GESTIÓN DE RIESGOS Y CONTROLES EN SISTEMAS DE INFORMACIÓN

MARLENE LUCILA GUERRERO JULIO

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERÍAS FISICO – MECÁNICAS

MATESRÍA EN INGENIERÍA ÁREA INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

BUCARAMANGA

2010

GESTIÓN DE RIESGOS Y CONTROLES EN SISTEMAS DE INFORMACIÓN

MARLENE LUCILA GUERRERO JULIO

Proyecto de Investigación para optar al título de:

Magister en Ingeniería Área Informática y Ciencias de la Computación

DIRECTOR DEL PROYECTO

MSc. LUIS CARLOS GOMEZ FLOREZ

Profesor Escuela de Ingeniería de Sistemas

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE INGENIERÍAS FISICO – MECÁNICAS

MATESRÍA EN INGENIERÍA ÁREA INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

BUCARAMANGA

2010

AGRADECIMIENTO

A Dios por darme la fortaleza para alcanzar esta meta. A Eduardo mi esposo quien me acompañó en este esfuerzo y a mis Padres que han sido mi guía y apoyo durante toda mi vida.

Al grupo de investigación en Sistemas y Tecnologías de la Información – STI de la Universidad Industrial de Santander y a la Maestría en Ingeniería área Informática y Ciencias de la Computación por los conocimientos adquiridos.

Marlene G.

TABLA DE CONTENIDO

INTRODUCCIÓN 14

1. ACERCAMIENTO A LA SITUACIÓN DE INTERÉS 16

1.1 Sistemas de Información 17

1.1.1 Elementos de un Sistema de Información 17

1.1.2 Tipos de Sistemas de Información 19

1.2 Seguridad de la Información 20

1.2.1 Criterios de la Seguridad de la Información 20

1.2.2 El Estado de la Seguridad de la Información en la Actualidad 20

1.2.3 La Seguridad de los Sistemas de Información 24

1.3 Alcance de la Propuesta de Investigación 24

2. LA METODOLOGÍA DE LOS SISTEMAS BLANDOS MSB. El pensamiento de sistemas blandos como guía del proceso de intervención. 27

2.1 Supuestos Onto-Epistemológicos de la MSB 27

2.1.1 Etapa 1. La Situación Considerada Problemática 29

2.1.2 Etapa 2. La Situación Problema Expresada 29

2.1.3 Etapa 3. Definición Raíz de los Sistemas de Actividad Humana más Relevantes 29

2.1.4 Etapa 4. Desarrollando los Modelos Conceptuales 30

2.1.5 Etapa 5. Comparación de los Modelos y el Mundo Real 31

2.1.6 Etapa 6. Cambios sistémicamente deseables y culturalmente factibles 31

2.1.7 Etapa 7. Acción para Mejorar la Situación 31

2.2 Aplicaciones de la MSB a Sistemas de Información 32

2.3 Aplicación de la MSB en el Contexto de la Investigación sobre GRCSI 34

3. NOCIONES ACERCA DE LA CALIDAD 35

3.1 Acercamiento Conceptual a la Teoría de la Calidad 35

3.1.1. La Calidad en la Literatura 35

3.1.2. La Calidad en los Estándares 39

3.1.3. La Calidad en los Sistemas de Información 47

4. NOCIONES ACERCA DE LA GESTIÓN DE RIESGOS 49

4.1 El Concepto de Gestión de Riesgos 49

4.2 Gestión de Riesgos y Controles en Sistemas de Información 50

4.2.1. El Concepto de "Riesgos y Controles en Sistemas de Información". 50

4.2.2. Modelos de Gestión de Riesgos y Controles en Sistemas de Información. 51

4.3 Revisando las Actividades de GRCSI en el Marco de los Estándares 61

4.3.1. Elaboración de una Imagen Enriquecida de los Procesos para la Gestión de Riesgos y Controles en los Sistemas de Información....64
4.3.2. Niveles de riesgo en SI y su identificación en la organización....68

5. HACIA UNA COMPRENSIÓN DEL SISTEMA DE ACTIVIDAD HUMANA – SAH PARA LA GESTIÓN DE RIESGOS Y CONTROLES EN SI....88

5.1 Propuesta del SAH para la Gestión de Riesgos y Controles en los Sistemas de Información....88
5.1.1. Definición Raíz....88
5.1.2. Elementos CATWOE....89
5.1.3. Descripción de las Actividades Propuestas Para la Gestión de Riesgos y Controles en los Sistemas de Información....90
5.1.4. Actividad A1. Establecer el Contexto Organizacional....90
5.1.5. Actividad A2. Identificar los Activos Críticos....97
5.1.6. Actividad A3. Identificar y Evaluar las Amenazas y Vulnerabilidades de los Activos Críticos 101
5.1.7. Actividad A4. Diseñar Escenarios de Riesgos con Respecto a su Impacto Organizacional .103
5.1.8. Actividad A5. Diseñar Estrategias de Tratamiento y Protección....106
5.1.9. Actividad A6. Documentación de Resultados y Revisión de Casos....119
5.1.10. Actividad A7. Monitoreo y Control....119

5.2 Estudio de Caso CPE – UIS Sistema EscuelaCol 1.0....120
5.2.1. A1 Establecer el contexto organizacional. 120
5.2.2. A2 Identificar los activos críticos en los diferentes espacios de la organización. 125
5.2.3. A3 Identificar y evaluar las amenazas y vulnerabilidades de los activos. 127
5.2.4. A4 Diseñar escenarios de riesgo en términos de su impacto organizacional. 129
5.2.5. A5 Diseñar estrategias de tratamiento y protección basados en estándares y buenas prácticas. 133
5.2.6. A6. Documentar los Resultados y Revisar los Casos....139
5.2.7. A7 Monitorear y Controlar. 140

6. CONCLUSIONES - La Importancia de la Gestión de Riesgos y Controles a Nivel Organizacional....141

7. RECOMENDACIONES....143

8. REFERENCIAS BIBLIOGRÁFICAS....144

LISTA DE FIGURAS

Figura 1. Acercamiento a la Situación de Interés *16*
Figura 2. Sistema de Información visto como sistema *18*
Figura 3. Sistema de Información visto como componentes software *19*
Figura 4.Tipos de Sistemas de Información *19*
Figura 5. Resultados de las estrategias aplicada por las empresas en materia de seguridad. *22*
Figura 6. Principales barreras detectadas por Deloitte para Garantizar las Seguridad *23*
Figura 7. Metodología de los Sistemas Blandos *28*
Figura 8. Modelo POM. *33*
Figura 9. Aplicación de la MSB al Contexto Investigativo *34*
Figura 10. Gestión de Calidad Total – TQM. *37*
Figura 11. Ciclo PDCA de la Gestión de la Calidad *39*
Figura 12. Familia de Normas ISO 9000 ..... *40*
Figura 13. Enfoque de procesos de la norma ISO 9000 ..... *41*
Figura 14. Modelo EFQM *43*
Figura 15. Modelo de Calidad Seis Sigma *45*
Figura 16. Requisitos de calidad de ISO 25000 ..... *46*
Figura 17. Ejemplo de Plan de Mantenimiento de Seguridad *55*
Figura 18. Agrupación de Riesgos según SOMAP. *56*
Figura 19. Roles identificados por los estándares respecto de la GRCSI *62*
Figura 20. Pintura Enriquecida – Unificación de Criterios Estándares GRCSI *66*
Figura 21. Niveles de Riesgo en Sistemas de Información *75*
Figura 22. Alineamiento de los Estándares sobre GRCSI con las Actividades del Negocio *86*
Figura 23. Sistema de Actividades de la Definición Raíz *90*
Figura 24. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 1. ..... *91*
Figura 25. Métodos Sugeridos para la Actividad 1. ..... *92*
Figura 26. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 2. ..... *98*
Figura 27. Métodos Sugeridos para la Actividad A2 ..... *99*
Figura 28. Esquema para el contraste entre los niveles de servicio, la BD y la información sensible y crítica. *100*
Figura 29. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 3. ..... *102*
Figura 30. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 4. ..... *103*
Figura 31. Métodos Sugeridos para la Actividad A4 ..... *104*
Figura 32. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 5 ..... *107*
Figura 33. Métodos para Llevar a Cabo la Actividad A5 ..... *108*
Figura 34. Esquema de Elaboración de un Plan de Tratamiento de riesgo Según AS/NZS *119*

LISTA DE TABLAS

Tabla 1. Productos de la Investigación---------- 25
Tabla 2. Aspectos de la Calidad – Cambios en su Ontología---------- 35
Tabla 3. Estándares de Calidad ---------- 46
Tabla 4. Casos de Fallos en la Calidad de los SI ---------- 48
Tabla 5. Procesos de la Gestión de Riesgos---------- 49
Tabla 6. Definiciones aceptadas en estándares sobre riesgos y controles --------- 50
Tabla 7. Actividades planteadas por OCTAVE para la gestión de riesgos en los sistemas de Información. ---------- 52
Tabla 8. Actividades relacionadas por ISM3 para la gestión de riesgos relacionados con la información ---------- 53
Tabla 9. Actividades relacionadas por AS/NZS para la GRCSI ---------- 54
Tabla 10. Actividades relacionadas por SP800-30 para la gestión de riesgos en sistemas de información. ---------- 55
Tabla 11. Actividades planteadas por SOMAP para la gestión de riesgos de la información ---------- 56
Tabla 12. Tipos de Amenazas según MAGERIT ---------- 57
Tabla 13. Actividades propuestas por MAGERIT para la gestión de riesgos en sistemas de información ---------- 59
Tabla 14. Actividades relacionadas por MEHARI para la gestión de riesgos de la información ---------- 59
Tabla 15. Actividades propuestas por ISO 27005 para la gestión de riesgos de la información ---------- 60
Tabla 16. Actividades relacionadas por SP800-39 para la seguridad de los sistemas de información ---------- 60
Tabla 17. Cuadro Comparativo de las Actividades Relacionadas por los Estándares para la GRCSI ---------- 63
Tabla 18. Actividades Planteadas para la GRCSI ---------- 67
Tabla 19. Niveles de Riesgo y Controles Definidos por PWC ---------- 69
Tabla 20. Niveles de Riesgo – Propuesta de Enriquecimiento de las Definiciones73
Tabla 21. Niveles de Riesgo y Controles---------- 76
Tabla 22. Selección de Estándares de Acuerdo con la Necesidad Organizacional ---------- 87
***Tabla 23. CATWOE de la definición raíz para la GRCSI*---------- 89**
Tabla 24. Niveles de Madurez en la Adquisición, Implementación y Uso de los SI ---------- 93
Tabla 25. Criterios de Dependencia de los Procesos de Negocio Respecto de los SI ---------- 95

Tabla 26. Niveles de Servicio de los SI ---------- 96
Tabla 27. Grado de Cumplimientos de los SI con la Implantación ---------- 96
Tabla 28. Relación entre los Niveles de Riesgos, los Activos y los Criterios de Seguridad. ----------100
Tabla 29. Esquema propuesto para la organización de la información sobre los escenarios de riesgo. ----------105
Tabla 30. Organización de la Información sobre los Impactos Generados por los Escenarios de Riesgo ----------106
Tabla 31. Niveles de Riesgo y Controles Propuestos----------108
Tabla 32. Matriz de comparación de los controles a seleccionar ----------118
Tabla 33. Esquema para la Documentación de Casos ----------119
Tabla 34. Niveles de servicio EscuelaCol 1.0 ----------122
Tabla 35. Usuario y Perfiles del Sistema ----------124
Tabla 36. Relación entre los niveles de riesgos los activos y los criterios de seguridad de EscuelaCol 1.0 ----------126
Tabla 37. Identificación de vulnerabilidades y amenazas asociadas a los activos de EscuelaCol 1.0 ----------128
Tabla 38. Escenarios de Riesgos 1 EscuelaCol 1.0----------129
Tabla 39. Escenarios de Riesgos 2 EscuelaCol 1.0----------130
Tabla 40. Escenarios de Riesgos 3 EscuelaCol 1.0----------131
Tabla 41. Escenarios de Riesgos 4 EscuelaCol 1.0----------131
Tabla 42. Escenarios de Riesgos 5 EscuelaCol 1.0----------132
Tabla 43. Escenarios de Riesgos 6 EscuelaCol 1.0----------132
Tabla 44. Escenarios de Riesgos 7 EscuelaCol 1.0----------133
Tabla 45. Niveles de Controles y Riesgos ----------134
Tabla 46. Plan de Tratamiento de Riesgos EscuelaCol 2.0 ----------136
Tabla 47. Esquema para la documentación de casos ----------139

LISTA DE ANEXOS

ANEXO A - Listas de Verificación para Detectar el Nivel Estratégico Organizacional en Términos de SI _____ *149*

ANEXO B - Lista de Verificación para Descubrir la Cultura Ante Riesgos de los Actores de SI _____ *151*

ANEXO C - Diccionario de Catalogación de Activos _____ *153*

ANEXO D - Identificación de Vulnerabilidades y Amenazas Asociadas a los Activos de los SI _____ *159*

RESUMEN

TÍTULO: GESTIÓN DE RIESGOS Y CONTROLES EN SISTEMAS DE INFORMACIÓN*.

AUTORES: GUERRERO, Marlene**

PALABRAS CLAVES: Gestión de Riesgos y Controles, Modelo, Aprendizaje, Intervención, Sistemas de Información, Pensamiento de sistemas blandos, Cambio Organizacional

DESCRIPCIÓN: La gestión de riesgos y controles en Sistemas de Información GRCSI es comúnmente vista como una función técnica encomendada a los expertos en Tecnologías de la Información, ingenieros de Software o programadores de Sistemas de Información. No obstante, la GRCSI es una labor que requiere de una perspectiva mucho más amplia que aporte al aprendizaje organizacional y a la apropiación de los procesos de cambio organizacional que ella requiere.

Este proyecto presenta el resultado de un proceso de investigación, abordado desde la perspectiva del pensamiento de sistemas blandos, que partiendo de un análisis del conocimiento dominante reflejado en los diferentes estándares vigentes en la actualidad, derivo el modelo que se incluye a continuación. En síntesis se presenta una revisión sobre los estándares de GRCSI más relevantes de la actualidad, en la búsqueda de una propuesta de integración de los roles y las actividades que las organizaciones deben desarrollar, con el fin de identificar las responsabilidades de los actores involucrados en los procesos de cambio, y en la búsqueda del entendimiento de los niveles de riesgo y sus implicaciones frente a los SI y los activos de la organización. Para finalizar se muestra para el Sistema de Actividad Humana – SAH de la Dirección Estratégica de Tecnología de Información, la transformación organizacional y la descripción de las actividades propuestas, mediante modelos conceptuales del SAH, tablas y esquemas de representación de las actividades de GRCSI y matrices de impacto organizacional.

***** Trabajo de investigación de Maestría

** Facultad de Ingenierías Fisicomecánicas. Maestría en Ingeniería Área Informática y Ciencias de la Computación. Director: GOMEZ, Luis Carlos.

SUMMARY

TÍTULO: RISK AND CONTROL MANAGEMENT IN INFORMATION SYSTEMS *.

AUTORES: GUERRERO, Marlene**

PALABRAS CLAVES: Risk management and controls, Model, Learning, Intervention, Information Systems, Soft System Thinking, organizational change.

DESCRIPCIÓN: Risk management and controls for Information Systems RMCIS is commonly seen as a technical function charged by experts in information technology as a software engineers or programmers Information Systems. However, RMCIS is a process that requires a much broader perspective that lets to have better comprehension of the organizational learning and of the processes of organizational change that it requires.

This work shows the results of a research process, approached from the perspective of soft systems thinking, starting from an analysis of knowledge dominant which reflected in the different current standards, and as an output is the model that is included below. In short presents a review of the more relevant current standards for RMCIS, in the search of a proposal for integration of the roles and activities that organizations should develop in order to identify the responsibilities of those involved in the processes of change, and the search for understanding of the of the levels of risk and its implications of exposures to the SI and the assets of the organization. To finish listed for each Human Activity System – HAS of the Strategic Management of Information Technology, its organizational changes and the description of the activities proposed by conceptual models of HAS, tables and diagrams to represent the management activities RMCIS and organizational impact matrices.

_____

***** Masters research

** Facultad de Ingenierías Fisicomecánicas. Maestría en Ingeniería Área Informática y Ciencias de la Computación. Director: GOMEZ, Luis Carlos.

INTRODUCCIÓN

En la actualidad, el auge en el desarrollo de los sistemas de información - SI, ha generado un mayor crecimiento y competitividad en las organizaciones, abriendo un sin número de posibilidades para ampliar las relaciones entre clientes, proveedores y empleados, y posibilitando la rapidez en las respuestas a los cambios en el entorno. Los SI tienen un impacto representativo en el valor de la empresa al apoyar los procesos de negocio, las actividades de procesamiento de la información y las actividades de administración, lo cual redunda en un posicionamiento estratégico de la misma.

Teniendo en cuenta entonces importancia y la complejidad de los procesos manejados por los SI, las empresas han empezado a plantearse inquietudes sobre las necesidades de administración del conocimiento de los SI y sobre las condiciones que podrían ocasionar la pérdida del activo e intangible más importante de la organización – la información –. No obstante, pocas organizaciones están conscientes de los retos que supone la gestión del conocimiento de los SI y de los riesgos que estos plantean por su propia naturaleza.

Según el estudio realizado por The Economist Intelligence Unit (ITGI, 2007) y soportado en los estudios presentados por Norton (Norton, 2004), Price Waterhose Coopers (PWC, 2004) y Wah (Wah, 1998), la gestión y el control de riesgos en Sistemas de Información –SI-, no logra aún ganar la importancia necesaria para las directivas de las organizaciones atribuyéndolo a dos premisas. En primera instancia a la falta de comprensión de las cuestiones de riesgos y en segundo lugar al hecho de no contar con una cultura corporativa, debidamente sensibilizada con los riesgos de su propio negocio. En el estudio realizado, se observa que aunque la mayoría de los directivos encuestados coinciden en que existe una necesidad representativa de prestar más atención a la gestión de riesgos en los SI, también coinciden en que se hace relevante implantar una cultura de riesgos en toda la organización que permita que esto se pueda llevar a cabo.

Lo anterior, cobra relevancia debido a que si los directivos no comprenden las razones detrás de las políticas de seguridad de la información y de gestión de riesgos, o no apoyan plenamente la lógica de la estrategia, es poco probable que participen en su desarrollo o se adhieran a él más tarde (Hirsch & Ezingeard, 2009).

Es en este escenario que el grupo de Investigación en Sistemas y Tecnologías de la Información STI[1] propone la elaboración del proyecto de maestría “Gestión de

[1] Grupo de investigación de la Universidad Industrial de Santander, clasificado B Colciencias

Riesgos y Controles en Sistemas de Información - GRCSI", el cual pretende, apoyar a las organizaciones en el reconocimiento de las implicaciones de la ocurrencia de un determinado espacio de riesgo dentro de su entorno complejo, a partir del diseño de un modelo centrado en niveles de riesgo y basado en la revisión y la integración de las actividades para la GRCSI propuestas por los estándares y la literatura.

En este informe se presenta la revisión de los estándares internacionalmente aceptados, la literatura y la práctica de la calidad y la gestión de riesgos y controles en SI, lo cual sirvió como punto de partida para el desarrollo de los modelos conceptuales de los sistemas de actividad humana SAH[2] (Checkland, 2007) encargados de dicha labor en las organizaciones.

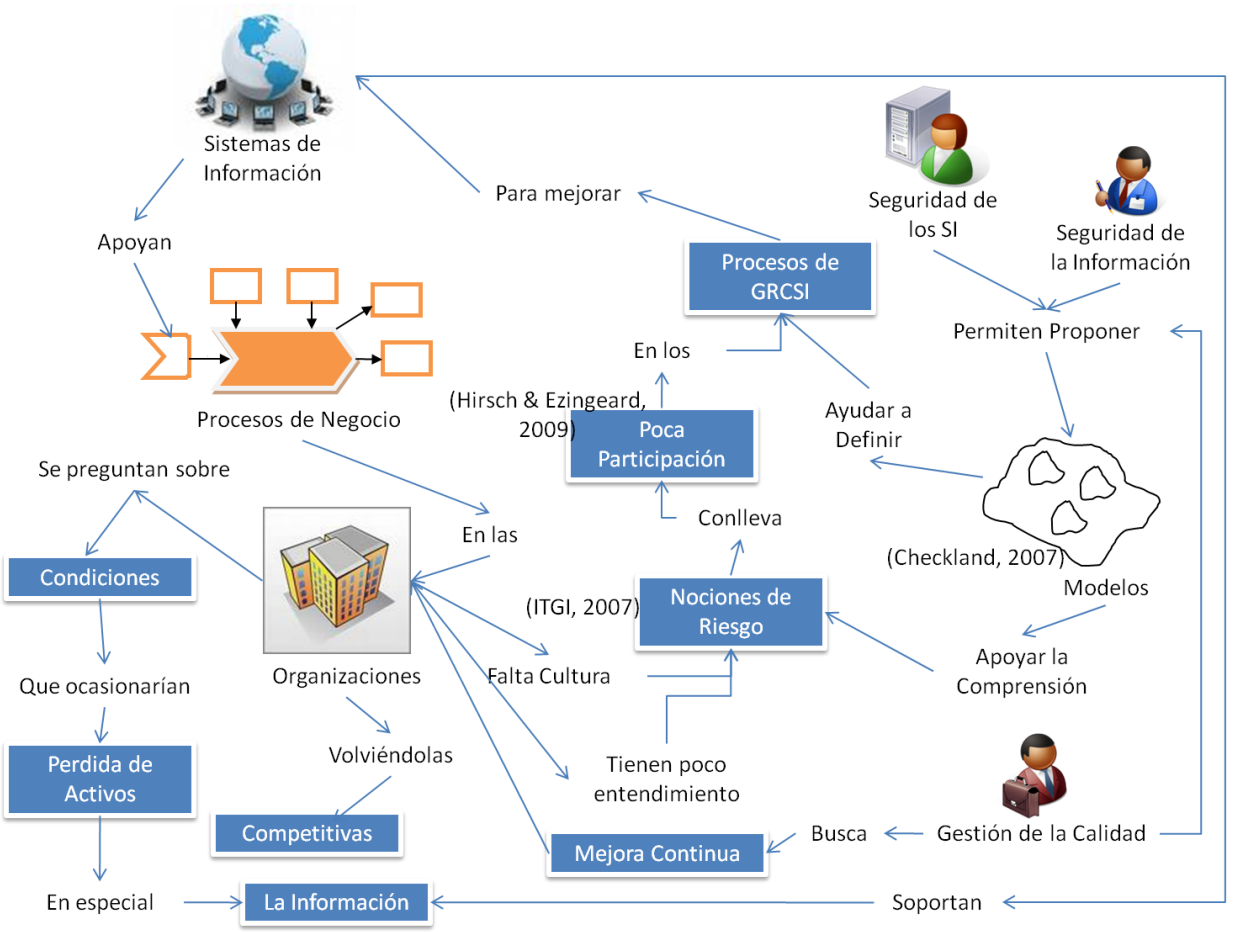
De igual manera, para cada una de las actividades propuestas se presenta el diseño de una serie de métodos sugeridos para llevarlas a cabo y apoyar a la dirección de tecnologías de información en el "hacer" de la GRCSI.

[2] En algunos documentos es posible encontrar la referencia a HAS por su sigla en inglés a Human Activity System.

1. ACERCAMIENTO A LA SITUACIÓN DE INTERÉS

Para poder describir la situación de interés es necesario centrarse en varios aspectos importantes. El primero aspecto tiene que ver con los Sistemas de Información, buscando realizar un acercamiento a los elementos que los componen y establecer los ejes de especial atención en un modelo de gestión de riesgos y controles en sistemas de información. El segundo aspecto es la calidad como elemento gestionador de los procesos de negocio de las organizaciones en pro de su mejora continua. Por último, se encuentra la seguridad de la información en donde se enmarca la seguridad de los sistemas de información, lo cual permitirá abrir la discusión sobre los riesgos y las amenazas a las cuales se ven expuestos los Sistemas de Información en la actualidad (ver figura 1).

Figura 1. Acercamiento a la Situación de Interés



Fuente. Autor

En este capítulo se abordarán algunos conceptos representativos sobre Sistemas de Información y sobre la Seguridad de la Información y los Sistemas de Información, para posteriormente en capítulos subsiguientes centrar la atención en la calidad como factor determinante en el diseño de modelos de GRCSI.

1.1 Sistemas de Información

De acuerdo con ANDREU – 1991, un sistema de información es "*un conjunto formal de procesos que, operando sobre una colección de datos estructurada según las necesidades de la empresa, recopilan, elaboran y distribuyen la información (o parte de ella) necesaria para las operaciones de dicha empresa y para las actividades de dirección y control correspondientes (decisiones), para desempeñar su actividad de acuerdo a su estrategia de negocio*" (Piattini, 2007).

De acuerdo con esta definición, los SI sirven para apoyar los procesos de negocio de las organizaciones y son un elemento primordial de su competitividad, en tanto sean correctamente desarrollados, implantados y operados luego por sus usuarios.

1.1.1 Elementos de un Sistema de Información

Para comprender mejor qué es un SI, debemos también conocer los elementos que lo componen. Existe unanimidad en la mayor parte de la bibliografía sobre SI en designar como componentes de un sistema a los siguientes [DEPABLO, 1989] y [ALTE, 1992]:

- Procedimientos y prácticas habituales de trabajo. Constituyen todos aquellos procesos de negocio de la organización.
- Información. Constituye el intangible más importante de la organización.
- Las personas o usuarios. Son todas aquellas personas que se encuentran vinculadas de manera activa con los procesos de negocio de la organización y con el sistema de información.
- El equipo de soporte. Se compone de todos aquellos sistemas informáticos de apoyo a los procesos (redes, computadores, etc.)

De acuerdo con esta perspectiva, se concibe al SI como un “sistema” en el que se encuentra interrelacionados personas, procesos e información (Ver figura 2).

Figura 2. Sistema de Información visto como sistema

Fuente. Autor

Por su parte, una perspectiva menos organizacional encontrada en Bennett & Bennett (2005), describe el SI centrándose en sus componentes software. En esta perspectiva se puede observar que todo SI debe tener:

- Una actividad humana que necesita información
- Algunos datos almacenados
- Un método input para la entrada de datos
- Algunos procesos que transformen los datos en información
- Un método de salida para la representación de la información

De acuerdo con esta perspectiva, los SI están compuestos por procesos, los cuales se ejecutan en el sistema a partir de unos métodos de entrada y una vez procesados devuelve resultados a través de métodos de salida (ver figura 3).

Figura 3. Sistema de Información visto como componentes software

Fuente. Autor

1.1.2 Tipos de Sistemas de Información

Laudon (2002), divide los sistemas de información en diferentes niveles de acuerdo con el nivel organizacional al cual prestan determinado servicio (ver figura 4).

Figura 4.Tipos de Sistemas de Información

Fuente. Traducción (Laudon, 2006)

De acuerdo con Laudon, se pueden encontrar Sistemas para Soporte Ejecutivo (ESS) los cuales pertenecerían al nivel estratégico; Sistemas de Soporte a las Decisiones (DSS), pertenecientes al nivel administrativo; Sistemas de Información Administrativos (MIS) del nivel administrativo; Sistemas para los Trabajadores del Conocimiento (KWS) del nivel de conocimiento; y los Sistemas de Procesamiento de Transacciones (TPS) pertenecientes al nivel operacional. Estos sistemas se encuentran interrelacionados para el constante intercambio de información entre los diferentes niveles de la organización.

1.2 Seguridad de la Información

De acuerdo con Whitman y Mattord (2009), la seguridad de la información tiene como principal objetivo la protección de los activos de información que se usan, almacenan o transmiten y la protección de los procesos y sistemas que la utilizan, garantizando su disponibilidad, integridad y confidencialidad, a través de múltiples medidas (políticas, entrenamiento, tecnología, etc.).

1.2.1 Criterios de la Seguridad de la Información

De acuerdo con ISO 27001 La seguridad de la información se cimenta en tres aspectos importantes: la disponibilidad, la integridad y la confidencialidad.

- Disponibilidad. Accesibilidad a la información cuando sea requerida por los procesos del negocio. Protección de los recursos y capacidades asociadas a los mismos.
- Integridad. Precisión y completitud de la información. Validez de la información de acuerdo con las expectativas de la empresa.
- Confidencialidad. Protección de la información sensible contra revelación no autorizada.

1.2.2 El Estado de la Seguridad de la Información en la Actualidad

La seguridad de la información es un tema de especial interés tanto para las organizaciones como para diversas empresas consultoras a nivel internacional y nacional. En concordancia con esto, empresas de reconocido prestigio en el ámbito de la consultoría como lo son Price Waterhouse Coopers, Deloitte y Ernst & Young desarrollan continuamente investigaciones orientadas a establecer el estado de la seguridad de la información en las organizaciones.

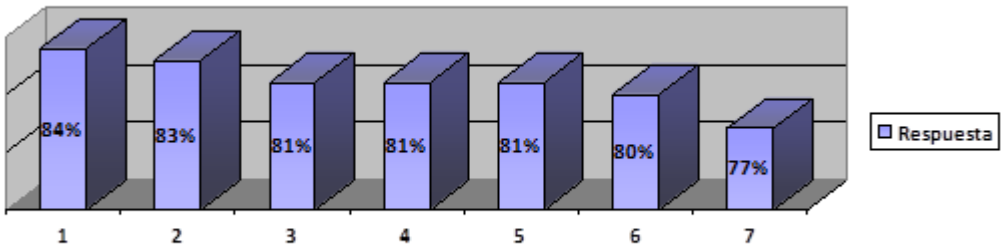
La primera investigación a la que se hará alusión es a la desarrollada por Price Waterhouse Coopers – PWC en su informe “Qué esperan los Ejecutivos de la Seguridad de la Información” (Brenner, 2009), en el que se entrevistaron a 7300 ejecutivos de tecnologías de la información de diversos negocios en Asia, Norte América, Sur América y China. En esta investigación se encontró que la mayoría de las empresas actualmente han dado mayor prioridad y han incrementado sus investigaciones en programas de seguridad y gestión de riesgos y controles en sistemas de información.

En la figura 5, PWC presenta las siete estrategias principales a las que actualmente las empresas le están apuntando en materia de seguridad de la información.

- Estrategia 1. Incrementar el enfoque de protección de datos.
- Estrategia 2. Priorizar las investigaciones de seguridad basadas en riesgo.
- Estrategia 3. Fortalecer los programas de gestión de riesgos y controles de la compañía.
- Estrategia 4. Reducir, mitigar o transferir los principales riesgos.
- Estrategia 5. Reenfocar el núcleo de las estrategias existentes.
- Estrategia 6. Acelerar la adopción de tecnologías de automatización relacionadas con la seguridad para incrementar la eficiencia u reducir costos.
- Estrategia 7. Adoptar un reconocido marco de trabajo de seguridad como un medio para la preparación de próximos requerimientos regulatorios.

Los resultados de la entrevista están agrupados de acuerdo con las respuestas “algo importante”, “importante”, “muy importante” o “máxima prioridad”.

Figura 5. Resultados de las estrategias aplicada por las empresas en materia de seguridad.



Adaptada de Brenner (2009).

Otro aspecto muy importante del estado de la seguridad de la información es provisto por Deloitte en su “Informe Anual de Seguridad de la Información en las Instituciones Financieras” (Deloitte, 2009) en el que se entrevistaron a más de 200 instituciones financieras, bancos y compañías aseguradoras de la región EMEA[3], Norte America, Latinoamerica, Japón y la región de Asia y Pacífico con el animo de profundizar sobre las estrategias utilizadas por estas organizaciones en materia de seguridad de la información, el presupuesto que se destina y las principales amenazas, ataques y soluciones tecnológicas para combatirlas.

En este informe, se destacan las tendencias claves en el mundo en materia de seguridad de la información, entre las cuales se encuentran:

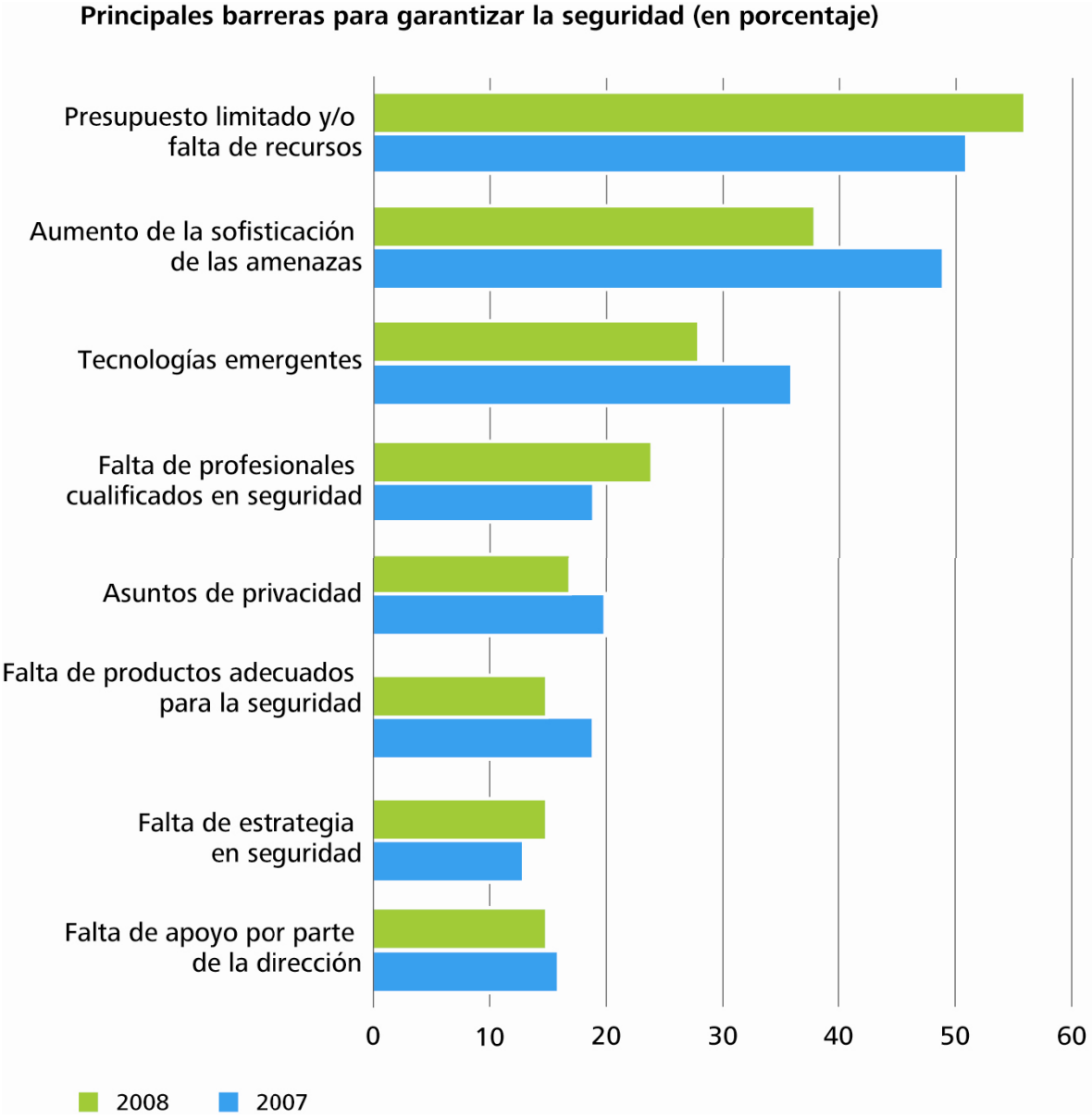
1. Cumplimiento regulatorio.
2. Gestión de accesos e identidades.
3. Protección de información y prevención de fugas.
4. Mejoras en las infraestructuras de seguridad.
5. Gobierno de la seguridad.

