, de forma eficaz y eficiente.

Los inventarios incluyen no sólo la relación de elementos a considerar, sino unos valores asignados por defecto para el análisis. Estos valores por defecto facilitan la aplicación de la metodología propuesta de diversas formas:

- Pueden utilizarse directamente para la realización de un análisis de riesgos rápido a costa de perder precisión
- Pueden utilizarse como punto de partida para un análisis individual de los diferentes elementos reales que forman parte del análisis de riesgos, permitiendo dar valores en función de la relación del elemento a analizar con un elemento tipo.

- Pueden utilizarse directamente en elementos que no sean particularmente relevantes para el análisis y como punto de partida para un análisis más detallado de los elementos más relevantes.

Los inventarios realizados se consideran genéricos y pueden adaptarse a las necesidades de diferentes análisis de riesgos, o sustituirse por otros que se adapten mejor a las necesidades específicas.

Los inventarios incluidos en la metodología son:

- Anexo I: Áreas de dominio.
- Anexo II: Dimensiones de Seguridad. Sólo contiene la lista de requerimientos de seguridad a considerar, así como, la escala de valoración de los mismos.
- Anexo III: Criterios de Valoración. Escala y criterios de valores para los activos de la organización.
- Anexo IV: Tipos de Activos. Lista de tipos de recursos de información y activos a considerar.
- Anexo V: Amenazas. Contiene la lista de amenazas y una estimación de la frecuencia y la degradación que causa a cada tipo de recursos de información, teniendo en cuenta cada uno de los requerimientos de seguridad.
- Anexo VI: Controles. Contiene la lista de controles y una estimación de la efectividad en la reducción de la frecuencia de cada amenaza sobre cada tipo de recurso, así como la efectividad en la reducción del impacto de cada amenaza sobre cada tipo de recurso y requerimiento de seguridad. Para la elaboración de este inventario se utilizó como punto de partida el listado de controles del código de buenas prácticas ISO/IEC 27002:2005. Debido a su elevado volumen, no se incluye la información de la eficacia de cada salvaguarda. [ISO27002.05]

IV.9. Fase IV: Desarrollo del Prototipo

Una vez definida la metodología de riesgo, se desarrolló una herramienta informática para soportar su implantación. El desarrollo se realizó utilizando la técnica de prototipo la cual modela el producto final y permite efectuar un test sobre determinados atributos del mismo sin necesidad de que está disponible todo su desarrollo.

a) Metodología a Utilizar

El modelo de "prototipado de requerimientos" es la creación de una implementación parcial de un sistema, con el propósito explícito de aprender sobre los requerimientos del sistema. Un prototipo es construido de una manera rápida tal como sea posible. Esto es dado a los usuarios, clientes o representantes de ellos, posibilitando que ellos experimenten con el prototipo. Estos usuarios luego proveen la retroalimentación sobre lo que a ellos les es funcional acerca del prototipo proporcionado, quienes capturan en la documentación actual de la especificación de requerimientos la información entregada por los usuarios para el desarrollo del sistema real. Este modelo permitió:

- Fluidez del ciclo de vida de desarrollo de sistemas.
- Reducir el riesgo de construir productos que no satisfagan las necesidades de los usuarios.
- Reducir costos y aumenta la probabilidad de éxito.
- Disponer de las herramientas adecuadas.
- No presenta calidad de interfaces ni robustez en procesos de almacenamiento.
- Una vez identificados todos los requisitos mediante el prototipo, se construye el producto de ingeniería final.

La siguiente figura denota las etapas del modelo de prototipado:

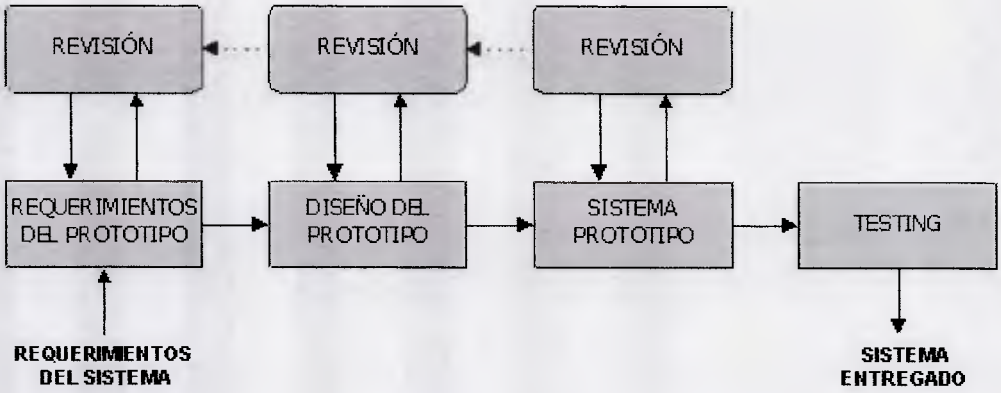


Figura 24: Etapas del Modelo de Prototipado

Según McCracken y Jackson, 1982:

> *"Este modelo consiste en un procedimiento que permite al equipo de desarrollo diseñar y analizar una aplicación que representa el sistema que sería implementado. Dicha aplicación, llamada prototipo, está compuesta por los componentes que se desean evaluar (i.e. las funciones principales)."*

Las etapas del modelo son:

- Investigación preliminar.
- Colecta y refinamiento de los requerimientos y proyecto rápido:
  - Análisis y especificación del prototipo.
  - Diseño y construcción del prototipo.
  - Evaluación del prototipo por el cliente.
  - Renacimiento del prototipo.
- Diseño técnico.
- Programación y test.
- Operación y mantenimiento.

b) Análisis y Especificación del Prototipo

La realización de una herramienta supone trabajar con una cierta cantidad de activos que serán recolectados para complementar la base de Magerit (Anexo IV) del Cuestionario Electrónico de Sistemas y Tecnología de Información (Cetys), el cual provee la información referente a los activos y recursos de información de las instituciones financieras. El número de amenazas típicamente está en el orden de las decenas, mientras que el número de controles está en los millares. Todo ello nos indica que hay que manejar multitud de datos y combinaciones entre ellos, lo que lleva lógicamente a buscar apoyo de herramientas automáticas.

Como requerimiento, la solución de apoyo a las inspecciones de análisis de riesgo tecnológico debe:

- permitir trabajar con un conjunto amplio de activos, amenazas y controles;
- permitir un tratamiento flexible del conjunto de activos para acomodar un modelo cercano a la realidad de la Organización supervisada y a los requerimientos del supervisor (Sudeban);
- ser utilizada a lo largo de los dos procesos que constituyen la inspección, especialmente como soporte al proceso Análisis de Riesgos y
- no ocultar al analista el razonamiento que lleva a las conclusiones, y
- contener base de datos contentiva de los riesgos posibles.

Las herramientas empleadas pueden hacer un tratamiento cualitativo o cuantitativo de la información. Una opción mixta es útil: un modelo cualitativo para el sistema de información completo, con capacidad de entrar en un modelo cuantitativo para aquellos componentes cuya protección va a requerir fuertes desembolsos.

Cabe destacar que los datos de caracterización de las posibles amenazas son datos tentativos en los primeros modelos; pero la experiencia permite ir ajustando las valoraciones a la realidad.

Sean herramientas cualitativas o cuantitativas, estas deben:

- Manejar un catálogo razonablemente completo de tipos de activos.
- Manejar un catálogo razonablemente completo de dimensiones de valoración de los activos.
- Ayudar a valorar los activos ofreciendo criterios de valoración.
- Manejar un catálogo razonablemente completo de amenazas y controles.
- Evaluar el impacto y el riesgo intrínseco y efectivo.
- Es interesante que la solución pueda importar y exportar los datos que manejan en formatos fácilmente procesables por otras herramientas, entre las cuales se cita XML – Extended Markup Language que es la opción tomada en este proyecto, que establece formatos XML de intercambio de datos.

Un extracto de los requerimientos definidos para la aplicación se muestra en los siguientes apartados.

c) ACTORES

Auditor	Persona encargada de realizar el análisis del riesgo. Como tal, adapta los distintos aspectos de la metodología (Requerimientos de seguridad y escalas de valoración) y de los inventarios (Tipos de recursos, amenazas, controles y valoraciones estándar de los mismos), crea y mantiene las inspecciones de análisis de riesgos, gestiona la realización de las valoraciones por los distintos evaluadores y obtiene los resultados del análisis de riesgos.
Evaluador	Persona que conoce o controla los distintos activos y recursos de información y que disponen de una opinión cualificada acerca de su valor para el negocio (activos de información) y/o las amenazas y controles (recursos de

	información). La herramienta recoge, consolida y procesa las valoraciones realizadas por los evaluadores.
Institución	Entidad que recibe del auditor los resultados de los análisis de riesgos realizados y los utiliza para la toma de decisiones.

d) Casos de Uso

Los casos de usos nos permiten organizar los requerimientos por cada funcionalidad del sistema a continuación se presenta una lista de los identificados:

CU01	Inicio sesión
CU02	Planificación de inspección
CU03	Requerimientos de seguridad de la información
CU04	Escalas de valoración
CU05	Inventario de activos
CU06	Inventario de amenazas
CU07	Inventario de controles
CU08	Inventario de pruebas
CU09	Inventario de Instrucciones
CU10	Inventario de Riesgo
CU11	Valoración de amenazas por activo.
CU12	Valoración por defecto de la eficacia de los controles
CU13	Valoración de los activos de información
CU14	Áreas de dominio
CU15	Perfiles de usuario
CU16	Modulo de Estimación del estado del riesgo
CU17	Modulo de Reporte
CU18	Inventario de Recursos de Información
CU19	Amenaza – Activo
CU20	Amenaza – Control

La especificación de los casos de usos se detalla en el anexo VIII.

e) Definición del Esquema Lógico de Datos

Las entidades y relaciones que constituyen el modelo lógico de datos, se representa en los siguientes esquema:

