ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

GUÍA Y ANÁLISIS DE GESTIÓN DE RIESGOS EN LA ADQUISICIÓN E IMPLANTACIÓN DE EQUIPAMIENTO Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES PARA PROYECTOS DE ALCANCE NACIONAL

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MÁSTER (MSc) EN GESTION DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

JONATHAN PATRICIO CARRILLO SÁNCHEZ

jcnazir@hotmail.com

DIRECTOR: PhD. ENRIQUE MAFLA G.

mafla@epn.edu.ec

Quito, agosto 2012

DECLARACIÓN

Yo Jonathan Patricio Carrillo Sánchez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Ing. Jonathan Patricio Carrillo Sánchez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Jonathan Patricio Carrillo Sánchez, bajo mi supervisión.

PhD. Enrique Mafla Gallegos
DIRECTOR DE TESIS

AGRADECIMIENTO

Al Eterno Dios de Israel, por su misericordia, por su bondad y por su gran Nombre; gracias por bendecirme tal como fueron bendecidos nuestros padres Avraham, Itzjak y Iaakov; En Todo, De Todo y Todo.

DEDICATORIA

A mi esposa Andrea y a mi hija Nathalia, ya que por su causa he podido mantener una actitud y una conducta inspirada y emprendedora, por ustedes el Eterno me ha guiado a aplicar con acierto y tiento las estrategias de vida y motivación para ser felices.

A mis padres y hermanos, gracias por ser mis amigos. Sin duda con su apoyo podremos guiar a otros para que alcancen su desarrollo integral.

CONTENIDO

RESUMEN ..... *ix*

CAPITULO 1 ..... *1*

INTRODUCCIÓN *1*

1.1 RIESGO Y GESTION DEL RIESGO 2
1.1.1 GESTION DEL RIESGO: CAUSA - RIESGO - EFECTO 6
1.1.2 FUENTES DEL RIESGO 7
1.1.3 MEJORES PRÁCTICAS: ENFOQUE EN LA GESTIÓN DE RIESGOS 8

1.2 MÉTODO PARA DESARROLLAR LA GUIA DE GESTION DE RIESGOS PARA PROYECTOS DE TI. 11
1.2.1 JUSTIFICACIÓN 11
1.2.2 OBJETIVOS 12
1.2.3 FASES DEL MÉTODO 12
1.2.4 ELEMENTOS DE TI Y ESCALA DE VALORACIÓN 15

CAPITULO 2 ..... *18*

GUIA DE GESTION DE RIESGOS PARA PROYECTOS DE TI *18*

2.1 EJECUCION DEL MÉTODO 18
2.1.1 FASE 1: DISGREGACIÓN 18
2.1.2 FASE 2: IDENTIFICACIÓN 20
2.1.3 FASE 3: EVALUACIÓN 25
2.1.3.1 CMMI 25
2.1.3.2 SPICE 27
2.1.3.3 PMBOK 28
2.1.3.4 PRINCE2 29
2.1.3.5 COBIT 31
2.1.3.6 RISK IT 33
2.1.3.7 OCTAVE 35
2.1.3.8 NIST 800-30 37
2.1.3.9 MAGERIT 39
2.1.2.3.10 RECOLECCION DE RESULTADOS 42
2.1.4 FASE 4: SELECCIÓN 50
2.1.5 FASE 5: DEFINICIÓN 54
2.1.5.1 GUÍA DE GESTION DE RIESGOS 55
2.1.5.1.1Especificación de la Guía 56

CAPITULO 3 ..... *68*

APLICACIÓN DE LA GUÍA Y ANÁLISIS DE RESULTADOS *68*

3.1 MARCO GENERAL DE REFERENCIA DEL PROYECTO 68
3.1.1 ALCANCE DEL PROYECTO 68
3.1.2 ESTABLECER EL CONTEXTO ORGANIZACIONAL Y ÁREAS CRÍTICAS 71
3.1.3 EQUIPO DEL PROYECTO 72
3.1.4 RECURSOS 73
3.1.5 CRITERIOS DE EVALUACIÓN 74