En la figura 6, Deloitte presenta las principales barreras para garantizar la seguridad de la información que fueron detectadas en el estudio. Como se puede observar, el presupuesto es uno de los principales factores que impiden un

[3] Europa, Oriente Medio y África.

adecuado aseguramiento de la información, seguido por la sofisticación de las amenazas actuales[4] y las tecnologías emergentes.

Figura 6. Principales barreras detectadas por Deloitte para Garantizar las Seguridad



Fuente. Deloitte (2009)

[4] Aspecto que fortalece el desarrollo de esta propuesta de investigación

Por último, se hará referencia al informe publicado por Ernst & Young denominado "Managing Risk in the Current Climate" (Ernst &Young, 2009), en donde se especifican las áreas que las organizaciones deben atender en materia de seguridad y gestión de riesgos.

Entra las áreas mencionadas por Ernst & Young se encuentran:

- Incrementar en la Comunicación y Visibilidad de los Riesgos
- Definir Políticas y Procedimientos de Riesgos.
- Subcontratar la Gestión de Riesgos.
- Implementar la Tecnología Relevante parta el Gobierno de las Metas de los Procesos.

1.2.3 La Seguridad de los Sistemas de Información

La seguridad de los sistemas de información tiene como objetivo principal el resguardo de los recursos asociados a los SI. En este sentido, la Seguridad de los Sistemas de Información busca garantizar que los SI cumplan con los criterios de confidencialidad, autenticidad, integridad y disponibilidad.

Anteriormente en el ítem 1.2.1 se describieron los criterios de integridad, confidencialidad y disponibilidad, a continuación se describe el término auntenticidad.

- Autenticidad. "Es la propiedad que permite que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores" (Maguerit, 1997).

Asegurar los recursos asociados a los SI es hoy en día un factor clave para las organizaciones, circunstancia por la cual se han establecido estándares a nivel mundial que buscan ofrecer guías o pautas sobre este tema. Estas guías y su intencionalidad serán descritas posteriormente en este libro.

1.3 Alcance de la Propuesta de Investigación

Este proyecto de investigación proporciona a las organizaciones un modelo para la gestión de riesgos y controles en sistemas de información, basado en la integración de las actividades propuestas por los estándares relacionados con la seguridad de la información, la seguridad de los sistemas de información y la

gestión de riesgos y controles a nivel organizacional y de sistemas de información. El modelo centra su atención en la GRCSI a través de la utilización de un esquema basado en niveles de riesgo y se guía por la definición raíz diseñada para la transformación organizacional.

La implementación de un modelo de gestión de riesgos y controles permite una reducción en los costos administrativos y operacionales, ya que se previenen los daños o alteraciones que se pueden realizar a la información teniendo en cuenta que la confidencialidad, integridad y disponibilidad de la misma de mantengan y además se controlen aspectos que tiene que ver con pérdidas que ocasionen mayores gastos de recuperación y restablecimiento.

A continuación en la tabla 1 se describen los productos que se obtuvieron a raíz de la investigación.

Tabla 1. Productos de la Investigación

No	**Objetivo**	**Actividades y/o Productos**
1	Diagnosticar las tendencias de la gestión de riesgos y controles y la calidad de sistemas de información, incluyendo los estándares, la literatura y las prácticas, con el fin de fundamentar el desarrollo de la propuesta.	1. Documento con el marco teórico de la propuesta de investigación. 2. Artículo de Investigación “Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información“, en estudio de publicación en la revista estudios Gerenciales Categoría A2 Colciencias. **Capítulo 3 y 4**

No	Objetivo	Actividades y/o Productos
2	Diseñar los procesos, pautas y modelos de Sistema de actividad Humana – SAH que posibiliten la gestión de los riesgos y controles en SI teniendo en cuenta el pensamiento blando.	1. Propuesta Inicial del SAH para la Gestión de Riesgos y Controles en los Sistemas de Información. 2. Elaboración de una Imagen Enriquecida de los Procesos para la Gestión de Riesgos y Controles en los Sistemas de Información. 3. Definición Raíz. 4. Transformación Organizacional y Descripción de las Actividades y Métodos Propuestos Para la Gestión de Riesgos y Controles en los Sistemas de Información. 5. Artículo de Investigación en revisión "Modelo para la Gestión de Riesgos y Controles en Sistemas de Información". **Capítulo 4 (ítem 4.3) y Capítulo 5 (ítem 5.1)**
3	Aplicar el modelo de gestión de riesgos y controles al sistema EscuelaCol 1.0 con el propósito de ilustrar su utilización y contribuir a la posible mejora de la herramienta.	1. Análisis Funcional del Sistema EscuelaCol 1.0 2. Definición de los Riesgos y Controles Asociados a EscuelaCol 1.0 3. Redefinición del Sistema – Propuesta Sistema EscuelaCol 2.0 4. Proyecto de Pregrado "Herramienta Software Open Source Orientada a Apoyar los Procesos de Evaluación y Promoción en la Educación Básica Primaria Escuelacol 2.0" **Capítulo 5 (Ítem 5.2)**

Fuente. Autor.

2. LA METODOLOGÍA DE LOS SISTEMAS BLANDOS MSB. El pensamiento de sistemas blandos como guía del proceso de intervención.

En la Ingeniería de sistemas la palabra «sistema» es utilizada únicamente como una etiqueta para abstraer algo que existe en el mundo fuera de nosotros mismos. Tal asunción es dada por el supuesto de que el mundo puede ser considerado como un conjunto de sistemas que interactúan, algunos de los cuales no funcionan muy bien y pueden ser rediseñados para trabajar mejor (Checkland, 2000). En el pensamiento plasmado en la metodología de los sistemas blandos de Peter Checkland (conocida también como SSM por sus siglas en inglés: Soft System Methodology) los supuestos son muy diferentes. El mundo suele ser muy complejo, problemático, misterioso. No obstante, el proceso de investigación que se hace en torno a él, puede ser organizado como un sistema de aprendizaje. Por lo tanto, el uso de la palabra «sistema» ya no se aplicará al mundo como instancia, sino al proceso de investigación del mundo que es la fundamental distinción intelectual entre las dos formas fundamentales de los sistemas de pensamiento, «duro» y «blandas».

La gestión de riesgos y controles en Sistemas de Información se encuentra rodeada por un alto componente social, político y humano, esto conlleva a que puedan existir perspectivas diferentes y a veces contradictorias sobre cómo se deberían llevar a cabo estos procesos en una organización. Es en este punto, en el que la metodología de los sistemas blandos de Peter Checkland (Checkland & Scholes, 1999) se convierte en una de las metodologías más propicias para este tipo de estudios, en los cuales se debe trabajar con diferentes percepciones de una misma situación, las cuales son examinadas y discutidas en torno a un procesos sistémico de aprendizaje, con el fin de definir acciones orientadas a su mejoramiento.

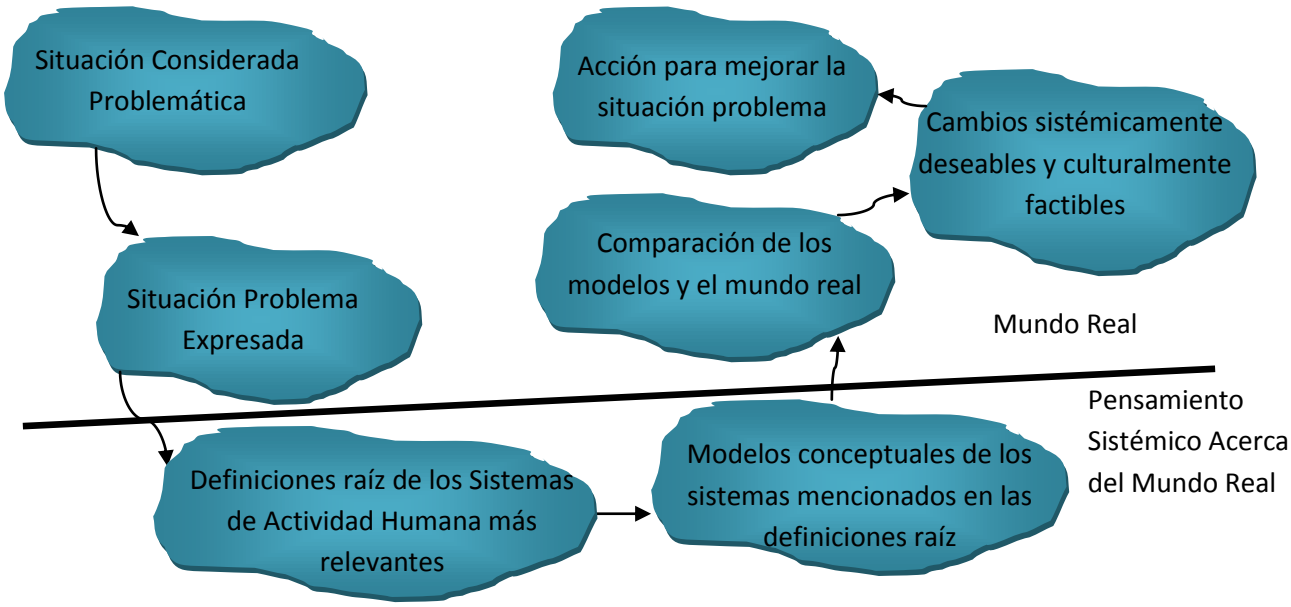
En los siguientes ítems se definirán los supuestos onto-epistemológicos de la metodología de los sistemas blandos y las aplicaciones o repercusiones de esta en el estudio de los sistemas de información.

2.1 Supuestos Onto-Epistemológicos de la MSB

La SSM fue desarrollada por Peter Checkland en la década de los 60’s en la Universidad de Lancaster. Esta metodología busca establecer comparaciones entre el mundo real tal como es y algunos modelos del mundo como podría ser. De estas comparaciones, surge un mejor entendimiento del mundo (“investigación”), y algunas ideas de cómo podría mejorarse (“acción”).

En la figura 7 se muestran las siete etapas de la metodología clásica de los sistemas blandos. Algunas de ellas pertenecientes al mundo real y otras a la descripción conceptual.

Figura 7. Metodología de los Sistemas Blandos



Fuente. Checland P., et al. Soft Systems Methodology: A Thirty Year Retrospective. 25 Pinewood Avenue, Bolton-le-Sands, Carnforth, Lancashire, LA5 8AR, UK. 2000.

El modelo de las siete etapas ha demostrado poca resistencia debido a que es fácil de explicar y ayuda a entender el proceso de intervención. Los factores que apoyan esta teoría según Checkland se describen a continuación:

- En primer lugar un punto estético e intangible pero importante es la utilización de los esquemas y líneas curveadas, los cuales son típicos en el trabajo en Ciencia e Ingeniería.
- En segundo lugar, aunque por casualidad, el ciclo de aprendizaje de este modelo del proceso consta de siete etapas. Miller reconocido por los experimentos de laboratorio sobre la percepción (1956) sugiere que la capacidad del canal de nuestro cerebro es tal que podemos hacer frente a alrededor de siete temas o conceptos de una sola vez, de ahí el título de su famoso artículo: «El mágico número siete, más o menos dos: algunos límites sobre nuestra capacidad de procesamiento de la información». Por tal motivo, el cómodo tamaño del modelo de la SSM implica que se puede retener en la mente y que no hay necesidad de buscarla en un libro, lo cual es muy útil cuando se utiliza de manera flexible en la práctica.

- Por último, el modelo de las siete etapas provee una formulación lo suficientemente rica para ser enseñada, lo cual se ve reflejado en su posterior uso por parte de otros autores tales como Watson y Smith (1988) y otros 18 estudios llevados a cabo en Australia entre 1977 y 1987.

2.1.1 Etapa 1. La Situación Considerada Problemática

La primera etapa de la SSM tiene como principal objetivo conocer, explorar y definir la situación de alguna manera. Es importante recalcar que en esta etapa no se busca definir el problema, sino hacer una evaluación del área general de interés. Para el caso específico de este proyecto el área general de interés es la gestión de riesgos y controles en Sistemas de Información y los Sistemas de Información de uso específico de las instituciones de educación básica y media.

2.1.2 Etapa 2. La Situación Problema Expresada

Checkland denomina "Pintura Rica" a la situación problema expresada por dos razones. La primera tiene que ver con que la situación necesita ser expresada en toda su riqueza, para lo cual provee algunas guías de los que debería ser incluido:

- Estructuras
- Procesos
- Entorno
- Personas
- Perspectivas de las Personas
- Conflictos

En segunda instancia, Checkland sugiere que la mejor forma de hacer lo anterior es a través de un dibujo.

2.1.3 Etapa 3. Definición Raíz de los Sistemas de Actividad Humana más Relevantes

Esta etapa pasa del mundo real al mundo de sistemas. A esta etapa Checkland la denomina "Definición Raíz" y es la única y más compleja parte de la metodología. Para po0der elaborar la definición raíz, lo primero que hay que hacer es entender los conceptos desde las diferentes perspectivas, las cuales se pueden extraer de la pintura rica. Estas perspectivas son denominadas "Holones"[5]. Cada Holón proporciona una base de valores por separado para evaluar la situación.

La SSM se basa en que tratar de abordar todas estas perspectivas en su conjunto es una tarea demasiado compleja. La claridad se adquiere cuando se abordan las principales perspectivas por separado, comprendiendo sus implicaciones y, a continuación, se utilizan esos entendimientos al tratar de reintegrar dichas

[5] Perspectivas con propósito aceptadas que pueden describir las actividades del mundo real.

perspectivas en una serie de conclusiones de evaluación y sugerencias para la acción futura.

Ahora bien, con el fin de seleccionar una perspectiva particular y realizar un estructurado y riguroso proceso de desarrollo de los modelos Checkland propone el mnemónico CATWOE. El punto de partida es una Transformación (T) para la perspectiva seleccionada y a partir de allí se identifican los otros elementos claves del sistema a saber:

- Clientes. Quién o Qué se beneficia de la transformación.
- Actores. Quienes facilitan la transformación para esos clientes.
- Transformación. Desde el comienzo hasta el final.
- Punto de Vista. Weltanschauung – lo que le da significado a la transformación.
- Propietarios. Quien es el responsable del "sistema" y / o podría causar que no exista.
- Entorno. Medio ambiente que influye pero no controla el sistema.

Esta construcción del CATWOE deberá realizarse para cada transformación, con el fin de proporcionar declaraciones para los sistemas relevantes. Chackland sugiere que estas deberán seguir la siguiente estructura:

"Un sistema que hace X, por medio de Y para hacer Z".

2.1.4 Etapa 4. Desarrollando los Modelos Conceptuales

Utilizando las definiciones raíz definidas en la etapa anterior se diseñan los modelos conceptuales de acuerdo con el siguiente proceso:

- Utilizando verbos en imperativo se describen las actividades necesaria spara llevar a cabo la transformación.
- Se seleccionan las actividades que podrían llevarse a cabo al mismo tiempo (por ejemplo, aquellas que no dependen de otras).
- Se indican las dependencias.
- Se reorganizan las actividades a fin de evitar la superposición de flechas cuando sea posible. Se añade un medio para evaluar el rendimiento y se incluyen los aspectos del medio ambiente identificados en el CATWOE.
- Finalmente, se verifica que el modelo demuestra las siguientes propiedades de los sistemas:
    - Un propósito definido
    - Un medio para evaluar el desempeño
    - Un proceso de toma de decisiones
    - Componentes que también sean sistemas (por ejemplo, la noción de subsistema)
    - Componentes que interactúen

- Un entorno (con el cual el sistema podría o no estar interactuando).
- Una interfaz entre el sistema y el entorno (que podría ser cerrado o abierto).
- Recursos
- Continuidad

2.1.5 Etapa 5. Comparación de los Modelos y el Mundo Real

Según Checkland, hay cuatro formas de realizar comparaciones entre los modelos diseñados y el mundo real a saber: realizando discusiones desestructuradas, elaborando cuestionamientos estructurados del modelo utilizando una matriz, diseñando escenarios o modelos dinámicos y tratando de modelar el mundo real utilizando la misma estructura que el modelo conceptual. La matriz es la más utilizada, ya que permite observar cada componente del modelo y responde a las preguntas ¿Existe en el mundo real?, ¿Cómo se comportan?, ¡Cómo se identifica y mide su desempeño?, ¡De todos los procesos este es el mejor?

2.1.6 Etapa 6. Cambios sistémicamente deseables y culturalmente factibles

En este punto la metodología tiende a dejar de ser secuencial y empieza a oscilar hacia adelante y hacia atrás a través de las siete etapas de la metodología a fin de obtener el mayor apalancamiento. Sobre la base de este análisis se exploran las posibles intervenciones. La evaluación de la viabilidad de estas intervenciones es un aspecto importante de la metodología, y Checkland sugiere varias maneras de hacerlo:

- Pasarlo por nuevos modelos utilizando diferentes CATWOE / BATWOVE, diferentes perspectivas, diferentes escalas (es decir, modelo de sub-sistemas).
- Llevar a cabo análisis basados en diferentes sistemas (por ejemplo, dinámica de sistemas, CAS, CHAT)
- Análisis "Propietario". ¿Quién fundamentalmente tiene la autoridad para ejecutar la acción?
- "Análisis del Sistema Social" ¿Cómo los distintos roles, normas y valores presentes en el mundo real se relacionan con el modelo conceptual?
- "Análisis Político". ¿Cómo se expresa el poder en la situación en estudio?

2.1.7 Etapa 7. Acción para Mejorar la Situación

Aquí es donde la metodología completa su ciclo. Sin embargo, esto no implica que sea el fin de la misma, pues su aplicación se transforma en un ciclo de continua conceptualización y habilitación de cambios, siempre teniendo en cuenta la mejora de la situación. Es decir, en esta etapa se toma la acción para mejorar la situación problema, ocasionando un cambio y permitiendo que el ciclo vuelva a empezar.

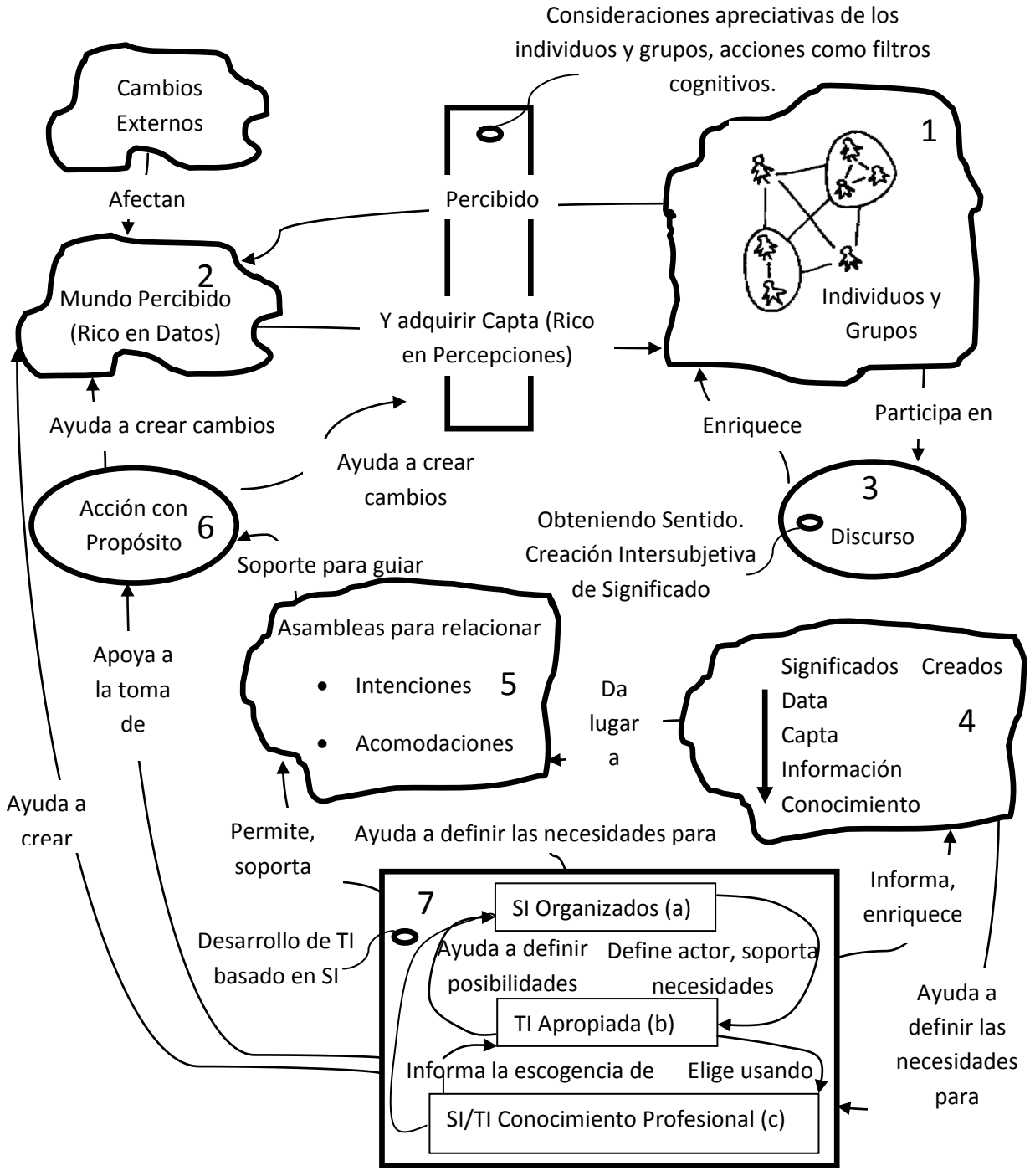
2.2 Aplicaciones de la MSB a Sistemas de Información

La metodología de los sistemas blandos ha sido involucrada en el desarrollo de los sistemas de información a través del proceso de investigación – acción en las organizaciones en los últimos años, con el fin de apoyar a la disciplina desde la perspectiva del contexto organizacional, la cual implica tener en cuenta los factores social - cultural, político y administrativo que en muchas ocasiones tienden a minimizarse o ser excluidos.

La idea central detrás de la labor descrita por Checkland y Holwell es la idea de que los modelos conceptuales desarrollados en la MSB puedan ser utilizados para iniciar y estructurar discusiones sobre la información soportada por las actividades que las personas realizan en el mundo real, proceso que normalmente se conoce como análisis de requerimientos. Durante el desarrollo de la MSB Checkland y Griffin (1970) diseñaron el primer modelo conceptual para determinar las necesidades de información de una empresa textil de mediano tamaño. Desde entonces ha habido intentos ocasionales para relacionar al pensamiento de sistemas en general y a la MSB en particular con el campo de los sistemas de información (Checkland & Scholes, 1999).

Por su parte, autores contemporáneos como Aileen Cater-Steel y Ka-Wai Lai entre otros (Cater-Steel & Al-Hakim, 2009), proveen una mirada a la aplicación de la MSB al mantenimiento y desarrollo de Sistemas de Información. La mayoría de estas perspectivas señalan que en los últimos años, el desarrollo de sistemas de información ha ido incrementando, de tal manera que han apoyado el cambio organizacional desde el punto de vista de la funcionalidad, la flexibilidad y la disponibilidad de la información. Sin embargo, los sistemas de información no están exentos de errores y/o cambios en el entorno operativo al cual le brindan servicio, por lo cual es necesario realizar periódicamente estudios pertinentes a evaluar los riesgos a los cuales están expuestos, con el fin de generar controles que permitan disminuir el costo asociado a la perdida de información y recursos informáticos. Consientes de este acercamiento constante al entendimiento de los sistemas de información, Checkland y Holwell desarrollan un modelo elaborado para el entendimiento de los procesos organizacionales denominado POM por sus siglas en inglés - Processes for Organization Meanings – (ver figura 8), el cual da cuenta de la distinción entre data, capta, información y conocimiento en relación con las actividades organizacionales y su consecuente acción. El concepto implícito en el modelo POM es contrario a la tradicional sabiduría sobre el desarrollo de sistemas de información.

Figura 8. Modelo POM.



Fuente. Adaptado de Checkland and Holwell (1998)

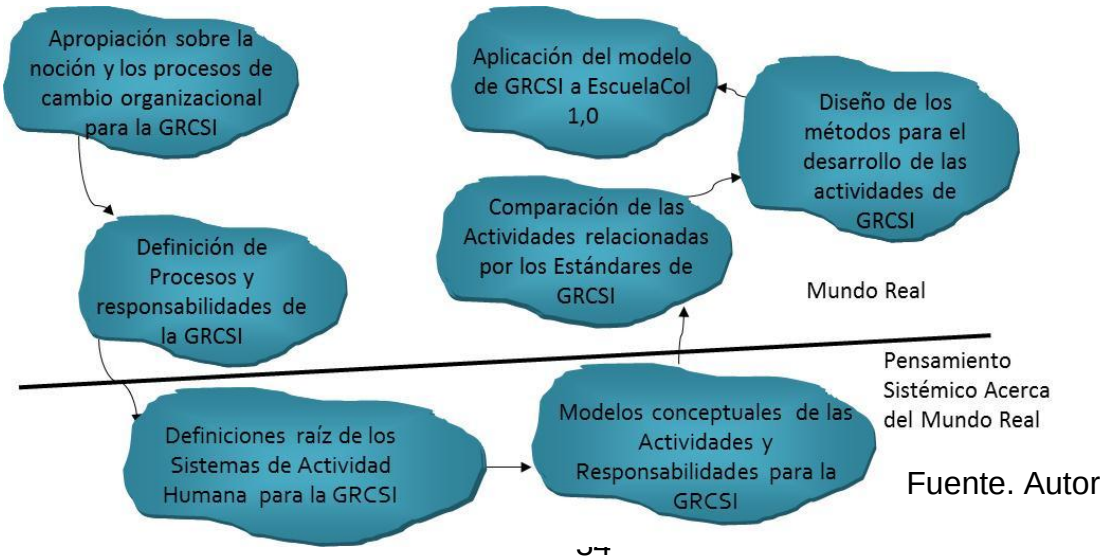
Actuales literaturas muestran el enfoque de aplicación de la MSB en el desarrollo de proyectos de SI. Dentro de las investigaciones realizadas se destaca el trabajo

de Sewchurran (Sewchurran, 2007), quien ofrece un marco sistémico para el modelado de Procesos de Negocios combinado con la metodología de los sistemas blandos con en lenguaje unificado de modelado - UML. En esta investigación Sewchurran busca aplicar la modelación de los procesos de producción de una planta de laminación de aluminio, como un paso en el desarrollo de nuevos sistemas de información. De igual manera, Kefi (Kefi, 2007) aplica los conceptos de la metodología de los sistemas blandos y el modelado complejo para construir y aplicar un enfoque de evaluación de tecnologías de información basado en sistemas de información, aplicado al data warehouse de una institución financiera líder en Europa. Un último estudio investigado, es el desarrollado por Rose (Rose, 2002), el cual presenta la interacción, transformación y desarrollo de sistemas de información como una extensión de la aplicación de la metodología de los sistemas blandos. Este último estudio fue utilizado satisfactoriamente para estructurar el desarrollo de una intranet para la universidad internacional Aalborg en Dinamarca.

2.3 Aplicación de la MSB en el Contexto de la Investigación sobre GRCSI

Para efectos específicos de la investigación sobre GRCSI, la metodología de los Sistemas Blandos permitirá abordar el tema de la apropiación de la GRCSI en las organizaciones, desde el punto de vista de la definición de los procesos y las responsabilidades de cada uno de los actores que intervienen. Esto permitirá establecer definiciones raíz orientadas a determinar los SAH para la GRCSI. Los modelos conceptuales que se diseñen y su contrastación con las actividades definidas por los estándares de GRCSI, posibilitarán el diseño de métodos para llevar a cabo las actividades de GRCSI. Los modelos y métodos diseñados, se aplicarán en el contexto específico en el que se encuentra el Sistema EscuelaCol 1.0, con el fin de generar propuestas de mejoramiento que redunden en la creación de una nueva versión del aplicativo (Figura 9).

Figura 9. Aplicación de la MSB al Contexto Investigativo



Fuente. Autor

3. NOCIONES ACERCA DE LA CALIDAD

3.1 Acercamiento Conceptual a la Teoría de la Calidad

Uno de los conceptos más importantes cuando se evalúan los riesgos y se definen controles en sistemas de información es la Calidad. Sin embargo autores y estándares debaten continuamente sobre su significado y los aspectos que la determinan. A lo largo de este capítulo se presentarán las investigaciones realizadas en términos de la concepción de calidad en la literatura, en los estándares y en la práctica, dando por último transcendencia a la importancia de la calidad en los sistemas de información.

3.1.1. La Calidad en la Literatura

Diversos autores definen la calidad como "el fenómeno estrella del siglo" (Udaondo, 1992), debido a que cada vez son más las empresas que han empezado a plantear la calidad como factor decisivo de su productividad y de la competencia. Los primeros acercamientos que se realizarán sobre el concepto de calidad intentarán discernir sobre su eje central y los elementos más representativos.

- **¿Qué se Entiende por Calidad?**

El concepto de calidad ha ido madurando con el tiempo. Se puede decir que inició con una visión clásica de control de calidad en la cual el objeto de preocupación eran los productos y los servicios, para luego pasar al concepto de aseguramiento de la Calidad en donde se considera que todas las actividades de la empresa se ven afectadas por la calidad y que por lo tanto debe ser incorporada como un proceso de gestión que permita planificar, implantar y controlar con miras a la mejora continua de la organización. El último término que ha calado en las organizaciones es el de Gestión de Calidad Total, en el cual se ve la Calidad como una serie de conceptos que ayudan a facilitar las relaciones interpersonales en cualquier tipo de organización y a entender los procesos que transforman el medio ambiente del ser humano (Guajardo, 2003), En la tabla 2 se describen los diferentes aspectos de cada una de estas visiones.

Tabla 2. Aspectos de la Calidad – Cambios en su Ontología

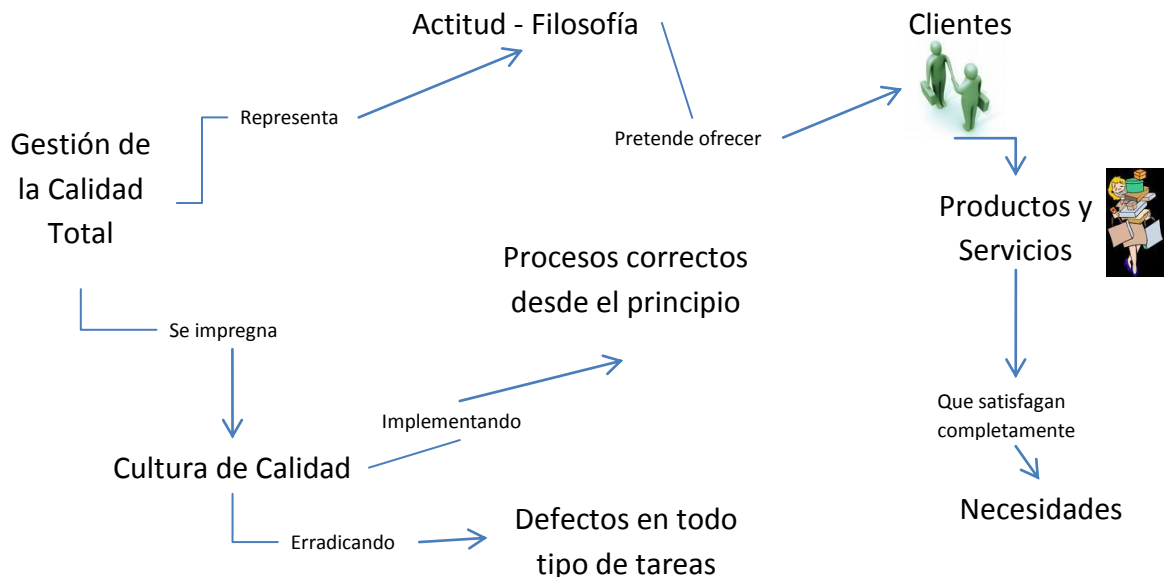
Aspectos de la Calidad	Control de Calidad	Aseguramiento de la Calidad	Gestión de la Calidad Total
Concepto	La Calidad se obtiene de conformidad con las especificaciones del producto o servicio	La Calidad se obtiene de acuerdo con la especificación de las normas. Se	La Calidad se obtiene cuando es apreciada por los clientes y por comparación con

Aspectos de la Calidad	Control de Calidad	Aseguramiento de la Calidad	Gestión de la Calidad Total
	final.	mide por la desviación de la conformidad.	modelos y otras organizaciones.
Objeto	Afecta a productos y servicios	Afecta a todas las actividades de la empresa	Afecta a los entes organizacionales y a su entorno
Alcance	Actividades de control	Gestión y asesoramiento, además de control	Gestión, asesoramiento, control y administración del conocimiento para la mejora continua.
Modo de Aplicación	Impuesta por la dirección	Por convencimiento y participativa	Por convencimiento y participativa
Metodología	Detectar y Corregir	Prevenir y cumplir normas	Planear, hacer, detectar y controlar
Responsabilidad	Del departamento de calidad	Compromiso de cada miembro de la empresa	Compromiso de cada miembro de la empresa
Necesidades de Formación	Especifica de control de calidad dirigida a los inspectores.	Formación específica del personal en las áreas de trabajo.	Formación continua tanto específica como de gestión y calidad total.
Clientes	Ajenos a la empresa	Internos y externos	Internos y externos

Fuente. Adaptado de Udaondo, 1992.

La gestión de la calidad total o TQM (por sus siglas en inglés) implica un alto compromisos de la alta gestión con todos los empleados no sólo para la reducción de los ciclos de desarrollo de los productos y servicios sino también para el reconocimiento y la celebración de resultados. La TQM hace necesario que la producción esté “just in time” y asegura la reducción de costes de productos y servicios y la implicación y enriquecimiento de los puestos de trabajo del personal “empowerment”. De igual manera, la TQM hace que las organizaciones generen propuestas de objetivos cuantificados y benchmarking que permitan tomar decisiones basadas en hechos. La figura 10 muestra en resumen el enfoque de un sistema de gestión de calidad total.

Figura 10. Gestión de Calidad Total – TQM



Fuente. Autor

- **Contribuciones al Concepto de Calidad**

Cuando se habla de Calidad, se deben reconocer las diferentes contribuciones que autores representativos han tenido en la construcción y en el debate del concepto. A continuación se describen algunos de dichos aportes.

Kaoru Ishikawa, uno de los autores más representativos en la teoría de la calidad, sostuvo que la calidad es un movimiento que debía imponerse y mostrarse ante toda la empresa, lo cual se vería reflejado no sólo en el producto, sino también en los costos, en la productividad, en la mejora de las técnicas, en las ventas, en los procesos administrativos y en las relaciones del personal (Ishikawa, 1997). Ishikawa es el promotor de los "círculos de calidad", en los cuales se capacitaba adecuadamente al personal en las áreas de control y mejora y se les enseñaban las siete herramientas para el control de calidad: la Gráfica de Pareto, el diagrama de causa-efecto, la estratificación, la hoja de verificación, el histograma, el diagrama de dispersión y la Gráfica de Control de Shewhart.