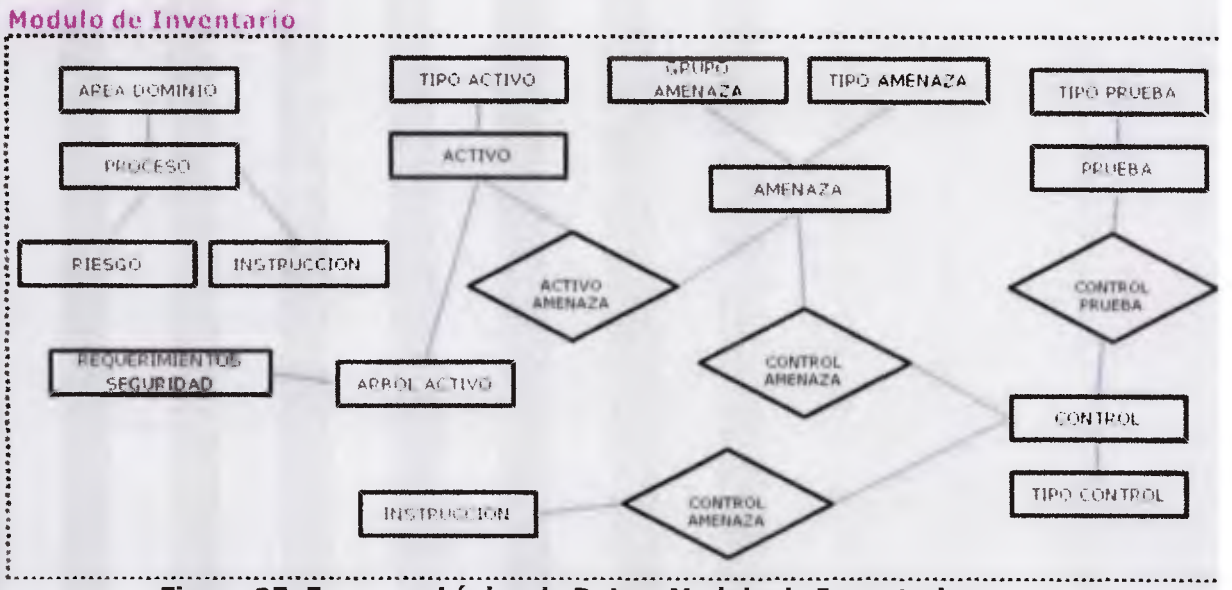


Figura 25: Esquema Lógico de Datos, Modulo de Inventario

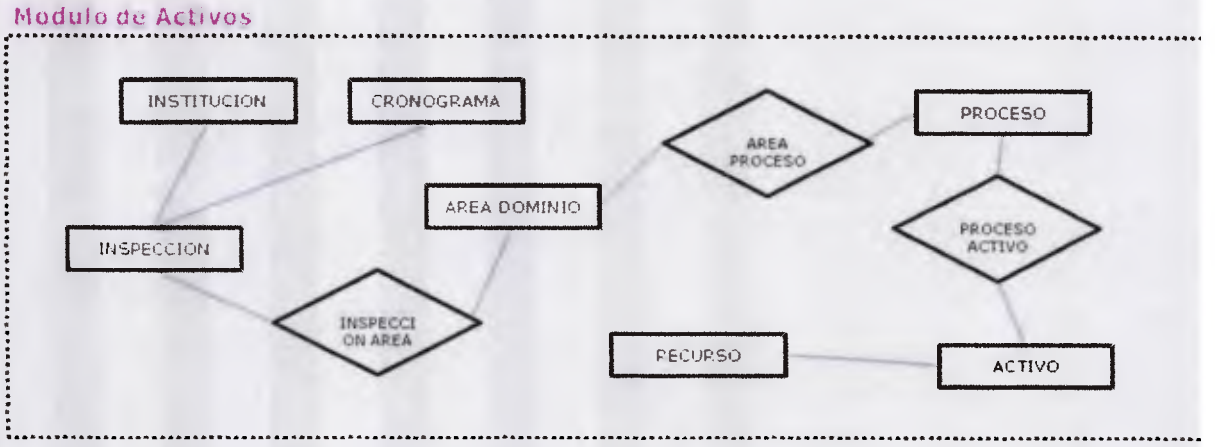


Figura 26: Esquema Lógico de Datos, Modulo de Activos

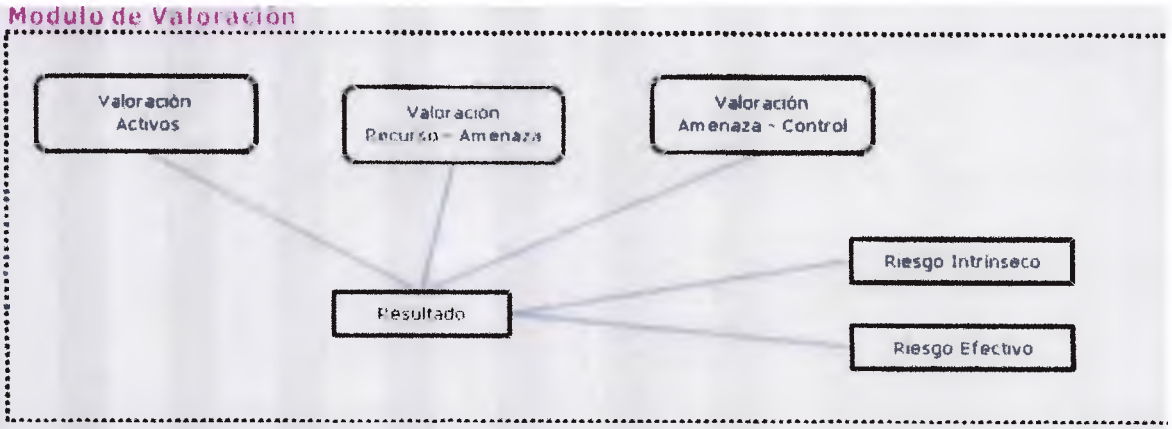


Figura 27: Esquema Lógico de Datos, Modulo de Valoración

f). DEFINICIÓN DE LAS INTERFACES

A continuación se presenta las interfaces más relevantes propuestas en el desarrollo del prototipo:

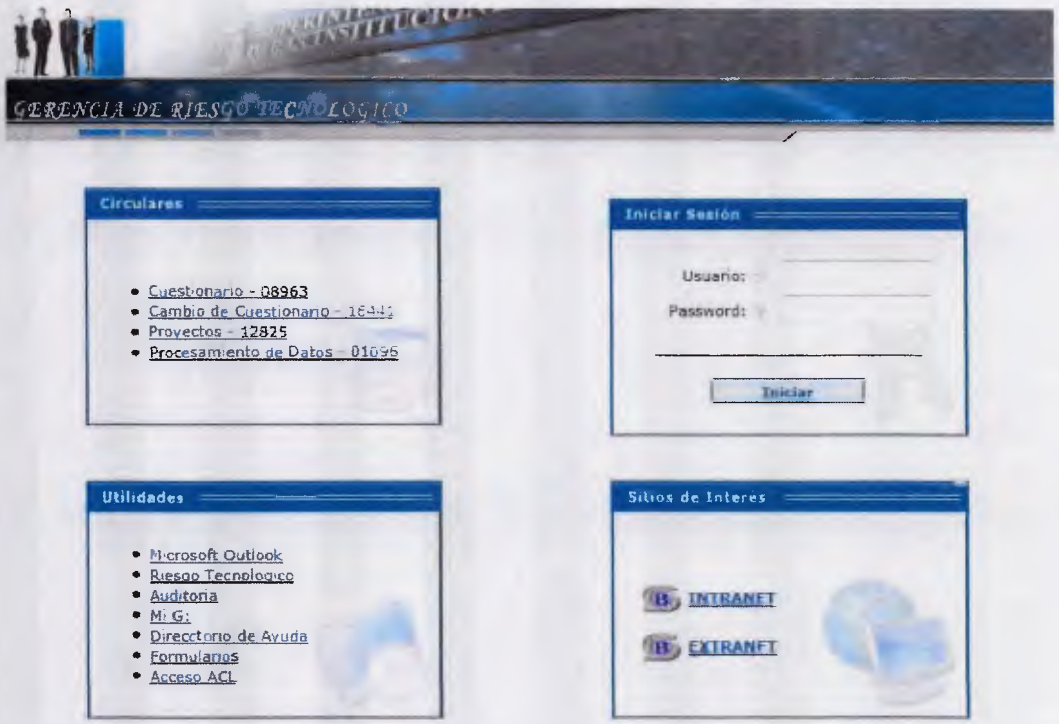


Figura 28: Prototipo - Inicio de Sesión

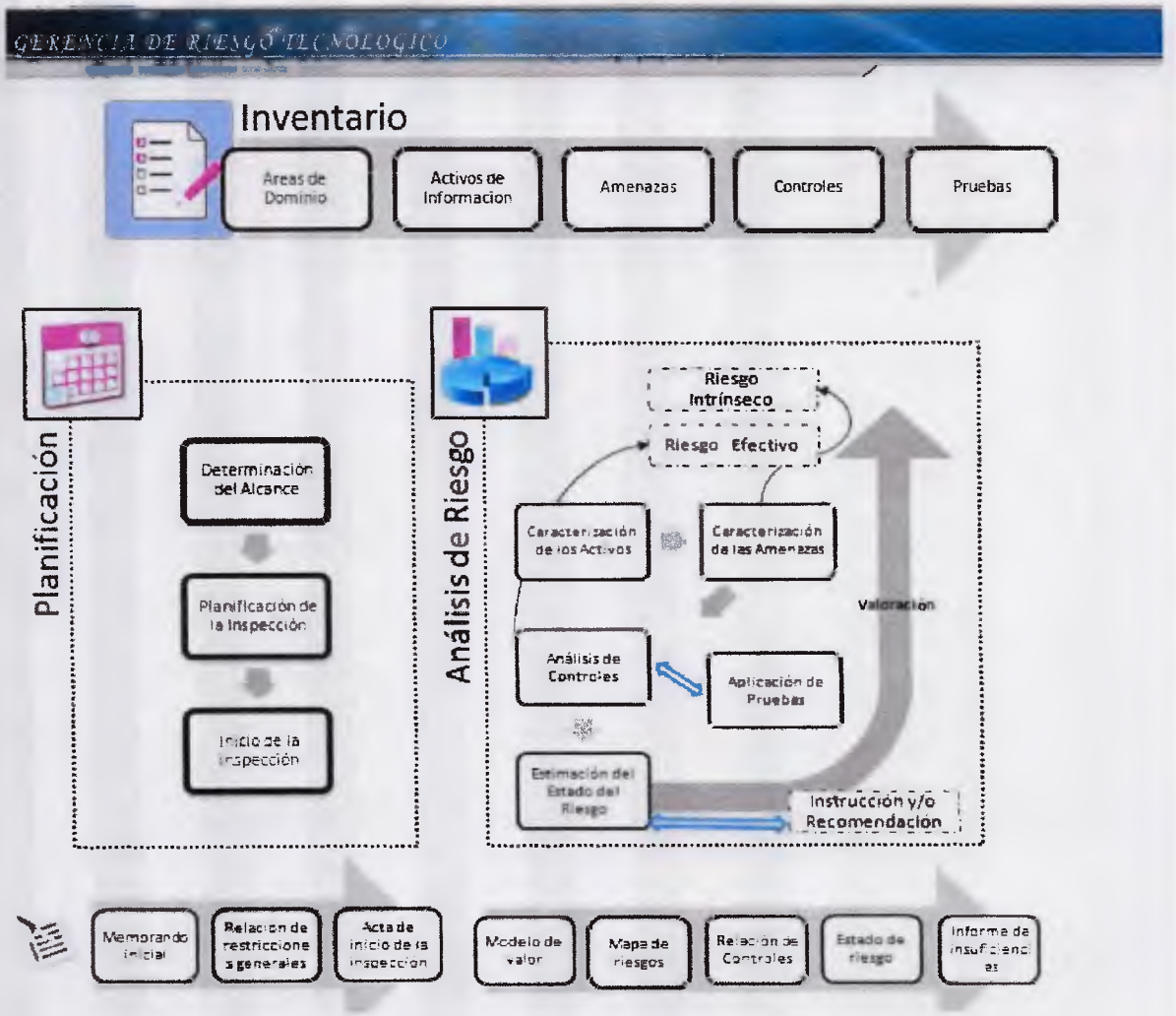


Figura 29: Prototipo - Menú Principal

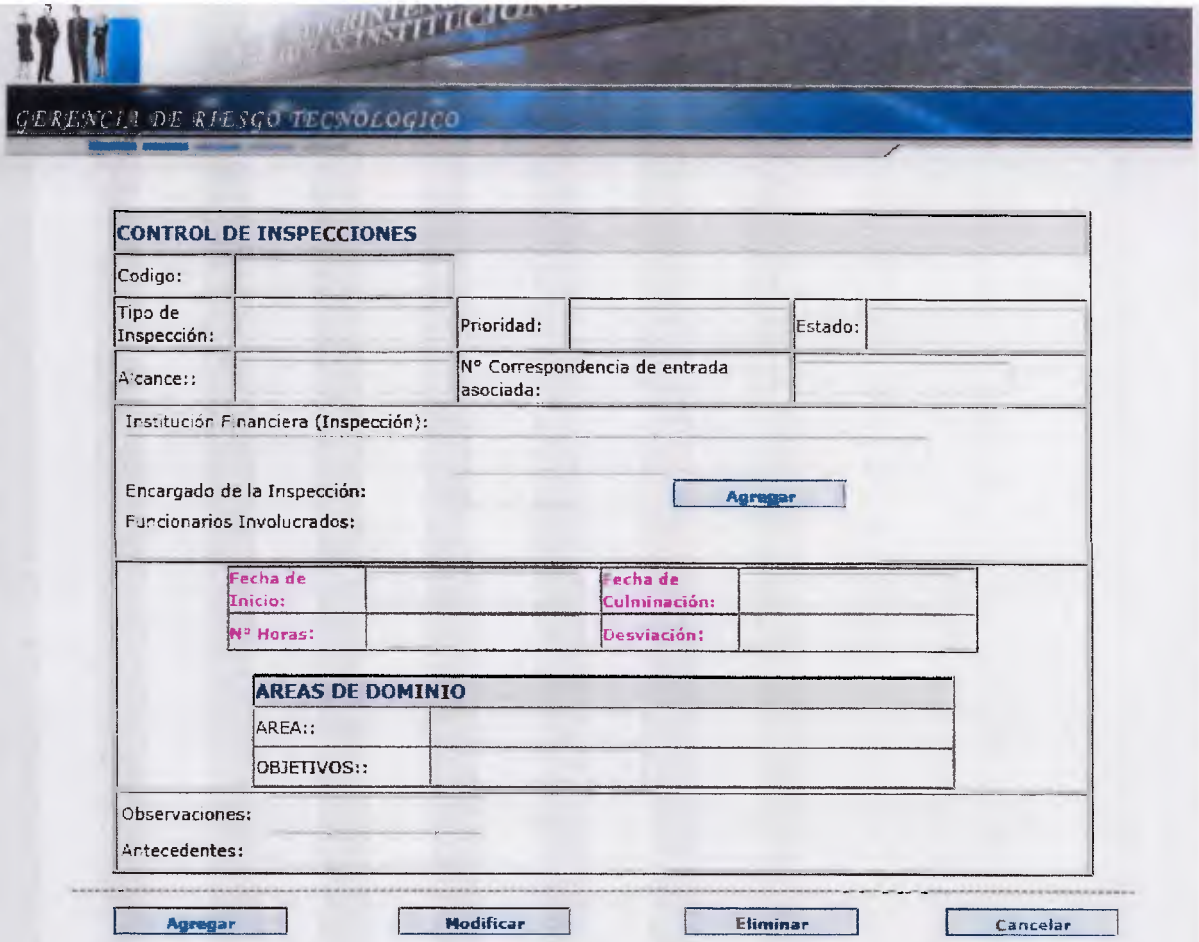


Figura 30: Prototipo - Control de Inspecciones

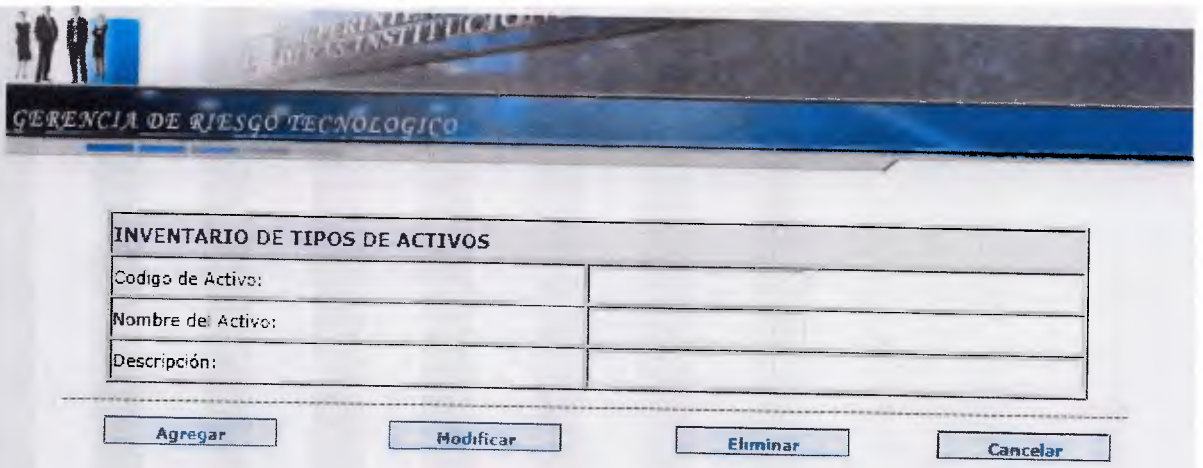


Figura 31: Prototipo - Inventario de Tipos de Activos

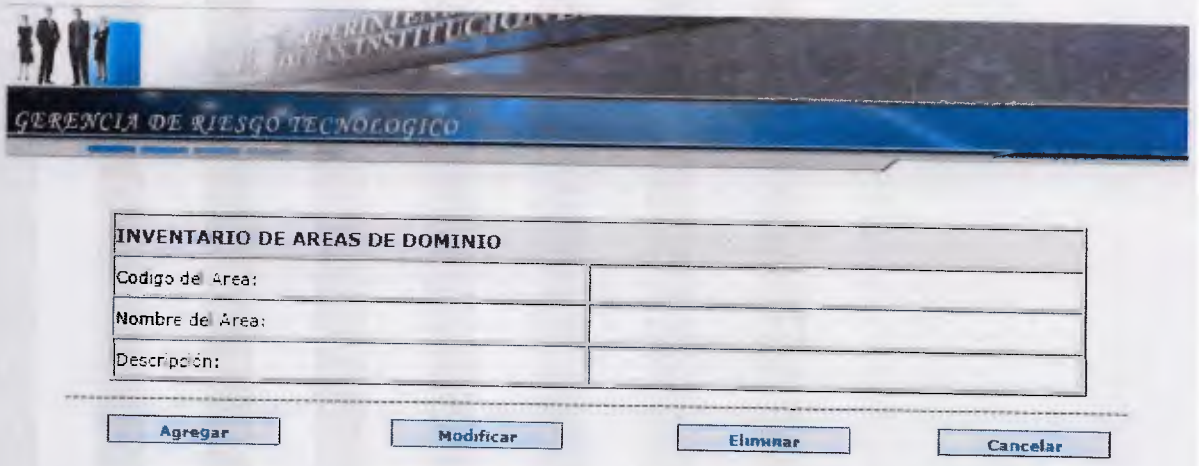


Figura 32: Prototipo - Inventario de Áreas de Dominio

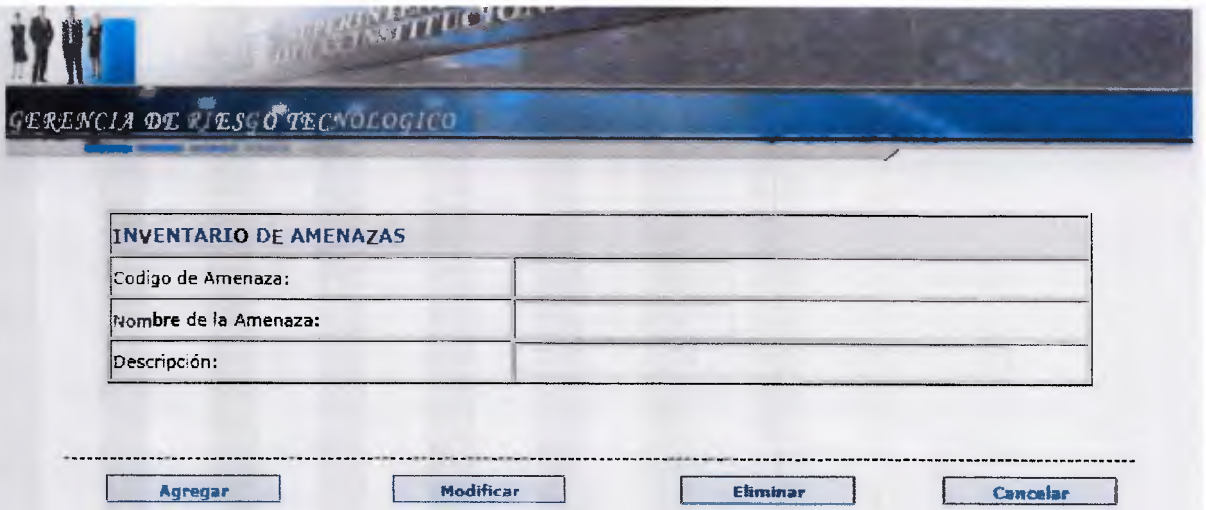


Figura 33: Prototipo - Inventario de Amenazas

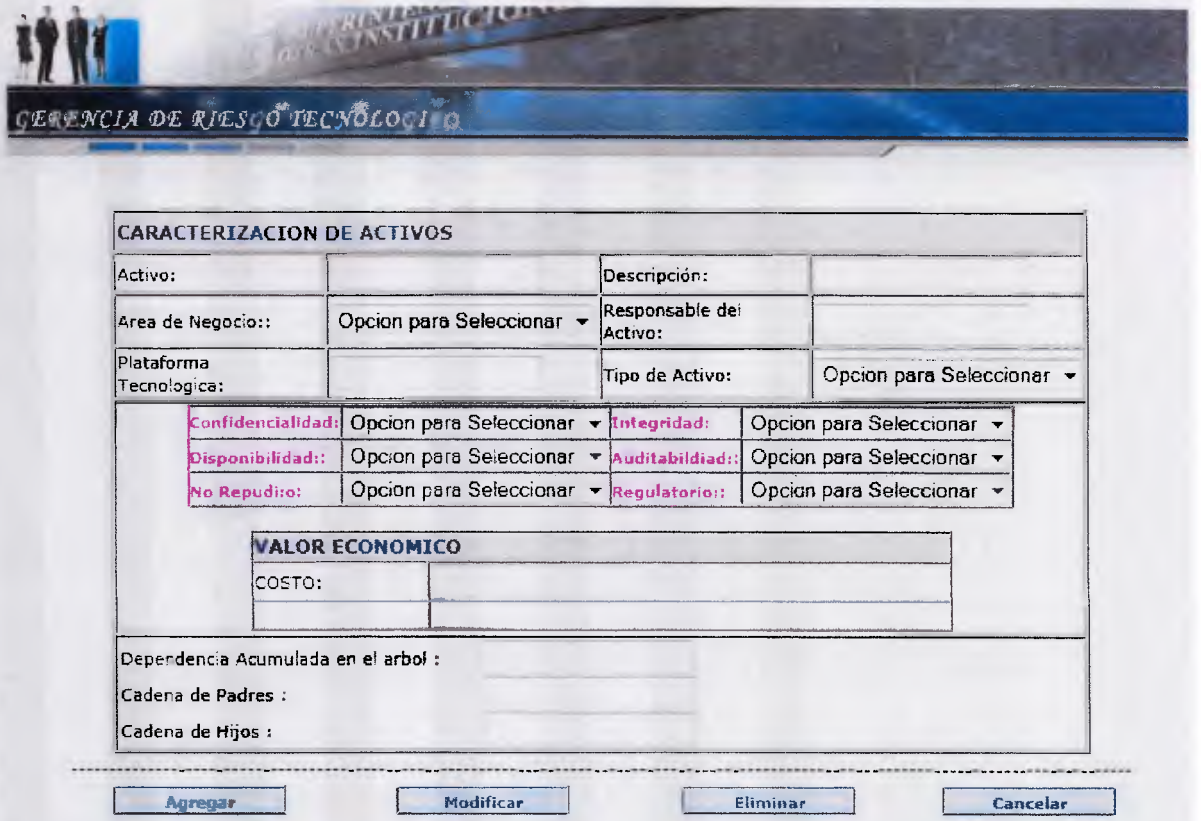


Figura 34: Prototipo - Caracterización de Activos

Figura 35: Prototipo - Generación de Informes

Es substancial destacar el apoyo de la organización para establecer un proyecto de desarrollo de software para la herramienta propuesta una vez completado y evaluado el prototipo presentado en este trabajo.