3.1.6 ACUERDOS 75

3.2 ANALISIS DE RIESGOS 76

3.2.1 IDENTIFICAR Y VALORAR LOS ACTIVOS DE LA ORGANIZACIÓN 76

3.2.2 ANALIZAR VULNERABILIDADES Y AMENAZAS 79

3.2.3 DETERMINAR LA PROBABILIDAD DE OCURRENCIA DE UNA AMENAZA. 81

3.2.4 IDENTIFICAR SALVAGUARDAS 82

3.2.5 VALORIZAR Y ESTIMAR EL IMPACTO 85

3.2.6 ANALIZAR, ESTIMAR Y PRIORIZAR EL RIESGO 87

3.3 GESTION DEL RIESGO 92

CAPITULO 4 94

CONCLUSIONES Y RECOMENDACIONES 94

4.1 CONCLUSIONES 94

4.2 RECOMENDACIONES: 95

REFERENCIAS BIBLIOGRAFICAS 97

ANEXOS 98

ANEXO A. OTRAS MEJORES PRACTICAS QUE GESTIONAN EL RIESGO 98

ANEXO B. EVALUACION DE ACTIVIDADES DE MEJORES PRACTICAS QUE GESTIONAN EL RIESGO 100

ANEXO C. CONTENIDO DEL CD ADJUNTO DE ESTA INVESTIGACIÓN 103

ANEXO D: EQUIPO DE TRABAJO QUE GESTIONARÁ EL RIESGO EN LOS PROYECTOS DE TI 104

ANEXO E. DIMENSIONES DE SEGURIDAD Y NIVEL DE MADUREZ PARA PROYECTOS DE TI 106

ANEXO F. ACTIVOS DE PROYECTOS DE TI 108

ANEXO G. RESUMEN MARCO LEGAL PROYECTO “PLAN AMANECER” 111

GLOSARIO DE TÉRMINOS 112

INDICE DE FIGURAS

FIGURA 1. RELACIÓN RIESGO - COSTE 5
FIGURA 2. PROCESO DE ANÁLISIS PARA DESARROLLAR LA GUÍA DE GESTIÓN DE RIESGOS DE TI 13
FIGURA 3. COMPARATIVA DE MEJORES PRÁCTICAS QUE GESTIONAN EL RIESGO – ESCALA DE MEDICIÓN (EM) 44
FIGURA 4. CMMI & SPICE - GESTIÓN DEL RIESGO DE TI 46
FIGURA 5. PMBOK & PRINCE2 - GESTIÓN DEL RIESGO DE TI 47
FIGURA 6. COBIT & RISK IT - GESTIÓN DEL RIESGO DE TI 48
FIGURA 7. OCTAVE & NIST 800-30 & MAGERIT - GESTIÓN DEL RIESGO DE TI 49
FIGURA 8. MEJORES PRÁCTICAS QUE GESTIONAN EL RIESGO - CONSOLIDACIÓN DE RESULTADOS 51
FIGURA 9. MEJORES PRÁCTICAS - ACTIVIDADES QUE GESTIONAN EL RIESGO – RANGO DE SELECCIÓN 52
FIGURA 10. MODELO DE GUÍA DE GESTIÓN DE RIESGOS CORRESPONDIENTE A PROYECTOS TI 55
FIGURA 11. RELACIÓN ACTIVO-AMENAZA-VULNERABILIDAD 61
FIGURA 12. PROCESO CONTRACTUAL ENTREGA-RECEPCIÓN DE PRODUCTOS Y SERVICIOS 71
FIGURA 13. CANTIDAD DE ACTIVOS – PLAN AMANECER 89
FIGURA 14. PROBABILIDAD ACUMULADA POR ÁREA DE GESTIÓN DE TI – PLAN AMANECER 90
FIGURA 15. IMPACTO ACUMULADO POR ÁREA DE GESTIÓN DE TI – PLAN AMANECER 91
FIGURA 16. RIESGO ACUMULADO POR ÁREA DE GESTIÓN DE TI – PLAN AMANECER 92