Otro de los autores representativos de la teoría de la calidad es Genichi Taguchi, quien centra su filosofía de calidad en dos aspectos fundamentales: diseñar productos atractivos para los clientes y que esos productos sean mejores que los ofrecidos por la competencia. Taguchi desarrolló una metodología denominada "Ingeniería de la Calidad" (Wu, 1996), la cual es utilizada para prevenir problemas de calidad desde las etapas tempranas del desarrollo y diseño del producto, incluyendo los problemas asociados con las funciones del producto, la contaminación, y otros costos derivados después de la fabricación y puesta en el mercado. La ingeniería de Calidad podía ser desarrollada en línea, la cual incluía

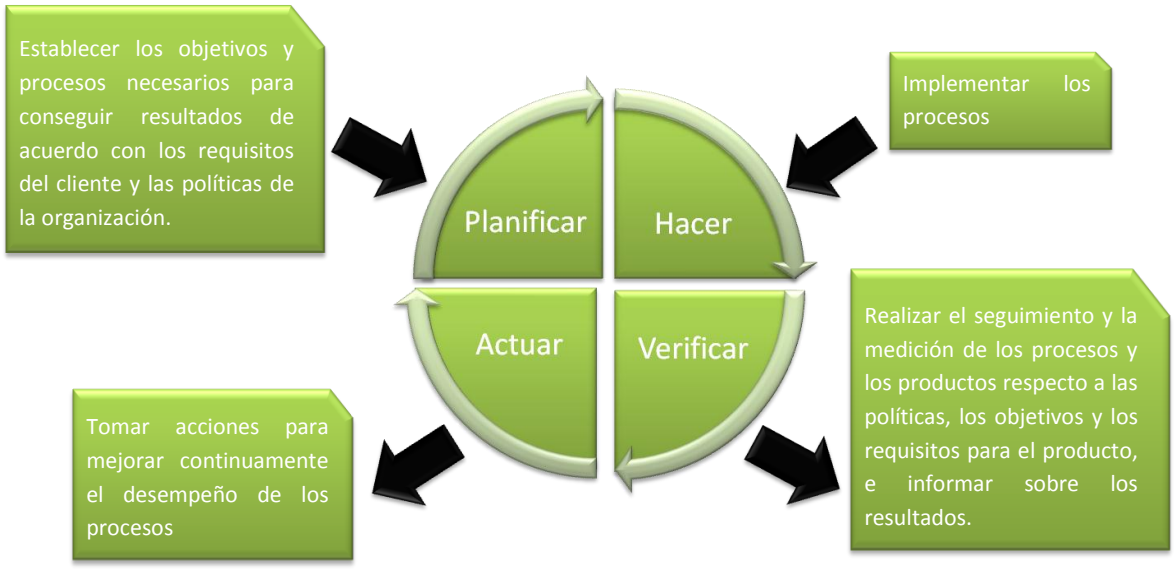
las actividades de ingeniería de calidad en línea, el área de manufactura, el control y la corrección de procesos, así como el mantenimiento preventivo; o fuera de línea, la cual se encargaba de la optimización del diseño de productos y procesos.

Por su parte, Philip B. Crosby, basa sus fundamentos en cuatro aspectos fundamentales: la calidad es el cumplimiento de los requisitos, el sistema de calidad es la prevención, la teoría del cero defectos debe ser el estándar de producción y la calidad de mide de acuerdo con el precio de incumplimiento (Crosby, 1990). Crosby propone un programa de catorce pasos para el mejoramiento de la calidad: La calidad debe ser compromiso en la dirección, Se debe conformar un equipo para el mejoramiento de la calidad, la calidad debe medirse, Se debe determinar el costo de la calidad, se debe crear una conciencia sobre la calidad, se deben establecer acciones correctivas, se debe planificar el día de cero defectos, se debe educar al personal, debe existir el día de cero defectos, se deben fijar metas, se deben eliminar las causas del error, debe haber reconocimiento, debe existir un Consejo de calidad y por último se debe repetir todo el proceso.

Edwards Deming también hace sus aportes al concepto de la calidad, estableciendo los catorce puntos de la alta administración (Deming, 1989): Crear constancia con el propósito de mejorar el producto y el servicio; Adoptar la nueva filosofía teniendo en cuenta la realidad americana; Dejar de depender de la inspección en masa; Acabar con la práctica de hacer negocios sobre la base del precio; Descubrir el origen de los problemas; Mejorar constantemente el sistema de producción y servicio; Implantar la formación; Desechar el miedo; Derribar las barreras entre las áreas de Staff; Eliminar los slogan, exhortaciones y metas para la mano de obra; Eliminar los objetivos numéricos para los directivos; Eliminar las barreras que privan a la gente de estar orgullosas de su trabajo; Estimular la educación y la auto mejora de todo el mundo; y Actuar para lograr la transformación. De igual manera, Deming populariza el modelo Shewhart PDCA (Plan – Do – Check – Act) que establece el conjunto de procesos que se pueden gestionar en una organización. La figura 11 muestra el ciclo PDCA.

Por último, aunque más enfocado a la teoría de la optimización de la producción, se encuentran los aportes de Shigeo Shingo, quien afirma que para reducir defectos dentro de las actividades de producción, el concepto más importante es reconocer que estos se originan en el proceso y que las inspecciones sólo pueden descubrirlos. Shingo propone la creación del sistema poka-yoke o sistema aprueba de errores, el cual consiste en la creación de elementos que detecten los defectos de la producción (Shingo, 1990). De igual manera, propone el concepto de inspección en la fuente “Just in Time” para detectar a tiempo los errores y establece que para que para que exista un sistema de control de calidad total se debe involucrar a todo el personal de la organización, en la prevención de errores a través de los “círculos de calidad cero”.

Figura 11. Ciclo PDCA de la Gestión de la Calidad



Fuente. Autor

3.1.2. La Calidad en los Estándares

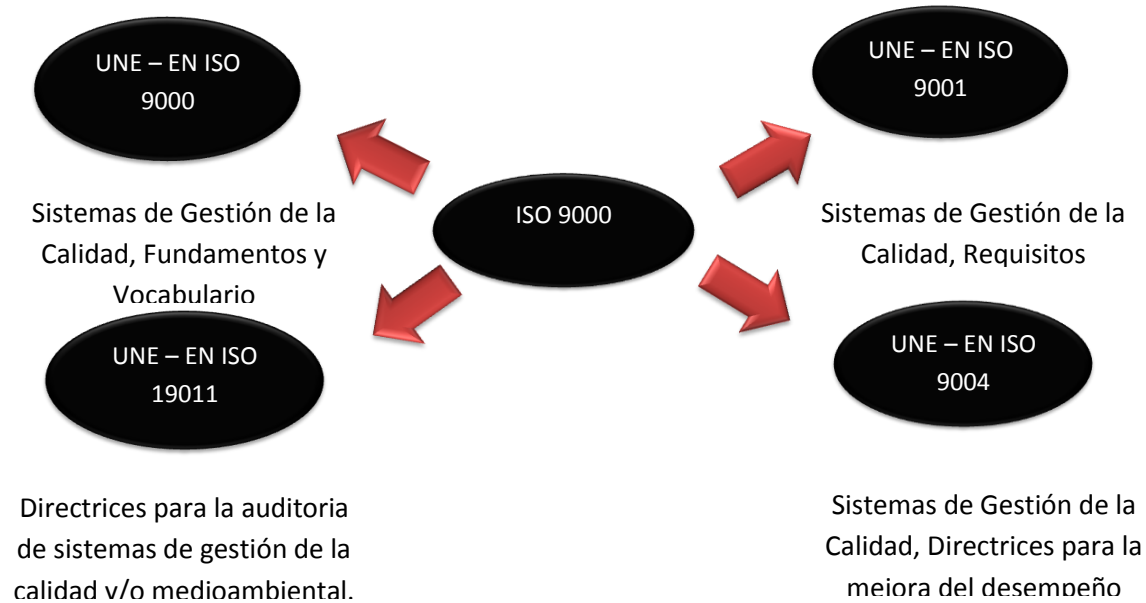
El auge organizacional representativo que la noción de Calidad ha ido tomando con el tiempo, ha propiciado que surjan a nivel internacional estándares destinados a ofrecer pautas y guías para que las empresas puedan integrar adecuadamente un sistema de gestión de calidad total. De acuerdo con esto, Ortega y Gaset afirma que "el <<buen gusto>> como norma equivale a una amonestación para que neguemos nuestro sincero gusto y lo sustituyamos por otro que no es el nuestro, pero que es >>bueno>>". No obstante, continúa la discusión arraigada de si la calidad debe verse representada en la manufactura de producto o en el servicio prestado al cliente. A continuación se describen los intereses de algunos de ellos.

- **Familia de Estándares de Calidad ISO 9000:2000**

ISO 9000 es una familia de estándares orientada al establecimiento de pautas para la creación y mejoramiento continuo de un sistema de gestión de calidad. Actualmente está compuesta por la norma ISO 9000, ISO 9001 ISO 9004 e ISO 9011. La figura 12 ilustra el interés de cada una de las normas.

La ISO 9000, define la calidad como "*el conjunto de características de un producto o servicio que le confieren la aptitud para satisfacer las necesidades del cliente*". Por tal motivo, se puede afirmar que la ISO9000 tiene una orientación enfocada al producto.

Figura 12. Familia de Normas ISO 9000



Fuente. Autor.

La familia de normas ISO 9000 no definen como debe ser el Sistema de la Calidad de una empresa, sino que fijan requisitos mínimos que deben cumplir los sistemas de la calidad. Dicho sistema se basa en los siguientes principios de gestión de calidad:

1. Enfoque al cliente. Las organizaciones deben velar por la satisfacción de las necesidades presentes y futuras de los clientes.
2. Liderazgo. En la organización debe existir personal capacitado para la creación y el mantenimiento del ambiente interno, en el cual los demás trabajadores puedan trabajar para lograr los objetivos organizacionales.
3. Participación del personal. El personal debe participar activa y responsablemente en las actividades de la organización.
4. Enfoque basado en procesos. El enfoque de la norma promueve el desarrollo, la implementación y mejora de un sistema de gestión de calida basado en procesos. La figura 13 muestra como los clientes juegan un papel fundamental en la definición de requisitos y en el seguimiento del nivel de satisfacción.

Figura 13. Enfoque de procesos de la norma ISO 9000

Fuente. (ISO, 2000a)

5. Enfoque de sistema para la Gestión. La eficacia y la eficiencia de una organización se mide a través de las interrelaciones entre los procesos y el sistema de gestión de calidad.
6. Mejora continua. La organización debe tener siempre presente la mejora continua del desempeño global.
7. Enfoque basado en hechos para la toma de decisiones. Las decisiones se deberán tomar basadas en datos e información.
8. Relaciones mutuamente beneficiosas con el proveedor. Se debe velar por mantener una relación mutuamente beneficiosa entre la organización y sus proveedores debido a su interdependencia.

- **Modelo EFQM (European Foundation Quality Model)**

EFQM es un modelo de calidad total, creado como marco para la obtención del premio European Quality Award, el cual es un medio para el reconocimiento de la calidad a nivel regional y nacional. Desde su creación en 1988 el modelo ha sufrido varias modificaciones, el actual se denomina EFQM Model of Excellence 2010.

EFQM considera que la calidad es la satisfacción de las necesidades y expectativas de sus clientes, de su personal, y de las demás entidades implicadas.

> *"la satisfacción del cliente, la satisfacción de los empleados y un impacto positivo en la sociedad se consiguen mediante el liderazgo en política y estrategia, una acertada gestión de personal, el uso eficiente de los*

recursos y una adecuada definición de los procesos, lo que conduce finalmente a la excelencia de los resultados empresariales" (EFQM, 2010).

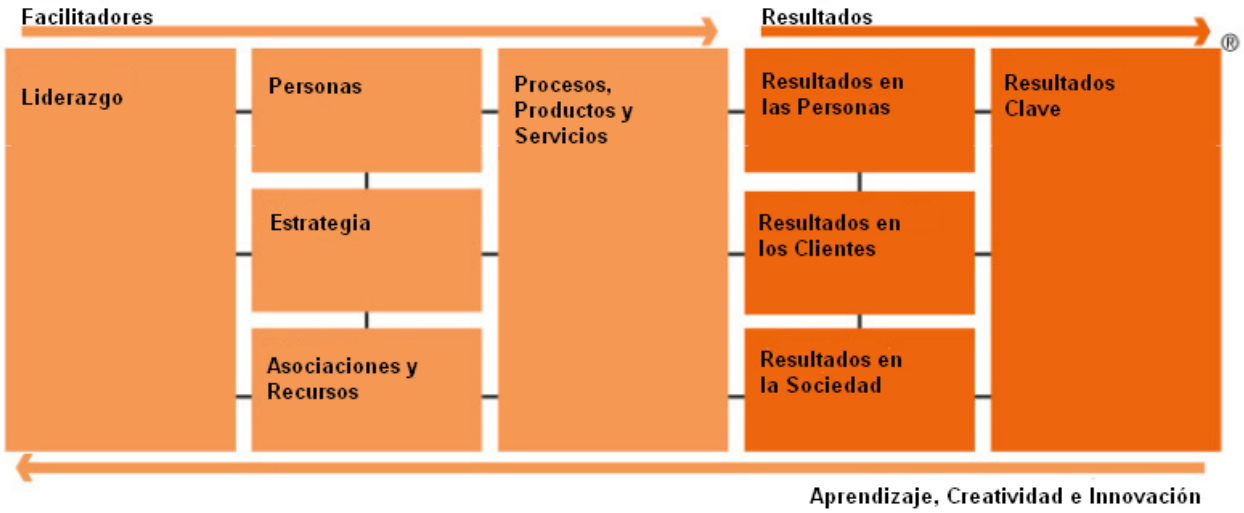
El modelo EFQM basa su sistema de gestión de calidad en las siguientes nociones de excelencia:

1. Responsabilidad por un futuro sostenible de la organización. Las organizaciones excelentes integran en su cultura una actitud ética, valores claros y altos estándares de comportamiento organizacional, con el fin de luchar por la sostenibilidad económica, social y ecológica.
2. Resultados equilibrados. Una organización excelente debe conocer su misión y los progresos que se obtienen a partir de la visión, con el fin de planear y lograr resultados equilibrados a corto y largo plazo.
3. Valor agrado a los clientes. Una organización excelente sabe que los clientes son su principal preocupación y por lo tanto está pendiente de sus necesidades y expectativas.
4. Líderes con visión, inspiración e integridad. Una organización excelente tiene líderes que planean y ejecutan el futuro y actúan como modelo por sus valores y ética.
5. Administración por procesos. Una organización excelente está administrada, estructurada y estratégicamente alineada con sus procesos, tomando decisiones basadas en hechos que permitan crear equilibrio y resultados sostenibles.
6. Reconocimiento del éxito de las personas. Una organización excelente da valor a sus empleados y crea una cultura de "empowerment" que permita un logro equilibrado de las metas personales y organizacionales.
7. Fomento de la creatividad y la innovación. Las organizaciones excelentes generar mayor valor y nivel de desempeño a través de la innovación continua y sistemática mediante el aprovechamiento de la creatividad de sus "stakeholders[6]".
8. Construcción de alianzas. Las organizaciones excelentes buscan, desarrollan y mantienen relaciones de confianza con distintos socios para asegurar el éxito mutuo. Estas asociaciones se pueden formar con los clientes, sociedad, proveedores, instituciones educativas u organizaciones no gubernamentales (ONG).

El modelo EFQM 2010 trae consigo cambios en la terminología de algunos de sus elementos. La figura 14, ilustra el modelo EFQM presentado para 2010.

[6] Algunos autores hacen referencia a los stakeholders para refereirse a cualquier persona o grupo que se verá afectado por el sistema directa o indirectamente (Sommerville, 2006)

Figura 14. Modelo EFQM



Fuente. Traducido de EFQM, 2010

1. Liderazgo. Los líderes desarrollan la misión, visión, valores y ética y actúan como modelos a seguir, definen, supervisan, revisan e impulsan la mejora del sistema de gestión de la organización y su funcionamiento, colaboran con los interesados externos, refuerzan una cultura de excelencia con las personas de la organización y garantizan que la organización sea flexible y gestione el cambio de manera efectiva.
2. Personas. Los planes de las personas apoyan las estrategias de la organización. El conocimiento y las capacidades de las personas debe desarrollarse. Las personas deben alinearse, participar y comunicarse de manera efectiva con toda la organización. Las personas deben ser recompensadas, reconocidas y atendidas.
3. Estrategia. La estrategia se basa en la comprensión de las necesidades y expectativas de los stakeholders y del ambiente externo. Las estrategias y políticas de apoyo se deben desarrollar, revisar y actualizar para garantizar la sostenibilidad económica, social y ecológica de la organización, estas deben ser comunicadas y desplegadas a través de planes, procesos y objetivos.
4. Asociaciones y Recursos. Los socios y proveedores deben administrarse para un beneficio sostenible. De igual manera, las finanzas se deberán administrar para asegurar el éxito. Los edificios, equipos, materiales y recursos naturales se deben utilizar de una manera sostenible. La tecnología se debe gestionar para apoyar la ejecución de la estrategia. La Información y el conocimiento se gestionarán para apoyar la toma eficaz de decisiones y para construir la capacidad de organización.
5. Procesos, Productos y Servicios. Las organizaciones excelentes diseñan, gestionan y mejoran los procesos para generar cada vez mayor valor para los clientes y otras partes interesadas.

6. Resultados en las Personas. La organización debe medir el grado de satisfacción de las necesidades y expectativas de las personas que integran la organización, dado que si los trabajadores no encuentran cubiertas sus necesidades es muy difícil poder lograr el grado de motivación, participación e implicación que requiere el correcto desempeño de las funciones de la organización.
7. Resultados en los Clientes. La organización debe medir el grado de satisfacción de las necesidades de los clientes externos, y la adopción de medidas para evaluarla.
8. Resultados en la Sociedad. La organización debe medir el grado de cumplimiento de sus obligaciones con la sociedad y la satisfacción de las expectativas de ésta.
9. Resultados Clave. Pretende asegurar que la organización mide el grado de cumplimiento de metas y objetivos y de aquellos elementos que ha identificado como logros importantes y medibles para el éxito de la organización a corto y largo plazo.

- **Marco Común de Evaluación – CAF**

El marco común de evaluación CAF (Ministerio Administraciones Públicas, 2005) fue creado por el Ministerio de Administraciones Públicas de España en concordancia con 15 países de la unión europea y tiene como fin generar lineamientos para la gestión de calidad y la autoevaluación de las organizaciones del sector público, permitiendo compartir experiencias de buenas prácticas y desarrollar actividades de benchmarking. El modelo CAF se basa en los nueve criterios definidos por EFQM anteriormente, aunque uno de sus principales propósitos es el de servir de puente entre los diferentes modelos de calidad.

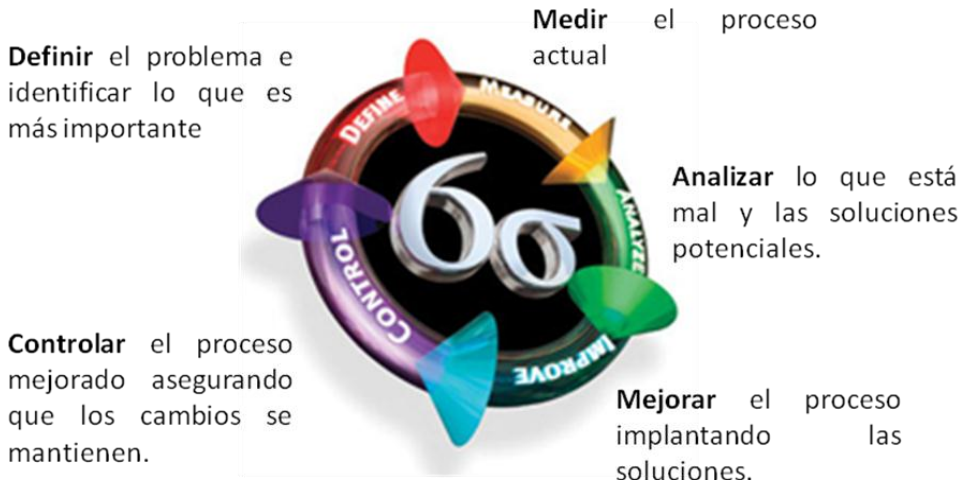
- **Modelo Seis Sigma**

En 1986, Motorola (Maya, Rodriguez-Salazar, & Rojas, 1996) crea una metodología de calidad de clase mundial denominada seis sigma, la cual está orientada a ofrecer productos y servicios más rápidos a un menor costo gracias a la prevención de los errores industriales (los errores deben ser menores o iguales a 3,4 por millón), los cuales pueden ser ocasionados por:

- Fallas internas, de los productos defectuosos; retrabajo y problemas en el control de materiales.
- b) Fallas externas, de productos regresados; garantías y penalizaciones.
- Evaluaciones del producto, debido a inspección del proceso y producto; utilización, mantenimiento y calibración de equipos de medición de los procesos y productos; auditorias de calidad y soporte de laboratorios.
- d) Prevención de fallas, debido al diseño del producto, pruebas de campo, capacitación a trabajadores y mejora de la calidad.

El modelo de calidad (Harry & Schoeder, 2000) planteado en seis sigma se ilustra en la figura 15.

Figura 15. Modelo de Calidad Seis Sigma



Fuente. Autor.

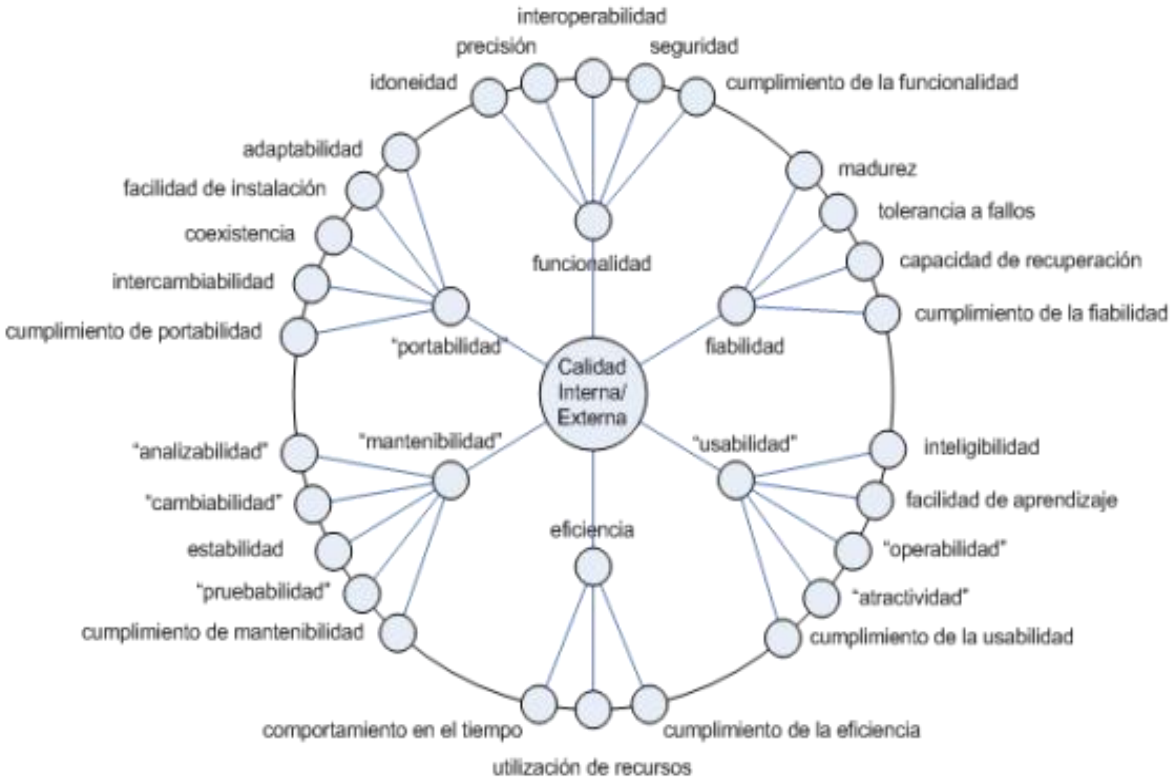
El modelo de calidad seis sigma se centra en el cliente y busca tomar decisiones basadas en hechos. De igual manera, busca alentar el trabajo en equipo en pro del mejoramiento continuo de la organización y de los procesos.

- **ISO 25000 - Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE**

La serie de normas SQUARE está basada en las normas ISO 9126 y en la ISO 14598 y está prevista, pero no limitada a los desarrolladores, adquisisores y evaluadores independientes de productos software, en particular a los responsables de definir los requisitos de calidad y la evaluación de dichos productos (ISO/IEC 25000, 2005)

Los criterios establecidos por ISO 25000 para la especificación de requisitos de calidad de productos software, sus métricas y su evaluación se muestran en la figura 16.

Figura 16. Requisitos de calidad de ISO 25000



Fuente. ISO 25000:2005

La tabla 3 presenta un resumen de lo expuesto anteriormente.

Tabla 3. Estándares de Calidad

Estándar	**Definición de Calidad**	**Tipo de Orientación**		**Certificable**
		Hacia el Producto	**Hacia el Servicio**	
ISO 9000	Conjunto de características de un producto o servicio que le confieren la aptitud para satisfacer las necesidades del cliente.	SI		SI (ISO 9001)

Estándar	Definición de Calidad	Tipo de Orientación		Certificable
		Hacia el Producto	Hacia el Servicio	
EFQM	Satisfacción de las necesidades y expectativas de sus clientes, de su personal, y de las demás entidades implicadas	SI	SI	NO
Seis Sigma	La calidad es cuantificable y es responsabilidad de los procesos desarrollados por cada empleado.	SI		NO
ISO 25000	Es un conjunto estructurado de características y que contemplan: fiabilidad, usabilidad, eficiencia, mantenibilidad y portabilidad.	SI		NO

Fuente. Autor

3.1.3. La Calidad en los Sistemas de Información

Teniendo en cuenta las investigaciones previas mencionadas en los ítems anteriores, se puede decir entonces que la calidad es el conjunto de características que posee una organización que le permiten satisfacer no solo las necesidades expresadas e implícitas de los clientes sino las necesidades organizacionales propias que permitan mantener su rentabilidad y sostenibilidad, por ende, para que exista calidad todos los entes organizacionales deben estar implicados y apropiados de las responsabilidades a lo que esto conlleva.

Dentro de las necesidades organizacionales expresadas e implícitas se encuentra la calidad de los Sistemas de Información como parte fundamental en el desarrollo de los procesos de negocio, por tal motivo, surge la necesidad de garantizar que los SI tengan calidad, en términos del producto, del proceso de desarrollo y de los datos que guardan, implicando esto una mejora en la mantenibilidad y la seguridad de la información.

No obstante, la calidad de los Sistemas de Información es un tema de constante preocupación no sólo de las organizaciones sino de los desarrolladores de software. El Standish Group (Piattini, 2007) llevo a cabo un estudio en donde se logró determinar que el 23% de los desarrollos de software fallan, en contraste con un 49% cuyo desarrollo es cuestionado y sólo un 28% satisfactorio. Lo anterior conlleva a que las organizaciones sean cada vez más conscientes de las pérdidas económicas acarreadas por la falta de calidad en los sistemas de información y a su importancia frente a la calidad de la organización.

Para dar una idea clara de las implicaciones organizacionales que las fallas en los sistemas de información generan, en la tabla 4 se describen en resumen algunos casos presentados por el foro sobre riesgos para el público en computación y sistemas relacionados de la ACM (Newman, 2010)

Tabla 4. Casos de Fallos en la Calidad de los SI

Organización	Caso
Aeropuerto de Japón	El 14 de Enero de 2010 un problema con el software de control de tráfico aéreo ocasionó que los vuelos no pudieran ser identificados de manera oportuna, originando la interrupción de los vuelos en el aeropuerto de Japón.
NASA	El orbitador climatológico de Marte se quemó en la atmósfera marciana en 1999 después de haber perdido su inserción orbital, por cálculos inconsistentes de la unidad. Ese mismo año el Mars Polar Lander se desplomo durante su aterrizaje en Marte, por un desajuste de software.
Therac 25	El 24 de Enero de 2010 el New York Times expuso que por lo menos 5 personas murieron por un error en las validaciones de entrada de la interfaz grafica de Therac 25 (herramienta utilizada para radicación).
ESA	El 4 de junio de 1996 la ESA (Agencia Espacia Europea) reutilizó el software de su predecesor el Ariane 4 para el montaje de su nave el Ariane 5, la conversión de un valor de 64 bits a uno de 16 bits causó un desbordamiento que terminó con la desintegración de la nave 40 segundos después de su despegue.
Intel Pentium	En 1993 Intel sacó al mercado un procesador con un error en la unidad de punto flotante, al descubrir el error se hizo necesario recoger toda la producción entregada y reemplazarla por procesadores no defectuosos. Esta operación tuvo un costo de 475 millones de dólares.

Fuente. Autor

4. NOCIONES ACERCA DE LA GESTIÓN DE RIESGOS

4.1 El Concepto de Gestión de Riesgos

La gestión de riesgos son todos los procesos usados para identificar, controlar y minimizar el impacto de los eventos inciertos. El objetivo de un programa de gestión de riesgos es el de reducir el riesgo en el desarrollo de algunas actividades o funciones llevándolas a un nivel aceptable (Peltier, 2001).

La gestión de riesgos consta de distintos procesos: análisis de riesgos, evaluación de riesgos, mitigación de riesgos y aseguramiento de la vulnerabilidad y evaluación de controles (ver tabla 5).

Tabla 5. Procesos de la Gestión de Riesgos

Término	Definición
Gestión de Riesgos	Identificar, controlar y minimizar el impacto de eventos inciertos. El objetivo de la gestión de riesgos es reducir el riesgo a un nivel aceptable. Soportar estos procesos con un administrador Senior es una demostración de su diligencia prevista.
Análisis de Riesgos	Una técnica para identificar y evaluar factores que podrían poner en peligro los sucesos de un proyecto o el alcance de las metas. Esta técnica también ayuda a definir medidas para reducir la probabilidad de ocurrencia de estos factores e identificar contramedidas para tratarlas satisfactoriamente.
Evaluación de Riesgos	El cálculo del riesgo. Riesgo es una amenaza que evidencia alguna vulnerabilidad que podría causar el daño de un activo.
Mitigación de Riesgos	Es el proceso en el cual una organización implementa controles y salvaguardas para prevenir la ocurrencia de los riesgos identificados, mientras que al mismo tiempo pone en práctica el medio de recuperación ya que el riesgo podría hacerse realidad a pesar de todos los esfuerzos.
Aseguramiento de la Vulnerabilidad y Evaluación de Controles	Examen sistemático de la infraestructura crítica, los sistemas interconectados, su información, o productos para determinar lo adecuado de las medidas de seguridad, identificar deficiencias de seguridad, evaluar alternativas de seguridad, y verificar lo adecuado de tales medidas antes de la implementación.

Traducido de: PELTIER, 2001

4.2 Gestión de Riesgos y Controles en Sistemas de Información

4.2.1. El Concepto de "Riesgos y Controles en Sistemas de Información".

En materia de riesgos y controles en sistemas de información, existen actualmente varios estándares e investigaciones, en la tabla 6 se describe la concepción sobre riesgo y control de algunos de los estándares más relevantes a nivel nacional e internacional.

Tabla 6. Definiciones aceptadas en estándares sobre riesgos y controles

Estándar	Riesgo	Control
Estándar de Auditoria de SI – Documento S11 - ISACA[7] (ISACA, 2002)	La posibilidad de ocurrencia de un acto o evento que podría tener un efecto adverso en la organización y en sus sistemas de información.	Políticas y procedimientos implementados para alcanzar un objetivo de control relacionado.
AS/NZS 4360:2004 Estándar Australiano de Administración de Riesgos (AS/NZS 4360:2004, 2004).	La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se le mide en términos de consecuencias y probabilidades.	Parte de la administración de riesgos que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.
Modelo Estándar de Control Interno – MECI (Miniterio de Educación Nacional, 2005)	¿Qué puede suceder?, ¿Dónde y Cuando?, ¿Cómo y por qué? Determinar consecuencias y posibilidades	***Control de Gestión***. Métodos Procedimientos Actuaciones Acciones Admón. Información, Admón. Recursos ***Control Estratégico.*** Esquema de organización Planes Principios Normas ***Control de Evaluación.*** Mecanismos de Evaluación y Verificación
MAGERIT – Versión 2.	Administración de riesgos, incluye políticas,	Estimación del grado de exposición a que una

[7] Information System Audit and Control Association – ISACA – www.isaca.org

Estándar	Riesgo	Control
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Ministerio de Administraciones Públicas, , 1997)**.**	procedimientos, guías, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, gerencial o legal. [17799:2005]	amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Fuente. Autor

Entonces, tomando en cuenta las investigaciones anteriores se puede decir que un riesgo es "*la posibilidad de ocurrencia de un acto o evento que podría tener un efecto adverso en la organización y en sus sistemas de información*". Esta definición debe ser contrastada con algunos conceptos que suelen utilizarse asociados al riesgo, tales como amenaza, vulnerabilidad, impacto y salvaguardas.

Amenaza. Condición del entorno del sistema de información, que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando alguno de los activos de la compañía (Silberfich, 2009).

Riesgo. Posibilidad de que se produzca un impacto en la organización (Silberfich, 2009).

Vulnerabilidad. Hecho o actividad que permite concretar una amenaza (Silberfich, 2009).

Impacto. Es el daño producido por la ocurrencia de una amenaza.

Salvaguardas. Protecciones u acciones que disminuyen el riesgo.

4.2.2. Modelos de Gestión de Riesgos y Controles en Sistemas de Información.

Indudablemente el primer camino a tomar cuando se plantea identificar los modelos existentes sobre gestión de riesgos y controles en sistemas de información es el de los estándares, los cuales proveen información sobre las etapas o fases a seguir por una organización en lo referente a este aspecto, no obstante, este documento pretende también observar cuales son los modelos más representativos utilizados por algunas empresas multinacionales de auditoría al momento de gestionar riesgos y controles en SI.

- **Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)**

Octave fue desarrollado por la Universidad Carnegie Mellon y es uno de los métodos relativamente nuevos para la evaluación y gestión de los riesgos en sistemas de información (Alberts, 1999). Su principal objetivo es el de garantizar la seguridad de los SI y una de sus particularidades, es que puede ser realizado por vía de la autogestión; es decir por personal de la organización, perteneciente tanto a las unidades funcionales como al área de TI, los cuales trabajan juntos para determinar las necesidades de seguridad de la organización. La tabla 7 resume las actividades planteadas por OCTAVE para la gestión de riesgos en los sistemas de Información.

Tabla 7. Actividades planteadas por OCTAVE para la gestión de riesgos en los sistemas de Información.

Actividades	A1. Identificación de los activos críticos. A2. Identificación de las amenazas y las vulnerabilidades de la organización. A3. Identificación de las exigencias de seguridad y las normas existentes. A4. Identificar los componentes claves y las vulnerabilidades técnicas que ocasionan los riesgos. A5. Evaluar riesgos y ponderar los riesgos A6. Desarrollar estrategias de protección basadas en buenas prácticas. A7. Establecer un plan de reducción de los riesgos.

Fuente. Autor.

- **ISM3 o Cubo ISM (Information Security Maturity Model) – ISM3 RA (Risk Assessment)**

Este modelo extiende los principios de calidad de la norma ISO9001 para el sistema de gestión de la seguridad de la información. ISM3 es un estándar orientado por procesos que utiliza niveles de madurez (Consortium ISM3, 2009). Para llegar a estos niveles de madurez, varios procesos claves deben ser considerados, algunos de estos procesos son disparados por eventos mientras que otros son periódicos o continuos. ISM3 reconoce que cada organización tiene un contexto y recursos únicos y que por lo tanto los diferentes procesos deben ser aplicados cuidadosamente, ya que pueden requerir más tiempo del esperado o requerir un orden lógico diferente. De igual manera, ISM3 reconoce la importancia de la utilización de los sistemas de información para la operacionalización de los

procesos, razón por la cual es de vital importancia conocer su nivel de dependencia. Las implementaciones de ISM3 son compatibles con la ISO27001, CMMI, COBIT e ITIL.

A continuación se presenta un resumen de la taxonomía de riesgos descrita por ISM3, en donde clasifican siete niveles de riesgo dependiendo de su efecto más no de su causa. De igual manera, en la tabla 8 se especifican las actividades relacionadas por ISM3 para la gestión de riesgos relacionados con la información.

1. Destrucción, corrupción o pérdida de los sistemas o la información activos.
2. Error en la destrucción de sistemas o información obsoleta o error en la detención de sistemas a voluntad.
3. Uso indebido del acceso a los sistemas de información.
4. Registro incorrecto del acceso a los sistemas de información
5. Acceso no autorizado, espionaje, robo y divulgación de sistemas de información
6. Bajo rendimiento o interrupción de los servicios de los sistemas activos o error en el acceso autorizado.
7. Obsolescencia de la información y de los Sistemas.