Capítulo V

Conclusiones y Recomendaciones

"Lo que escucho, lo olvido;
lo que veo, lo recuerdo; lo que hago, lo entiendo."

Confucio 451 B.C.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Las debilidades presentadas en la diversidad de las metodologías de análisis de riesgo y la aplicación de las mismas por parte de la Sudeban, permitió la presentación de este trabajo, orientado a describir una metodología adaptable a las necesidades del ente supervisor. Una vez concluida la investigación, se pueden emitir las siguientes conclusiones:

- Se realizo la narrativa sobre el proceso de inspección realizado por Sudeban con el fin de comprender como realizan el análisis y gestión de riesgo a las instituciones Financieras de Venezuela.
- Se analizaron los fundamentos teóricos en materia de metodologías de análisis y gestión de riesgos.
- Se enmarco el proyecto en la modalidad de proyecto factible, el cual consiste es una investigación elaboración y desarrollo de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de la organización. En el ámbito educativo, se presenta como una alternativa para el desarrollo de investigaciones innovadoras que buscan la creación de un nuevo producto.
- Se establecieron y cumplieron las fases para el desarrollo de la metodología: diagnostico del proceso actual de inspección, investigación documental, formulación del modelo y desarrollo del prototipo.
- Finalmente, la implementación del modelo permite organizar de forma sistemática los procesos de inspección contribuyendo con el uso eficiente de los recursos de fiscalización de la Sudeban, adicionalmente, los datos obtenidos en la aplicación del mismo proporciona un conjunto de estrategias y herramientas enfocadas a la administración y creación de conocimiento orientados apoyar los procesos de toma de decisiones por medio de la inteligencia organizacional o Business Intelligence (BI).

También se pueden mencionar las siguientes recomendaciones:

Como se ha mencionado a través del proyecto, el análisis de riesgos se realiza a partir del inventario de activos de información, recursos de información, amenazas y controles, teniendo en cuenta la información de que dispone la Organización. Para dar validez al análisis de estos inventarios es conveniente verificar que su grado de implantación y su eficacia se corresponden con las registradas en los inventarios.

En función de los controles seleccionadas se pueden realizar distintos tipos de prueba:

- **Pruebas de caja negra:** Son pruebas técnicas en las que se simula la realización de un ataque por parte de un atacante que no dispone de información sobre la infraestructura tecnológica de la Organización. Pueden realizarse desde el interior, simulando las potenciales actividades de un empleado que intente cometer fraude o desde el exterior, simulando las potenciales actividades de un atacante externo a la Organización.
- **Pruebas de caja blanca:** Son pruebas técnicas en las que se verifica la configuración real de los sistemas de información en referencia a las guías o estándares de configuración publicados por la Organización, por los fabricantes o por distintas organizaciones independientes.
- **Pruebas de procedimiento:** Son pruebas destinadas a conocer el grado de cumplimiento de los procedimientos establecidos por parte de los encargados de la ejecución de los diferentes controles. Generalmente se basan en la verificación del cumplimiento de las especificaciones del control para una selección de los casos planteados durante un periodo de tiempo definido.
- **Pruebas sustantivas:** Son pruebas destinadas a conocer el grado de cumplimiento de una determinada propiedad en los miembros de una determinada población, mediante el análisis de la población completa o de una muestra representativa.

En aras de la aplicabilidad de la metodología el personal de la Gerencia de Riesgo Tecnológico de la Sudeban deberá definir mecanismos que aseguren que los controles definidos y almacenados en las tablas de inventarios son consistente con sus necesidades.

Para la implementación de la herramienta, se deben definir un conjunto de formularios que permitirán hacer la toma de datos más eficaz, eficiente y homogénea en las Instituciones Financieras para luego ser incorporados en la herramienta propuesta. En la elaboración de los cuestionarios se debe tomar en cuenta tanto las necesidades de información de la metodología como las adaptaciones particulares realizadas en ella.

En otro orden de ideas, para realizar el análisis de riesgo continuo se recomienda establecer distintos tipos de mecanismos, que pueden estar relacionados entre sí. Algunos de los principales mecanismos para ello son:

- **Establecimiento de procedimientos de mantenimiento del análisis de riesgos**. Muchos de los cambios que se producen en las organizaciones, tanto en las áreas de negocio y soporte como en las áreas de TI, se realizan utilizando determinados procesos de gestión del cambio. Como parte constituyente de estos procesos de gestión de cambios debe incluirse la actualización del análisis de riesgos, de modo que el análisis de riesgos pueda evolucionar en paralelo a la Organización. Asimismo, deben establecerse procedimientos que actualicen el análisis de riesgos a partir de la información del entorno que la Organización reciba por distintas vías. El desarrollo de estos procedimientos de actualización debe llevar asociada la asignación de funciones y responsabilidades, así como la dotación de recursos técnicos, humanos y económicos necesarios.
- **Carga automática de recursos de información** en la herramienta de análisis de riesgos, de modo que la valoración del riesgo se adapte permanentemente con los cambios en los recursos empleados. Este mecanismo debe estar acompañado de los procedimientos necesarios para mantener la integridad del sistema. El establecimiento de las

relaciones entre los activos y los recursos de información se deberá realizar, en general, de forma manual, reflejándose las sustituciones de unos recursos por otros en el soporte de determinados activos o la asignación de los activos que van a soportar los nuevos recursos que se incorporen.

- **Establecimiento de procedimientos periódicos de revisión** del análisis de riesgos. Aunque se lleven a cabo los procedimientos adecuados para la evolución del análisis de riesgos con la evolución de la Organización y de su entorno, es conveniente realizar periódicamente una revisión completa del análisis realizado. Esto se debe a que los procedimientos de actualización continua pueden pasar por alto determinados cambios leves que, sostenidos en el tiempo, pueden terminar impactando sobre la valoración de los riesgos.

Establecer un proyecto de desarrollo de software donde se incluyan todas las actividades de elaboración de sistemas para la herramienta propuesta una vez completado y evaluado el prototipo presentado en este trabajo.

En líneas futuras, es importante evaluar la incorporación de la gestión del riesgo en el modelo propuesto, este proceso se realiza una vez estimado el estado del riesgo y se procede a notificar a la institución financiera objeto de la inspección el análisis de los resultados identificados, así como, de las recomendaciones para mitigar los mismos, con el fin de que ellos definan su plan de trabajo para su gestión y mitigación para luego ser remitidos a la Sudeban para posterior revisión y control previo.

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, S. y. (1998). *Metodología de la Investigación Científica.* La Habana: Alsi Colección Científica.

ASBA. (Mayo de 2010). *Riesgo Operativo.* Obtenido de *www.**asbaweb**.org*

AENOR – Asociación Española de Normalización y Certificación. (2008). UNE 71504 - *Metodología de Análisis y Gestión de Riesgos para los Sistemas de Información.* Recuperado el Diciembre de 2010, de http://www.aenor.es

AS/NZS – Australian Standards / New Zealand Standards. (2008). *AS/NZS 4360:2004 Risk management.* AENOR.

BSI – British Standards Institution. (2006). BS 7799-3:2006 *Information Security Management Systems.* Guidelines for information Security Risk Management.

Caralli R., S. J. (2007). *OCTAVE.* Recuperado el Enero de 2011, de Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process: http://www.cert.org/octav

Christopher J. Alberts, A. J. (2003). *Managing information Security Risks.* The OCTAVE Approach. Recuperado el Enero de 2011, de OCTAVE: http://www.cert.org/octave/

Christopher J. Alberts, A. J. (2001). *Method Implementation Guide.* Recuperado el Enero de 2011, de OCTAVE: http://www.cert.org/octave

Christopher J. Alberts, A. J. (s.f.). *OCTAVE-S Implementation* Guide. (2005, Ed.) Recuperado el Enero de 2011, de OCTAVE: (http://www.cert.org/octave)

Cazares, L. y. (1991). Técnicas Actuales de Investigación Documental. Mexico: Trillas.

Chang Kimlem, N. E. (1998). *Instituciones Financieras.* Valencia: Vadell Hermanos Editores, C.A. .

Comite Directivo de COBIT, C. D. (1998). *COBIT Objetivos de Control.*

Comité de Basilea. (2003). *Sanas Prácticas para la Gestión y Supervisión del Riesgo.* Obtenido de www.bis.org/publ/bcbs96.pdf

Coopers & Lybrand. (1997). Los Nuevos Conceptos de Control Interno. Informe COSO. España: Dias Santo C.A.

Davenport, T. (1999). *Some principles of Knowledge Management.* Recuperado el Enero de 2010, de University of Texas at Austin: http://www.knowledge-management-online.com

Gaceta Oficial de la Republica Bolivariana de Venezuela. (2006). *Ley General de Bancos y Otras Instituciones Financieras.* Venezuela: Euven.

Guilarte, M. (s.f.). *Bases Teóricas de la gerencia del conocimiento y su aplicación en la PYME.* Recuperado el Mayo de 2010, de http://biblio.ivic.ve/simposios/informacion/papers/pdf/paper08.pdf

Hansche S., B. J. (2004). (ISC) *Guide to the CISSP Exam*.

Harris, S. (2006). CISSP *Exam Guide: All In One* (3rd ed.).

Hernández, A. (Mayo de 2010). *El proyecto factible como modalidad en la investigación*. Obtenido de http://www.ucla.edu.ve/dmedicin/departamentos/medicinapreventivasocial/SE

ISACA. (2008). Seguridad de la información, CISM review manual 2008. ISACA.

ISF – Information Security Forum. (2006). Information Risk Analysis Methodologies. Obtenido de IRAM: http://www.securityforum.org/

ISO, International Organitation Standards. (2005). ISO/IEC 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI) .

ISO, International Organitation Standards. (2008). ISO/IEC 27005, Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de Seguridad de la Información.

ISO, International Organization Standards. (2004). ISO/IEC TR 13335-1, Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

ISO, International Organization Standards. (1997). ISO/IEC TR 13335-2, Information technology - Security techniques - Management of information and communications technology security - Part 2: Managing and planning. Switzerland.

ISO, International Organization Standards. (1998). ISO/IEC TR 13335-3, Information technology - Security techniques – Management of information and communications technology security. Part 3: Techniques for the management of IT Security.

ISO, International Organization Standards. (2000). ISO/IEC TR 13335-4, Information technology - Security techniques – Management of information and communications technology security – Part 4: Selection of safeguards.

ISO, International Organization Standards. (2001). ISO/IEC TR 13335-5, Information technology - Security techniques – Management of information and communications technology security – Part 5: Management guidance on network security.