Tabla 8. Actividades relacionadas por ISM3 para la gestión de riesgos relacionados con la información

Actividades	A1. Medir el estado actual de la seguridad de los sistemas y la organización A2. Identificar las amenazas y debilidades. A3. Establecer que procesos son apropiados para el cumplimiento de los objetivos de seguridad. A4. Dar prioridad a la inversión de los procesos de seguridad.

Fuente. Autor

- **AS/NZS 4360:2004 Estándar Australiano de Administración de Riesgos**

El estándar australiano para la administración de riesgos AS/NZS: 2004 proporciona un marco genérico para establecer el contexto, la identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de riesgos.

Este estándar considera que la gestión de riesgos debe ser una filosofía organizacional y que debe ser parte de su cultura de manera que no sea vista como una actividad separada de los procesos de la organización. La tabla 9 muestra las actividades propuestas por AS/NZS para la gestión de riesgos.

Tabla 9. Actividades relacionadas por AS/NZS para la GRCSI

Actividades	A1. Comunicar y Consultar A2. Establecer el contexto A3. Identificar Riesgos A4. Analizar Riesgos A5. Evaluar Riesgos A6. Controlar los Riesgos A7. Monitorear y Revisar

Fuente. Autor.

- **Risk Management Guide for Information Technology Systems SP800 – 30.**

La guía para la gestión de riesgos de sistemas de tecnología de información fue desarrollada por el Instituto Nacional de estándares y Tecnología (National Institute of Standards and Technology – NIST) (Stonebumer, 2002). Esta guía se enfoca en la premisa que un proceso eficaz de gestión del riesgo es un componente importante de un exitoso programa de seguridad informática. El objetivo principal del proceso de gestión de una organización de riesgo debe ser proteger a la organización y su capacidad para llevar a cabo su misión, no sólo sus activos de TI. Por lo tanto, el proceso de gestión de riesgos no debe ser tratado primordialmente como una función técnica realizada por los expertos que operan y administran los sistemas de información, sino como una función esencial de gestión de la organización.

Uno de los aportes más importantes que tiene la guía es que promueve el seguimiento y aprendizaje de los riesgos a través de su transferencia y documentación. Un ejemplo de un plan de implementación de seguridad se muestra en la figura 17.

Figura 17. Ejemplo de Plan de Mantenimiento de Seguridad

(1) Riesgo (Vulnerabilidad/Amenaza)	(2) Nivel de Riesgo	(3) Controles Recomendados	(4) Prioridad de Acción	(5) Controles Planeados Seleccionados	(6) Recursos Requeridos	(7) Equipo Responsable/Personas	(8) Fecha de Inicio/Fecha de Fin	(9) Requerimientos de Mantenimiento/Comentarios
Usuario no autorizado puede hacer Telnet al servidor de la compañía y buscar archivos	Alto	•Desactivar la entrada al Telnet •Desactivar el acceso de todo el mundo a los archivos sensitivos de la compañía •Desactivar el usuario invitado o agregar dificultad para adivinar el password.	Alta	•Desactivar la entrada al Telnet •Desactivar el acceso de todo el mundo a los archivos sensitivos de la compañía •Desactivar el usuario invitado	10 horas para reconfigurar y pruebas del sistema	Jhon Doe, Administrador del Servidor; Jimm Smith, Administrador del Firewall de la compañía	01/09/09 hasta 02/09/09	Realizar la revisión periódica del sistema de seguridad y pruebas para garantizar la seguridad adecuada proporcionada por el servidor

Fuente. SP800-30

A continuación en la Tabla 10 se presenta las actividades relacionadas por SP800-30 para la gestión de riesgos en sistemas de información.

Tabla 10. Actividades relacionadas por SP800-30 para la gestión de riesgos en sistemas de información.

Actividades	A1. Identificación de Sistemas A2. Identificación de Amenazas A3. Identificación de vulnerabilidades A4. Análisis de Controles A5. Identificación de Probabilidades A6. Análisis de Impacto A7. Determinación del riesgo A8. Recomendaciones de control A9. Documentación de Resultados

Fuente. Autor

- **Open Information Security Risk Management**

La guía para la gestión de riesgos de seguridad de la información fue creada por The Security Officers Management and Analysis Project – SOMAP (SOMAP, 2006). Esta guía define el riesgo como:

> "El daño potencial que puede surgir de un proceso actual o de algún acontecimiento futuro" *SOMAP (2006)*.

Partiendo de esta definición agrupa los diferentes riesgos a los cuales se puede ver sometida la información. La figura 18 ilustra dicha agrupación.

Figura 18. Agrupación de Riesgos según SOMAP.

Fuente. Traducido de SOMAP, 2009

En la tabla 11 se presenta las actividades planteadas por SOMAP para la gestión de riesgos de la información.

Tabla 11. Actividades planteadas por SOMAP para la gestión de riesgos de la información

Actividades	A1. Identificar los Riesgos A2. Planear Políticas y Controles A3. Implementar Protecciones A4. Monitorear y Evaluar

Fuente. Autor.

- **MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Versión 2.0**

La metodología MAGERIT fue creada por el Ministerio de Administraciones Públicas de España y tiene como principales objetivos concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo, ofrecer un método sistemático para analizar tales riesgos, ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control y preparar a la Organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

MAGERIT busca proteger la misión de la organización teniendo en cuenta las dimensiones de la seguridad: disponibilidad, integridad, confidencialidad y autenticidad. De acuerdo con estas dimensiones se define el riesgo como:

> "La estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización"

MAGERIT busca entonces en la gestión de riesgos la implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. La gestión de riesgos debe encajar entonces en todas las funciones de seguridad de la organización.

Por otro lado, MAGERIT ofrece una perspectiva de las diferentes amenazas que podrían afectar los activos de los sistemas de información. La tabla 12 muestra un resumen de dichos aspectos.

Tabla 12. Tipos de Amenazas según MAGERIT

Amenaza	Descripción	Tipos de Activos
Desastres Naturales	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.	• [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información AUX] equipamiento auxiliar • [L] instalaciones

Amenaza	Descripción	Tipos de Activos
De Origen Industrial	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	• [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información AUX] equipamiento auxiliar [L] instalaciones
Errores y Fallos No Intencionados	Fallos no intencionales causados por las personas.	• [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [P] Personal
Ataques Intencionados	Fallos deliberados causados por las personas.	• [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [P] Personal

Fuente. Autor

Por último, la tabla 13 especifica las actividades propuestas por MAGERIT para la gestión de riesgos en sistemas de información.

Tabla 13. Actividades propuestas por MAGERIT para la gestión de riesgos en sistemas de información

Actividades	A1. Identificación y Valoración de Activos (Valor cualitativo y cuantitativo) A2. Valoración de Amenazas A3. Determinación del Impacto (Acumulado y repercutido) A4. Determinación del Riesgo (Acumulado y repercutido) A5. Implantar Salvaguardas A6. Revisión de la Actividad A3. Impacto Residual A7. Revisión de la Actividad A4. Riesgo Residual

Fuente. Autor

- **Método Armonizado para la Gestión de Riesgos – MEHARI**

MEHARI fue desarrollado por el CLUSIF (Club se la Seguridad de la Información de Francia) (CLUSIF, 2007) para ayudar a tomar decisiones (a los responsables de la seguridad, administradores de riesgos y gerentes) sobre cómo gestionar la seguridad de la información y minimizar los riesgos. MEHARI específica que una situación de riesgo se caracteriza por la potencialidad y los efectos inherentes a la ausencia de cualquier medida de seguridad y ofrece un marco metodológico, instrumentos y bases de conocimiento para analizar los principales problemas, explorar las vulnerabilidades, reducir la gravedad de los riesgos y supervisar la seguridad de la información. La tabla 14 presenta las actividades relacionadas por MEHARI para la gestión de riesgos de la información.

Tabla 14. Actividades relacionadas por MEHARI para la gestión de riesgos de la información

Actividades	A1. Evaluación de la exposición inherente A2. Evaluación del Impacto Intrínseco A3. Evaluación del impacto de reducción de riesgo a partir de una auditoria de seguridad MEHARI A4. Evaluación de la Potencialidad del Impacto. A5. Evaluación de la Gravedad del Escenario A6. Expresar las Necesidades de Seguridad.

Fuente. Autor

- **ISO 27005**

Esta Norma es la primera de la serie ISO 27000 que proporciona directrices para la Gestión del riesgo de Seguridad de la Información en una Organización (ISO Directory, 2008). Esta guía es aplicable a todos los tipos de organización. Aunque

no proporciona o recomienda una metodología específica, establece una serie de factores, para determinar el alcance real del sistema de gestión de la seguridad de la información (SGSI). La tabla 15 presenta las actividades propuestas por ISO 27005 para la gestión de riesgos de la información.

Tabla 15. Actividades propuestas por ISO 27005 para la gestión de riesgos de la información

Actividades	A1. Establecer el contexto. A2. Evaluación del riesgo. a. Identificación del riesgo b. Estimación del riesgo c. Valoración del riesgo A3. Tratamiento del riesgo. A4. Aceptación del riesgo. A5. Comunicación del riesgo. A6. Seguimiento del riesgo.

Fuente. Autor

- **Managing Risk from Information Systems SP800-39. Una Perspectiva Organizacional**

La guía para la gestión de riesgos de sistemas de información fue desarrollada por el Instituto Nacional de estándares y Tecnología (National Institute of Standards and Technology – NIST). La SP800-39 proporciona a las organizaciones un proceso estructurado y flexible para la gestión de riesgos relacionados con el funcionamiento y el uso de sistemas de información. Este documento es utilizado por las organizaciones para determinar una adecuada reducción del riesgo necesaria para proteger los sistemas de información y la infraestructura de apoyo a la misión de organización y los procesos de negocio (Ross, 2008). El conjunto de actividades que se deben desarrollar de acuerdo con la guía se muestran en la tabla 16.

Tabla 16. Actividades relacionadas por SP800-39 para la seguridad de los sistemas de información

Actividades	A1. Categorizar los Sistemas de Información A2. Seleccionar los Controles de Seguridad A3. Implementar los Controles de Seguridad A4. Evaluar los Controles de Seguridad A5. Autorizar los Sistemas de Información A6. Monitorear el Estado de la Seguridad

Fuente. Autor

4.3 Revisando las Actividades de GRCSI en el Marco de los Estándares[8]

En los estándares revisados en los ítems anteriores, se pueden identificar varios estándares que aportan elementos fundamentales al momento de considerar las actividades a desarrollar por una organización para la gestión de riesgos y controles en sistemas de información.

Un primer grupo conformado por 4 estándares, constituido por el Operationally Critical Threat, Asset, and Vulnerability Evaluation – OCTAVE (Alberts, 1999), el Risk Management Guide for Information Technology Systems SP800-30 (Stonebumer, 2002), la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGUERIT Versión 2.0 (1997) y el Managing Risk from Information Systems SP800-39 (Ross, 2008), están dirigidos a la seguridad de los sistemas de información. En ellos, la GRCSI es tenida en cuenta para garantizar la continuidad de los procesos de negocio que tienen un nivel determinado de dependencia de los sistemas de información y para evaluar y generar salvaguardas de las distintas amenazas a las que se exponen los SI, por su naturaleza o por fuentes externas.

Un segundo grupo de 4 estándares, conformado por la norma ISO 27005 (2008), el Information Security Maturity Model – ISM3 (2009), el Open Information Security Risk Management - SOMAP (2006) y el Método Armonizado para la Gestión de Riesgos – MEHARI (2007), están orientados a los aspectos de seguridad de la información, en donde la GRCSI encaja como elemento destinado a garantizar la disponibilidad, la integridad, la confidencialidad y la confiabilidad de la información.

Complementando los dos grupos de estándares anteriores, en lo relacionado con la GRCSI, se encuentra el Estándar Australiano de Administración de Riesgos AS/NZS 4360 (2004), el cual está orientado a la administración de riesgos a nivel organizacional, ofreciendo una identificación de las oportunidades y amenazas para la adecuada toma de decisiones de acuerdo con cada contexto organizacional.

Ahora bien, si se reconoce a la GRCSI como parte de la seguridad de los sistemas de información y de la seguridad de la información (Blakley, 2001) y estas a su vez como parte del entorno organizacional, es prioritario distinguir cuales serían los roles asociados a la GRCSI, con el fin de determinar las actividades que las

[8] La siguiente revisión hace parte del artículo de investigación “Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información”, en revisión por parte de la revista Estudios gerenciales clasificada A2 Colciencias.

organizaciones deberían desarrollar, para involucrarse en el cambio de responsabilidades que esto implica (Ashenden, 2008; Ashenden y Ezingeard, 2005). Algunos de los estándares revisados, ofrecen una perspectiva sobre los roles supeditados a la GRCSI en las organizaciones (Figura 1), lo cual permitió identificar cual sería el personal que estaría involucrado o comprometido en la GRCSI.

La especificación de los roles de la GRCSI, posibilita abordar las actividades involucradas en este proceso. En este punto, los estándares revisados, proveen diferentes posturas sobre cómo llevarlas a cabo, por ello, se realizó una comparación, ubicando para cada estándar el listado de actividades en orden lógico y asociándolas mediante las similitudes y diferencias entre ellas, para finalmente obtener una propuesta de actividades resultado de su agrupación. La tabla 18, presenta el resultado del ejercicio anteriormente descrito. Como se puede ver en algunas casillas en la que se agrupan las actividades, aparecen diferentes nombres, esto para hacer ver que en ciertas ocasiones, aunque los estándares relacionan actividades con diferente nombre, tienen definiciones o propósitos similares. De igual manera, en la figura 19, aparece una imagen enriquecida que ilustra el resultado de la agrupación de las actividades para la GRCSI, permitiendo apreciar la secuencia e interacción entre ellas.

Figura 19. Roles identificados por los estándares respecto de la GRCSI

Roles	Perspectiva
•Administradores Funcionales y de Negocio •Departamento de Seguridad de la Información o Jefes de Información (CIO) o Jefes de Seguridad de Sistemas de Información (ISSO). o Profesionales de Seguridad de TI o Entrenadores de Seguridad / Profesionales en Materia de Seguridad •Operarios •Stakeholders •Propietarios de los Sistemas de Información	Toda la organización deberá estar comprometida e involucrada con los procesos de la GRCSI. La GRCSI es responsabilidad de la administración y del personal capacitado en el área de la seguridad de la información y la seguridad de los SI.

Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

Tabla 17. Cuadro Comparativo de las Actividades Relacionadas por los Estándares para la GRCSI

Estándar / **Actividad**	**ISO 27005**	**OCTAVE**	**ISM3**	**AS/NZS**	**SP800-30**	**SOMAP**	**MAGUERIT**	**MEHARI**	**SP800-39**
A1. Establecer el contexto. Medir y caracterizar el estado actual de la seguridad de los sistemas y la organización. Evaluar la Exposición Inherente.	X		X	X	X			X	X
A2. Identificar y valorar los activos críticos.		X					X		
A3. Identificar las amenazas y las vulnerabilidades de la organización.		X	X		X		X		
A4. Identificar los componentes claves y las vulnerabilidades técnicas que ocasionan los riesgos.		X		X	X				
A5. Evaluar el riesgo. Identificar el riesgo. Estimar el riesgo. Valorar el riesgo	X	X		X	X	X	X		X
A6. Determinar y evaluar el Impacto.							X	X	
A7. Evaluar la Gravedad del Escenario								X	
A8. Tratar el riesgo. Identificar las exigencias de seguridad y las normas existentes. Desarrollar estrategias de protección basadas en buenas prácticas. Implementar Protecciones.	X	X	X	X	X	X	X		X
A9. Aceptar el riesgo. Dar prioridad a la	X		X					X	X

Actividad \ Estándar	ISO 27005	OCTAVE	ISM3	AS/NZS	SP800-30	SOMAP	MAGUERIT	MEHARI	SP800-39
inversión de los procesos de seguridad.									
A10. Comunicar el riesgo.	X							X	
A11. Realizar seguimiento al riesgo. Establecer un plan de reducción de los riesgos. Monitorear y Revisar.	X	X	X	X	X	X	X	X	X
A12. Documentar Resultados					X				X

Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

4.3.1. Elaboración de una Imagen Enriquecida de los Procesos para la Gestión de Riesgos y Controles en los Sistemas de Información

La GRCSI se encuentra rodeada por un alto componente social, político y humano (Checkland, 2000a; Checkland y Scholes, 1999a; Checkland y Holwell, 1998), esto conlleva a que puedan existir perspectivas diferentes aunque a veces complementarias sobre cómo se deberían llevar a cabo estas actividades en una organización. Es en este punto, en el que el pensamiento de sistemas blandos (Checkland y Scholes, 1999b; Checkland y Poulter, 2006) se convierte en una de las metodologías más propicias para este tipo de estudios, en los cuales se debe trabajar con diferentes perspectivas de una misma situación, las cuales son examinadas y discutidas en torno a un proceso sistémico de aprendizaje (Checkland, 2000b), con el fin de definir acciones orientadas a su mejoramiento.

Los riesgos tienen un impacto potencial en el sistema de gestión de la seguridad (Fairley, 1994; Chittister y Haimes, 1993), por lo tanto, la GRCSI es una labor que requiere el esfuerzo y coordinación de los entes de la organización, en pro de la protección de los activos del negocio y del cumplimiento de la misión organizacional (McFadzean, et. al., 2001). No obstante, los modelos proveídos por los diferentes estándares sólo son guías o pautas y cada organización debe velar

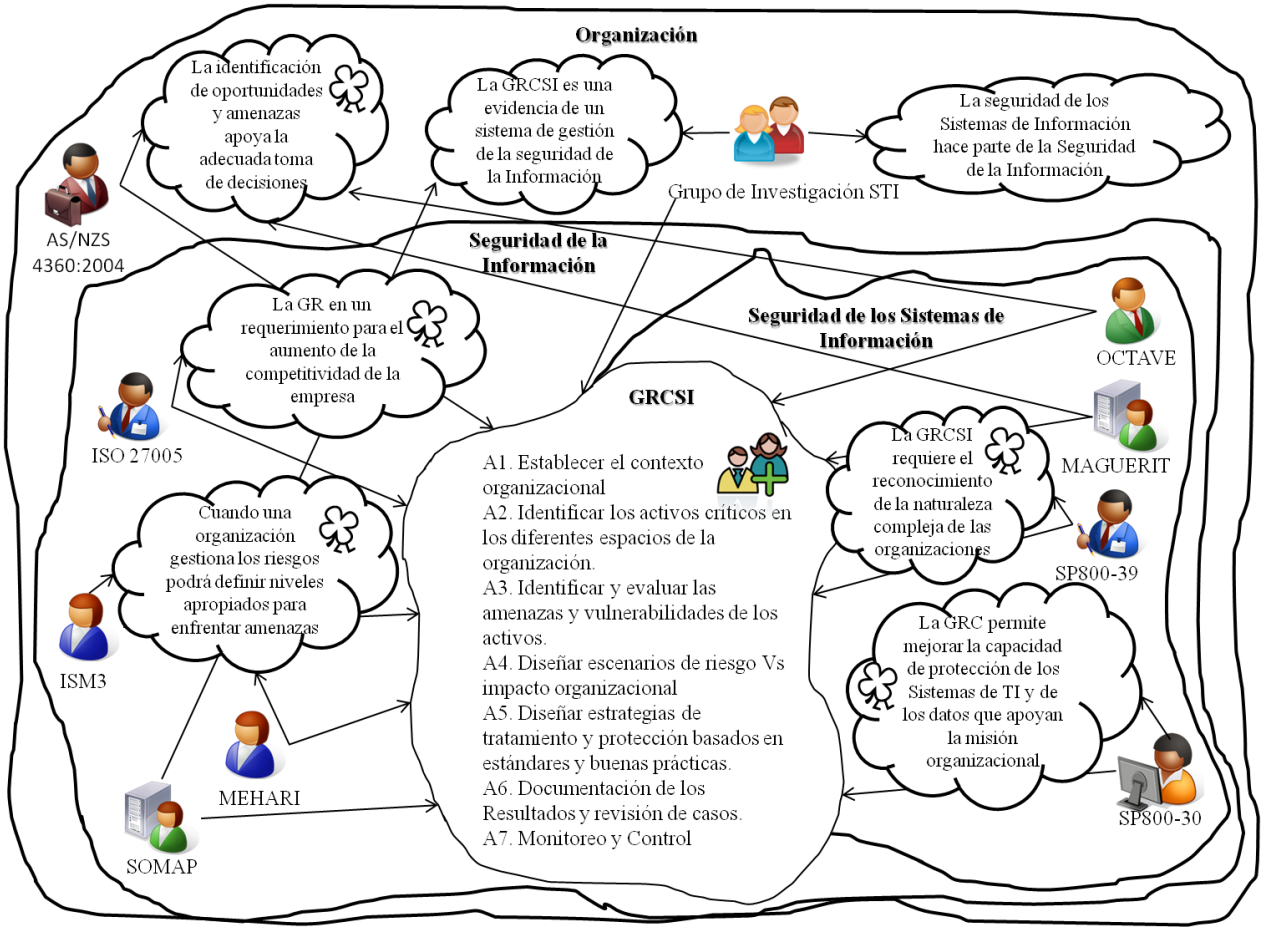
por reconocer en su naturaleza intrínseca y en su contexto las necesidades y requerimientos de gestión (Landoll, 2005).

De la comparación de los estándares revisados se logró evidenciar algunas actividades claves vinculadas en cada uno de ellos y en las cuales se pudo detectar que existían coincidencias. Lo anterior permitió crear la imagen enriquecida que se presenta en la figura 20, en la que se puede observar la perspectiva planteada por el grupo de investigación en Sistemas y Tecnologías de la Información -STI- y que es compartida por la mayoría de los estándares presentados, en especial por el estándar SOMAP. Bajo esta perspectiva se presenta a la GRCSI como parte del sistema de seguridad de los sistemas de información y como reflejo del sistema de gestión de riesgos a nivel organizacional. Esta idea es apoyada por los estándares AS/NZS, MAGUERIT y OCTAVE, en los cuales, la identificación de los niveles de riesgo en los Sistemas de Información, es un factor clave para el aumento de la competitividad de las organizaciones al apoyar la acertada toma de decisiones sobre la inversión en la protección de los activos.

Por su parte, estándares como ISO 27005 ayudan a considerar la GRCSI dentro del esquema de calidad organizacional, como un requerimiento para aumentar su competitividad.

Ahora bien, de acuerdo con la perspectiva planteada por los estándares SP800-39, SP800-30, MEHARI, e ISM3, el impacto generado por los riesgos es diferente dependiendo de los escenarios organizacionales en que se presenten, por tal motivo, las organizaciones deberán definir los niveles apropiados de riesgo teniendo en cuenta su naturaleza compleja para posteriormente asociarlos con los escenarios en los cuales se podrían presentar.

Figura 20. Pintura Enriquecida – Unificación de Criterios Estándares GRCSI



Fuente. Autor

Teniendo en cuenta las actividades comunes encontradas anteriormente en la revisión de los estándares y la imagen enriquecida elaborada, se plantea una posible consolidación de las actividades necesarias para la GRCSI, la cual se muestra en la tabla 18.

Tabla 18. Actividades Planteadas para la GRCSI

Actividad	Descripción
A1. Establecer el contexto organizacional.	Clarificar la Estrategia de la Organización en términos de los SI con el fin de especificar aquellos que apoyan los procesos de negocio. De igual manera se debe determinar la información sensible[9] y especificar los roles de los actores y sus responsabilidades en el uso de SI.
A2. Identificar los activos críticos en los diferentes espacios de la organización.	Catalogar los activos y la información sensible, con el fin de relacionarlos con los niveles de riesgo y con los criterios de la seguridad de los sistemas de información (la disponibilidad, autenticidad, integridad y confidencialidad).
A3.Identificar y evaluar las amenazas y vulnerabilidades[10] de los activos.	Detectar y evaluar las condiciones del entorno del SI que ante determinada circunstancia podrían dar lugar una violación de seguridad, afectando alguno de los activos de la compañía y a aquellos hechos o actividades que permitirían concretarlas.
A4. Diseñar escenarios de riesgo en términos de su impacto organizacional.	Diseñar escenarios en los cuales se posibilitaría la existencia de los riesgos. Esta actividad permite ponderar el impacto organizacional que cada uno de los escenarios tendría en los activos del negocio.

[9] Información sensible es aquella, así definida por su propietario, que debe ser especialmente protegida, pues su revelación, alteración, pérdida o destrucción puede producir daños importantes a alguien o algo (Ribagorda, 1997) (TCSEC, 1985). Algunos autores y normas como la RFC4949 de 2007, suelen denominarla información crítica, haciendo alusión a que es necesaria para el desarrollo y la evaluación del cumplimiento de los procesos de negocio.

[10] Los conceptos de Amenaza, Vulnerabilidad y Riesgo, en el sentido planteado por Silberfich (Silberfich, 2009), en donde se explica que la Amenaza es una condición del entorno del sistema de información, que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando alguno de los activos de la compañía. Por su parte, la Vulnerabilidad es un hecho o actividad que permite concretar una amenaza y el Riesgo es la posibilidad de que se produzca un impacto en la organización.

Actividad	Descripción
A5. Diseñar estrategias de tratamiento y protección basados en estándares y buenas prácticas.	Seleccionar alternativas de mitigación que mejoren la seguridad de la organización mediante la reducción del riesgo.
A6. Documentar los Resultados y revisar casos.	Realizar seguimiento y desarrollar un aprendizaje de los casos de estudio generados a partir de la documentación de los resultados de la gestión.
A7. Monitorear y Controlar.	Contrastar los resultados obtenidos con las especificaciones de mejoramiento con el fin de generar nuevas estrategias o nuevas definiciones de espacios de riesgo.

Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

Así como reconocer las actividades que hacen parte de la GRCSI, de acuerdo con los estándares es importante para que haya un proceso de cambio organizacional, también es imperativo que las organizaciones sean capaces de asimilar y asociar los niveles de riesgo con los eventos inseguros que se podrían presentar, de manera que se logre un alineamiento organizacional con las políticas de seguridad y que se logre un entendimiento de las implicaciones de los riesgos frente a los SI. A continuación se presenta una revisión sobre los niveles de riesgo en sistemas de información, el cual permitirá abordar el tema de la importancia de la GRCSI en el entorno organizacional.

4.3.2. Niveles de riesgo en SI y su identificación en la organización

Un nivel de riesgo es una clasificación en el plano organizacional y de sistemas de información, de los espacios en los que se pueden presentar determinados riesgos. En la literatura, Price – Waterhouse Cooper – PWC (Elissondo, 2008) define siete niveles de riesgo asociados a los sistemas de información y algunos controles utilizados para mitigarlos, los cuales, tal y como se muestra en diversos estudios (Castilla, et. al., 2004; CGRN, 1995) dan cuenta de aplicaciones y resultados plausibles en contextos reales. Los niveles definidos por PWC se presentan en la tabla 19.

Tabla 19. Niveles de Riesgo y Controles Definidos por PWC

Riesgo	Definición	Medios de Control
Acceso a funciones de procesamiento	Riesgo que se ocasiona cuando personas no autorizadas tienen acceso a las funciones de procesamiento de las transacciones de los programas de aplicación permitiéndoles leer, modificar, agregar o eliminar datos o ingresar transacciones no autorizadas para su procesamiento.	La segregación de funciones en el departamento de sistemas (organización de la estructura jerárquica de acceso al sistema de información), ani-keylogers y control de acceso, de manera que se creen políticas de seguridad informática en las que se determine la forma en que cada persona asociada al SI debe actuar y la funciones de procesamiento que se deberán proteger de ellos
Ingreso de datos	Riesgo que se ocasiona cuando los datos permanentes y de transacciones ingresados para el procesamiento puedan ser imprecisos, incompletos o ingresados más de una vez.	Controles de edición y validación (Formato, campos faltantes, límites, validación, procesamiento de duplicados, correlación de campos, balanceo, digito verificador), controles de lote y doble digitación de campos críticos.
Ítems rechazados o en suspenso	Riesgo que surge cuando falla la conexión con el servidor y las transacciones que deben ser rechazadas y/o quedan pendientes no son detectadas, analizadas y corregidas.	Controles programados, los cuales incluyen servidores espejo, bloqueo del cliente y bases de datos en la maquina cliente que permitan guardar la última transacción realizada para que posteriormente pueda ser actualizada, Controles de usuario Que permitan verificar anomalías en las transacciones realizadas por la maquina cliente.

Riesgo	Definición	Medios de Control
Procesamiento	Riesgo que se ocasiona cuando las transacciones a ser procesadas por el sistema de información se pierden o se procesan de forma incompleta o inexacta.	Formularios prenumerados, rutinas de control de secuencia, controles de balanceo, de lote, rótulos de archivos, transmisión de datos y procedimientos de enganche y recuperación.
Estructura organizativa del Dpto. de Sistemas	Riesgo que surge cuando la estructura organizacional y/o los procedimientos operativos del Departamento de Sistemas no garantizan un ambiente de Procesamiento que conduzca al manejo adecuado de la información.	Segregación de funciones en el departamento de Sistemas y controles y procedimientos operativos.
Cambios a los programas	Riesgo que se ocasiona cuando los programadores efectúan cambios incorrectos y/o no autorizados en el software de aplicación. De igual manera, se da cuando los cambios autorizados o el software nuevo no se documentan de manera adecuada.	Procedimientos de iniciación, aprobación y documentación, procedimientos de catalogación y mantenimiento, intervención de los usuarios, procedimientos de prueba y supervisión efectiva
Acceso general	Riesgo que surge cuando personas no autorizadas tiene acceso a los archivos de datos o a los programas de aplicación, permitiéndoles leer, modificar, agregar o eliminar algún ítem o segmento de programas.	Software de control de acceso, análisis de Logs e informes gerenciales, anti – keylogers, control de acceso físico y protección de datos.

Fuente. Elissondo (2004)

Los siete niveles de riesgo son el punto de partida de la propuesta de esta investigación, los cuales se enriquecieron a partir de la indagación realizada en los estándares de seguridad de la información y en los de seguridad de los Sistemas de información. Esto permitió la identificación, en el plano organizacional y de sistemas de información, de los espacios en los que se pueden presentar los niveles de riesgo.

En primera instancia se unificaron los riesgos “Acceso General” y “Acceso a Funciones de Procesamiento” y se denominarán “Acceso”, dado que ambos niveles de riesgo apuntan a que personas autorizadas o no, tienen acceso a la información o a las funciones de procesamiento de los Sistemas de Información, con el fin de leer, modificar o eliminar la información o los segmentos de programación o con el fin de ingresar transacciones no autorizadas para que sean procesadas por los SI. Como contribución a la definición planteada por PWC, se incorporó a esta concepción los ataques que se dan por Man in the Middle (Haig, 2009), los cuales son conocidos en Criptografía como ataques en los que el enemigo adquiere la capacidad de leer (Sniffing), insertar (Spoofing), denegar (negación de servicio) y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. De igual manera, tomando como referencia a ISM3 se incorpora a este nivel, el acceso indebido ocasionado por software malicioso y el registro incorrecto del acceso de usuarios por parte del Sistema de Información (es decir, errores en la bitácora del SI).

Por otro lado, enfoques sobre sistemas de información como los presentados por Laudon (2008) y McLeod (2000), permiten argumentar que hoy en día, los SI han pasado de un enfoque centrado en los datos a un enfoque centrado en la información y el conocimiento. De acuerdo con esto, los SI utilizan la información que es capturada por diversos medios para la ejecución de las transacciones y el apoyo a la toma de decisiones. Siguiendo este orden de ideas, es apropiado pretender que en la actualidad no se hable de un riesgo de “ingreso de datos” sino de un riesgo de “ingreso de información”.

En cuanto al nivel de riesgo de “procesamiento”, se reestructuró la definición con el fin de centrase en el riesgo que surge cuando los procesos de los SI no garantizan el adecuado procesamiento de la información, ocasionando que las salidas esperadas no sean correctas, la información se pierda y los procesos subsecuentes fallen o se retarden.

En el nivel de riesgo “Estructura Organizativa del Departamento de Sistemas”, se incorporaron los riesgos establecidos por ISM3, que surgen cuando no se actualizan los sistemas de información obsoletos y cuando no se tienen adecuados procedimientos para garantizar la continuidad del negocio, en caso de la destrucción de instalaciones y/o sistemas de información o del cambio o pérdida del personal clave. Por otro lado, teniendo en cuenta el despliegue y la incorporación de las Tecnologías de la Información y de las redes en los procesos de negocio en toda la organización, no tiene sentido pensar que este nivel de

riesgo se dé únicamente en el departamento de sistemas, ya que el riesgo de un inadecuado manejo de la información ocasionado por un inapropiado ambiente de procesamiento, podría presentarse en cualquier dependencia e involucrar a todo el personal de la organización encargado de desarrollar los procesos y de operar los SI. Por tal motivo, este nivel se denominará “Estructura Organizativa”.

Cada una de las definiciones de los niveles de riesgo proporcionadas por PWC se restructuraron teniendo en cuenta las descripciones sobre “riesgo” y “nivel de riesgo”, presentadas en este artículo, procurando que para cada nivel de riesgo la definición cuente con los siguientes elementos:

- Donde ocurre. Es la denominación de cada nivel de riesgo.
- Qué lo ocasiona. Cuáles son las causas que posibilitan la ocurrencia del riesgo.
- Impacto posible. Conjunto de posibles efectos sobre los activos de la organización.

De esta manera y a través de la identificación de los criterios de la seguridad de los SI afectados por cada nivel de riesgo y de los actores involucrados, se logra enriquecer la propuesta de PWC, llegando a las definiciones presentadas en la tabla 23 y al esquema mostrado en la figura 21.

Por otro lado, los controles proporcionados en el esquema de PWC, se ampliaron teniendo en cuenta los aportes proporcionados por MAGUERIT, obteniendo el resultado presentado en la tabla 20.

Como se puede observar en lo expuesto anteriormente, algunos de los estándares revisados soportan y ayudan a complementar los niveles de riesgo propuestos por PWC. No obstante, son relativamente pocos los que ofrecen una descripción guiada por niveles de riesgo, que contribuya a que las organizaciones reconozcan el impacto de los riesgos en sus procesos de negocio.

Tabla 20. Niveles de Riesgo – Propuesta de Enriquecimiento de las Definiciones

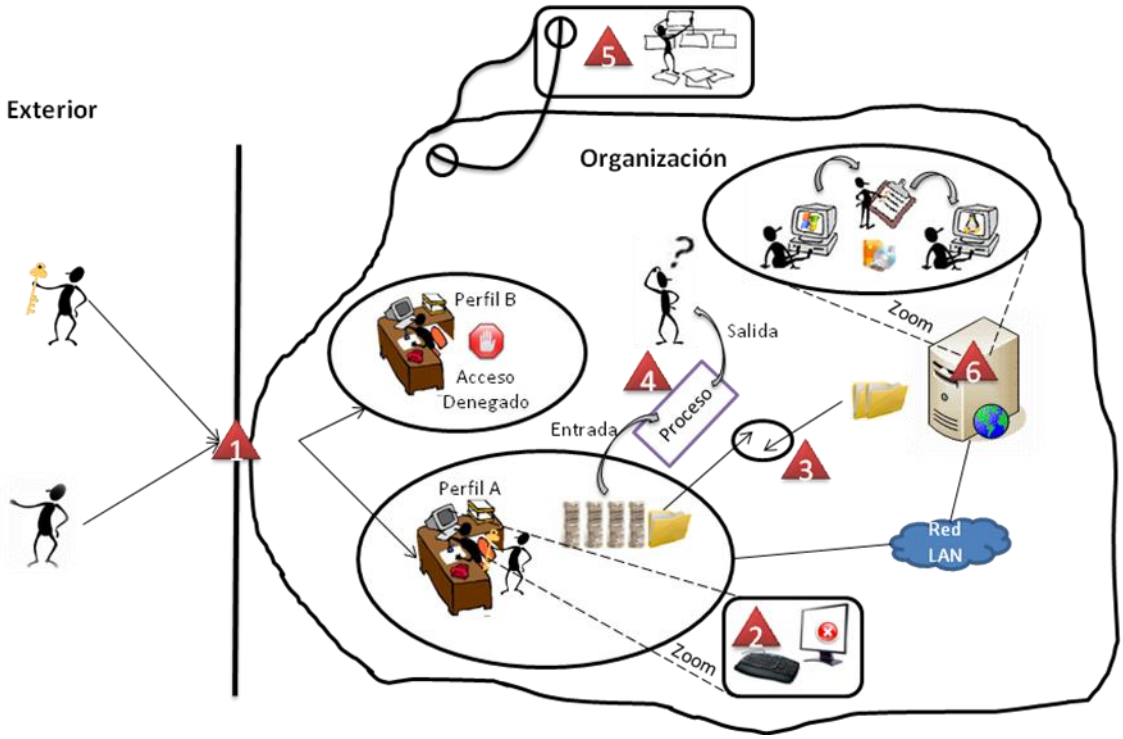
Nivel de Riesgo	Definición	Criterios de la Seguridad de los SI Afectados				Actores Involucrados
		1	2	3	4	
Acceso	Este nivel de riesgo surge cuando personas autorizadas o no, tienen acceso a la información o a las funciones de procesamiento de los Sistemas de Información, con el fin de leer, modificar o eliminar la información o los segmentos de programación o con el fin de ingresar transacciones no autorizadas para que sean procesadas por los SI.	X	X	X	X	Personal interno o externo de la organización y/o departamento de sistemas.
Ingreso de Información	Este nivel de riesgo surge cuando la información es ingresada a los SI de manera imprecisa, incompleta o más de una vez, ocasionando que las transacciones no puedan ser ejecutadas y/o que la información no sea correcta.		X	X		Personal de la organización, proveedores y clientes de ella, encargados de realizar las transacciones en los sistemas de información.
Ítems rechazados o en suspenso	Este nivel de riesgo surge cuando no se detectan, analizan y corrigen las transacciones rechazadas y/o pendientes, ocasionando que la información no se actualice correctamente o se pierda o que las transacciones no se	X		X		Clientes, Personal del departamento de Sistemas.

Nivel de Riesgo	Definición	Criterios de la Seguridad de los SI Afectados				Actores Involucrados
		1	2	3	4	
	ejecuten.					
Procesamiento	Este nivel de riesgo surge cuando los procesos de los SI no garantizan el adecuado procesamiento de la información, ocasionando que las salidas esperadas no sean correctas, la información se pierda y los procesos subsecuentes fallen o se retarden.	X		X		Clientes, Personal del departamento de Sistemas.
Estructura Organizativa	Este nivel de riesgo surge cuando la estructura organizativa no garantiza un adecuado ambiente para el procesamiento de la información y/o no define apropiados planes de continuidad del negocio, ocasionando que no existan procedimientos definidos y optimizados para el manejo de la información y de los SI, no se actualicen los SI y no se reaccione adecuadamente ante contingencias.	X	X	X	X	Personal de la organización encargado de desarrollar los procesos. Personal interno o externo encargado de la operación de los SI. Proveedores de servicios de TI.
Cambio a los Programas	Este nivel de riesgo surge cuando los programadores efectúan cambios	X	X	X	X	Personal adscrito al departamento

Nivel de Riesgo	Definición	Criterios de la Seguridad de los SI Afectados				Actores Involucrados
		1	2	3	4	
	incorrectos, no autorizados y/o no documentados en el software de aplicación, ocasionando perdida de información, repetición de esfuerzo, inconsistencias en los procesos e inconformidad en los clientes y usuarios.					de sistemas o de los proveedores de servicios de TI encargados del mantenimiento del software.

Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

Figura 21. Niveles de Riesgo en Sistemas de Información



Convenciones

▲1. Nivel de Riesgo Acceso. 2. Nivel de Riesgo de Ingreso de Información 3. Nivel de Riesgo Ítems Rechazados o en Suspenso. 4. Nivel de Riesgo

Procesamiento. 5. Nivel de Riesgo Estructura Organizativa. 6. Nivel de Riesgo Cambio a los Programas

Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

Tabla 21. Niveles de Riesgo y Controles

Nivel	Riesgo	Controles	Descripción
1	**Acceso**	Segregación de funciones en la organización	Separar o independizar las funciones de los usuarios de los sistemas de información, con el fin de evitar la incompatibilidad entre las mismas, los fraudes y los errores ocasionados por accesos autorizados o no autorizados.
		Anti-keylogger	Aplicación diseñada para evitar, detectar y/o eliminar programas tipo keylogger, es decir, aquellos que registran las pulsaciones que realiza un usuario sobre su teclado. Puede tratarse de una aplicación independiente o una herramienta dentro de otra, como puede ser un antivirus o

Nivel	Riesgo	Controles	Descripción
			un antiespía[11].
		Control de Acceso (Contraseñas encriptadas, Certificados Digitales, Dispositivos a Nivel de Tokens o Tarjetas, Lectores Biométricos, Alarmas, firma Electrónica, Dispositivos RFID [12], control de numero de intentos fallidos)	Control de acceso a los servicios, a las aplicaciones, al sistema operativo, a los soportes de información, a las instalaciones, etc.
		Registro de Actuaciones e incidentes	Registros a nivel de log´s que permitan determinar lo que los usuarios hacen en el sistema e informes gerenciales sobre la ocurrencia de fallas que afecten el buen funcionamiento del acceso de los usuarios a los sistemas de información.
		Administración de	Desactivación de

[11] Antiespía. Tipo de aplicación que se encarga de buscar, detectar y eliminar spywares en el sistema (Cualquier aplicación informática que recolecta información valiosa de la computadora desde donde está operando).

[12] Sigla en inglés que hace referencia a Radio Frequency Identification Devices (Dispositivos de identificación por radiofrecuencia).

Nivel	Riesgo	Controles	Descripción
		Cuentas	cuentas de usuarios inactivos y cambio periódico de claves de acceso.
		Desconexiones Automáticas	Desconexiones de sesión por tiempo sin actividad dentro del sistema.
		Asegurar los protocolos de transferencia	Reemplazar todos los protocolos inseguros por protocolos seguros (http por https, telnet por ssh (versión 2), pop3 por secure pop, etc.)
		Cifrado y Marcado de Información	El cifrado consiste en el envío codificado de la información que transita por la red (texto cifrado o criptograma), para prevenir su alteración o pérdida. Por su parte, el marcado consiste en la incorporación de etiquetas o marcas a la información de acuerdo con atributos definidos por el usuario (v. gr., reservada, confidencial, información personales, etc.) o con información adicional acerca de la estructura del texto enviado.
2	**Ingreso de**	Edición y Validación	Comprobación de tipo

Nivel	Riesgo	Controles	Descripción
	Información		de formato, campos faltantes, límites, validación, procesamiento de duplicados, correlación de campos, balanceo, digito verificador.
		Lote	Procesar la información por lotes de manera que se pueda comprobar que la información ingresada es correcta.
		Doble Digitación de Campos Críticos.	Incluir en el sistema dos veces la misma información. Se coloca a más de un digitador a introducir la información en el sistema en archivos diferentes y posteriormente se hace una comparación de los contenidos de los archivos (mediante un programa especial o el S.O).
		Lectores de Código de Barras y Lectores RFID	Los lectores de código de barras y los lectores RFID mejoran la exactitud en el ingreso de información a los SI, ya que envían la información capturada directamente a la computadora o terminal como si la información

Nivel	Riesgo	Controles	Descripción
			hubiera sido tecleada.
		Intervención efectiva de los operarios en el procesamiento automatizado de información con código de barras o RFID	Aunque los usuarios no conozcan la totalidad de los códigos, pueden estar en capacidad de discernir sobre fallas en la captura de la información de los tipos de producto, por ejemplo, si el código detectado es el de un tipo de leche pero el producto que se escaneó es mantequilla. De igual manera, si el código o tag (etiqueta electrónica) no es reconocido por los lectores, el usuario puede estar en capacidad de reportar estos errores.
		Mantenimiento preventivo de los escáneres de los lectores de Código de Barras y de los lectores de tags.	Procedimientos de diagnóstico sobre el estado de los lectores con el fin de impedir desgastes o daños en los aparatos que ocasionen lecturas inadecuadas.
3	**Ítems Rechazados o en Suspenso**	Controles programados	Son aquellos que se programan en las rutinas del sistema de información (v. gr., llamado a servidores

Nivel	Riesgo	Controles	Descripción
			espejo o llamado a bases de datos en la maquina cliente que permitan guardar la última transacción realizada para que posteriormente pueda ser actualizada).
		Interrupción de las Operaciones del Cliente	Bloqueo de la maquina cliente hasta que se restablezca la conexión.
		Controles de usuario	Verificación de anomalías en las transacciones realizadas por la maquina cliente.
4	**Procesamiento**	Formularios Prenumerados y Rutinas de Control de Secuencia	Asignar a los formularios del SI una numeración correlativa en original y copias, en forma simultánea a su procesamiento e impresión.
		Consistencia en la Recuperación de las transacciones.	Recuperación adecuada de las transacciones luego de interrupciones en el procesamiento.
		Protección Contra Software Malintencionado	Protección frente a código dañino: virus, troyanos, malware, puertas traseras, etc.
		Control de lote	Procesar la información por paquetes de manera que se pueda comprobar

Nivel	Riesgo	Controles	Descripción
			la adecuada salida de los procesos.
		Totalización de valores críticos	Comparar los totales de valores críticos antes y después del procesamiento.
		Rótulos de Archivos	Identificación del contenido de los archivos utilizando patrones de rotulación.
		Controles de Balanceo	Equilibrar y contrastar las variables correlacionadas y las actualizaciones del SI.
		Procedimientos de Enganche y Recuperación.	Mecanismos que al reiniciar la ejecución de un proceso interrumpido permitan continuar con el mismo sin repetir operaciones o sin dejar de procesar algunas. Lo mismo que mecanismos que permitan recuperar información que por la interrupción pueda quedar sin registro de su nuevo estado.
		Transmisión de Información	Cifrar la información que transita por la red, de manera que no se ocasionen fallas por modificaciones realizadas sin

Nivel	Riesgo	Controles	Descripción
			consentimiento.
5	Estructura Organizativa	Segregación de funciones	Separar o independizar las funciones de los usuarios de los sistemas de información, con el fin de evitar la incompatibilidad entre las mismas, los fraudes y los errores.
		Controles y Procedimientos Operativos.	Coordinar adecuadamente la responsabilidad en el manejo de la información. Establecer manuales de operación y controles operativos diarios. Supervisar a los usuarios privilegiados. Controlar el Software sensible. Controlar el desarrollo de sistemas. Generar políticas y planes de contingencia. Desarrollar procedimientos y lineamientos de seguridad. Definir la función de administración de seguridad y entrenar a los profesionales en seguridad.
		Planes de Continuidad	Diseñar planes de recuperación de los

Nivel	Riesgo	Controles	Descripción
			servicios prestados por los sistemas de información.
		Copias de Seguridad	Elaborar procedimientos para la realización periódica de backup´s y para su respectivo almacenamiento (gestión de servicios de custodia de información).
		Capacitar Usuarios	Capacitar al personal encargado de utilizar y realizar mantenimiento a los SI.
		Revisión de la Configuración	Procedimientos para las actualizaciones periódicas de la configuración de los sistemas de información.
		Procedimientos de Mantenimiento para los SI	Generar procedimientos para el mantenimiento preventivo y correctivo de los SI. Utilización de órdenes de trabajo para controlar los mantenimientos realizados.
6	**Cambio a los Programas**	Procedimientos de iniciación, aprobación y documentación.	Generar órdenes de trabajo al momento de realizar cambios a los sistemas de información, informando a los usuarios

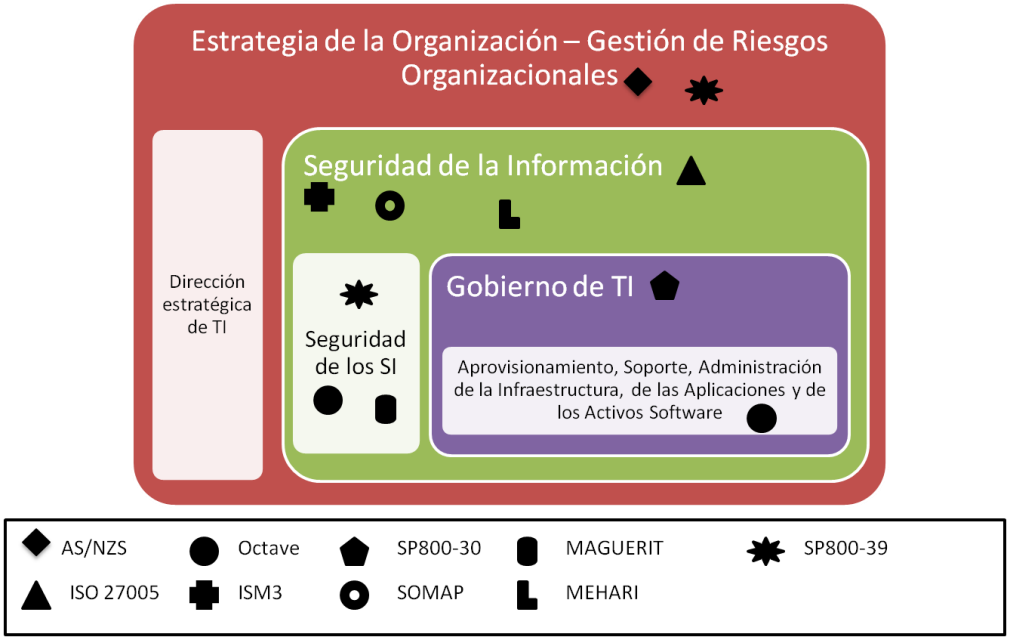
Nivel	Riesgo	Controles	Descripción
			correspondientes los cambios a realizar. En caso de que los cambios sean considerables se debe proceder nuevamente a capacitar a los usuarios.
		Procedimientos de Catalogación y Mantenimiento.	Establecer políticas para llevar a cabo los mantenimientos preventivos y correctivos de los SI y documentar los resultados obtenidos en los mismos.
		Intervención de los usuarios.	Catalogación de la información provista por los usuarios del SI respecto de fallas ocasionadas por las transacciones.
		Procedimientos de Prueba	Realizar a cabalidad las pruebas de subsistemas y las pruebas de integridad del SI cuando se consolidan los módulos.
		Supervisión Efectiva	Revisión periódica de las actividades desarrolladas por los programadores de software.

Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

Ahora bien, la comprensión sobre el propósito organizacional de los diferentes estándares en lo concerniente a los diferentes modelos de GRCSI, no se logra únicamente teniendo claridad sobre los niveles de riesgo, los roles y las actividades a desarrollar, también es necesario reconocer cuando se puede utilizar un determinado estándar según el propósito de gestión de riesgos requerido (Figura 22).

La escogencia de la aplicación de los estándares implica un reconocimiento de las necesidades propias de cada organización (García, 2008). En la tabla 22 se presenta una conclusión de la aplicación de los estándares revisados respecto de las necesidades de gestión de riesgos de la organización.

Figura 22. Alineamiento de los Estándares sobre GRCSI con las Actividades del Negocio



Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

Tabla 22. Selección de Estándares de Acuerdo con la Necesidad Organizacional

Propósito de Gestión de Riesgos	Estándar
Manejo del riesgo de los activos relacionados con la información	ISM3, SOMAP, MEHARI o ISO 27005
Aseguramiento de los activos relacionados con los sistemas de información (personas, maquinas, líneas de comunicación, etc.)	SP800-39, MAGUERIT u OCTAVE.
Gestión de los riesgos asociados con el gobierno de las tecnologías de la información, en lo referente al aprovisionamiento, soporte y administración de la infraestructura, de las aplicaciones y de los activos software	SP800-30 u OCTAVE.
Gestión de riesgos a nivel organizacional relacionados más con las estrategias de la organización que con las de la dirección de TI	AS/NZS o SP800-39

Tomada de Guerrero, Marlene y Gómez, Luis. (2010). Revisión de estándares relevantes y literatura de gestión de riesgos y controles en Sistemas de Información. Revista Estudios Gerenciales. En Revisión.

5. HACIA UNA COMPRENSIÓN DEL SISTEMA DE ACTIVIDAD HUMANA – SAH PARA LA GESTIÓN DE RIESGOS Y CONTROLES EN SI

En la revisión de la literatura, los estándares y la práctica sobre gestión de riesgos y controles en sistemas de información, se logró evidenciar los acuerdos y unificación de criterios no sólo a nivel conceptual respecto de lo que se considera es o no un riesgo, sino también a nivel de las actividades necesarias para llevar a cabo una adecuada gestión de los mismos y una eficiente definición de los controles que podrían mitigarlos.

Ese capítulo tiene como propósito describir las actividades que una organización deberá llevar a cabo para la gestión de riesgos y controles en sus sistemas de información, utilizando las definiciones raíz que se generen a partir de la comparación entre los acuerdos y desacuerdos descritos en el capítulo anterior.

5.1 Propuesta del SAH para la Gestión de Riesgos y Controles en los Sistemas de Información

El SAH que se presentará a continuación es producto de la revisión realizada a los distintos estándares sobre gestión de riesgos y controles en sistemas de información, lo cual permitió plantear un sistema pertinente para la GRCSI.

5.1.1. Definición Raíz

La siguiente definición raíz corresponde al sistema planteado para la GRCSI para la cual se enuncian sus elementos CATWOE.

La GRCSI es un sistema que hace parte del Sistema de Gestión de Seguridad de la Información de una organización, el cual es desarrollado por la dirección estratégica de tecnologías de información y de responsabilidad de todos los entes organizacionales mediante el alineamiento con los estándares de seguridad de SI que permitan el establecimiento del contexto organizacional, la identificación de los activos críticos en los diferentes espacios de la organización, la identificación y evaluación de las amenazas y vulnerabilidades de los activos, el diseño de escenarios de riesgo de acuerdo con su impacto organizacional, el diseño de estrategias de tratamiento y protección basados en estándares y buenas prácticas, la documentación de los resultados y revisión de casos y la implementación de procesos de monitoreo y control; con el fin de proteger la misión y los activos de la organización y apoyar a los administradores de Tecnologías de la Información a equilibrar los costos económicos y operacionales de las medidas de seguridad utilizadas para proteger los Sistemas de Información que apoyan los procesos de negocio de las organizaciones.

5.1.2. Elementos CATWOE

Como se había mencionado en el capítulo 2, con el fin de seleccionar una perspectiva particular y realizar un estructurado y riguroso proceso de desarrollo de los modelos se especificarán los elementos del CATWOE para la definición raíz planteada. El punto de partida es una Transformación (T) para la perspectiva seleccionada y a partir de allí se identifican los otros elementos claves del sistema para la GRCSI.

Tabla 23. CATWOE de la definición raíz para la GRCSI

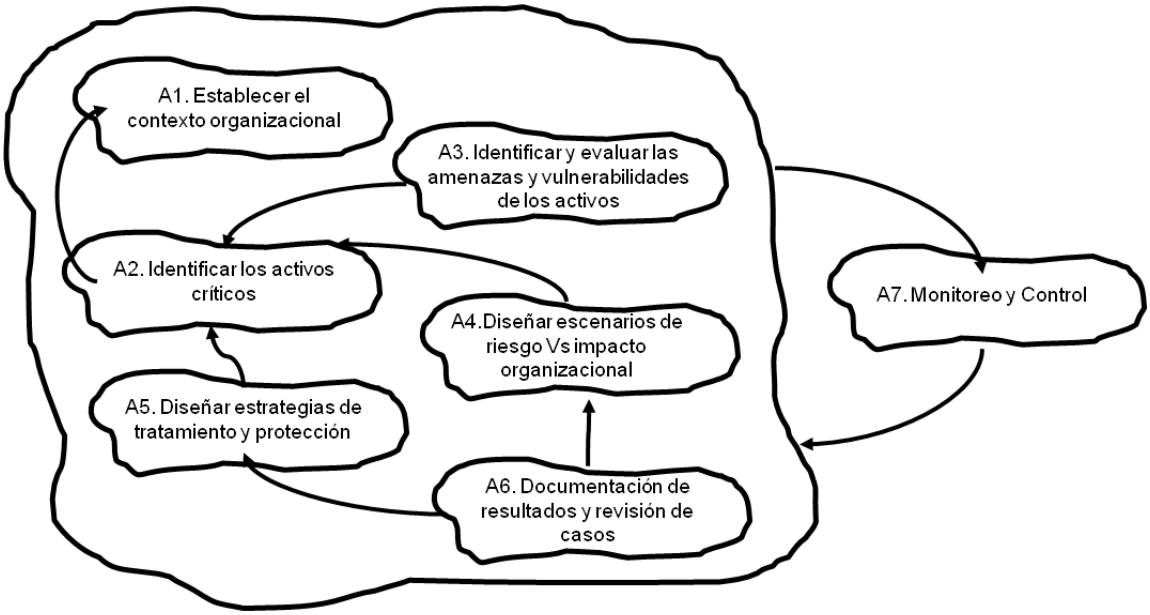
Sigla	Significado	Descripción
C	Clientes	Miembros y Clientes de la Organización
A	Actores	Dirección de Tecnologías de Información (TI)
T	Transformación	Dirección de TI con necesidades de definir la exposición a riesgos de los SI en su contexto organizacional→Contexto organizacional identificado y establecido. Organización con necesidad de identificar los activos expuestos a amenazas y el impacto organizacional ocasionadas por la vulnerabilidad de los SI → Organización con elementos de acción para identificar los activos expuestos a amenazas y con conocimiento de los niveles de riesgo de los SI. Entes organizacionales con necesidad de conocer su rol y responsabilidad dentro de la GRCSI →Roles y responsabilidades definidas. Organización con necesidades de aprendizaje sobre los casos de riesgo presentados históricamente en la organización →Organización son documentación de resultados sobre las estrategias de mitigación implantadas, monitoreo y control.
W	Punto de Vista	La GRCSI ayuda a proteger los activos de la organización y ayuda a los administradores de Tecnologías de la Información a equilibrar los costos administrativos y operacionales de las medidas de seguridad utilizadas para proteger los Sistemas de Información que apoyan los procesos de negocio de las organizaciones, mediante el alineamiento con los estándares de seguridad de SI.

O	Propietarios	Administración
E	Restricciones	Recursos, Estándares utilizados

5.1.3. Descripción de las Actividades Propuestas Para la Gestión de Riesgos y Controles en los Sistemas de Información

Teniendo en cuenta la definición raíz se planteó el sistema de actividades (Figura 23) que permita la transformación deseada. El SAH planteado para la GRCSI busca que la Dirección de TI sea capaz de definir los niveles de riesgo de los SI en su contexto organizacional propio y que la organización pueda identificar los activos relacionados con los SI que por su propia vulnerabilidad o por factores externos están expuestos a amenazas. De igual manera, se busca que los entes organizacionales conozcan su rol y responsabilidad dentro de la GRCSI y que aprendan de los casos de riesgo ocurridos en la organización para evitar la repetición de esfuerzos y el desgaste organizacional.

Figura 23. Sistema de Actividades de la Definición Raíz



Fuente. Autor

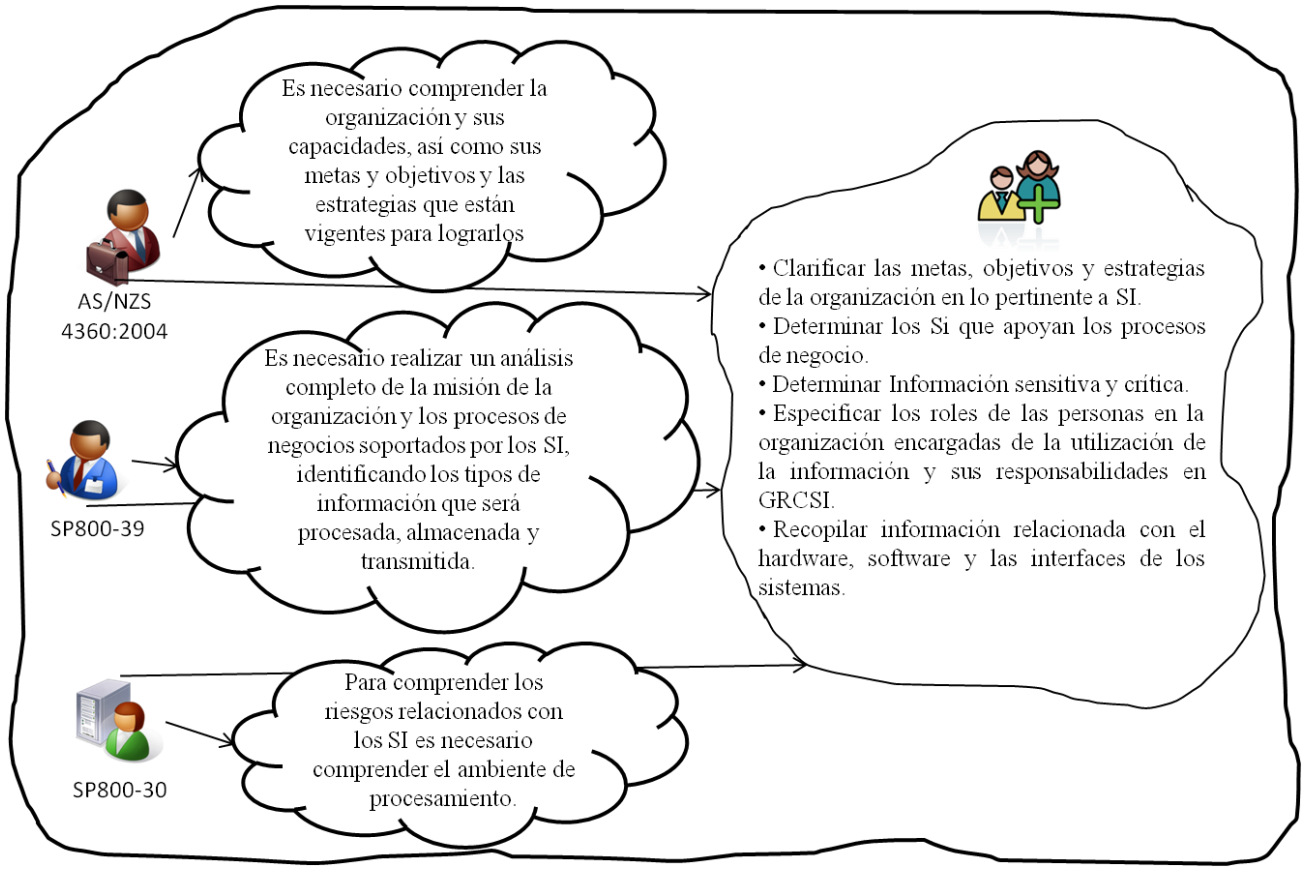
5.1.4. Actividad A1. Establecer el Contexto Organizacional

El establecimiento del contexto organizacional es la actividad primaria a desarrollar por parte de la empresa, dado que esto permite identificar los roles y sus responsabilidades frentes a la GRCSI. Como se ha expresado anteriormente, cada organización tiene una cultura particular, por lo cual la aplicación de esta actividad requiere de un repensar de la organización en términos de sus

necesidades, características, sistemas de información que apoyan los procesos de negocio, roles y responsabilidades de los actores de los sistemas de información y la caracterización de la información que es manejada por los Sistemas de Información.

El establecimiento del contexto organizacional es una actividad contemplada directamente en los modelos planteados por AS/NZS, SP800-30 y SP800-39, los cuales permitieron plantear comparaciones tendientes a detectar las unificaciones de criterio sobre las subactividades relacionadas con esta actividad y diseñar un diagrama de actividades en el que se describe el proceso a seguir para establecer el contexto organizacional en el modelo de GRCSI.

Figura 24. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 1.



Fuente. Autor.

Las actividades a desarrollar para el establecimiento del contexto organizacional y su alineamiento con los Sistemas de Información y los procesos de negocio, deberán ser responsabilidad inicialmente de los administradores de la

organización y del comité de seguridad encargado específicamente para esta labor.

Las subactividades pertinentes para la actividad 1 son:

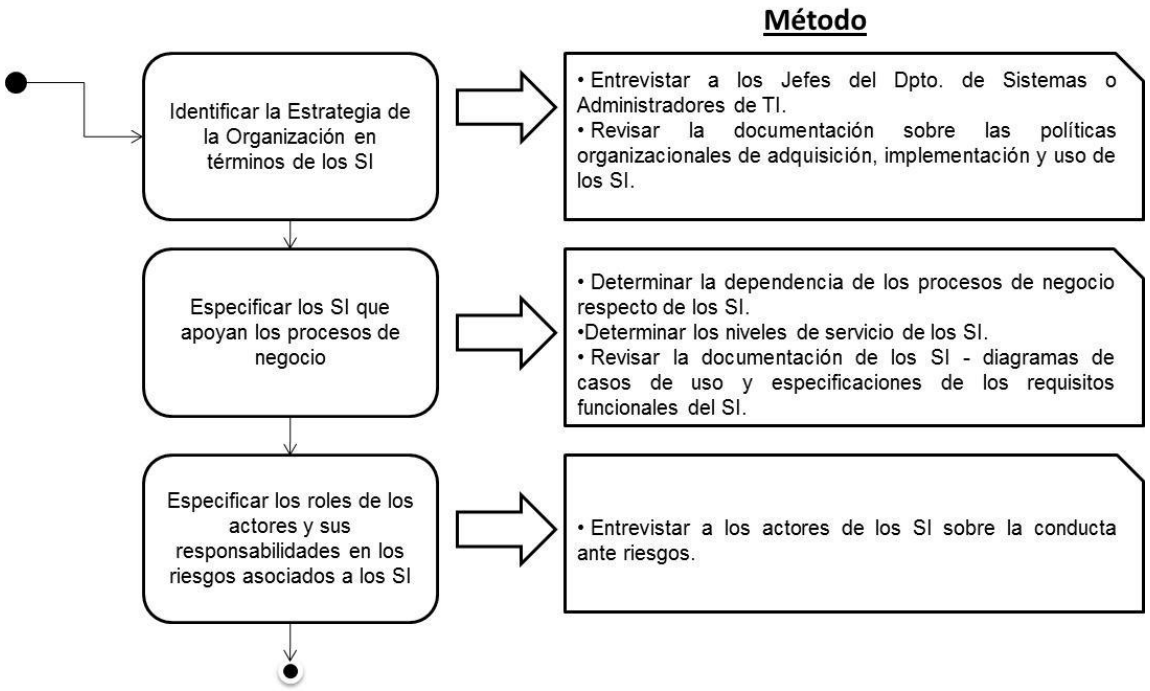
A.1.1. Identificar la Estrategia de la Organización en términos de los SI

A.1.2. Especificar los SI que apoyan los procesos de negocio

A.1.3. Especificar los roles de los actores y sus responsabilidades en la GRCSI

Los métodos propuestos para la consecución de las subactividades se presentan en la figura 25.

Figura 25. Métodos Sugeridos para la Actividad 1.



Fuente. Autor

Actividad A.1.1. Identificar la Estrategia de la Organización en Términos de los SI

Las organizaciones efectivas deben ser capaces de identificar las estrategias asociadas a los SI, las cuales deben estar enmarcadas dentro de la estrategia organizacional, de manera que los proyectos y las inversiones relacionadas con SI

sean especificadas a los distintos actores de la organización y sean administrados de manera adecuada.

Desde una perspectiva organizacional una manera de realizar esta actividad se describe a continuación.

- **Entrevistar a los Jefes del Departamento de Sistemas o Administradores de TI**. Esta actividad es desarrollada por los líderes de seguridad de la información en la organización. Uno de los métodos que se podrían utilizar para esta actividad son las listas de verificación con preguntas orientadas a descubrir los intereses y/o necesidades organizacionales en términos de la estrategia asociada a SI (Ver Anexo A – Lista de Verificación para Detectar el nivel estratégico organizacional en términos de SI).

- **Revisar la Documentación sobre las Políticas Organizacionales de Adquisición, Implementación y Uso de los SI**. Esta actividad es desarrollada por el grupo de trabajo encargado del gobierno de TI y SI con el fin de esclarecer si la organización tiene un nivel de madurez asociado con la adquisición, implementación y uso de los SI.

  Soportado en los niveles de madurez establecidos por COBIT (Control Objectives for Information and Related Technologies) (ISACA, 2007) y CMM (Capability Madurability Model) (Paulk, Weber, Curtis, & Chrissis, 2001), se propone el siguiente esquema de revisión de los niveles de madurez.

Tabla 24. Niveles de Madurez en la Adquisición, Implementación y Uso de los SI

Actividad / **Niveles**	**Adquisición e Implementación**	**Uso**
Nivel 0. No existente	La organización no contempla dentro de su estrategia organizacional el desarrollo de proyectos asociados con SI y TI.	La organización no utiliza SI para el apoyo a los procesos de negocio.

Actividad / Niveles	Adquisición e Implementación	Uso
Nivel 1. Inicial	La organización apoya el desarrollo de proyectos de adquisición e implementación de SI pero no tiene control o claridad sobre los mismos y no necesariamente se llevan a cabo.	La organización utiliza SI pero no realiza revisiones de la utilización de los mismos por parte de los actores.
Nivel 2. Definido	La organización lleva cabo proyectos de SI y TI asociados con la estrategia organizacional.	La organización define estrategias de revisión de la utilización de los SI y ha establecido los roles y responsabilidades de cada actor.
Nivel 3. Cuantificado	La organización administra la inversión de los desarrollos de proyectos de SI y TI a través de indicadores de gestión.	La organización utiliza indicadores para medir la utilización de los SI por parte de los actores.
Nivel 4. Optimizado	La organización genera estrategias de aprendizaje sobre los proyectos ejecutados y mide los resultados obtenidos en términos de su estrategia organizacional.	La organización genera estrategias para garantizar el adecuado uso de los SI.

Fuente. Autor

Actividad A.1.2. Especificar los SI que Apoyan los Procesos de Negocio.

Actualmente muchas organizaciones soportan sus procesos de negocio con SI. Por lo tanto, un reconocimiento del contexto organizacional implica especificar los SI que apoyan los procesos de negocio, de manera que se clarifique la dependencia de la ejecución de los procesos con respecto a la disponibilidad de los SI. Esta actividad es desarrollada por el grupo de trabajo encargado del gobierno de TI.

Desde una perspectiva organizacional una manera de realizar esta actividad se describe a continuación.

- **Determinar la Dependencia de los Procesos de Negocio Respecto de los SI.** Dentro de las organizaciones no todos los procesos de negocio están soportados por SI y en otros casos aunque así lo estén, la dependencia de la continuidad del servicio de los mismos no es demasiado alta. Por lo tanto, una organización efectiva debe medir que tanto depende la disponibilidad de sus procesos de negocio de los SI. A continuación se presenta una posible jerarquización de esta dependencia.

  ISM3 plantea un esquema de dependencia de los procesos de negocio respecto de los SI, el cual será utilizado como punto de partida para la propuesta que se presenta a continuación.

Tabla 25. Criterios de Dependencia de los Procesos de Negocio Respecto de los SI

Criterio de Dependencia	Descripción
No Existente	La organización tiene alternativas diferentes al uso de los SI para el desarrollo de sus procesos de negocio, por lo cual no hay una dependencia en tiempo real de la continuidad del servicio.
Parcial	La organización tiene alternativas diferentes al uso de los SI para el desarrollo de sus procesos de negocio pero tiene una dependencia en tiempo real para la continuidad del servicio.
Relativo	La organización no tiene alternativas diferentes al uso de los SI para el desarrollo de sus procesos de negocio, pero no tiene una dependencia en tiempo real para la continuidad del servicio.
Absoluto	La organización no tiene alternativas diferentes al uso de los SI para el desarrollo de sus procesos de negocio y además pero tiene una dependencia en tiempo real para la continuidad del servicio.

Fuete. Autor.