Jiménez, W. (Mayo de 2008). *Curso sobre Formulación y Desarrollo de Proyectos Factibles*. Obtenido de http://www.slideshare.net/4066684/proyecto-factible-2009-uno /factible.pdf

Jones, J. (2005). *An Introduction to Factor Analysis of Information Risk*. Obtenido de FAIR – Factor Analysis of Information Risk: www.riskmanagementinsight.com. Recuperado el 2010 de DICIEMBRE

López F., Amutio. M. (2006). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Método (MAGERIT versión 2)*. (M. d. Públicas, Ed.) Recuperado el 2010 de DICIEMBRE, de MAGERIT: http://administracionelectronica.gob.es

López F., Amutio. M. (2006). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Guía de Técnicas (MAGERIT versión 2).* (M. d. Públicas, Ed.) Recuperado el 2010 de DICIEMBRE, de MAGERIT: http://administracionelectronica.gob.es

Morles, V. (1994). Planteamiento y Análisis de la Investigación. Caracas: El Dorado.

Portal de la norma ISO 15504-SPICE en Castellano. (s.f.). Obtenido de www.iso15544.es

Rocío, G. R. (s.f.). *El nuevo paradigma de la Gestión del Conocimiento y su aplicación al ámbito educativo.* Recuperado el Enero de 2010, de http://www.alide.org.pe/download/Foro/nuevoparadigma.PDF

Rodriguez, A. (1980). *Técnica y Organización Bancarias.* Buenos Aires: Macchi Hnos.

Rumbaugh, J. B. (2000). *El proceso unificado de desarrollo de software.* Madrid: Addison Wesley.

Sampieri, H. R., Carlos, F. C., & Baptista Lucio, P. (1991). *Metodología de la Investigación.* México: MCGRAW-HILL.

Soley, J. S., & Rahnema, A. (2004). *Basilea II, Una nueva forma de relación Banca-Empresa.* Madrid: McGraw Hill.

Sudeban, Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras. Caracas. 2007.

SOMAP – Security Officers Management & Análisis Project. (2006). Open Information Security Risk Assessment Guide. Obtenido de SOMAP: http://www.somap.org/

Stoneburner G., G. A. (2002). NIST SP 800-30, Risk Management Guide for Information Technology Systems. NIST Special Publication.

Telecommunications Agency. (2003). *CRAMM.* Recuperado el Diciembre de 2010, de CCTA Risk Análisis and Management Method (CRAMM): http://www.cramm.com.

University, C. M. (2006). *CMMI® for Development*, Version 1.2. U.S.

UPEL. (2005). Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales de la Universidad Pedagógica Experimental Libertador. Caracas: FEDUPEL.

Universidad Nacional Abierta. (1991). *Tecnica de Documentación de Investigación II.* Caracas: UNA. Primera Edición.

ANEXO I ÁREAS DE DOMINIO

A continuación una descripción de las áreas de dominio o procesos de negocio objeto de revisión en las inspecciones.

Planeación Estratégica	Aspectos asociados al plan estratégico de tecnología y su relación con el plan estratégico del negocio
Continuidad del Negocio	Aspectos asociados a la existencia, uso y prueba del plan de contingencias tecnológicas y de continuidad del negocio.
Proveedores Externos	Especifica los procedimientos y la metodología para la selección y evaluación de los proveedores externos, así como, la relación con terceras personas contratadas para cubrir o satisfacer algún servicio.
Sistemas de Información	Abarca actividades inherentes al procesamiento de datos en línea y en lotes, así como el uso, guarda y custodia de los respaldos y restauración de la información contenida en medios magnéticos. Aspectos considerados en el análisis, diseño, desarrollo e implantación de sistemas de información. Controles mínimos necesarios para administrar de manera efectiva las estructuras de información empleadas por los sistemas de información que almacenan datos.
Proyectos Tecnológicos	Especifica y controla los proyectos tecnológicos aprobados por la gerencia.
Plataforma Tecnológica	Abarca la información relacionada con la plataforma tecnológica de la institución financiera.
Seguridad	Incluye toda la información relacionada con los aspectos de seguridad de la institución.
Infraestructura de Telecomunicación	Establece los controles mínimos necesarios que aseguran el adecuado funcionamiento de los componentes de la red.
Canales Electrónicos	Maneja los sistemas, equipos, productos y servicios ofrecidos por las Instituciones Financieras a través del uso de Internet Banking, cajeros automáticos (ATM), puntos de ventas (POS), dispensadoras de chequera, sistemas de atención de reclamos y otros servicios que se encuentren automatizados a través de plataformas de cómputo.

Tabla 16:Áreas de Dominio del Modelo

ANEXO II DIMENSIONES DE SEGURIDAD

En este anexo se describen los requerimientos de seguridad básicos definidos en la metodología de análisis de riesgos y la escala a utilizar para su valoración (López F., 2006).

Definición de los requerimientos de seguridad

Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. ¿Qué importancia tendría que el activo no estuviera disponible?
Integridad de los datos	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento. ¿Qué importancia tendría que los datos fueran modificados sin control?
Confidencialidad de los datos	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso. ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
Autenticidad de los usuarios del servicio	Aseguramiento de la identidad u origen. ¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree? ¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?
Trazabilidad	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio? ¿Qué importancia tendría que no quedara constancia del acceso o modificación a los datos

Tabla 17:Dimensiones de Seguridad (Fuente Magerit - (López F., 2006))

Conviene destacar que los distintos requerimientos de seguridad no son totalmente independientes entre sí, existiendo algunos requerimientos para los que se espera una elevada correlación. Algunos ejemplos de estas correlaciones son:

- Un requerimiento elevado de confidencialidad se espera que generalmente lleve asociado un elevado requerimiento de trazabilidad, debido a la necesidad de identificar accesos no autorizados a la información.

- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de trazabilidad, debido a la necesidad de identificar modificaciones no autorizadas de la información.
- Un requerimiento elevado de disponibilidad se espera que generalmente lleve asociado un elevado requerimiento de integridad, debido a que el impacto entre no disponer de información para la ejecución de un proceso y que la información disponible no sea fiable, será generalmente similar.
- Un requerimiento elevado de confidencialidad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de usuarios, por la necesidad de garantizar la identidad de las personas que acceden a la información.
- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de usuarios, por la necesidad de garantizar la identidad de las personas que modifican la información.
- Un requerimiento elevado de integridad se espera que generalmente lleve asociado un elevado requerimiento de autenticidad de datos, debido a que el impacto de utilizar datos no fiables y utilizar datos no auténticos será, en muchos casos, similar

Escala de valoración de requerimientos de seguridad

Criterios de valoración		Valor				
		Crítico (10)	**Alto (5)**	**Medio (2)**	**Bajo (1)**	**Nulo (0)**
Estrategia de la Organización		Imposibilidad de seguir la estrategia fijada	Impacto grave sobre la estrategia	Impacto moderado sobre la estrategia	Impacto leve sobre la estrategia	No afecta a la estrategia de la Organización
Operaciones	Daños personales	Pérdida de varias vidas	Pérdida de una vida	Lesiones graves a una o varias personas	Daños leves a una o varias personas	No afecta a la seguridad de las personas
	Orden público	Alteración seria del orden público	Manifestaciones o presiones significativas	Protestas puntuales	Generación de malestar	No afecta al orden público
	Actividad de la Organización	Interrupción permanente de las actividades	Interrupción prolongada de las actividades	Interrupción breve de las actividades	Entorpecimiento de las actividades	No afecta a la actividad de la Organización
	Intereses comerciales (valor comercial)	Interés muy grande para la competencia	Alto interés para la competencia	Interés moderado para la competencia	Bajo interés para la competencia	Sin interés para la competencia
	Impacto sobre terceros (clientes, proveedores) (Evaluar la gravedad mediante los otros criterios)	Grave impacto para muchos terceros	Grave impacto para pocos terceros. Impacto moderado para muchos terceros	Grave impacto para un tercero. Impacto moderado para pocos terceros. Impacto leve para muchos terceros.	Impacto moderado para un tercero. Impacto leve para pocos terceros.	Impacto leve para un tercero. Sin impacto para terceros
	Relaciones internacionales	Impacto en las relaciones internacionales a	Impacto en las relaciones internacionales a	Impacto en las relaciones internacionales	Impacto leve en las relaciones internacionales	No tiene impacto en las relaciones internacionales

		alto nivel	nivel diplomático			
Información financiera y de gestión		Deficiencias materiales en la información	Deficiencias significativas en la información	Deficiencias moderadas en la información	Deficiencias leves en la información	Sin impacto sobre la información
Cumplimiento	Obligaciones legales y reglamentarias	Incumplimiento excepcionalmente grave de la ley	Incumplimiento grave de la ley	Incumplimiento moderado de la ley	Incumplimiento leve de la ley	Sin impacto sobre el cumplimiento
	Obligaciones contractuales	Incumplimiento excepcionalmente grave de obligaciones contractuales. Posible cancelación de contratos Relevantes.	Incumplimiento grave de obligaciones contractuales. Posibilidad de incurrir en penalizaciones relevantes.	Incumplimiento moderado de obligaciones contractuales. Posibilidad de deterioro de las relaciones con terceros relevantes.	Incumplimiento leve de obligaciones contractuales.	Sin impacto sobre el cumplimiento

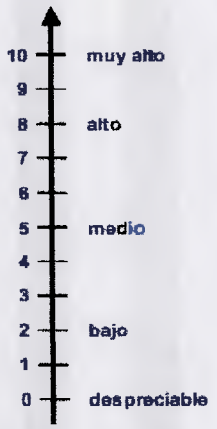
Tabla 18:Criterios de Valoración de Activos (Fuente Magerit - (López F., 2006))

ANEXO III CRITERIOS DE VALORACIÓN

Para valorar los activos vale, teóricamente, cualquier escala de valores. A efectos prácticos es sin embargo muy importante que

- se use una escala común para todas las dimensiones, permitiéndo comparar riesgos,
- se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas3 y
- se use un criterio homogéneo que permita comparar análisis realizados por separado

Para valorar los activos se ha elegido una escala detallada de diez valores, dejando el valor cero (0) como determinante de lo que sería un valor despreciable (a efectos de riesgo). La escala, se detallada a continuación:



valor		*criterio*
10	muy alto	daño muy grave a la organización
7-9	alto	daño grave a la organizacion
4-6	medio	daño importante a la organizacion
1-3	bajo	daño menor a la organizacion
0	despreciable	irrelevante a efectos prácticos

Tabla 19:Tabla de Valoración y Criterio de los Activos (Fuente Magerit - (López F., 2006))

La tabla siguiente pretende guiar con más detalle a los usuarios valorando de forma homogénea activos cuyo valor es importante por diferentes motivos, habiéndose tomado en consideración los siguientes:

- seguridad de las personas
- información de carácter personal
- obligaciones derivadas de la ley, del marco regulatorio, de contratos, etc.
- capacidad para la persecución de delitos
- intereses comerciales y económicos
- pérdidas financieras e interrupción del servicio
- orden público y política corporativa

ANEXO IV TIPOS DE ACTIVOS

En este anexo se detallan los tipos de activos incluidos en el inventario base de la metodología de análisis de riesgos. (López F., 2006).