- **Determinar los Niveles de Servicio de los SI.** Esta actividad está orientada a establecer los servicios prestados por el sistema de información

a los diferentes actores, los cuales podrán clasificarse en niveles de acuerdo con su relevancia. Los niveles de servicio podrían clasificarse de acuerdo con las siguientes especificaciones.

Tabla 26. Niveles de Servicio de los SI

Nivel de Servicio	Discriminación
Alto	Servicios relacionados con la función principal del SI. Corresponde a los casos de uso más relevantes del SI
Medio	Servicios relacionados con la administración y auditoria del SI
Bajo	Demás servicios prestados por el SI

Fuente. Autor

- **Revisar la Documentación de los SI.** La revisión de los manuales de usuario, administración, configuración e instalación del SI, es de vital importancia para el establecimiento de los riesgos asociados con los cambios realizados a los programas.

  De igual manera, la revisión de los diagramas de casos de uso del sistema implantado y de las especificaciones de los requisitos realizadas por la organización, permitirá detectar el grado de cumplimiento de los requisitos contractuales del SI.

Tabla 27. Grado de Cumplimientos de los SI con la Implantación

Grado de Cumplimiento	Discriminación
Alto	Los requisitos establecidos en el contrato están contemplados en los casos de uso del SI implantado.
Medio	Los casos de uso relevantes del SI han sido contemplados en los casos de uso del SI implantado.
Bajo	La implantación del SI no se corresponde con la especificación de requisitos del cliente.

Fuente. Autor

Actividad A.1.3. Especificar los Roles de los Actores y sus Responsabilidades en los Riesgos Asociados a los SI

Los actores de los SI cumplen con un rol de acuerdo con sus necesidades y los servicios prestados por el SI. De acuerdo con esto, surgen responsabilidades en términos de la información que manejan. Esta actividad debe ser desarrollada por los jefes de información (CIO) en concordancia con los administradores funcionales y de negocio.

Desde una perspectiva organizacional una manera de realizar esta actividad se describe a continuación.

- **Entrevista a los Actores de los SI sobre la Conducta Ante Riesgos.** Determinar la cultura de riesgo de los actores relacionados con los SI, permite detectar y generar estrategias de mitigación de los riesgos ocasionados a dolo o por negligencia (desconocimiento, falta de apropiación) de los actores. Uno de los métodos que se podrían utilizar para esta actividad son las listas de verificación con preguntas orientadas a descubrir la conducta organizacional de los actores de SI ante riesgos (Ver Anexo B – Lista de Verificación para Descubrir la Cultura Ante Riesgos de los Actores de SI).

5.1.5. Actividad A2. Identificar los Activos Críticos

Los activos críticos relacionados con los Sistemas de Información son: la Información, los Servicios, las Aplicaciones Informáticas, los Equipos Informáticos, los Soportes de Información, el Equipamiento Auxiliar, las Redes de Comunicaciones, las Instalaciones y las Personas. Esta actividad busca determinar la información sensible y crítica con el fin de identificar la información que puede estar expuesta a determinado nivel de riesgo dentro de los definidos en el numeral 4.3.1.

La identificación de los activos críticos es una actividad contemplada por los modelos planteados por OCTAVE y MAGERIT, los cuales permitieron plantear comparaciones tendientes a detectar las unificaciones de criterio sobre las subactividades relacionadas con esta actividad y diseñar un diagrama de actividades en el que se describe el proceso a seguir para identificar los activos críticos en el modelo de GRCSI.

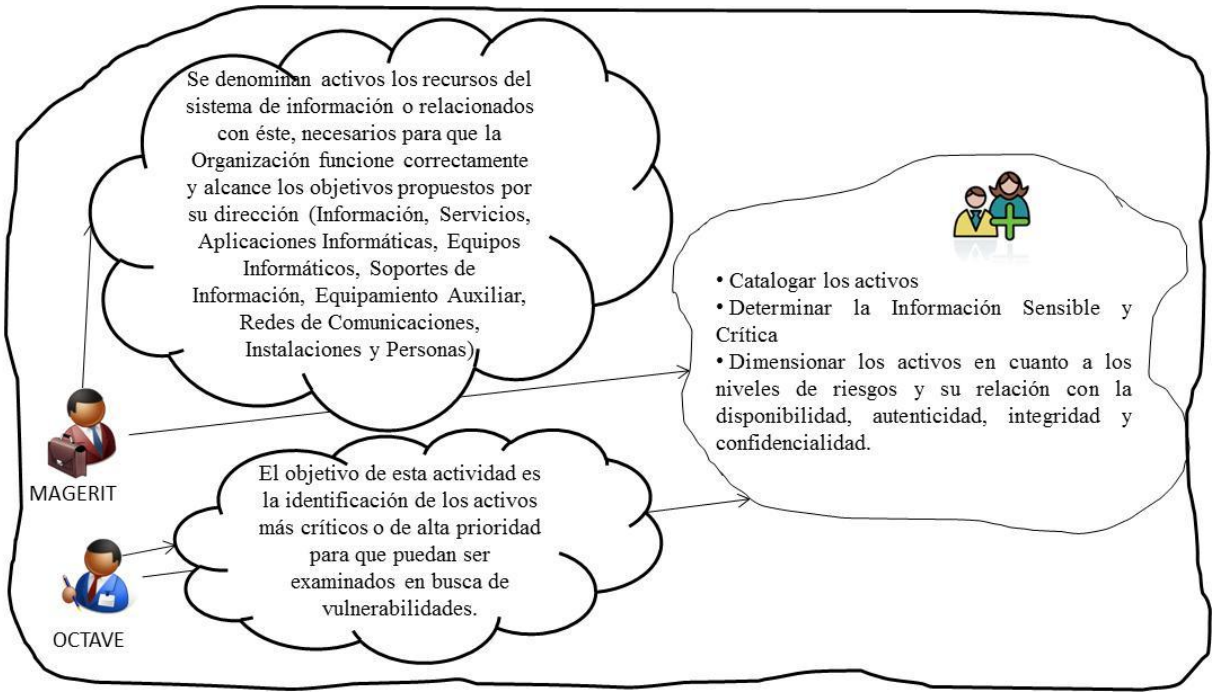
Las actividades pertinentes para la identificación de los activos críticos que se describen a continuación deberán ser responsabilidad inicialmente de la dirección de tecnologías de la información.

A.2.1. Catalogar los Activos Relacionados con los SI

A.2.2. Determinar la Información Sensible y Crítica

A.2.3. Dimensionar los activos en cuanto a los niveles de riesgos y su relación con la disponibilidad, autenticidad, integridad y confidencialidad.

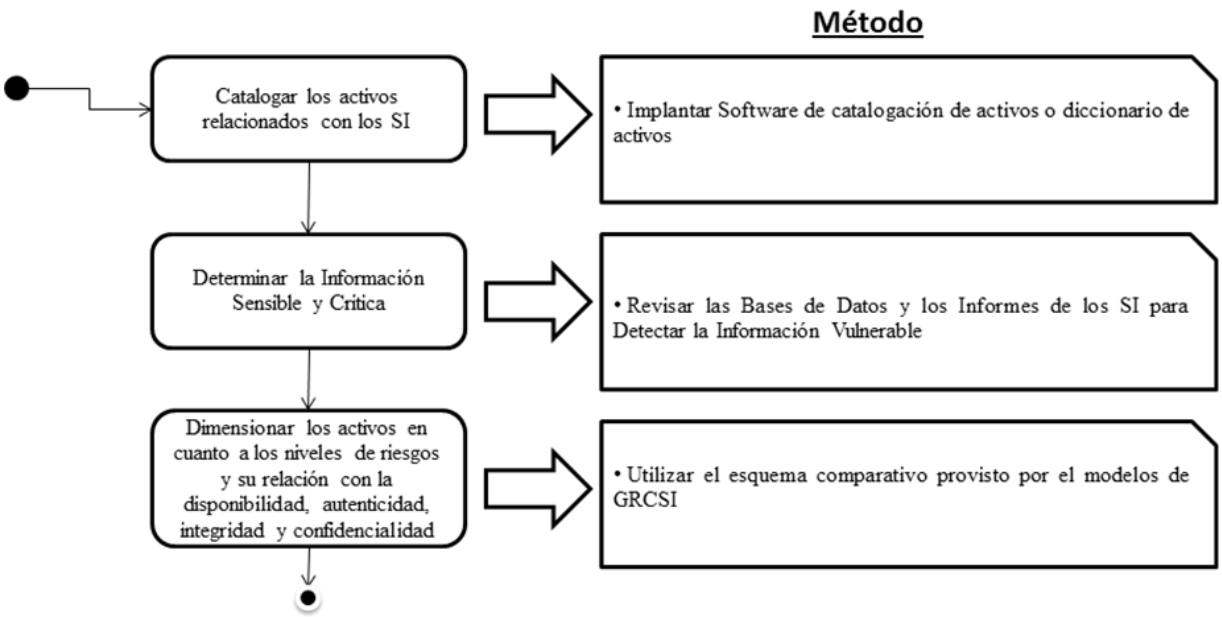
Figura 26. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 2.



Fuente. Autor

Los métodos propuestos para la consecución de las subactividades se presentan en la figura 27.

Figura 27. Métodos Sugeridos para la Actividad A2



Fuente. Autor

Actividad A.2.1. Catalogar los Activos Relacionados con los SI

Ofrecer información a la organización sobre los recursos asociados a los SI es de suma importancia para la toma de decisiones acertadas sobre las políticas y estrategias de control relacionadas con las vulnerabilidades de los mismos. Esta actividad debe ser desarrollada por los jefes de seguridad de sistemas de información (ISSO).

Para el desarrollo de esta actividad se puede Uno de los métodos que se puede desarrollar un software de catalogación de activos que permita gestionar y controlar los recursos asociados a los SI o se puede llevar un consolidado de catalogación de activos manual, el cual podría ser como el que se muestra en el anexo C.

Actividad A.2.2. Determinar la Información Sensible y Crítica

Clarificar que información es sensible y crítica permite a las organizaciones generar estrategias para protegerla de ser divulgada, modificada o perdida. Esta actividad es responsabilidad de los CIO. Una manera de realizar esta actividad se describe a continuación.

- **Revisar las Bases de Datos y los Informes de los SI para Detectar la Información Vulnerable.** El contraste entre la Base de Datos del SI y los

niveles de servicio del mismo, permitirán la identificación de la información que es susceptible de ser resguardada o que hay que proteger de los riesgos relacionados son la seguridad de la información. La figura 28 muestra un esquema guía para dicho contraste.

Figura 28. Esquema para el contraste entre los niveles de servicio, la BD y la información sensible y crítica.

Nivel de Servicio Detectado	Tablas de la BD que los Soportan	Información Relevante y Crítica

Fuente. Autor

Actividad A.2.3. Dimensionar los activos en cuanto a los niveles de riesgos y su relación con la disponibilidad, autenticidad, integridad y confidencialidad

Esta actividad le corresponde al grupo de trabajo de seguridad de TI y SI e implica el reconocimiento de los activos que pueden estar expuestos a determinados niveles de riesgo. De igual manera, en esta actividad se deben tener en cuenta los criterios de seguridad que podrían verse afectados. La tabla 28 muestra cómo se pueden relacionar estos tres factores (Activos, Niveles de Riesgo, Criterios de Seguridad).

Tabla 28. Relación entre los Niveles de Riesgos, los Activos y los Criterios de Seguridad.

Nivel de Riesgo	Activos en Riesgo	Relación con los Criterios de Seguridad
Acceso	Información	Confidencialidad
Ingreso de Información	Información	Autenticidad, Integridad
Ítems Rechazados o en Suspenso	Información Servicios	Disponibilidad, Autenticidad
Procesamiento	Servicios	Integridad

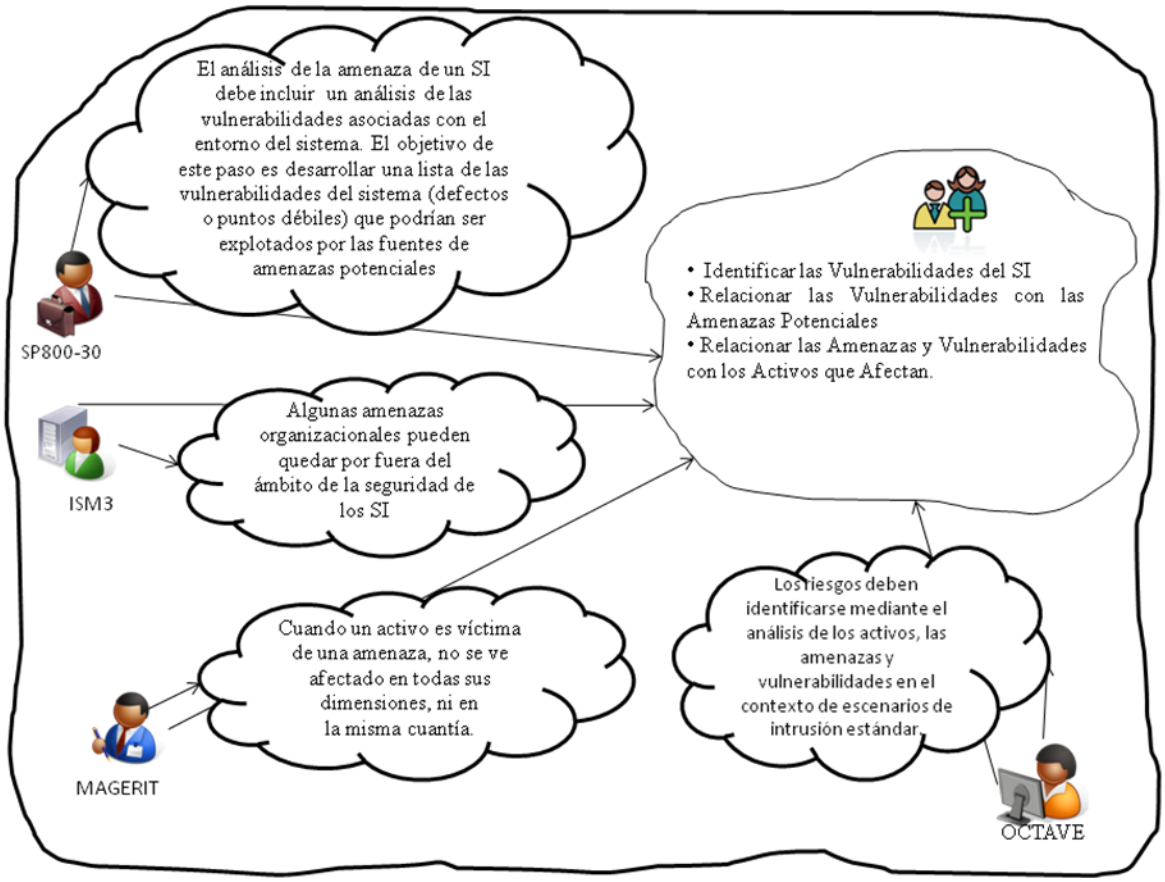
Nivel de Riesgo	Activos en Riesgo	Relación con los Criterios de Seguridad
Estructura Organizativa	Personas Instalaciones Aplicaciones Informáticas Equipos Informáticos Redes de Comunicaciones Equipamiento Auxiliar Soportes de Información	Disponibilidad, Integridad. Autenticidad, Confidencialidad
Cambio a los Programas	Aplicaciones Informáticas Soportes de Información	Integridad, Disponibilidad

Fuente. Autor

5.1.6. Actividad A3. Identificar y Evaluar las Amenazas y Vulnerabilidades de los Activos Críticos

Detectar y evaluar las condiciones del entorno del sistema de información que ante determinada circunstancia podrían dar lugar a que se produjese una violación de seguridad, afectando alguno de los activos de la compañía y los hechos o actividades que permitirían concretarlas, es uno de los aspectos más importantes en materia de GRCSI. Esta actividad está contemplada en los modelos inmersos en OCTAVE, ISM3, SP800-30 y MAGUERIT, los cuales permitieron plantear comparaciones tendientes a detectar las unificaciones de criterio sobre las subactividades relacionadas con esta actividad y diseñar un diagrama de actividades en el que se describe el proceso a seguir para identificar los activos críticos en el modelo de GRCSI.

Figura 29. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 3.



Fuente. Autor

Las actividades a desarrollar para la detección y evaluación de vulnerabilidades y amenazas deberán ser responsabilidad inicialmente de la dirección de tecnologías de la información.

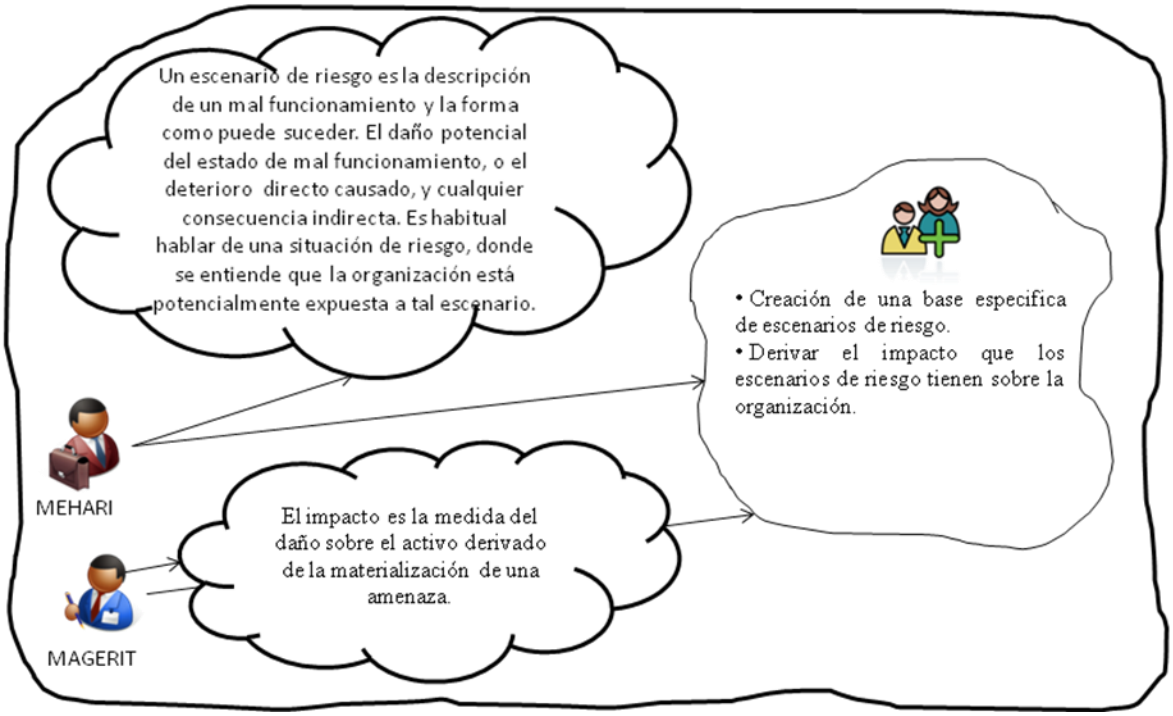
Aunque las vulnerabilidades y amenazas de los activos relacionados con los SI tienen que ver en primera instancia con la propia naturaleza del SI. El anexo D provee un esquema de relación entre las amenazas y vulnerabilidades y como estos están relacionados con los activos de los SI. Las amenazas han sido catalogadas utilizando el catalogo V11 de MAGERIT (MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2006).

5.1.7. Actividad A4. Diseñar Escenarios de Riesgos con Respecto a su Impacto Organizacional

Un escenario de riesgo es la descripción hipotética de un mal funcionamiento del SI. La evaluación del potencial impacto de un escenario de riesgo, provee a la organización las herramientas necesarias para la medición y la actuación.

Aunque cada SI por su naturaleza intrínseca estará expuesto a escenarios de riesgo específico, estándares como MEHARI proveen una lista de 170 escenarios clasificados en 12 familias, los cuales podrían ser utilizados como guía. Por otro lado, MAGERIT, presenta algunas consideraciones a tener en cuenta al momento de definir los escenarios de riesgo tales como: la identificación de las causas que originan el escenario, la especificación de las consecuencias directas e indirectas de la ocurrencia del escenario y la medición de la probabilidad de ocurrencia. Ambos estándares permitieron elaborar la pintura rica con las actividades requeridas para la actividad A4 (ver figura 30).

Figura 30. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 4.



Fuente. Autor.

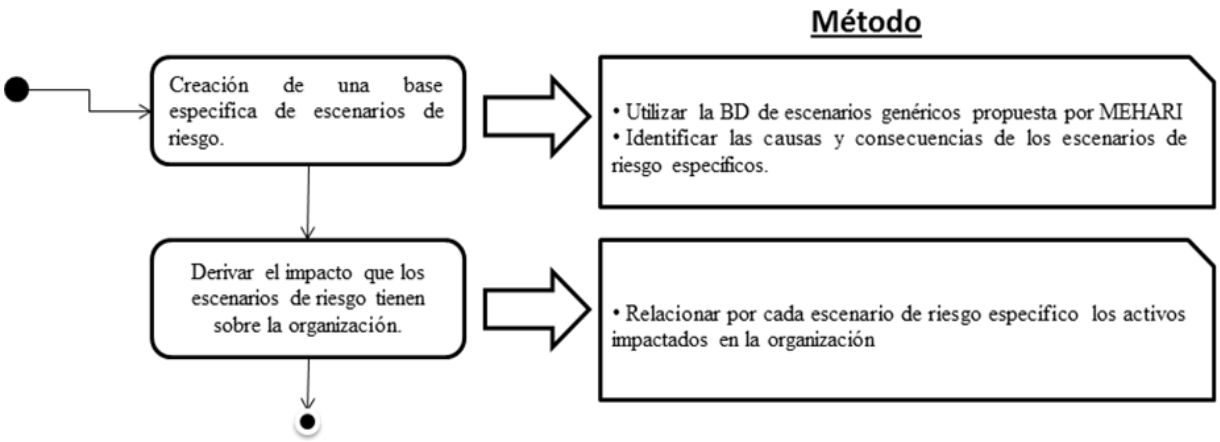
Las actividades propuestas para llevar a cabo la actividad A4 son:

A.4.1. Creación de una base especifica de escenarios de riesgo.

A.4.2. Derivar el impacto que los escenarios de riesgo tienen sobre la organización.

Algunos métodos sugeridos para llevar a cabo las subactividades se describen en la figura 31.

Figura 31. Métodos Sugeridos para la Actividad A4



Fuente. Autor.

Actividad A.4.1. Creación de una base especifica de escenarios de riesgo.

A partir de la referencia elaborada en la base de escenarios MEHARI, se identifican los escenarios específicos, teniendo en cuenta los siguientes criterios:

- El tipo de consecuencia.
- Los tipos de causas que pueden dar lugar a la situación de riesgo.
- La probabilidad de que se ocasione el escenario.

Muchos factores pueden originar la ocurrencia de un escenario de riesgo y es precisamente esto los que deriva en la probabilidad de que se este se concrete. MEHARI provee la escala de probabilidad de ocurrencia que se muestra continuación.

- Nivel 4 – Muy Probable. La probabilidad de ocurrencia del riesgo es alta y se puede producir en un tiempo relativamente corto. Cuando ocurre el riesgo no sorprende a nadie.

- Nivel 3 – Es probable. Estos son los escenarios que fácilmente podrían ocurrir, en un plazo más o menos corto. La esperanza de que el riesgo ocurra no es alta, pero sin duda muestra un cierto grado de optimismo. Cuando el escenario ocurre, las personas se decepcionan, pero nadie se sorprende.

- Nivel 2 – Es poco probable. Estos son los escenarios que, razonablemente, no se consideran que sucederán. La experiencia demuestra que nunca se han producido. Sin embargo, pueden ser "posibles".

- Nivel 1 – Muy poco probable. La ocurrencia del riesgo es totalmente improbable. Estas situaciones no son estrictamente imposibles, pues siempre hay una posibilidad infinitamente pequeña de que ocurran.

- Nivel 0 – No se considera. Estos son los escenarios que son tan imposibles que no están incluidos en el conjunto de escenarios para ser analizados. A menudo, y por diferentes razones, los escenarios que no se van a analizar se clasifican en este nivel.

Como estrategia de organización de la información sobre los escenarios específicos detectados se propone la tabla 29.

Tabla 29. Esquema propuesto para la organización de la información sobre los escenarios de riesgo.

Descripción del escenario de Riesgos:	
Causa que Originan el Escenario	**Consecuencias Directas e Indirectas del Escenario**
Probabilidad de Ocurrencia:	

Fuente. Basado en MEHARI, 2010.

Actividad A.4.2. Derivar el impacto que los escenarios de riesgo tienen sobre la organización.

Las consecuencias directas e indirectas de los escenarios de riesgo, permiten determinar el impacto sobre los activos de la organización. Se denomina entonces "impacto" a la medida del daño derivado de la materialización de un riesgo. La tabla 30 muestra un esquema que podría ser utilizado para organizar la información sobre los escenarios y su impacto sobre los activos organizacionales.

Tabla 30. Organización de la Información sobre los Impactos Generados por los Escenarios de Riesgo

Descripción del escenario de Riesgos:	
Activo Impactado*	**Criterio de Seguridad****

*Los relacionados en el anexo C

**Disponibilidad: ¿Qué importancia tendría que el activo no estuviese disponible cuando se requiera?

Autenticidad: ¿Qué importancia tendría que quien accede al activo no fuese quien se cree?

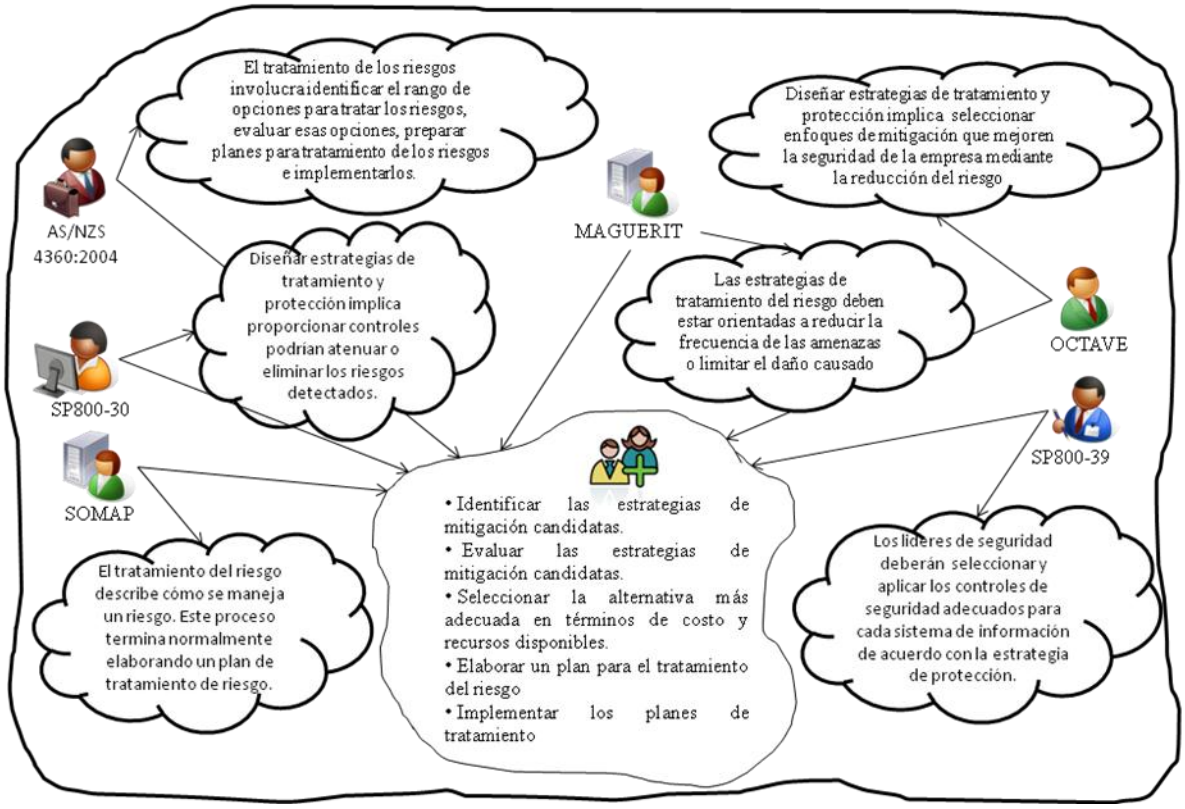
Integridad: ¿Qué importancia tendría que el activo fuese modificado indebidamente?

Confidencialidad: ¿Qué importancia tendría que el activo fuese conocido por personas no autorizadas?

5.1.8. Actividad A5. Diseñar Estrategias de Tratamiento y Protección

Una de las actividades más representativas en la GRCSI es diseñar las estrategias de tratamiento y mitigación de los riesgos encontrados. Esta actividad implica seleccionar estrategias que mejoren la seguridad de la empresa mediante la reducción del riesgo. Actualmente, estándares como ISO 27005, OCTAVE, ISM3, AS/NZS 4360:2004, SP800-30, SOMAP, MAGUERIT y SP800-39 proveen información sobre el propósito de esta actividad, lo cual permitió elaborar la pintura enriquecida que se muestra en la figura 32.

Figura 32. Pintura Enriquecida – Unificación de Criterios sobre la Actividad 5



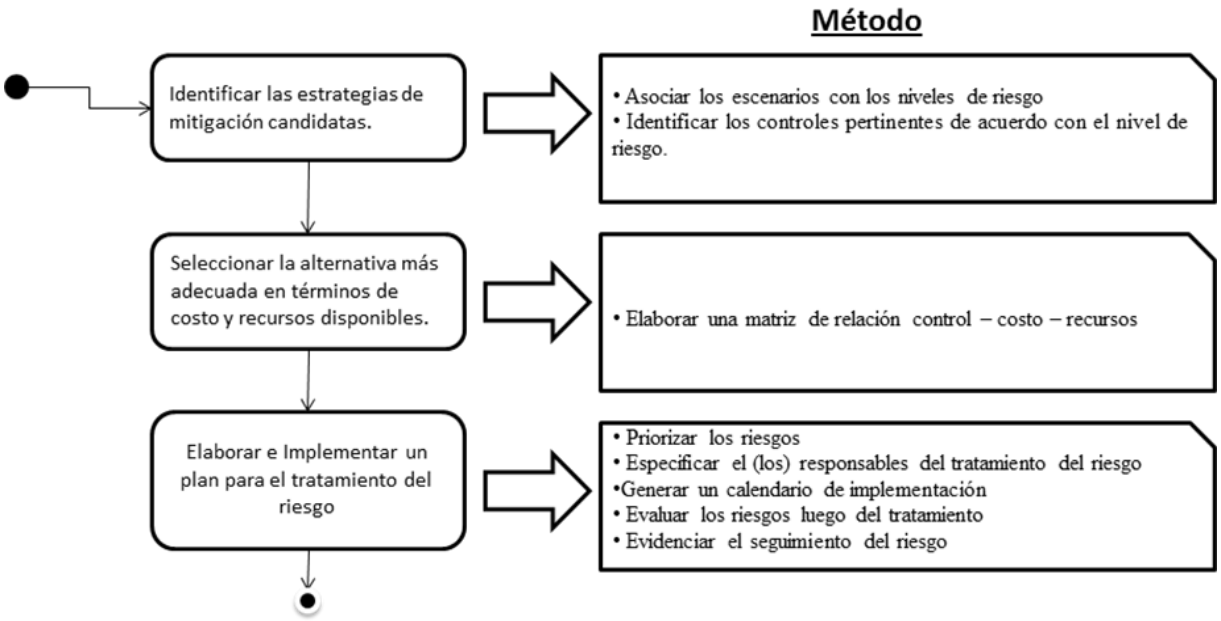
Fuente. Autor

Las actividades propuestas para llevar a cabo la actividad A5 son:

A.5.1. Identificar las estrategias de mitigación candidatas.
A.5.2. Seleccionar la alternativa más adecuada en términos de costo y recursos disponibles.
A.5.3. Elaborar e Implementar un plan para el tratamiento del riesgo

Algunos métodos sugeridos para llevar a cabo las subactividades se describen en la figura 33.

Figura 33. Métodos para Llevar a Cabo la Actividad A5



Fuente. Autor

Actividad A.5.1. Identificar las estrategias de mitigación candidatas.

Basándose en el levantamiento de los escenarios de riesgo realizado en el ítem 5.1.7, se procede a asociar cada escenario de riesgo con los niveles definidos en el ítem 4.3.1. Posteriormente se procede a identificar de acuerdo con la tabla 31, el tipo de estrategia de mitigación (control) más adecuado para su tratamiento.

Tabla 31. Niveles de Riesgo y Controles Propuestos

Nivel	Riesgo	Controles	Descripción
1	**Acceso**	Segregación de funciones en la organización	Separar o independizar las funciones de los usuarios de los sistemas de información, con el fin de evitar la incompatibilidad entre las mismas, los fraudes y los errores ocasionados por accesos autorizados o

Nivel	Riesgo	Controles	Descripción
			no autorizados.
		Anti-keylogger	Aplicación diseñada para evitar, detectar y/o eliminar programas tipo keylogger, es decir, aquellos que registran las pulsaciones que realiza un usuario sobre su teclado. Puede tratarse de una aplicación independiente o una herramienta dentro de otra, como puede ser un antivirus o un antiespía[13].
		Control de Acceso (Contraseñas encriptadas, Certificados Digitales, Dispositivos a Nivel de Tokens o Tarjetas, Lectores Biométricos, Alarmas, firma Electrónica, Dispositivos RFID [14], control de numero de intentos	Control de acceso a los servicios, a las aplicaciones, al sistema operativo, a los soportes de información, a las instalaciones, etc.

[13] Antiespía. Tipo de aplicación que se encarga de buscar, detectar y eliminar spywares en el sistema (Cualquier aplicación informática que recolecta información valiosa de la computadora desde donde está operando).

[14] Sigla en inglés que hace referencia a Radio Frequency Identification Devices (Dispositivos de identificación por radiofrecuencia).

Nivel	Riesgo	Controles	Descripción
		fallidos)	
		Registro de Actuaciones e incidentes	Registros a nivel de log´s que permitan determinar lo que los usuarios hacen en el sistema e informes gerenciales sobre la ocurrencia de fallas que afecten el buen funcionamiento del acceso de los usuarios a los sistemas de información.
		Administración de Cuentas	Desactivación de cuentas de usuarios inactivos y cambio periódico de claves de acceso.
		Desconexiones Automáticas	Desconexiones de sesión por tiempo sin actividad dentro del sistema.
		Asegurar los protocolos de transferencia	Reemplazar todos los protocolos inseguros por protocolos seguros (http por https, telnet por ssh (versión 2), pop3 por secure pop, etc.)
		Cifrado y Marcado de Información	El cifrado consiste en el envío codificado de la información que transita por la red (texto cifrado o criptograma), para prevenir su alteración o

Nivel	Riesgo	Controles	Descripción
			pérdida. Por su parte, el marcado consiste en la incorporación de etiquetas o marcas a la información de acuerdo con atributos definidos por el usuario (v. gr., reservada, confidencial, información personales, etc.) o con información adicional acerca de la estructura del texto enviado.
2	**Ingreso de Información**	Edición y Validación	Comprobación de tipo de formato, campos faltantes, límites, validación, procesamiento de duplicados, correlación de campos, balanceo, digito verificador.
		Lote	Procesar la información por lotes de manera que se pueda comprobar que la información ingresada es correcta.
		Doble Digitación de Campos Críticos.	Incluir en el sistema dos veces la misma información. Se coloca a más de un digitador a introducir la información en el sistema en archivos diferentes y posteriormente se hace una comparación de los

Nivel	Riesgo	Controles	Descripción
			contenidos de los archivos (mediante un programa especial o el sistema operativo).
		Lectores de Código de Barras y Lectores RFID	Los lectores de código de barras y los lectores RFID mejoran la exactitud en el ingreso de información a los SI, ya que envían la información capturada directamente a la computadora o terminal como si la información hubiera sido tecleada.
		Intervención efectiva de los operarios en el procesamiento automatizado de información con código de barras o RFID	Aunque los usuarios no conozcan la totalidad de los códigos, pueden estar en capacidad de discernir sobre fallas en la captura de la información de los tipos de producto, por ejemplo, si el código detectado es el de un tipo de leche pero el producto que se escaneó es mantequilla. De igual manera, si el código o tag (etiqueta electrónica) no es reconocido por los lectores, el usuario puede estar en capacidad de reportar

Nivel	Riesgo	Controles	Descripción
			estos errores.
		Mantenimiento preventivo de los escáneres de los lectores de Código de Barras y de los lectores de tags.	Procedimientos de diagnóstico sobre el estado de los lectores con el fin de impedir desgastes o daños en los aparatos que ocasionen lecturas inadecuadas.
3	**Ítems Rechazados o en Suspenso**	Controles programados	Son aquellos que se programan en las rutinas del sistema de información (v. gr., llamado a servidores espejo o llamado a bases de datos en la maquina cliente que permitan guardar la última transacción realizada para que posteriormente pueda ser actualizada).
		Interrupción de las Operaciones del Cliente	Bloqueo de la maquina cliente hasta que se restablezca la conexión.
		Controles de usuario	Verificación de anomalías en las transacciones realizadas por la maquina cliente.
4	**Procesamiento**	Formularios Prenumerados y Rutinas de Control de Secuencia	Asignar a los formularios del SI una numeración correlativa en original y copias, en forma simultánea a su

Nivel	Riesgo	Controles	Descripción
			procesamiento e impresión.
		Consistencia en la Recuperación de las transacciones.	Recuperación adecuada de las transacciones luego de interrupciones en el procesamiento.
		Protección Contra Software Malintencionado	Protección frente a código dañino: virus, troyanos, malware, puertas traseras, etc.
		Control de lote	Procesar la información por paquetes de manera que se pueda comprobar la adecuada salida de los procesos.
		Totalización de valores críticos	Comparar los totales de valores críticos antes y después del procesamiento.
		Rótulos de Archivos	Identificación del contenido de los archivos utilizando patrones de rotulación.
		Controles de Balanceo	Equilibrar y contrastar las variables correlacionadas y las actualizaciones del SI.
		Procedimientos de Enganche y Recuperación.	Mecanismos que al reiniciar la ejecución de un proceso interrumpido permitan continuar con el mismo sin repetir

Nivel	Riesgo	Controles	Descripción
			operaciones o sin dejar de procesar algunas. Lo mismo que mecanismos que permitan recuperar información que por la interrupción pueda quedar sin registro de su nuevo estado.
		Transmisión de Información	Cifrar la información que transita por la red, de manera que no se ocasionen fallas por modificaciones realizadas sin consentimiento.
5	**Estructura Organizativa**	Segregación de funciones	Separar o independizar las funciones de los usuarios de los sistemas de información, con el fin de evitar la incompatibilidad entre las mismas, los fraudes y los errores.
		Controles y Procedimientos Operativos.	Coordinar adecuadamente la responsabilidad en el manejo de la información. Establecer manuales de operación y controles operativos diarios. Supervisar a los usuarios privilegiados. Controlar el Software sensible. Controlar el

Nivel	Riesgo	Controles	Descripción
			desarrollo de sistemas. Generar políticas y planes de contingencia. Desarrollar procedimientos y lineamientos de seguridad. Definir la función de administración de seguridad y entrenar a los profesionales en seguridad.
		Planes de Continuidad	Diseñar planes de recuperación de los servicios prestados por los sistemas de información.
		Copias de Seguridad	Elaborar procedimientos para la realización periódica de backup´s y para su respectivo almacenamiento (gestión de servicios de custodia de información).
		Capacitar Usuarios	Capacitar al personal encargado de utilizar y realizar mantenimiento a los SI.
		Revisión de la Configuración	Procedimientos para las actualizaciones periódicas de la configuración de los sistemas de información.

Nivel	Riesgo	Controles	Descripción
		Procedimientos de Mantenimiento para los SI	Generar procedimientos para el mantenimiento preventivo y correctivo de los SI. Utilización de órdenes de trabajo para controlar los mantenimientos realizados.
6	**Cambio a los Programas**	Procedimientos de iniciación, aprobación y documentación.	Generar órdenes de trabajo al momento de realizar cambios a los sistemas de información, informando a los usuarios correspondientes los cambios a realizar. En caso de que los cambios sean considerables se debe proceder nuevamente a capacitar a los usuarios.
		Procedimientos de Catalogación y Mantenimiento.	Establecer políticas para llevar a cabo los mantenimientos preventivos y correctivos de los SI y documentar los resultados obtenidos en los mismos.
		Intervención de los usuarios.	Catalogación de la información provista por los usuarios del SI respecto de fallas ocasionadas por las transacciones.

Nivel	Riesgo	Controles	Descripción
		Procedimientos de Prueba	Realizar a cabalidad las pruebas de subsistemas y las pruebas de integridad del SI cuando se consolidan los módulos.
		Supervisión Efectiva	Revisión periódica de las actividades desarrolladas por los programadores de software.

Fuente. Autor

Actividad A.5.2. Seleccionar la alternativa más adecuada en términos de costo y recursos disponibles.

Una vez que se ha determinado cual es el nivel de riesgo al que está expuesto el sistema de información, los líderes de seguridad deben seleccionar la alternativa más conveniente para la organización en términos no sólo de la relación costo-beneficio, sino también en términos de los recursos que se encuentran disponibles para su implantación. Para realizar esta actividad, se podría realizar una matriz para comparar las alternativas propuestas como la que se muestra en la tabla 32.

Tabla 32. Matriz de comparación de los controles a seleccionar

		Recursos		
		No disponible	Adquirible	Disponible
Costo	Alto	Control 1	Control 2	Control 5
	Medio	Control 4	Control 6	Control 9
	Bajo	Control 3	Control 8	Control 7

Fuente. Autor

A.5.3. Elaborar e Implementar un plan para el tratamiento del riesgo

Desarrollar y establecer un plan, permite llevar a cabo de manera ordenada las decisiones tomadas y planeadas para el tratamiento del riesgo. El estándar AS/NZS propone el esquema que se muestra en la figura 35 para elaborar un plan de tratamiento de riesgos.

Figura 34. Esquema de Elaboración de un Plan de Tratamiento de riesgo Según AS/NZS

Programa y plan de tratamiento de riesgos

Fecha de revisión de riesgo.....
Compilado por.....Fecha.....
Función/actividad..... Revisado por.....Fecha.....

El riesgo en orden de prioridad del Registro de Riesgo	Opciones posibles de tratamiento	Opciones preferidas	Puntaje de Riesgo luego del tratamiento	Resultado del análisis de costo/beneficio A: acepta B: rechaza	Persona responsable por implementación de la opción	Calendario de implementación	Cómo será monitoreado este riesgo y las opciones de tratamiento

Tomado de AS/NZS, 2004

5.1.9. Actividad A6. Documentación de Resultados y Revisión de Casos

La documentación de los resultados es una actividad que permitirá a las organizaciones realimentar sus resultados y aprender sobre las situaciones de riesgo presentadas a partir de la revisión de los casos históricos más representativos y sus respectivas estrategias de tratamiento. En la tabla 33 se provee un esquema para la documentación de casos.

Tabla 33. Esquema para la Documentación de Casos

Caso Presentado	Frecuencia de Ocurrencia	Mecanismo (s) de Mitigación	Resultados

Fuente. Autor

5.1.10. Actividad A7. Monitoreo y Control

El monitoreo y el control, ayuda a evaluar si las estrategias de mitigación de los riesgos implantadas lograron cumplir con el alcance propuesto. Un programa

continuo de monitoreo bien diseñado y bien administrado puede transformar efectivamente una evaluación estática de los controles de seguridad y de los procesos de determinación del riesgo, en un proceso dinámico, que proporciona información esencial del estado de la seguridad, en el momento necesario para que los administradores puedan tomar decisiones acertadas. El monitoreo y control proporciona a las organizaciones herramientas eficaces para producir cambios en torno a los planes de seguridad, a los informes de evaluación de la seguridad y a los planes de acción.

5.2 Estudio de Caso CPE – UIS Sistema EscuelaCol 1.0

A través de la realización del proyecto de pregrado "Herramienta Software Open Source Orientada a Apoyar los Procesos de Evaluación y Promoción en la Educación Básica Primaria Escuelacol 2.0" se aplicó el modelo de gestión de riesgos y controles en sistemas de información propuesto en esta investigación al sistema EscuelaCol 1.0. Lo anterior, permitió observar la puesta en marcha del modelo en un Sistema de Información real, con el fin de proporcionar acciones con propósito que permitan el mejoramiento y redefinición del mismo.

La aplicación del modelo que se mostrará a continuación fue trabajada en colaboración con los desarrolladores del proyecto EscuelaCol 2.0[15].

5.2.1. A1 Establecer el contexto organizacional.

- **A1.1. Clarificar la Estrategia de la Organización en términos de los SI.**

El *"Prototipo de Herramienta Software para Apoyar los Procesos de Evaluación y Promoción en Instituciones Educativas - EscuelaCol 1.0*" (Ramírez & Téllez, 2008); desarrollado en la Universidad Industrial de Santander en el grupo STI busca apoyar los procesos de registro y control de la información académica, concerniente a la evaluación y promoción de los estudiantes en las escuelas de educación básica primaria.

EscuelaCol pretendía llegar a las instituciones de bajos recursos, para facilitar sus procesos de evaluación y promoción de alumnos bajo la premisa de que cada institución posee una reglamentación y unas costumbres diferentes y que es la herramienta la que debe ser adaptable a la situación de cada institución con sus características especiales y únicas; permitiendo complementar las actividades que

[15] Díaz, M.; Naranjo, M. Herramienta Software Open Source Orientada a Apoyar los Procesos de Evaluación y Promoción en la Educación Básica Primaria Escuelacol 2.0. UIS. 2010.

se realizan en dichos establecimientos; asimismo permite administrar la información de la mejor manera posible para ser utilizada en cualquier momento apoyando la toma decisiones.

Al no ser una herramienta desarrollada para un cliente específico, las fases de análisis, diseño y desarrollo se basaron en la legislación colombiana decreto 230 del 2002 y ley 115 de 1994 del Ministerio de Educación Nacional (MEN), además de consultas informales a miembros de entidades educativas públicas y privadas de la ciudad de Bucaramanga.

Debido a que EscuelaCol 1.0 no se instaló en la institución educativa, para el estudio de la actividad A.1.1 se realizaron pruebas de campo a través de la utilización de la base de datos escuelacol-datos-ejemplo.sql que contiene información real de prueba. De igual manera, con el fin de conocer las capacidades de la herramienta, se intentó utilizar una base de datos vacía, para iniciar el proceso desde cero (datos de estudiantes, datos de profesores, cursos, logros e indicadores de logros, etc.), es decir iniciar un año escolar nuevo; no obstante al momento de realizar la prueba se presentaron inconvenientes con la base de datos proporcionada por los autores del proyecto, evidenciándose fallas e inconsistencias imposibilitando la instalación de la misma.

- **A.1.2. Especificar los SI que apoyan los procesos de negocio.**

EscuelaCol 1.0 apoya las siguientes actividades administrativas y académicas:

- Matrícula Académica.
- Registro de Notas. (Evaluación).
- Promoción de Estudiantes.
- Información Académica y Personal de los Estudiantes.
- Generación de Actas y Reportes.
- Manejo Documental y de Archivo.

El apoyo a estas actividades de índole administrativo y académico, proporcionado por EscuelaCol 1.0, permite manejar la información eficientemente, apoyando a docentes y administrativos, mejorando los procesos y logrando un aprovechamiento de los recursos informáticos eficientemente. Este prototipo ayuda a reducir los problemas existentes en cada una de la instituciones tales como pérdida de información, falta de seguridad y resguardo de información. A

continuación se describe cada uno de los requerimientos funcionales de la herramienta de acuerdo a los niveles de servicio que presta el SI EscuelaCol 1.0.

Tabla 34. Niveles de servicio EscuelaCol 1.0

Nivel de Servicio	Discriminación
Alto	**Matrícula** ➢ Pre-inscripción de alumnos: La aplicación cuenta con un proceso de pre-matrícula en el que se pueden inscribir los alumnos admitidos o promovidos. ➢ Acceso a Datos: la herramienta cuenta con una ventana principal en la que se puede acceder rápidamente a los datos personales del alumno ya que estos pueden ser requeridos con cierta urgencia y frecuencia en el desempeño de las actividades. ➢ Actualización de Datos: se establecen permisos para que ciertos usuarios puedan realizar cambios en la información de los alumnos en el proceso de matrícula o en cualquier momento del año. ➢ Manejo Documental: La herramienta permite al personal administrativo llevar un control sobre la documentación que el estudiante ha entregado o tiene pendiente. **Evaluación** ➢ Estructura Académica: La herramienta permite establecer la estructura de cada grado y cada asignatura; logros e indicadores de logro para la evaluación del estudiante. ➢ Editar Estructura: Los docentes pueden realizar modificaciones a la estructura de su materia. ➢ Manejo de Notas: existe un registro de notas para cada materia y en cada semestre (4 en total según decreto 230 de 2002) además una nota final o definitiva de cada materia. ➢ Recuperaciones: Las materias son evaluables en el rango entre D y E establecido por el MEN. Los logros e indicadores de logro se evalúan como aprobado o no aprobado teniendo en cuenta que debe existir posibilidad para el docente de establecer la recuperación del mismo.

	➢ Accesibilidad a información académica: Tanto directivos como docentes pueden acceder a la información académica de los estudiantes. **Promoción** ➢ Datos históricos: Se lleva un control de las notas obtenidas por los estudiantes a lo largo de su vida escolar. ➢ Selección de estudiantes en riesgo: El sistema puede seleccionar al final de cada período escolar a aquellos estudiantes que no cumplan los requisitos mínimos de promoción. ➢ Pre-matrícula automática: Los estudiantes promovidos entran en estado de pre-matrícula automáticamente. ➢ Sugerencias y recomendaciones: El módulo de matrículas permite al comité generar comentarios y sugerencias respecto a la situación de cada estudiante. **Manejo Documental y de Archivo** ➢ Generación de informes: El sistema genera los cuatro reportes de notas anules.
Medio	El sistema cuenta con un control de usuarios que de acuerdo a los permisos establecidos puede hacerse uso de la información. EscuelaCol maneja cuatro tipos de usuarios: administrador, profesores, miembros del comité y directivos cada uno de estos puede acceder a diferentes funcionalidades o características predefinidas por el sistema.
Bajo	No se encontró ningún Servicio.

Fuente Díaz y Naranjo (2010)

Con la ayuda del proyecto de pregrado se realizaron encuenstas a tutores de Computadores Para Educar que estuvieron en campo en el 2008 por diferentes regiones del país, permitiendo identificar las necesidades y problemas de las instituciones en el manejo de la información referente a los procesos de evaluación y promoción de estudiantes además se evidenció la falta de adquisición de SI que ayuden con los diferentes procesos en las instituciones educativas. Después de realizar dicha encuesta y analizar cada uno de los resultados y tabularlos se concluye que la mayoría de las instituciones educativas visitadas se encuentran en nivel 1 inicial, asociado a la adquisición e

implementación de SI; pero la herramienta EscuelaCol 1.0 al no estar en funcionamiento en las instituciones educativas se encuentra en nivel 0 de uso, es decir tienen conocimiento que existen SI, pero no tiene control o claridad sobre los mismos y no necesariamente se llevan a cabo y se usan.

- **A.1.3. Especificar los roles de los actores y sus responsabilidades en la GRCSI.**

A continuación se describen los usuarios identificados en la herramienta así como la descripción de los privilegios para cada uno.

Tabla 35. Usuario y Perfiles del Sistema

Usuarios	Directorio		Notas		Docentes		Promoción		Estructura		Usuarios		Reportes	Matrícula
	Ver	Editar	Ver	Editar	Ver	Editar	Ver	Editar	Ver	Editar	Ver	Editar		
Administrador	P	P	P		P	P	P		P	P	P	P	P	P
Profesores	P		P	P	P	P	P		P					
Miembros del Comité	P		P		P		P	P	P					
Directivos	P	P	P		P	P	P		P	P	P		P	P

Fuente EscuelaCol 1.0 (2008)

Cada usuario puede acceder a diferentes funcionalidades o características predefinidas en el sistema, están definidas en siete categorías:

- Directorio: hace referencia al acceso de la información personal de cada estudiante.
- Acceso a notas: solamente tiene acceso los usuarios con perfil de docentes para editarla en aquellas materias que se registren a su nombre, sin embargo, los otros usuarios podrán observar las calificaciones obtenidas por los alumnos.

- Datos docentes: permite la creación y la modificación de docentes, materias y datos de identificación del mismo en el sistema.
- Promoción: proceso de evaluación de casos de riesgo, solo tienen acceso a modificaciones y correcciones los miembros del comité.
- La estructura: permite la creación y manipulación de clases, materias, logros, indicadores, etc.
- Los usuarios: crear y editar por el administrador del sistema.
- La generación de reportes y matrícula de estudiantes: accedida por el administrador del sistema o por usuarios directivos que hace referencia a cargos directivos de la institución y la secretaria.

5.2.2. A2 Identificar los activos críticos en los diferentes espacios de la organización.

- **A.2.1. Catalogar los Activos Relacionados con los SI**

El prototipo EscuelaCol 1.0 como se ha mencionado anteriormente es una herramienta que maneja lo relacionado con los procesos de evaluación y promoción de estudiantes; estos procesos contienen información crucial para el buen funcionamiento de las instituciones ya que sin un adecuado tratamiento ocasionarían graves perjuicios tanto para el estudiante quien es el directamente afectado como para el establecimiento educativo.

- **A.2.2. Determinar la Información Sensible**

Los activos de información sensibles identificados en la herramienta son:

1. El historial académico de los estudiantes.
2. Las notas de logros e indicadores para cada uno de los períodos académicos.
3. La nota definitiva por cada materia.
4. Los reportes generados.
5. La base de datos y backup.
6. La promoción de estudiantes al siguiente año escolar.
7. Las materias perdidas con los registros de estudiantes.
8. La matrícula académica.

9. La información personal y familiar de los estudiantes.
10. La información del personal docente y administrativo.
11. Creación de materias para cada curso.

Estos activos se evidenciaron aplicando diferentes pruebas con personal de instituciones educativas de la ciudad, además por la información proporcionada en la base de datos de la herramienta EscuelaCol 1.0 y los anexos del libro de Ramírez & Tellez (2008).

Lo anteriores activos se pueden agrupan en 4 activos de información:

1. Matrícula.
2. Evaluación.
3. Promoción.
4. Manejo Documental y de Archivos.

- **A.2.3. Dimensionar los activos en cuanto a los niveles de riesgos y su relación con la disponibilidad, autenticidad, integridad y confidencialidad.**

Una vez identificados los activos críticos de la organización se busca identificar los riesgos a los cuales está expuesta la herramienta, para mejorar la seguridad de la información en el SI. Los activos dependen de otros componentes como son el software, el hardware y la infraestructura diseñados para soportar de forma eficiente dichos procesos.

La identificación de los activos críticos es esencial para conocer qué debe protegerse y que debe resguardarse. En la siguiente tabla se muestra la relación de los niveles de riesgo con los activos del SI y como se ven afectados según los criterios de seguridad.

Tabla 36. Relación entre los niveles de riesgos los activos y los criterios de seguridad de EscuelaCol 1.0

Nivel de riesgo	Activos en riesgo	Relación con los criterios de seguridad	Actores involucrados
Acceso	Información, solo personas autorizadas puedan hacer uso de la aplicación.	Disponibilidad, Confidencialidad, Autenticidad, Integridad	Usuarios del SI.

Nivel de riesgo	Activos en riesgo	Relación con los criterios de seguridad	Actores involucrados
Ingreso de Información	Información personal de estudiantes y cuerpo administrativo y docente e ingreso de datos de todos los formularios del SI de una manera incorrecta ocasionando que las transacciones o consultas que puedan ser ejecutas.	Autenticidad, Integridad	Docentes, secretaria y personal administrativo de cada institución educativa.
Ítems rechazados o en suspenso	Información y Servicios. Hacer pre matrículas y promoción de estudiantes	Disponibilidad, Integridad	Docentes, secretaria y administrativos de la institución educativa.
Procesamiento	Servicios como la matrícula promoción y reportes	Disponibilidad, Integridad	Usuarios del SI
Estructura Organizativa	Personas	Disponibilidad, Confidencialidad, Autenticidad, Integridad	Personal encargado de desarrollar el SI. Proveedores de servicios de TI
Cambio a los Programas	Aplicaciones Informáticas Soportes de Información.	Disponibilidad, Confidencialidad, Autenticidad, Integridad	Personal encargado del mantenimiento del SI

Fuente Díaz y Naranjo (2010)

5.2.3. A3 Identificar y evaluar las amenazas y vulnerabilidades de los activos.

- **A.3.1 Identificar las vulnerabilidades del SI**

Esta actividad se basa en el ítem anterior en el cual se ha mencionado los activos críticos que se consideran importantes en EscuelaCol 1.0; ahora se evalúa cómo estos pueden ser amenazados y que vulnerabilidades presentan frente a las diferentes condiciones del entorno en el cual funciona el sistema de información, identificando las circunstancias que podrían dar lugar a que se ocasione una violación de seguridad afectando algunos de los activos y aquellos hechos o actividades que pueden concretarse y ocasionen daño en la información.

Las vulnerabilidades identificadas en EscuelaCol 1.0 a las cuales están expuestos tanto los activos de la organización como la propia herramienta son:

1. Ataques de contraseña.
2. Pérdidas de copias de Backus.
3. Falta de validación de todos los campos en los diferentes formularios del SI.
4. Ingreso de datos erróneos.
5. Acceso no autorizado a aplicaciones e información.
6. Falta de capacitación a los usuarios para el manejo del SI.
7. La no disponibilidad de la información para los usuarios del SI.

- **A.3.2. Relacionar las vulnerabilidades con las amenazas potenciales y A.3.3. Relacionar las amenazas y vulnerabilidades con los activos que afectan.**

De acuerdo al anexo D a continuación se relacionan las vulnerabilidades identificas en el SI asociándolas con las amenazas identificas en dicho anexo y que activos son afectados por las vulnerabilidades identificadas.

Tabla 37. Identificación de vulnerabilidades y amenazas asociadas a los activos de EscuelaCol 1.0

Amenaza	Vulnerabilidad	Activos
De origen industrial	Perdidas de copias de Backpus.	Información existente en la base de datos del SI
Errores y Fallos	Ataques de contraseña	Los activos que puede afectar son: servicios del SI como la matrícula, la promoción, que usuarios registrados no puedan ingresar a la aplicación.
	Ingreso de datos erróneos	Información ingresada por los formularios existentes el SI
	Acceso no autorizado a aplicaciones e información.	Notas de los diferentes estudiantes. El administrador de la herramienta pueda editar las notas de los diferentes cursos, cosa que no debe ocurrir, porque este solo puede

		verlas más no editarlas.
	Falta de capacitación a los usuarios para el manejo del SI	Información. los usuarios al no saber utilizar el SI afectan lo que se guarda en la base de datos *Esco.sql*
	La no disponibilidad de la información para los usuarios del SI	Servicios como la promoción de estudiantes y el pre-matrícula.
	Falta de validación de todos los campos en los diferentes formularios del SI	Tablas de la base de datos del SI como lo son: estudiantes, padres, matrícula, indicadores, cursos, logros, nota logro y nota indicador

Fuente Díaz y Naranjo (2010)

5.2.4. A4 Diseñar escenarios de riesgo en términos de su impacto organizacional.

- **A.4.1. Creación de una base especifica de escenarios de riesgo.**

A continuación se explican los escenarios de riesgos a los cuales se ven expuesto los activos de EscuelaCol 1.0, las causas en que puede presentarse y el impacto o consecuencia organizacional que ocasionaría la ocurrencia de dicho riesgo de acuerdo al método de MEHARI.

Tabla 38. Escenarios de Riesgos 1 EscuelaCol 1.0

Descripción del escenario de Riesgos: Alteración de archivos o datos de la aplicación debido a un error de validación por usuarios autorizados.(Información incompleta)	
Causa que Originan el Escenario	**Consecuencias Directas e Indirectas del Escenario**
Los usuarios ingresan al sistema, registran la información, esta puede estar completa o incompleta, el sistema no verifica, ni valida los diferentes campos. Además digitan información errónea en los campos obligatorios. Un campo obligatorio en el registro de información de estudiantes es el nombre del estudiante, puede ocurrir que la secretaria digite mal el nombre del estudiante, es decir en vez de	La no validación de los campos, tanto de texto, como numéricos, ocasionan graves daños, para el sistema y para el estudiante, ya que no refleja la verdadera información, permitiendo tomar decisiones equivocadas. La falta de información, en los registros hechos, genera inconsistencia, esto se puede ver reflejado en la matrícula académica, las notas parciales y finales

escribir María de Jesús, escriba solo María y en la información personal.
Probabilidad de Ocurrencia: Muy probable.

Fuente Díaz y Naranjo (2010)

Tabla 39. Escenarios de Riesgos 2 EscuelaCol 1.0

Descripción del escenario de Riesgos: Alteración por error de procedimientos, la configuración de datos de la aplicación en la base de datos (duplicación de datos).	
Causa que Originan el Escenario Los usuarios registran los datos de un estudiante más de una vez, ya que el sistema no valida la existencia de datos anteriores. Un profesor está ingresando las notas de sus estudiantes en un determinado período escolar, por falta de concentración puede escribir las notas de una materia varias veces. Al momento de digitar los logros para los diferentes períodos del año escolar en curso, estos son los mismos, es decir el logro del período uno es el mismo para los siguientes períodos.	**Consecuencias Directas e Indirectas del Escenario** La duplicidad de datos, genera errores en las base de datos, además ocasiona consultas más lentas e inestabilidad. Al generar informes, se presentan graves problemas ya que se tiene duplicidad en la información para un mismo estudiante es el caso de las notas de un período académico, se pueden encontrar incoherencias con éstas, no se sabe si el estudiante aprobó el logro o no ya que aparecen diferentes notas para esa materia y período académico, provocando inconformismo por parte de los estudiantes ya que se verán afectados en el registro académico
Probabilidad de Ocurrencia: Es probable	

Fuente Díaz y Naranjo (2010)

Tabla 40. Escenarios de Riesgos 3 EscuelaCol 1.0

Descripción del escenario de Riesgos: Alteración de los datos de forma individual por usuarios autorizados (ingreso de datos incorrectos).	
Causa que Originan el Escenario	**Consecuencias Directas e Indirectas del Escenario**
El personal encargado de manejar el SI no esté capacitado, es decir no sabe cómo funciona la herramienta, ocasionando ingreso de datos incorrectos como por ejemplo notas de estudiantes, información personal, materias, entre otros.	Si hay datos incorrectos en la información proporcionada por la herramienta conlleva a inconformismos tanto de directivos, como de estudiantes, ocasionando el retiro del software del establecimiento. Otro punto a tratar es la generación de ciertos roces entre docentes y estudiantes por la inconsistencia en sus informes académicos, creando ambientes de trabajo desagradables y el retiro de estudiantes de la institución.
Probabilidad de Ocurrencia: Es probable.	

Fuente Díaz y Naranjo (2010)

Tabla 41. Escenarios de Riesgos 4 EscuelaCol 1.0

Descripción del escenario de Riesgos: Divulgación de los datos de la aplicación con previa consulta o captura (Validación incorrecta).	
Causa que Originan el Escenario	**Consecuencias Directas e Indirectas del Escenario**
Las fallas de seguridad permiten el ingreso de un personal ajeno al sistema. Un usuario registrado en el sistema puede acceder sin permisos a módulos de uso exclusivo de otro usuario, permitiéndole alterar e incluso registrar información errónea en el sistema.	En una herramienta software lo que prima es la confidencialidad de la información que se maneja, los procesos y aplicaciones que realiza; si no hay seguridad puede que personas ajenas ingresen al sistema y puedan hacer y deshacer en éste sin mayor dificultad, ocasionando pérdidas enormes para la organización. Se puede perder la confidencialidad de los datos, la información puede ser

	ingresada por personas autorizadas pero que no tienen permisos a cierta información.
Probabilidad de Ocurrencia: Es poco probable	

Fuente Díaz y Naranjo (2010)

Tabla 42. Escenarios de Riesgos 5 EscuelaCol 1.0

Descripción del escenario de Riesgos: Falta de disponibilidad o pérdida de los datos publicados en el SI por usuarios autorizados (pérdida de la información).	
Causa que Originan el Escenario	**Consecuencias Directas e Indirectas del Escenario**
Se está digitando las notas de un curso en un momento, ocurre un corte de energía eléctrica, al llegar la energía, el sistema no informa en qué estado quedó esta actividad o proceso y el docente da por hecho que estas notas fueron grabadas en la herramienta.	Al no tener todas las notas de los estudiantes por cada uno de sus períodos, se pueden tomar decisiones equivocadas como el no promover al estudiante al siguiente año escolar o hacer actividades de refuerzo para poder aprobar el año en curso.
Probabilidad de Ocurrencia: Muy poco probable	

Fuente Díaz y Naranjo (2010)

Tabla 43. Escenarios de Riesgos 6 EscuelaCol 1.0

Descripción del escenario de Riesgos: La pérdida o destrucción maliciosa de documentos y archivos, a raíz del olvido por parte del departamento de tecnología de hacer el debido mantenimiento tanto al hardware como al software (daño de equipo donde se encuentra el software).	
Causa que Originan el Escenario	**Consecuencias Directas e Indirectas del Escenario**
El mantenimiento inadecuado a los equipos de cómputo donde se encuentre instalado el software, puede generar daños y errores en sistema operativo del PC.	Si no se tiene un respaldo o copias de seguridad de las últimas versiones de la herramienta, este riesgo puede ocasionar hasta el cierre del establecimiento educativo, ya que no tendría historial de sus estudiantes y por ende los estudiantes podrían decir que se encontraban en otro año escolar

	o que no debía ciertos logros; esto puede ocurrir si la organización no cuenta con respaldo de las notas en papel o planillas del profesor donde lleven las calificaciones de sus estudiantes.
Probabilidad de Ocurrencia: Muy poco probable	

Fuente Díaz y Naranjo (2010)

Tabla 44. Escenarios de Riesgos 7 EscuelaCol 1.0

Descripción del escenario de Riesgos: perdida de material de archivos e información de los diferentes formularios de la aplicación para mantener durante un largo período, a raíz de un error de procesamiento por el mal uso de la herramienta por parte de los usuarios.	
Causa que Originan el Escenario Un usuario ingresa al sistema de información empieza a navegar por el mismo abriendo muchas pestañas sin hacer un uso adecuado de los mismos, ingresando información inadecuada es decir que no corresponde a la realidad de la organización	**Consecuencias Directas e Indirectas del Escenario** Antes de acceder al software se debe capacitar a los usuarios que ingresaran al sistema, para evitar que hayan inconvenientes de mal uso de la misma. Si el personal no tiene conocimiento del manejo de la herramienta puede bloquear el SI impidiendo que otros usuarios puedan ingresar a la aplicación.
Probabilidad de Ocurrencia: Es probable	

Fuente Díaz y Naranjo (2010)

5.2.5. A5 Diseñar estrategias de tratamiento y protección basados en estándares y buenas prácticas.

- **A.5.1. Identificar las estrategias de mitigación candidatas.**

Hasta el momento se ha hecho una revisión del software EscuelaCol 1.0 en la cual se ha identificado su estructura organizacional, su información sensible y cada uno de sus activos más importantes, además se han aclarado sus requerimientos funcionales e identificado los roles y perfiles de la aplicación; posteriormente se han identificado las amenazas y vulnerabilidades a las cuales puede estar

expuesta la herramienta y a partir de estos se han mencionado algunos niveles de riesgos que pueden afectar los activos críticos de la organización.

Ahora se diseñan las estrategias para asegurar la información, con el fin de propender a la disponibilidad, integridad, confidencialidad y autenticidad del sistema de información y de la información para los usuarios en la nueva versión de la herramienta EscuelaCol 2.0.

Información incompleta.
Duplicación de datos.
Ingreso de datos incorrectos. } Ingreso de información

Perdida de la información } Ítems rechazados o en suspenso

Validación incorrecta } Acceso

El mal uso de la herramienta por parte de los usuarios } Estructura organizativa

Daño de equipo donde se encuentra el software } Cambio a los programas

Tabla 45. Niveles de Controles y Riesgos

Nivel de Riesgo	Medios de control
Acceso	❖ Protección de los datos. ❖ Segregación de funciones en el departamento de sistemas: organización de la estructura jerárquica de acceso al sistema de información. ❖ Anti-Keylogers: software de control de espías y robots que capturen información sobre claves de acceso y registros. ❖ Control de acceso (contraseñas encriptadas, certificados digitales, dispositivos a nivel de tokens o tarjetas, etc.): control de acceso a los servicios, acceso a las aplicaciones, acceso al sistema operativo, acceso a los soportes de información, acceso físico a las instalaciones. ❖ Registro de actuaciones e incidencias: registros a nivel de log´s que permitan determinar lo que los usuarios hacen en el sistema. ❖ Administración de cuentas: desactivación de cuentas de usuarios inactivos y cambio periódico de claves de acceso. ❖ Desconexiones automáticas: desconexiones de sesión

Nivel de Riesgo	Medios de control
	por tiempo sin actividad dentro del sistema.
Ingreso de Información	❖ Controles de edición y validación Formato: tipo de datos con su respectivo tamaño, y de esta manera tener control sobre la entrada de datos. Campos faltantes: existen datos que no pueden quedar en blanco en cierto momento, ya que puede suceder que alguien después ingrese datos erróneos. Validación: comparar datos al momento de registrarlos, con los ya existentes en el sistema. Procesamiento duplicado: se combinan 2 acciones: la primera es la pre-numeración de formatos para el ingreso de datos o registros de transacciones, ayudando a que no exista un mismo código para diferentes registros y por último que el sistema controle el cumplimiento de la secuencia de los formatos pre-numerados. Correlación de campos: un campo tiene sentido en la medida en que exista otro campo que lo autorice, es decir que tenga relación con él. ❖ Lote: procesar la información por paquetes de manera que se pueda comprobar que la información ingresada es correcta. ❖ Doble digitación de campos críticos: es incluir en el sistema dos veces la misma información.
Items rechazados o en suspenso	❖ Controles Programados: son aquellos que se programan en las rutinas y de esta manera se evita correr el riesgo de ítems rechazados o en suspenso. ❖ Controles de Usuarios: Reportes que deben generar o revisar los usuarios del sistema. ❖ Interrupción de las operaciones del cliente: bloqueo de la maquina cliente hasta que se restablezca la conexión.
Estructura organizativa	❖ Controles y procedimientos operativos: coordinar adecuadamente la responsabilidad en el manejo de la información. Establecer manuales de operación y controles operativos diarios. Supervisar a los usuarios privilegiados. Controlar el software sensitivo. Controlar el desarrollo de sistemas. Generar políticas y planes de contingencia. Desarrollar procedimientos y lineamientos de seguridad. Definir la función de administración de seguridad y entrenar a los profesionales de seguridad.
Cambio a los programas	❖ Procedimientos de iniciación, aprobación y documentación: Generar órdenes de trabajo para los mantenimientos, de manera que se posibilite el seguimiento a los mantenimientos realizados. ❖ Procedimientos de catalogación y mantenimiento:

Nivel de Riesgo	Medios de control
	establecer políticas para llevar a cabo los mantenimientos preventivos y correctivos de los SI y documentar los resultados obtenidos en los mismos. ❖ Intervención de los usuarios: catalogación de la información provista por los usuarios del SI respecto de fallos ocasionados por las transacciones. ❖ Procedimientos de pruebas: realizar a cabalidad las pruebas de subsistemas y las pruebas de integridad del SI cuando se consolidan los módulos. ❖ Supervisión efectiva: revisión periódica de las actividades desarrolladas por los programadores de software.