La relación que sigue clasifica los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características que recoge el epígrafe. Nótese que las pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipo

[S] Servicios Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requieren una serie de medios. Los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la Organización a terceros), bien como servicios instrumentales (donde tanto los usuarios como los medios son propios), bien como servicios contratados (a otra organización que los proporciona con sus propios medios).	[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual) [ext] a usuarios externos (bajo una relación contractual) [int] interno (usuarios y medios de la propia organización) [cont] contratado a terceros (se presta con medios ajenos) [www] world wide web [telnet] acceso remoto a cuenta local [email] correo electrónico [file] almacenamiento de ficheros [ftp] transferencia de ficheros [edi] intercambio electrónico de datos [dir] servicio de directorio [idm] gestión de identidades [ipm] gestión de privilegios [pki] PKI - infraestructura de clave pública
[D] Datos / Información Elementos de información que, de forma singular o agrupados de alguna forma, representan el conocimiento que se tiene de algo. Los datos son el corazón que permite a una organización prestar sus servicios. Son en cierto sentido un activo abstracto que será almacenado en equipos o	[vr] datos vitales (vital records) [com] datos de interés comercial [adm] datos de interés para la administración pública [int] datos de gestión interna [voice] voz [multimedia] multimedia [source] código fuente [exe] código ejecutable [conf] datos de configuración [log] registro de actividad (log) [test] datos de prueba [per] datos de carácter personal (3) [A] de nivel alto

soportes de información (normalmente agrupado en forma de bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. Es habitual que en un análisis de riesgos e impactos, el usuario se limite a valorar los datos, siendo los demás activos meros sirvientes que deben cuidar y proteger los datos que se les encomiendan.	[M] de nivel medio [B] de nivel básico [label] datos clasificados [S] secreto [R] reservado [C] confidencial [DL] difusión limitada [SC] sin clasificar
[SW] Aplicaciones (software) Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. No preocupa en este apartado el denominado "código fuente" o programas que serán datos de interés comercial, a valorar y proteger como tales. Dicho código aparecería como datos	[prp] desarrollo propio (in house) [sub] desarrollo a medida (subcontratado) [std] estándar (off the shelf) [browser] navegador web [www] servidor de presentación [app] servidor de aplicaciones [email_client] cliente de correo electrónico [file] servidor de ficheros [dbms] sistema de gestión de bases de datos [tm] monitor transaccional [office] ofimática [av] anti virus [os] sistema operativo [ts] servidor de terminales [backup] sistema de backup
[HW] Equipos informáticos (hardware) Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión	[host] grandes equipos [mid] equipos medios [pc] informática personal [mobile] informática móvil [pda] agendas electrónicas [easy] fácilmente reemplazable [data] que almacena datos [peripheral] periféricos [print] medios de impresión [scan] escáneres [crypto] dispositivos criptográficos [network] soporte de la red [modem] módems [hub] concentradores [switch] conmutadores [router] encaminadores

de datos.	[bridge] pasarelas [firewall] cortafuegos [wap] punto de acceso wireless [pabx] centralita telefónica
[COM] Redes de comunicaciones Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.	[PSTN] red telefónica [ISDN] rdsi (red digital) [X25] X25 (red de datos) [ADSL] ADSL [pp] punto a punto [radio] red inalámbrica [sat] por satélite [LAN] red local [MAN] red metropolitana [Internet] Internet [vpn] red privada virtual
[SI] Soportes de información En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.	[electronic] electrónicos [disk] discos [san] almacenamiento en red [disquette] disquetes [cd] cederrón (CD-ROM) [usb] dispositivos USB [dvd] DVD [tape] cinta magnética [mc] tarjetas de memoria [ic] tarjetas inteligentes [non_electronic] no electrónicos [printed] material impreso [tape] cinta de papel [film] microfilm [cards] tarjetas perforadas
[AUX] Equipamiento auxiliar En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.	[power] fuentes de alimentación [ups] sistemas de alimentación ininterrumpida [gen] generadores eléctricos [ac] equipos de climatización [cabling] cableado [robot] robots [tape] ... de cintas [disk] ... de discos [supply] suministros esenciales [destroy] equipos de destrucción de soportes de información [furniture] mobiliario: armarios, etc [safe] cajas fuertes
[L] Instalaciones En este epígrafe entran los lugares donde se hospedan los	[site] emplazamiento [building] edificio [local] local [mobile] plataformas móviles [car] vehículo terrestre: coche, camión, etc.

sistemas de información y comunicaciones.	[plane] vehículo aéreo: avión, etc. [ship] vehículo marítimo: buque, lancha, etc. [shelter] contenedores [channel] canalización
[P] Personal En este epígrafe aparecen las personas relacionadas con los sistemas de información.	[ue] usuarios externos [ui] usuarios internos [op] operadores [adm] administradores de sistemas [com] administradores de comunicaciones [dba] administradores de BBDD [des] desarrolladores [sub] subcontratas [prov] proveedores

Tabla 20:Tipos de Activos (Fuente Magerit - (López F., 2006))

ANEXO V INVENTARIO DE AMENAZAS

En este anexo se detallan las amenazas incluidas en el inventario base de la metodología de análisis de riesgos de Magerit (López F., 2006). Para cada amenaza se presenta un cuadro como el siguiente:

[codigo] descripcion sucinta de lo que puede pasar	
Tipos de activos: ▯ que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

Figura 36: Descripción de Amenaza (Fuente Magerit - (López F., 2006))

[N] Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[N.1] Fuego	
Tipos de activos. ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion incendios posibilidad de que el fuego acabe con recursos del sistema.	

[N.2] Daños por agua	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion inundaciones: posibilidad de que el agua acabe con recursos del sistema	

[N.*] Desastres naturales	
Tipos de activos: ▯ [HW] equipos informaticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de informacion ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	Dimensiones: 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion: otros incidentes que se producen sin intervencion humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ... Se excluyen desastres específicos tales como incendios (ver [N 1]) e inundaciones (ver [N 2]). Se excluye al personal por cuanto se ha previsto una amenaza especifica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.	

[I] De origen industrial

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

[I 1] Fuego	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de informacion ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	Dimensiones: 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion incendio: posibilidad de que el fuego acabe con los recursos del sistema.	

[I.2] Daños por agua	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	Dimensiones: 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion escapes, fugas inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	

[I.*] Desastres industriales	
Tipos de activos	**Dimensiones:**
▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion otros desastres debidos a la actividad humana: explosiones, derrumbes, ... contaminación química, ... sobrecarga eléctrica, fluctuaciones eléctricas, ... accidentes de tráfico, ... Se excluyen amenazas especificas como incendio (ver [I.1]) e inundación (ver [I.2]). Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas	

[I 3] Contaminación mecánica	
Tipos de activos:	**Dimensiones:**
▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción vibraciones, polvo, suciedad ...	

[I 4] Contaminación electromagnetica	
Tipos de activos:	**Dimensiones:**
▯ [HW] equipos informaticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información (electronicos) ▯ [AUX] equipamiento auxiliar	1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion interferencias de radio campos magneticos, luz ultravioleta, ...	

[I 5] Averia de origen fisico o lógico	
Tipos de activos ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de informacion ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripción: fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante	

[I 6] Corte del suministro electrico	
Tipos de activos ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información (electrónicos) ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion cese de la alimentación de potencia	

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de informacion ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion deficiencias en la aclimatación de los locales, excediendo los margenes de trabajo de los equipos excesivo calor, excesivo frío, exceso de humedad, ...	

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción cese de la capacidad de transmitir datos de un sitio a otro Típicamente se debe a la destruccion física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destruccion, detención o simple incapacidad para atender al tráfico presente	

[I.9] Interrupcion de otros servicios y suministros esenciales	
Tipos de activos: ▯ [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad
Descripcion otros servicios o recursos de los que depende la operación de los equipos por ejemplo papel para las impresoras toner, refrigerante, ...	

[I.10] Degradacion de los soportes de almacenamiento de la informacion	
Tipos de activos: ▯ [SI] soportes de informacion	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos
Descripcion como consecuencia del paso del tiempo	

[I 11] Emanaciones electromagnéticas	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad
Descripcion hecho de poner vía radio datos internos a disposición de terceros Es una amenaza donde el emisor es víctima pasiva del ataque. Practicamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivandose una fuga de informacion Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés *"Transient Electromagnetic Pulse Standard"*). Abusando del significado primigenio, es frecuente oir hablar de que un equipo disfruta de *"TEMPEST protection"* queriendo decir que se ha diseñado para que no emita, electromagneticamente, nada de interes por si alguien lo captara No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.	

[E] Errores y fallos no intencionados

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

[E.1] Errores de los usuarios	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc	

[E 2] Errores del administrador	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / informacion ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción equivocaciones de personas con responsabilidades de instalación y operación	

[E.3] Errores de monitorizacion *(log)*	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / informacion ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [T_S] trazabilidad del servicio 2. [T_D] trazabilidad de los datos
Descripción: inadecuado registro de actividades falta de registros, registros incompletos, registros incorrectamente fechados registros incorrectamente atribuidos, ...	

[E.4] Errores de configuracion	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / informacion ▯ [SW] aplicaciones (software) ▯ [HW] equipos informaticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: introducción de datos de configuracion erroneos Practicamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

[E.7] Deficiencias en la organización	
Tipos de activos: ▯ [P] personal	**Dimensiones:** 1. [D] disponibilidad
Descripcion: cuando no esta claro quien tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omision, etc	

[E.8] Difusión de software dañino	
Tipos de activos: ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripcion: propagación inocente de virus espías *(spyware)* gusanos troyanos, bombas logicas, etc.	

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [T_S] trazabilidad del servicio
Descripción: envio de informacion a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera	

[E.10] Errores de secuencia	
Tipos de activos ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: alteración accidental del orden de los mensajes transmitidos	

[E.14] Escapes de información	
Tipos de activos ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	Dimensiones: 1. [C] confidencialidad
Descripcion la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en si misma se vea alterada.	

[E 15] Alteracion de la informacion	
Tipos de activos ▯ [D] datos / información	Dimensiones: 1. [I] integridad
Descripcion alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas especificas.	

[E.16] Introduccion de información incorrecta	
Tipos de activos: ▯ [D] datos / informacion	Dimensiones: 1. [I] integridad
Descripcion inserción accidental de información incorrecta. Esta amenaza solo se identifica sobre datos en general, pues cuando la informacion está en algún soporte informatico, hay amenazas especificas.	

[E.17] Degradación de la informacion	
Tipos de activos: ▯ [D] datos / informacion	Dimensiones: 1. [I] integridad
Descripción degradacion accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la informacion está en algún soporte informático, hay amenazas específicas	

[E.18] Destrucción de informacion	
Tipos de activos ▯ [D] datos / información	Dimensiones: 1. [D] disponibilidad
Descripcion: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas especificas	

[E.19] Divulgación de información	
Tipos de activos: ▯ [D] datos / informacion	**Dimensiones:** 1. [C] confidencialidad
Descripcion: revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripcion defectos en el codigo que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	

[E.21] Errores de mantenimiento / actualizacion de programas (software)	
Tipos de activos: ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad
Descripcion defectos en los procedimientos o controles de actualizacion del codigo que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	
Tipos de activos: ▯ [HW] equipos informáticos (hardware)	**Dimensiones:** 1. [D] disponibilidad
Descripción defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizandose mas allá del tiempo nominal de uso	

[E.24] Caida del sistema por agotamiento de recursos	
Tipos de activos: ▯ [S] servicios ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: la carencia de recursos suficientes provoca la caida del sistema cuando la carga de trabajo es desmesurada	

[E.28] Indisponibilidad del personal	
Tipos de activos: ▯ [P] personal interno	Dimensiones: 1. [D] disponibilidad
Descripción ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriologica, ...	

[A] Ataques intencionados

Fallos deliberados causados por las personas. La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

[A.4] Manipulación de la configuracion	
Tipos de activos: ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	Dimensiones: 1. [I] integridad 2. [C] confidencialidad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos 7. [D] disponibilidad
Descripcion: prácticamente todos los activos dependen de su configuración y esta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc	

[A.5] Suplantación de la identidad del usuario	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [A_S] autenticidad del servicio 3. [A_D] autenticidad de los datos 4. [I] integridad
Descripcion cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organizacion o por personal contratado temporalmente	

[A.6] Abuso de privilegios de acceso	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad
Descripcion: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas	

[A.7] Uso no previsto	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales programas personales, almacenamiento de datos personales, etc.	

[A.8] Difusión de software dañino	
Tipos de activos: ▯ [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A_S] autenticidad del servicio 5. [A_D] autenticidad de los datos 6. [T_S] trazabilidad del servicio 7. [T_D] trazabilidad de los datos
Descripción: propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc.	

[A.9] [Re-]encaminamiento de mensajes	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [T_S] trazabilidad del servicio
Descripcion envio de información a un destino incorrecto a traves de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas entre procesos o entre unos y otros Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	

[A.10] Alteración de secuencia	
Tipos de activos: ▯ [S] servicios ▯ [SW] aplicaciones (software) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripcion alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes perjudicando a la integridad de los datos afectados.	

[A.11] Acceso no autorizado	
Tipos de activos ▯ [S] servicios ▯ [D] datos / información ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dim1nsiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio
Descripción el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	

[A.12] Analisis de tráfico	
Tipos de activos: ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios A veces se denomina 'monitorización de tráfico".	

[A.13] Repudio	
Tipos de activos ▯ [S] servicios	**Dimensiones:** 1. [T_S] trazabilidad del servicio
Descripcion negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	

[A.14] Interceptacion de información (escucha)	
Tipos de activos: ▯ [D] datos / informacion ▯ [SW] aplicaciones (software) ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	

[A.15] Modificacion de la informacion	
Tipos de activos: ▯ [D] datos / informacion	Dimensiones: 1. [I] integridad
Descripcion alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza solo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

[A.16] Introduccion de falsa informacion	
Tipos de activos: ▯ [D] datos / información	Dimensiones: 1. [I] integridad
Descripcion inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la informacion está en algún soporte informático, hay amenazas específicas	

[A.17] Corrupcion de la información	
Tipos de activos: ▯ [D] datos / informacion	Dimensiones: 1. [I] integridad
Descripcion degradacion intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio Esta amenaza sólo se identifica sobre datos en general, pues cuando la informacion está en algún soporte informático, hay amenazas específicas.	

[A.18] Destruccion la informacion	
Tipos de activos: ▯ [D] datos / informacion	Dimensiones: 1. [D] disponibilidad
Descripcion: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algun soporte informático. hay amenazas específicas	

[A.19] Divulgación de información	
Tipos de activos: ▯ [D] datos / informacion	Dimensiones: 1. [C] confidencialidad
Descripción revelación de informacion	

[A.22] Manipulación de programas	
Tipos de activos ▯ [SW] aplicaciones (software)	Dimensiones: 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción alteracion intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza	

[A.24] Denegacion de servicio	
Tipos de activos ▯ [S] servicios ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones	Dimensiones: 1. [D] disponibilidad
Descripcion la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	

[A.25] Robo	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de informacion ▯ [AUX] equipamiento auxiliar	Dimensiones: 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de informacion los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organizacion o personas contratadas de forma temporal lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias En el caso de equipos que hospedan datos, ademas se puede sufrir una fuga de informacion	

[A.26] Ataque destructivo	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de informacion ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: vandalismo, terrorismo, acción militar, ... Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organizacion o por personas contratadas de forma temporal.	

[A.27] Ocupación enemiga	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripcion: cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	

[A.28] Indisponibilidad del personal	
Tipos de activos: ▯ [P] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción ausencia deliberada del puesto de trabajo como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ...	

[A.29] Extorsión	
Tipos de activos: ▯ [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	

[A.30] Ingeniería social	
Tipos de activos ▯ [P] personal interno	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A_S] autenticidad del servicio 4. [A_D] autenticidad de los datos 5. [T_S] trazabilidad del servicio 6. [T_D] trazabilidad de los datos
Descripción abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

Tabla 21:Inventario de Amenazas (Fuente Magerit - (López F., 2006))

Para completar la anterior presentación amenaza por amenaza, los siguientes cuadros agrupan las amenazas según el tipo de activo, indicando en qué dimensión de seguridad puede afectarles significativamente. Nótese que debido a las dependencias entre activos, los activos inferiores soportan el valor de los activos superiores, siendo aquellos la vía por la que resultan perjudicados estos.

[S] Servicios				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
E.1 E.2 E.4 E.24	E.1 E.2 E.4 E.9 E.10	E.2 E.4 E.9	E.2 E.4 E.9	E.2 E.3 E.4 E.9
A.4 A.7 A.24	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.5 A.6 A.9 A.11	A.4 A.5 A.9 A.11	A.4 A.9 A.13

Tabla 22:Amenazas por Activos de Servicio (Fuente Magerit - (López F., 2006))

[D] Datos / Información				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
E.1 E.2 E.3 E.18	E.1 E.2 E.3 E.15 E.16 E.17	E.2 E.3 E.14 E.19	E.2 E.4	E.2 E.3 E.4

A.4 A.18	A.4 A.11 A.15 A.16 A.17	A.4 A.11 A.14 A.19	A.4 A.11	A.4

Tabla 23:Amenazas por Activos de Datos / Información (Fuente Magerit - (López F., 2006))

[SW] Aplicaciones (software)				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
I.5				I.5
E.1 E.2 E.4 E.8 E.20 E.21	E.1 E.2 E.4 E.8 E.9 E.10 E.20 E.21	E.2 E.4 E.8 E.9 E.14 E.20	E.2 E.4 E.8 E.9	E.2 E.3 E.4 E.8 E.9
A.4 A.7 A.8	A.4 A.5 A.6 A.8 A.9 A.10 A.11 A.22	A.4 A.5 A.6 A.8 A.9 A.11 A.14 A.22	A.4 A.5 A.8 A.9 A.11 A.22	A.4 A.8 A.9 A.22

Tabla 24:Amenazas por Activos de Aplicaciones (Fuente Magerit - (López F., 2006))

[HW] Equipos informáticos (hardware)				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7		I.11		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
E.2 E.4 E.23 E.24	E.2 E.4	E.2 E.4	E.2 E.4	E.2 E.4
A.4 A.7 A.24	A.4 A.6 A.11	A.4 A.6 A.11	A.4 A.11	A.4

A.25 A.26 A.27		A.14 A.25 A.27		

Tabla 25:Amenazas por Activos de Equipos informáticos (Fuente Magerit - (López F., 2006))

[COM] Redes de comunicaciones				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.8		I.11		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
E.2 E.4 E.24	E.2 E.4 E.9 E.10	E.2 E.4 E.9 E.14	E.2 E.4 E.9	E.2 E.4 E.9
A.4 A.7 A.24 A.25 A.26 A.27	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.5 A.6 A.9 A.11 A.12 A.14 A.25	A.4 A.5 A.9 A.11	A.4 A.9

Tabla 26:Amenazas por Activos de Redes de Comunicación (Fuente Magerit - (López F., 2006))

[SI] Soportes de información				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.10 I.10				N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
A.7 A.25 A.26 A.27	A.11	A.11 A.25 A.27	A.11	

Tabla 27:Amenazas por Activos de Soportes de Información (Fuente Magerit - (López F., 2006))

[AUX] Equipamiento auxiliar				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.9				N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
A.7 A.25 A.26 A.27	A.11	A.11 A.25 A.27	A.11	

Tabla 28:Amenazas por Activos de Equipamiento Auxiliar (Fuente Magerit - (López F., 2006))

[L] Instalaciones				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
N.1 N.2 N.* I.1 I.2 I.*				N.1 N.2 N.* I.1 I.2 I.*
A.7 A.26 A.27	A.11	A.11 A.27	A.11	

Tabla 29:Amenazas por Activos de Instalaciones (Fuente Magerit - (López F., 2006))

[P] Personal				
Disponibilidad	**Integridad**	**Confiabilidad**	**Autenticidad**	**Trazabildiad**
E.7 E.28				
A.28	A.29 A.30	A.29 A.30	A.29 A.30	A.29 A.30

Tabla 30:Amenazas por Activos de Personal (Fuente Magerit - (López F., 2006))

ANEXO VI INVENTARIO DE CONTROLES

En este anexo se detallan los controles incluidos en el inventario base de la metodología de análisis de riesgos. [ISO27002.05]

Políticas, normas y procedimientos	- Política de seguridad de la información - Revisión de la política de seguridad de la información
Organización y estructura	- Compromiso de la dirección con la seguridad de la información - Coordinación de la seguridad de la información - Asignación de las responsabilidades de la seguridad de la información - Proceso de la autorización para las instalaciones de tratamiento de la información - Acuerdos de confidencialidad - Contacto con autoridades - Contacto con los grupos de interés especial - Revisión independiente de la seguridad de la información - Identificación de los riesgos relacionados con externos - Abordando la seguridad al tratar con clientes - Abordando la seguridad en acuerdos con terceros
Control de activos	- Inventario de activos - Propiedad de los activos - Uso aceptable de los activos - Guías de clasificación - Etiquetado y tratamiento de la información
Control de empleados	- Roles y responsabilidades – Investigación - Términos y condiciones de la ocupación - Responsabilidades de la dirección - Conocimiento, educación, y entrenamiento en la seguridad de la información - Proceso disciplinario - Responsabilidades de la terminación - Devolución de activos - Retirada de los derechos de acceso
Control de la seguridad física	- Perímetro de seguridad física - Controles de entrada física - Asegurar oficinas, salas, e instalaciones - Protección contra amenazas externas y ambientales - Trabajo en áreas seguras - Acceso público, entrega, y áreas de carga - Localización y protección de equipos - Mantenimiento de suministros - Seguridad del cableado - Mantenimiento de los equipos - Seguridad de equipos fuera de los locales de la organización - Eliminación y re-utilización segura de equipos - Extracción de propiedades
Control de las	- Procedimientos operacionales documentados

operaciones de los sistemas de información	- Gestión del cambio - Segregación de tareas - Separación de los entornos de desarrollo, pruebas, e instalaciones operacionales - Entrega de servicio - Supervisión y revisión de los servicios de terceros - Gestión de cambios en servicios de terceros - Gestión de capacidades - Aceptación de sistemas - Controles contra código malicioso - Controles contra código móvil - Copia de seguridad de la información - Gestión de soportes extraíbles - Eliminación de soportes - Procedimientos de utilización de la información - Seguridad de la documentación de sistemas - Procedimientos y políticas de intercambio de información - Acuerdos de intercambio - Soportes físicos en tránsito - Mensajería electrónica (Correo Electrónico, EDI, etc.) - Sistemas de información de negocio - Comercio electrónico - Transacciones On-line - Información pública disponible - Registros de auditoría - Monitorización de uso de sistemas - Protección de información de registros - Registros de administrador y operadores - Registro de fallos - Sincronización de relojes
Control de acceso lógico	- Política de control de acceso - Registro de usuario - Gestión de privilegios - Gestión de contraseñas de usuarios - Revisión de los derechos de usuario - Uso de contraseñas - Equipo informático de usuario desatendido - Política de puesto de trabajo vacío - Procedimientos de inicio de sesión segura - Identificación y autenticación del usuario - Sistema de gestión de contraseñas - Uso de las utilidades del sistema - Sesiones inactivas - Limitación del tiempo de conexión - Restricción de acceso a la información - Aislamiento de sistemas sensibles - Informática móvil – Teletrabajo
Control de las comunicaciones	- Controles de red - Seguridad de servicios de red - Política de uso de servicios de red - Autenticación de usuarios por conexiones externas - Identificación de equipos en red