Fuente Autores

- **A.5.3. Elaborar e Implementar un plan para el tratamiento del riesgo**

Se han mencionado los niveles de riesgo a los cuales está expuesta la herramienta y los posibles controles que pueden ser aplicados a la nueva herramienta a desarrollar EscuelaCol 2.0 con el objetivo de disminuir de manera significativa los escenarios de riesgos, las posibles amenazas y vulnerabilidades a los cuales puede estar expuestos la información de los establecimientos educativos que van a hacer uso de la aplicación; para la implementación de los controles mencionados en la tabla 48 se propone desarrollar y establecer un plan que permita llevar a cabo de manera ordenada las decisiones tomadas y planeadas para el tratamiento del riesgo. El estándar AS/NZS[16] propone el esquema que se muestra en siguiente tabla para elaborar un plan de tratamiento de riesgos.

Tabla 46. Plan de Tratamiento de Riesgos EscuelaCol 2.0

Programa y plan de tratamiento de riesgos
Fecha de revisión del riesgo: 12/02/2010 Compilado por: Autores Fecha: 12/04/2010 Revisado por: Guerrero Fecha: 12/06/2010

[16] Estándar Australiano para la Administración de Riesgos-AS/NZS: 2004 proporciona un marco genérico para establecer el contexto, la identificación, análisis, evaluación, tratamiento, seguimiento y comunicación de riesgos.

El riesgo en orden de prioridad del registro de riesgos	Opciones posibles de tratamiento	Opciones preferidas	Puntaje del riesgo luego del tratamiento	Resultado del análisis de costo/beneficio A: acepta B: rechaza	Persona responsable por implementación de la opción	Calendario de implementación	Como será monitoreado este riesgo y las opciones de tratamiento
Acceso	Control de acceso	✓		A	Autores	1/02/2010	Se explica en la actividad A6 numeral 1.
	Protección de los datos.	✓		A	Autores	13/02/2010	Se explica en la actividad A6 numeral 1
	Administración de cuentas	✓		A	Autores	21/02/2010	La herramienta cuenta en el módulo "Administración: Usuarios y Perfiles" la opción de crear usuarios con su respectivo perfil como la modificación de un usuario creado.
	Desconexiones automáticas	✓		A	Autores	30/02/2010	Al programar en JSP y trabajar con sesiones automáticamente después de cierto tiempo de inactividad en el SI, cierra la sesión y el usuario debe nuevamente ingresar su usuario y contraseña
Ingreso de información	Controles de edición y validación	✓		A	Autores	1/02/2010	Se explica en la actividad A6 numeral 2.
	Doble digitación de campos críticos	✓		A	Autores	1/02/2010	Se explica en la actividad A6 numeral 2.

Programa y plan de tratamiento de riesgos

Fecha de revisión del riesgo: 12/02/2010
Compilado por: Autores Fecha: 12/04/2010
Revisado por: Guerrero Fecha: 12/06/2010

El riesgo en orden de prioridad del registro de riesgos	**Opciones posibles de tratamiento**	**Opciones preferidas**	**Puntaje del riesgo luego del tratamiento**	**Resultado del análisis de costo/beneficio A: acepta B: rechaza**	**Persona responsable por implementación de la opción**	**Calendario de implementación**	**Como será monitoreado este riesgo y las opciones de tratamiento**
Ítems rechazados o en suspenso	Controles Programados	✓		A	Autores	8/02/2010	Se explica en la actividad A6 numeral 3.
	Controles de Usuarios	✓		A	Autores	9/02/2010	Se explica en la actividad A6 numeral 3.
Estructura organizativa	Controles y procedimientos operativos	✓		A	Autores	11/04/2010	Generar manuales para cada usuario o uno general de la aplicación y entregarlos en formato digital o impreso al personal de la empresa para que lo estudie y analice, de esta manera haga un buen uso de la información proporcionada por el software.
Cambio a los programas	Intervención de los usuarios	✓		B	Autores	21/04/2010	No se puede implementar este control por que el SI no se ha implantado en ninguna institución educativa.
	Procedimientos de pruebas	✓		A	Autores	21/04/2010	En el momento del desarrollo se harán

Programa y plan de tratamiento de riesgos Fecha de revisión del riesgo: 12/02/2010 Compilado por: Autores Fecha: 12/04/2010 Revisado por: Guerrero Fecha: 12/06/2010							
El riesgo en orden de prioridad del registro de riesgos	**Opciones posibles de tratamiento**	**Opciones preferidas**	**Puntaje del riesgo luego del tratamiento**	**Resultado del análisis de costo/beneficio A: acepta B: rechaza**	**Persona responsable por implementación de la opción**	**Calendario de implementación**	**Como será monitoreado este riesgo y las opciones de tratamiento**
							pruebas funcionales e integrales para asegurar el perfecto funcionamiento del SI.
	Supervisión efectiva	✓		A	Autores	25/05/2010	Cada vez que se desarrolle un módulo se hará la revisión con los requisitos funcionales con los que debe cumplir el SI

Fuente Díaz y Naranjo (2010)

5.2.6. A6. Documentar los Resultados y Revisar los Casos

La documentación de los resultados es una actividad que permite a las organizaciones realimentar sus resultados y aprender sobre las situaciones de riesgo presentadas a partir de la revisión de los casos históricos más representativos y sus respectivas estrategias de tratamiento. Los controles implantados pueden ser vistos en Fuente Díaz y Naranjo (2010).

A continuación se describen la documentación de casos implementados en EscuelaCol 2.0.

Tabla 47. Esquema para la documentación de casos

Caso presentado	**Frecuencia de ocurrencia**	**Mecanismo(s) de mitigación**	**Resultados**
Al momento de digitar los logros para los diferentes	Muy probable	Estos mecanismos se explicaron	implementado y aceptado

Caso presentado	Frecuencia de ocurrencia	Mecanismo(s) de mitigación	Resultados
períodos del año escolar en curso, estos son los mismos, es decir el logro del período uno es el mismo para los siguientes períodos.		anteriormente en los controles aplicados para el ingreso de datos	en EscuelaCol 2.0
Al entrar al módulo de matrícula y hacer la pre-matrícula de un estudiante el sistema no informa del estado actual en que se encuentra el estudiante a matrícular. Por otra parte si se da click sobre matrícula y seguidamente sobre pre-matrícula la aplicación no muestra los resultados.	Muy probable	Estos mecanismos se explicaron anteriormente en los controles aplicados para Ítems en rechazo o en suspenso	implementado y aceptado en EscuelaCol 2.0
Al ingresar un directivo de la herramienta, tiene la posibilidad de ingresar al módulo de calificaciones y editar las notas de cualquier curso que desee, alterando las notas de los profesores de sus respectivos cursos y materias. Otra cosa que puede ocurrir es que cualquier persona ajena puede ingresar a la aplicación sabiendo la ruta específica del módulo al que quiere ir, es decir el sistema no mantiene la sesión.	Es probable	Estos mecanismos se explicaron anteriormente en los controles aplicados para Acceso general	implementado y aceptado en EscuelaCol 2.0

Fuente Díaz y Naranjo (2010)

5.2.7. A7 Monitorear y Controlar.

En este punto solo queda hacer uso y exploración de la herramienta para verificar su funcionalidad. Aplicados los controles y teniendo en cuenta la norma actual del MEN se llegó al desarrollo de la segunda versión de EscuelaCol, obteniendo como producto final una herramienta útil para las instituciones educativas colombianas, facilitando los procesos de evaluación y promoción en cuanto al manejo de documental y reduciendo los errores de pérdida de información.

6. CONCLUSIONES - La Importancia de la Gestión de Riesgos y Controles a Nivel Organizacional

La GRCSI no es una tarea simple, ya que son muchos los activos que debe ser protegidos y son muchas y diversas las amenazas a las cuales pueden estar expuestos. A esto se le suma la naturaleza compleja del sistema organizacional en la que se circunscribe, lo cual conlleva a necesidades de protección específicas. Por tal motivo, la GRCSI es una labor que lleva tiempo, requiere de esfuerzo, cuesta dinero y no es suficiente con realizarla una sola vez (Silberfich, 2009).

La complejidad de la GRCSI se debe atacar metodológicamente, de manera que se cubra la mayor parte posible de lo que se desea cubrir y se logre explicar a los diferentes entes implicados lo que se necesita y espera de ellos como participes del proceso de GRCSI.

La GRCSI debe contar con el compromiso e involucramiento de la dirección de TI, los responsables de la gerencia y los sectores estratégicos de la organización y las diversas áreas de TI, ya que a menudo, las decisiones de protección de la información se realizan en forma ad hoc, basado en la experiencia previa del departamento de TI con las vulnerabilidades y las amenazas que actualmente se conocen, ocasionando que los riesgos tiendan a no ser gestionados de forma sistemática o sean administrados por las personas equivocadas.

Una adecuada comprensión de los niveles de riesgo asociados con los sistemas de información, ayudará a las organizaciones a reconocer las implicaciones de la ocurrencia de un determinado espacio de riesgo dentro de su entorno complejo, logrando con esto apropiarse de las políticas de seguridad y su respectivo alineamiento con los procesos de negocio.

Los niveles de riesgo de PWC ofrecen una descripción que contribuye a que las organizaciones reconozcan el impacto de los riesgos en sus procesos de negocio. No obstante, al aplicar una metodología para la revisión de la estructura de sus definiciones, se logró evidenciar que no todas contenían los elementos asociados a los conceptos de “nivel de riesgo” y “riesgo”. Esto posibilitó la discusión y definición de una estructura en la que se diferenciara ¿Dónde ocurre el nivel de riesgo? ¿Qué ocasiona el nivel de riesgo? y ¿Cuál es el impacto posible?

Por su parte, abordar la complejidad de la ausencia de los procesos de cambio organizacional, necesarios para llevar a cabo una adecuada GRCSI, es una labor que implica en los actores el reconocimiento de las actividades organizacionales necesarias para su implantación en el negocio y de las responsabilidades que como participes en el proceso de cambio deben estar dispuestos a enfrentar.

La Gestión de riesgos y Controles en Sistemas de Información no debe verse divorciada de la calidad del software, ya que la calidad es uno de los factores fundamentales a tener en cuenta para evitar la ocurrencia de los riesgos asociados a los SI. Durante el desarrollo de aplicaciones se garantiza a través de distintas metodologías y técnicas de aseguramiento de la calidad del software que las aplicaciones se ajusten a los estándares y que tengan la menor cantidad de errores posibles. No obstante, amenazas relacionadas con la naturaleza misma del sistema de información o con factores externos pueden llegar a verse reflejados en la ocurrencia de riesgos. Es en este punto en que modelos de gestión de riesgos y controles en sistemas de información como el planteado en esta investigación ayudan a las organizaciones y a los desarrolladores de software a reconocer no sólo los niveles de riesgo de los SI sino también las implicaciones sobre los activos organizacionales que su ocurrencia pudiera ocasionar.

El modelo brinda a las organizaciones una serie de actividades definidas y organizadas metodológicamente para llevar a cabo la gestión de riesgos y controles en Sistemas de Información – GRCSI, las cuales son producto de la revisión e integración de las actividades relacionadas por los estándares y la literatura sobre GRCSI.

La integración de las actividades relacionadas por los estándares, permitirán concretar futuras investigaciones, orientadas a la definición de los procesos culturales y de cambio organizacional requeridos para llevar a cabo la GRCSI.

Para cada una de las actividades se propuso un conjunto de métodos, los cuales apoyan a los distintos involucrados en el “hacer” que conlleva la GRCSI.

Por otro lado, el modelo centra la GRCSI en la concepción de niveles de riesgo, lo cual permite apoyar a las organizaciones en el reconocimiento de los espacios organizacionales y de sistemas de información en los que se podría dar la ocurrencia de riesgos.

De igual manera, el modelo propuesto contribuye a la definición de medidas de mitigación asociadas a cada uno de los niveles de riesgo, las cuales deben ser posteriormente profundizadas por parte de las organizaciones de acuerdo con la complejidad de su entorno.

El modelo diseñado no tiene la pretensión de convertirse en un patrón para todas las organizaciones, por lo cual la definición inicial de los controles sugeridos para los seis niveles de riesgo planteados es un punto de partida que posteriormente puede ser ampliado por los responsables de la GRCSI en cada organización.

7. RECOMENDACIONES

El desarrollo de este proyecto de investigación permitió sugerir diversos métodos para la gestión de riesgos y controles en sistemas de información, por lo cual se recomienda generar proyectos orientados a construir herramientas software que permitan sistematizarlos, de manera que su utilización sea más ágil.

Por otro lado, se recomienda, continuar desarrollando estudios relacionados con la cultura organizacional hacia los riesgos y controles en sistemas de información, que permitan indagar sobre los procesos de cambio organizacional necesarios para una adecuada incorporación de la GRCSI en las organizaciones.

Futuros proyectos de investigación del grupo STI podrían orientarse a relacionar la gestión de proyectos con la gestión de riesgos y controles en sistemas de información, para lo cual será necesario indagar sobre los fundamentos definidos por el PMBOK.

Por último, se recomienda desarrollar investigaciones orientadas a la aplicación del modelo y los métodos diseñados en este proyecto de investigación en diversas organizaciones.

8. REFERENCIAS BIBLIOGRÁFICAS

4360:2004, A. (2004). *"Estándar Australiano. Administración de Riesgos". Tercera edición.* Australia: Standards.

Adams, J. (2005). Risk management, it's not rocket science: it's more complicated. *Journal The Social Affair Unit*.

Alberts, C. (1999). *Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM) Framework, Version 1.0. TECHNICAL REPORT. CMU/SEI-99-TR-017. ESC-TR-99-017 .* Londres.

Arroyo, T. (2007). *Códigos de buenas prácticas en materia de gestión de los riesgos de la información. Alineamiento entre ISO, COBIT e ITIL en beneficio del negocio.* Recuperado el 27 de Agosto de 2009, de http://crsi.ie.edu/wwwCrsi/portals/0/skins/dnn-crsi-public/Home/tabid/36/Default.aspx

Bennett, M., & Bennett, F. (2005). *Object Oriented Systems Analysis and Design Using UML.* México: McGraw Hill.

Brenner, B. (2009). *Price Waterhouse Coopers.* Recuperado el Diciembre de 2009, de The Global State of Information Security: www.pwc.com/gx/en/information-security-survey

Cater-Steel, A., & Al-Hakim, L. (2009). *Information Systems Research Methods, Epistemology, and Applications.* Estados Unidos: IGI Publishing.

Checkland, P. (2000). *Soft Systems Methodology: A Thirty Year Retrospective.* Lancashire: Wiley.

Checkland, P., & Scholes, J. (1999). *Iformation, Systems, and Information Systems. Cybernetics and humans knowing, Vol. 6, No 3 .* Londres: Willey.

Checkland, P., & Scholes, J. (1999). *Soft System Methodology in Action.* London: Wiley.

CLUSIF. (2007). *MEHARI 2007. Guide de l'analyse des risques.* Recuperado el 11 de Diciembre de 2009, de http://www.clusif.asso.fr

Consortium, I. (2009). *Information Security Managemente Maturity Model. Versión 2.0 .* Madrid.

Crosby, P. (1990). *Hablemos de Calidad.* España: McGrawHill.

Deloitte. (17 de Febrero de 2009). Confianza y Garantía. Informe Anual de Seguridad de la Información en Instituciones Financieras. Estado Unidos.

Deming, E. (1989). *Calidad, Productividad y Competitividad. La salida de la crisis.* Madrid, España: Ediciones Díaz de Santos.

Diaz, M., & Naranjo, M. (2010). *Herramienta Software Open Source Orientada a Apoyar los Procesos de Evaluación y Promoción en la Educación Básica Primaria Escuelacol 2.0.* Bucaramanga: UIS.

Directory, I. (2008). *Introduction To ISO 27005 (ISO27005).* Colombia: ICONTEC.

EFQM. (Enero de 2010). *Introducing the EFQM Excellence Model 2010.* Recuperado el 12 de Enero de 2010, de http://ww1.efqm.org/en/PdfResources/EFQMModel_Presentation.pdf

Elissondo, L. (2008). *Informática Aplicada a los Negocios - Seguridad en los Sistemas de Información.* Colombia.

Ellmann, E. (2008). *Confiabilidad. Una Estrategia de Negocio Diferente.* Recuperado el 26 de Enero de 2010, de http://www.mantenimientomundial.com/sites/mmnew/bib/notas/Ellmann.pdf

Guajardo, E. (2003). *Administración de la Calidad Total. Conceptos y Enseñanzas de los Granes Maestros de la Calidad.* México: Editorial Pax México.

Haig, B. (2009). *Man in the Middle .* New York: Grand Central Publishing.

Harry, M., & Schoeder, R. (2000). *Six SigmThe breaktrough Management Strategy.* Mc Graw Hill .

Hirsch, C., & Ezingeard, J.-N. (2009). Perceptual and cultural aspects of risk management alignment: a case study. *Journal of Information System Security*, 20.

I. I. (2005). *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE.* ISO. Agosto.

ISACA. (2002). *Documento S11.* Recuperado el 26 de Junio de 2009, de http://www.isaca.org

ISACA. (2007). *Student Book COBIT 4.1. .* Estados Unidos: ISACA.

Ishikawa, K. (1997). *Qué es el Control Total de Calidad. La modalidad Japonesa.* Colombia: Grupo editorial Norma.

ITGI. (26 de Noviembre de 2007). *Sociedad de la Información ITGI.* Recuperado el 20 de Febrero de 2009, de La gestión de los riesgos será el cuarto factor clave para el rendimiento de la empresa, junto con las personas, los procesos y la tecnología.: http://sociedaddelainformacion.wordpress.com/category/seguridad/gestion-de-riesgos/

Kefi, H. (2007). Using a systems thinking Perspective to construct and Apply an Evaluation Approach of technology-based Information systems. *Information Resources Management Journa*, 108-121.

M. d. (1997). *MAGUERIT. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* España: Ministerio de Administraciones Públicas.

M. d. (2005). *CAF. Comon Assessment Framework.* España: Editorial Ministerio de Administraciones Públicas.

M. d. (2005). *DECRETO 1599 de 2005.* Recuperado el 22 de Agosto de 2009, de http://www.cra.gov.co/portal/www/resources/xtu_presentacion%20meci.pdf

Maya, H., Rodriguez-Salazar, J., & Rojas, J. (1996). *Estrategias de Manufactura aplicando la metodología Six-Sigma .* México: Editorial Oceánica.

Newman, P. (Enero de 2010). *Newman, P. ACM. Forum on Risks to the Public in Computers and Related Systems. Volume 25: Issue 91*. Recuperado el 26 de Enero de 2010, de http://catless.ncl.ac.uk/Risks/25.91.html

Paulk, M., Weber, C., Curtis, B., & Chrissis, M. (2001). *The Capability Maturity Model: Guidelines for Improving the Software Process.* Estados Unidos: Addison-Wesley.

Peltier, T. (2001). *Information Security Risk Analysis.* Estados Unidos: Auerbach.

Piattini, M. (2007). *Análisis y Diseño de Aplicaciones Informáticas de gestión.* Colombia: Alfa y Omega.

Piattini, M. (2007). *Calidad de Sistemas de Información. Editorial Alfa y Omega.* España: Alfa y Omega.

PÚBLICAS, M. D. (2006). *MAGUERIT versión 2.0. Catalogo del elementosl.* España: Ministerio de Administraciones Públicas.

Ramírez, L., & Tellez, M. (2008). *Prototipo de Herramienta Software para Apoyar los Procesos de Evaluación y Promoción en Instituciones Educativas - EscuelaCol 1.0.* Bucaramanga: UIS.

Rose, J. (2002). Interaction, transformation and information systems development – an extended application of Soft Systems Methodology. *Information Technology & People Volume 15 Issue 3*, 242 - 268.

Ross, R. (2008). *Managing Risk from Information Systems. Recommendations of the National Institute of Standards and Technology.* Gaithersburg: NIST Special Publication 800-39.

Sewchurran, K. (2007). A Systemic Framework for Business Process Modeling Combining Soft Systems Methodology and UML. *Information Resources Management Journal, Volume 20, Issue 3*.

Shingo, S. (1990). *A Study of the Toyota Production System .* Estados Unidos.

Silberfich, P. A. (2009). Análisis y Gestión de riesgos en TI. ISO 27005 – Aplicación Práctica. *Quinto Congreso Argentino de Seguridad de la Información*, (pág. 43). Argentina.

SOMAP. (Septiembre de 2006). *Open Information Security Risk Management Handbook. Versión 1.0.* Recuperado el 15 de Diciembre de 2009, de http://ufpr.dl.sourceforge.net/project/somap/Infosec%20Risk%20Mgmt%20Handbook/Version%201.0/somap_handbook_v1.0.0.pdf

Sommerville, I. (2006). *Ingeniería del Software*. Séptima Edición. Colombia: Pearson Adisson Wesley.

Sparks, G., & et, a. (2005). *Una Introducción al UML. El modelado de procesos de negocio.* Recuperado el 2 de Junio de 2009, de http://www.craftware.net/es/descargas/modelo_de_proceso_de_negocio.pdf

Stonebumer, G. (2002). *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST .* Estados Unidos: Special Publication 800-30.

Udaondo, M. (1992). *Gestión de Calidad .* Madrid, España: Ediciones Díaz de Santos S.A. .

Whitman, M., & Mattord, H. (2009). *Principles of Information Security.* Canada: Thomson.

Wu, Y. (1996). *Diseño Robusto Utilizando los Métodos Taguchi.* Madrid, España: Ediciones Díaz de Santos.

Young, E. &. (2009). *managing Risk in the Current Climate.* Estados Unidos.

ANEXO A - Listas de Verificación para Detectar el Nivel Estratégico Organizacional en Términos de SI

Ítem de Evaluación	Grado Cumplimiento			Ponderación				
	C	NC	NA	0	1	2	3	4
¿La administración tiene claramente definidos planes estratégicos para el cumplimiento de los objetivos de la misión y la visión en términos de los SI?								
¿En los planes estratégicos de SI se encuentra definida la distribución de los recursos financieros?								
¿Los planes estratégicos han definido metas e indicadores de evaluación de los proyectos de SI?								
¿Se realiza seguimiento a los cronogramas de actividades de los proyectos de SI?								
¿Existe un plan para la adquisición o restructuración de tecnologías que incluya:								
a) Arquitectura de Sistemas?								
b) Dirección Tecnológica?								
c) Aspectos de Contingencia?								
d) Estrategias de Migración?								
¿Se han efectuado evaluaciones a los planes estratégicos de SI y TI?								
¿La organización ha establecido un comité encargado del direccionamiento y asesoramiento de la aplicación de SI a los procesos de negocio?								
¿Existe un marco de trabajo para el proceso de TI que incluya:								
a)Estructura y relaciones de procesos de TI y SI? b) Propiedad de TI y SI? c) Medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas?								
¿La organización ha establecido un comité de para la administración y priorización de la inversión de los SI?								
¿Se han definido roles y responsabilidades de los actores relacionados con los SI?								
¿Se administran y controlan los riesgos de los								

Ítem de Evaluación	Grado Cumplimiento			Ponderación				
	C	NC	NA	0	1	2	3	4
SI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento?								
¿Se han definido e implantado políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI para garantizar la protección de los activos de información de la empresa y satisfacer los requerimientos contractuales?								
¿Se han definido procesos para informar al personal relevante sobre la adquisición e implementación de los SI?								
¿Al momento de adquirir los sistemas de información o desarrollarlos, se aplican estándares para la aprobación de dichos sistemas?								
¿Se han definido, planeado e implantado mediciones para monitorear el cumplimiento continuo del sistema de administración de la calidad de los servicios relacionados con los SI?								
¿Los SI están ligados al marco de trabajo de la organización de tal manera que se defina como afectaría un fallo o una mala administración de los mismos?								
¿Se han asignado prioridades y planeado las actividades identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución de control en todos los niveles para implantar las respuestas a los riesgos asociados a los SI?								
¿Los proyectos de SI están vinculados al portafolio de proyectos de la organización?								
¿Se documentan los inconvenientes evidenciados en la ejecución de cada uno de los proyectos de SI?								

Convenciones: C → Cumple NC → No cumple NA → No Aplica

ANEXO B - Lista de Verificación para Descubrir la Cultura Ante Riesgos de los Actores de SI

Ítem de Evaluación	Grado Cumplimiento			Ponderación				
	C	NC	NA	0	1	2	3	4
¿Se han realizado sesiones de capacitación de forma regular respecto a los procesos, los roles y las responsabilidades de los actores de los SI en caso de riesgo?								
¿Cuenta la organización con un modelo de gestión de riesgos para la estructura organizacional encargada del manejo de los SI?								
¿La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear planes de seguridad de los SI?								
¿Se toman medidas cuando el desempeño y la capacidad de los SI no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos?								
¿Se monitorea continuamente el desempeño y la capacidad de los recursos de SI de manera que se atiendan temas como contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos?								
¿Se ha definido una estrategia de distribución definida y administrada para asegurar que los planes de contingencia ante riesgos se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera?								
¿En el momento de proceder a ejecutar los procesos asociados a los riesgos de los SI, se han adaptado patrones con el fin de generar un óptimo rendimiento y alcanzar un sistema de calidad?								
¿Al momento de adquirir los sistemas de información o desarrollarlos, la gerencia de TI aplica estándares para la aprobación de dichos sistemas?								
¿Se han determinado todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios,								

Ítem de Evaluación	Grado Cumplimiento			Ponderación				
	C	NC	NA	0	1	2	3	4
legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos?								
¿Los involucrados y comprometidos en el desarrollo de cada proyecto tienen conocimiento de cómo se relacionan con otros proyectos y cuáles son los riesgos que podrían ocasionar en su desarrollo?								
¿La dirección es consciente de los procesos destinados a la gestión de riesgos en SI y se involucra en los mismos?								
¿Se Identifican, documentan y analizan los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos?								
Cuando se adquiere una solución, ¿se realiza la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema?								
En caso de actualizaciones a sistemas existentes, ¿se realiza un análisis de impacto, justificación costo/beneficio y administración de requerimientos?								
¿Se realiza una adecuada transferencia de conocimiento a la gerencia, de manera que se realice una adecuada administración de privilegios, segregación de tareas, controles automatizados, respaldo/recuperación, seguridad física y archivo de la documentación de los riesgos?								

Convenciones:

C → Cumple

NC → No cumple

NA → No Aplica

ANEXO C - Diccionario de Catalogación de Activos

Familia de Activos	Clase	Subclase	Ejemplo
Información	Información Personal	Ninguna	Fotografías familiares, documentos personales.
	Información Empresarial	Sensible y Crítica	Información sobre clientes y proveedores, cuentas bancarias.
		Otro tipo de Información	Noticias públicas
Materiales y Suministros	Papelería e Impresos	Libros, normas y manuales	Estándares y normas
		Revistas, catálogos y artículos Técnicos	Revistas especializadas, fichas técnicas
		Guías, mapas, planos y tablas	Planos de redes y edificios
		Documentos de referencia	Procedimientos, investigaciones internas
Servicios	Servicios TIC	Ingeniería de Software	Servicios de programación de aplicativos
		Administración y Soporte Técnico	Servicios de mantenimiento de redes, instalaciones de Software y Hardware
		Seguridad de Información	Servicios de respuesta a incidentes, asesoría de seguridad
		Manejo de Datos	Servicios de Almacenamiento de datos, data center
		Internet	Servicios relacionados con los Aplicativos WEB
		Ingeniería Electrónica y Telecomunicaciones	Sistemas de control, circuitos electrónicos
		Gestión y Calidad del Servicio	Servicios de Gestión de proyectos, control de calidad
Infraestructura Tecnológica	Dispositivos de comunicaciones	Dispositivos de Comunicación	Teléfonos, radios, etc.

Familia de Activos	Clase	Subclase	Ejemplo
	y accesorios		
	Dispositivos de TI	Tarjetas Controladoras del Sistema	memorias DDR3, memoria DIMM, tarjetas de red, etc.
		Módulos o Interfaces del Sistema	Interfaz MIDI, interfaz CODEC, interfaz de puerto infrarrojo.
		Dispositivos de Soporte Físico	Rack's, gabinetes de datos.
		Dispositivos de Almacenamiento	DVD's, Dispositivos USB.
	Equipos informáticos y Accesorios	Computadores	servidores de red, servidores de impresión, notebook's, estaciones de trabajo
		Accesorios Periféricos	Switch's de monitor, switch's de impresoras, sistemas de video conferencia.
		Equipos de Entrada de Datos	Lector de huellas digitales, lector de código de barras.
		Insumos Informáticos	Mouse pad, caja porta DVD, fundas.
		Monitores y Pantallas	Monitores CRT, monitores LCD, monitores de pantalla táctil, pantallas de plasma.
		Impresoras	Impresoras de chorro de tinta, Impresoras láser Impresoras multifuncionales.
	Equipos de voz, datos, redes multimedia, plataformas y accesorios	Equipos de comunicación telefónica	Central telefónica privada (PBX), identificador de llamadas, bloqueador analógico y digital de llamadas salientes.

Familia de Activos	Clase	Subclase	Ejemplo
		Equipos de comunicación televisiva	Equipos de video profesional, Transcoder de video, Adaptador de antena de tv cable.
		Equipos de radiocomunicaciones	Equipo básico de radiocomunicaciones, equipo central de radiocomunicaciones, equipo de comunicación satélite, Antena de acceso inalámbrico.
		Equipos de Seguridad de Red	Firewall de hardware, equipo de seguridad de red virtual (VPN). l
		Equipos de Servicios de Red	Gateway, router de red, switch de fibra óptica, módem de acceso al proveedor de internet (ISDN)
	Software de Base y Aplicaciones	Software de gestión	Software de call center, software de gestión de recursos humanos, software de logística y planificación, paquete de ofimática.
		Software de planificación y contabilidad	Software de contabilidad, software de planificación de recursos empresariales, software de análisis financiero.
		Software de música y utilitarios	Software utilitario doméstico, software de edición de música.
		Software de edición y creación	Software de edición gráfica, software de diseño gráfico, software de retoque fotográfico, software de escáner (OCR)
		Software de consulta	Software de

Familia de Activos	Clase	Subclase	Ejemplo
		y gestión de datos	clasificación, software de particionado, software de gestión de relaciones con clientes (CRM), software de administración de bases de datos, software de búsqueda y administración de información.
		Software de desarrollo	Software de gestión de configuraciones, software de integración de aplicaciones, software de desarrollo de interfaz gráfica.
		Software educativo	Software de traducción de idiomas, software de traducción de texto a voz, software corrector ortográfico.
		Software de aplicaciones específicas	Software de gestión de instalaciones, software de diseño asistido (CAD), software de punto de venta (POS), software de fabricación asistida (CAM), software de información geográfica (GIS)
		Software de aplicaciones de red	Software de servidor de aplicaciones, software de voz sobre IP, software de explorador de internet.
		Software de administración de red	Software de control de tráfico de redes, software de administración de redes.
		Software de acceso de red	Software de servidor de comunicaciones, software de LAN,

Familia de Activos	Clase	Subclase	Ejemplo
			software de switch o router, software de conmutación de WAN, software de interconectividad de plataformas.
		Software de entorno operativo	Software de sistema de archivos, software de sistema operativo de servidor.
		Software de seguridad y protección	Software de servidor de autenticación, software administración de red privada virtual (VPN), software de reconocimiento de voz.
		Software de controladores de dispositivos	Driver's del sistema.
		Software de intercambio de información	Software de correo electrónico, software de video conferencia, software estándar de teléfonos móviles.
	Bases de Datos	Soporte impreso	Documentación de texto, documentación de gráficos.
		Soporte magnético	Microfilmación de información impresa, microfilmación de salida directa de computadora.
		Soporte electrónico	Base de datos jerárquica, base de datos en red, base de datos relacional.
Infraestructura Física	Centros de Datos	Equipos de suministro de energía	Sistema de alimentación ininterrumpida (UPS), regulador de tensión.
		Equipos de acondicionamiento	Acondicionador de aire, extractor de humedad,

Familia de Activos	Clase	Subclase	Ejemplo
		térmico	equipo de control de temperatura.
		Cableado estructurado	Cable coaxial, cable de plotter, cables de impresora, cables UTP, conector fibra óptica.
		Seguridad de la instalación	Cajas fuertes, equipos intercomunicadores, equipo de control de incendios, circuito cerrado de televisión, sistema de alarma.
Servicios TIC´s Ofrecidos	Servicios de tecnología	Servicios de hosting	Hosting de aplicación y páginas WEB.
		Servicios de centros de datos	Servicio de almacenamiento, servicio de infraestructura.
		Servicios de seguridad informática	Soporte técnico, análisis de vulnerabilidades.
	Servicios de información	Servicios web	Servicio de trámite, servicio de capacitación.
		Servicios telefónicos	Servicio de trámite, servicio de consulta.
		Servicios presenciales	Servicio de trámite, servicio de consulta, servicio de capacitación.
Personal	Personal Clave	Estructura Organizativa	CIO, ISSO, etc.
	Otro tipo de Personal	Auxiliares	Personal de soporte, personal de aseo.

Fuente. Basado en ITIL, OCTAVE y MAGERIT

ANEXO D - Identificación de Vulnerabilidades y Amenazas Asociadas a los Activos de los SI

Amenazas	Vulnerabilidades	Activos
Desastre natural (Fuego, Inundaciones, etc.)	Incidente producido por intensión o negligencia humana o por eventos fortuitos del ambiente natural.	Infraestructura física y tecnológica, Información, materiales y suministros, personal.
De origen industrial	Fallas eléctricas o mecánicas que ocasionen incendios, escapes, interferencias y/o fugas.	Infraestructura física y tecnológica, Información, materiales y suministros, personal.
	Averías de origen físico y/o lógico de los programas o equipos de comunicación, auxiliares y de cómputo.	Servicios, Información, Infraestructura física y tecnológica,
	Fallas en el suministro de energía	Servicios
	Degradación de los soportes de información como consecuencia del paso del tiempo.	Información
Errores y Fallos	Equivocaciones de los actores en la utilización de los servicios que provee el SI.	Servicios, Información.
	Equivocaciones de las personas encargadas de la instalación y configuración del SI.	Servicios, Información, Infraestructura física y tecnológica.
	Errores del SI en el registro de log’s.	Servicios, Información.

Amenazas	Vulnerabilidades	Activos
	Acciones organizacionales descoordinadas que generen errores.	Personal, Información.
	Propagación de virus informático, espías, gusanos, bombas lógicas, etc.	Información, Servicios.
	Envío de información por caminos de red diferentes a los deseados ocasionando que personas no deseadas tengan acceso a la misma o alteración de la información que transita por la red.	Información
	Inserción accidental de información incorrecta o alteración de la información.	Información
	Destrucción de la Información por defectos en el código u operaciones defectuosas.	Información, Infraestructura tecnológica.
	Revelación de información por indiscreción del personal de la organización.	Información
	Defectos en los procedimientos o controles de actualización del código que ocasionen la utilización de programas defectuosos.	Infraestructura tecnológica, Información.
	Falta de recursos operativos para el funcionamiento adecuado del SI.	Servicios
	Ausencia del personal del	Personal, servicios.

Amenazas	Vulnerabilidades	Activos
	puesto de trabajo relacionado con los SI.	
	Suplantación del personal autorizado para utilizar los privilegios sobre el SI o abuso de los privilegios del personal autorizado.	Información, servicios.
	Alteración del funcionamiento de los programas que soportan los procesos persiguiendo un beneficio directo o indirecto cuando una persona lo utiliza.	Información, Servicios, Infraestructura tecnológica.
	Sustracción de equipamiento y soportes de información por personal interno y/o externo de la organización, vandalismo o actos terroristas que ocasionen destrucción.	Información, infraestructura tecnológica y física, materiales y suministros
	Presiones o amenazas sobre el personal que obliguen a obrar de mala fe o abuso de la buena fe para hacer que el personal interno obre según beneficios de terceros.	Personal, información, infraestructura tecnológica y física, materiales y suministros

Basado en MAGERIT