	- Protección de los puertos de diagnostico remoto - Segregación de redes - Control de conexión a redes - Control de encaminamiento de la red
Control de la adquisición, desarrollo y mantenimiento de aplicaciones	- Análisis y especificación de requerimientos de seguridad - Validación de los datos de entrada - Control del proceso interno - Integridad de mensajes - Validación de los datos de salida - Política de uso de los controles criptográficos - Gestión de claves - Control del software en producción - Protección de los datos de prueba de sistema - Control de acceso al código de fuente del programa - Procedimientos de control de cambios - Revisión técnica de las aplicaciones tras cambios en el sistema operativo - Restricciones en cambios de paquetes de software - Fuga de información - Desarrollo externalizado del software - Control de vulnerabilidades técnicas
Gestión de los incidentes de seguridad	- Comunicación de eventos de seguridad de la información - Comunicación de vulnerabilidades - Responsabilidades y procedimientos - Aprendiendo de las incidencias de seguridad de la información - Recogida de pruebas
Gestión de la continuidad	- Inclusión de la seguridad de la información en el proceso de la gestión de la continuidad del negocio - Continuidad del negocio y valoración del riesgo - Desarrollo e implementación de planes de continuidad incluyendo la seguridad de la información - Marco de planificación para la continuidad del negocio - Prueba, mantenimiento y reevaluación de los planes de continuidad
Cumplimiento regulatorio	- Identificación de la legislación aplicable - Derechos de propiedad intelectual (IPR) - Salvaguarda de los registros de la Organización - Protección de datos de carácter personal y de la intimidad de las personas - Evitar el mal uso de los recursos de tratamiento de la información - Reglamentación de los controles de cifrado - Cumplimiento con políticas y estándares de seguridad - Comprobación del cumplimiento técnica - Controles de auditoría de sistemas de información - Protección de las herramientas de auditoría de sistemas

Tabla 31:Inventario de Controles (Fuente Magerit - (López F., 2006))

ANEXO VII DESCRIPCIÓN DE CASOS DE USO

A continuación se presentan los casos de usos que engloban las funcionalidades del sistema a desarrollar.

Código: Nombre: Datos: Requerimientos:	CU01 Inicio sesión Nombre de usuario de red, contraseña -La aplicación presentará un formulario donde se podrán introducir el nombre de usuario y la contraseña las cuales serán tomadas del servicio de directorio activo. -El servicio de directorio validará el nombre de usuario y la contraseña y sólo permitirá el acceso a la aplicación en caso de que sean correctos. -En caso de que el nombre de usuario y la contraseña no sean correctos se mostrará un mensaje de error y no se permitirá el acceso.

Código: Nombre: Datos: Requerimientos:	CU02 Planificación de inspección Código de la inspección, fecha de inicio, Institución donde se realiza la inspección, descripción del alcance, áreas de dominio a revisar, objetivos de cada área y descripción de los antecedentes. -La aplicación presentará un formulario donde se podrán introducir los datos del proceso de planificación de la inspección. -Se debe contar con un listado de las áreas de dominio e instituciones financieras. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -Se debe contar con una sección para incluir el cronograma de actividades.

Código: Nombre: Datos: Requerimientos:	CU03 Requerimientos de seguridad de la información Identificador del requerimiento de seguridad, Nombre descriptivo del requerimiento de seguridad. -La aplicación presentará un formulario donde se podrán introducir los requerimientos de seguridad. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de requerimientos de seguridad que estén en uso en la inspección de valoración

Código:	CU04
Nombre:	Escalas de valoración
Datos:	Identificador de la escala de valoración, Nombre descriptivo de la escala de valoración, Una lista de entre 3 y 10 valores válidos de la escala, incluyendo para cada uno de ellos: - Posición dentro de la escala - Nombre corto del valor - Nombre descriptivo del valor - Descripción del valor - Rango (valor máximo y mínimo) cuantitativo del valor - Valor cuantitativo correspondiente al valor
Requerimientos:	-La aplicación presentará un formulario donde se podrán introducir las escalas de valoración. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de escalas que estén en uso en los requerimientos de seguridad.

Código:	CU05
Nombre:	Inventario de activos
Datos:	Código del grupo de activo Nombre del activo de información. Descripción del contenido del activo de información. Descripción del uso que se da a esta información en el contexto del proceso considerado y de otros procesos que puedan estar relacionados. Recursos de información que se utilizan para procesar y almacenar el activo de información. Valor económico del activo en bolívares Valor no económico del activo Cadena de padres e hijos
Requerimientos:	-La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación. -La aplicación permitirá mantener la relación de activos y recursos de información

Código:	CU06
Nombre:	Inventario de amenazas
Datos:	Código del grupo de amenaza Identificador de tipo de amenaza, Nombre descriptivo del tipo de amenaza
Requerimientos:	-La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación,

	modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación.

Código: Nombre: Datos: Requerimientos:	CU07 Inventario de controles Identificador de tipo de control, Descripción del control, Área de dominio donde aplica Grado de implementación Indicador de mecanismo existente Indicador de mecanismo propuesto Indicador de mecanismo para la simulación Código del grupo al que pertenece -La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación.

Código: Nombre: Datos: Requerimientos:	CU08 Inventario de Pruebas Identificador de la prueba, Descripción de la prueba, Área de dominio donde aplica -La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación.

Código: Nombre: Datos: Requerimientos:	CU09 Inventario de Instrucciones Identificador de la instrucción, Descripción de la instrucción, riesgo al que aplica, Tipo de instrucción Tres campos de texto libre para indicar taxonomías adicionales de las instrucciones, tales como: preventiva/detectiva,técnica/procedimental, general/específica, etc -La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación. -Se dispondrá de una opción de exportación de los datos.

Código: Nombre: Datos: Requerimientos:	CU10 Inventario de Riesgos Identificador del riesgo, Descripción del riesgo, áreas de dominio al que aplica -La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación. -

Código: Nombre: Datos: Requerimientos:	CU11 Valoración de amenazas por activo. Se dispondrá de una tabla con todas las combinaciones posibles entre tipo de recurso, amenaza y requerimiento de seguridad, con un porcentaje de degradación asignado. Se creará un requerimiento de seguridad ficticio (vacío) en que se registrará la frecuencia de realización de la amenaza sobre el tipo de recurso, en forma de porcentaje (100% = una vez al año) -La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación. -

Código: Nombre: Datos: Requerimientos:	CU12 Valoración por defecto de la eficacia de los controles. Se dispondrá de una tabla con todas las combinaciones posibles entre amenaza, instrucciones y requerimientos de seguridad, con un porcentaje de eficacia en la reducción de la degradación asignado. Se creará un requerimiento de seguridad ficticio (vacío) en que se registrará la eficacia en la reducción de la frecuencia de realización de la amenaza, en forma de porcentaje. -La aplicación presentará un formulario donde se podrán introducir el inventario. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de objetos del inventario si están siendo usados en la aplicación. -

Código:	CU13
Nombre:	Valoración de los activos de información
Datos:	
Requerimientos:	-La aplicación presentará un formulario donde se podrán introducir la valoración. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -La aplicación deberá permitir realizar la valoración de los activos de información teniendo en cuenta los diferentes requerimientos de seguridad definidos en la metodología. -El Evaluador de riesgos seleccionará los auditores encargados de la valoración y les asignará permisos de valoración en la inspección de análisis. -La aplicación creará para cada usuario valorador una matriz con los activos seleccionados en el alcance de la inspeccion en las filas y los requerimientos de seguridad en las columnas. -Por defecto, todos los activos tendrán una aloración vacía. -Cada usuario tendrá la posibilidad de exportar/importar la matriz en formato Microsoft Excel para su tratamiento. -Una vez cumplimentada la matriz, el usuario deberá marcarla como finalizada. Una vez marcada, no podrá hacer modificaciones sobre las valoraciones introducidas. -El evaluador de riesgos podrá marcar como finalizada o eliminar las valoraciones de cada usuario en cualquier momento. -Una vez finalizadas todas las valoraciones, el auditor de riesgos podrá obtener el resultado de la valoración, que se calculará automáticamente como la media de los valores introducidos para cada par activo de información – requerimiento de seguridad. -Los valores vacíos no se tendrán en cuenta en el cálculo. -Si una casilla sólo presenta valores vacíos se valorará como cero. -Una vez calculado el resultado de la valoración, no será posible crear o modificar las valoraciones.

Código:	CU14
Nombre:	Áreas de Dominio
Datos:	Identificador del área, Nombre descriptivo del área.
Requerimientos:	-La aplicación presentará un formulario donde se podrán introducir las áreas. -La aplicación permitirá las operaciones de agregación, modificación y consultar. -No se permitirá la eliminación de áreas que estén en

	uso en la inspección.

Código: Nombre: Datos: Requerimientos:	CU15 Perfiles de Usuario Identificador del perfil Nombre del perfil -La aplicación presentará un formulario donde se podrán introducir los perfiles. -La aplicación permitirá las operaciones de agregación, modificación y consultar.

Código: Nombre: Datos: Requerimientos:	CU16 Modulo de Estimación del estado del riesgo Código de la inspección -La aplicación presentará un formulario donde se podrán seleccionar el código de la inspección. -La aplicación muestra el mapa de riesgo intrínseco y efectivo una vez cargado todos los datos de la inspección. -Una vez realizada la valoración de activos y de amenazas, la aplicación utilizará la información obtenida para realizar el cálculo del riesgo intrínseco por activo de información y por recurso de información

Código: Nombre: Datos: Requerimientos:	CU17 Modulo de Reporte Código de la inspección -La aplicación presentará un formulario donde se podrán seleccionar el código de la inspección. -La aplicación muestra el informe de la inspección. -El sistema deberá mostrar informes y gráficos con los resultados de los análisis realizados. Estos informes serán: Riesgo intrínseco, Listado del riesgo intrínseco por activo, Listado del riesgo intrínseco por activo desglosado por requerimiento de seguridad, gráfico de barras de riesgo intrínseco por activo, gráfico de barras de riesgo intrínseco por activo desglosado por requerimiento de seguridad -Mapa de riesgos por activos, sobre la matriz de activos (por filas) y requerimientos de seguridad (por columnas), con un código semafórico cuyos umbrales serán configurables por el usuario en la propia pantalla, utilizando por defecto los percentiles 33 y 66. -Mapa de riesgos por recursos. -Mapa de riesgos por activos, con las amenazas. -Mapa de riesgos por recursos, con las amenazas.

Código: Nombre: Datos: Requerimientos:	CU18 Inventario de Recursos de Información Identificador del recurso Nombre del recurso, tipo de recurso -La aplicación presentará un formulario donde se podrán introducir los perfiles. -La aplicación permitirá las operaciones de agregación, modificación y consultar.

Código: Nombre: Datos: Requerimientos:	CU19 Amenaza – Activo Código de la amenaza Código del Activo Vulnerabilidad, degradación, Impacto, Riesgo Intrínseco y Efectivo -Representa las amenazas que pueden afectar a cada activo. -La aplicación presentará un formulario donde se podrán introducir las amenazas a los activos. -La aplicación permitirá las operaciones de agregación, modificación y consultar si los activos no tienen relaciones.

Código: Nombre: Datos: Requerimientos:	CU20 Amenaza – Control Código de la amenaza Código del control Disminución de la vulnerabilidad Disminución del impacto -Representa los controles aplicados a la amenaza. -La aplicación presentará un formulario donde se podrán introducir las amenazas a los activos. -La aplicación permitirá las operaciones de agregación, modificación y consultar si los activos no tienen relaciones.