INDICE DE TABLAS

TABLA 1. MEJORES PRÁCTICAS QUE GESTIONAN EL RIESGO 14
TABLA 2. ELEMENTOS DE TI 16
TABLA 3. ESCALA DE VALORACIÓN 17
TABLA 4. MEJORES PRÁCTICAS SOMETIDAS A ANÁLISIS PARA DESARROLLAR LA GUÍA DE GESTIÓN DE RIESGOS TI 19
TABLA 5. RESULTADOS FASE I: DISGREGACIÓN - CARACTERÍSTICA/ÁREA QUE GESTIONA EL RIESGO 20
TABLA 6. RESULTADOS FASE II: IDENTIFICACIÓN - ACTIVIDADES QUE GESTIONAN EL RIESGO 24
TABLA 7. CMMI – EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 25
TABLA 8. SPICE – EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 27
TABLA 9. PMBOK – EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 28
TABLA 10. PRINCE2 – EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 29
TABLA 11. COBIT – EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 31
TABLA 12. RISK IT – EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 33
TABLA 13. OCTAVE - EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 35
TABLA 14. NIST 800-30 - EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 37
TABLA 15. MAGERIT - EVALUACIÓN DE ACTIVIDADES QUE GESTIONAN EL RIEGO 39
TABLA 16. COMPARATIVA DE MEJORES PRÁCTICAS QUE GESTIONAN EL RIESGO – NIVEL DE PUNTUACIÓN (NP) 42
TABLA 17. COMPARATIVA DE MEJORES PRÁCTICAS QUE GESTIONAN EL RIESGO – RANGO DE SELECCIÓN .. 43
TABLA 18. MEJORES PRÁCTICAS - CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN 50
TABLA 19. MEJORES PRÁCTICAS – LISTA DE ACTIVIDADES - RANGO DE SELECCIÓN SATISFACTORIO 54
TABLA 20. CARACTERÍSTICAS DE ANÁLISIS CUANTITATIVO Y CUANTITATIVO 61
TABLA 21. EQUIPO DE PROYECTO 73
TABLA 22. RESUMEN DE COSTOS DE RECURSOS PARA EJECUTAR EL PROYECTO 74
TABLA 23. ACUERDOS DE FORMATOS PARA EJECUTAR PROYECTOS 76
TABLA 24. SÍNTESIS: IDENTIFICACIÓN Y VALORIZACIÓN DE ACTIVOS – PLAN AMANECER 78
TABLA 25. SÍNTESIS: ANÁLISIS DE VULNERABILIDADES Y AMENAZAS – PLAN AMENECER 80
TABLA 26. SÍNTESIS: PROBABILIDAD DE OCURRENCIA DE AMENAZAS – PLAN AMANECER 82
TABLA 27. SÍNTESIS: IDENTIFICACIÓN DE SALVAGUARDAS – PLAN AMANECER 84
TABLA 28. ESCALA DE VALORES DE DEGRADACIÓN PARA LOS ACTIVOS 85
TABLA 29. SÍNTESIS: ESTIMACIÓN DE IMPACTO – PLAN AMANECER 87
TABLA 30. SÍNTESIS: ESTIMACIÓN Y PRIORIZACIÓN DEL RIESGO 88

RESUMEN

Partiendo de la base del control estatal dirigido por la Contraloría General del Estado, la presente investigación se orienta a desarrollar una Guía de Gestión de Riesgos para proyectos de Tecnologías de Información mediante un método propuesto en este documento con el objetivo de cumplir las metas institucionales por medio de los proyectos que corresponden al uso, manejo y gestión de TI.

Para desarrollar la Guía se procedió a analizar los procesos de varios modelos aplicables a proyectos de TI y de esta manera obtener una guía de Gestión del Riesgo basada en mejores prácticas y aplicable a diferentes entornos.

Los modelos considerados y que son la base para desarrollar la guía son: CMMI, SPICE, PMBOK, PRINCE2, COBIT, RISK IT, OCTAVE, NIST 800-30 y MAGERIT. Los elementos de TI considerados para realizar el análisis y comparación de resultados mediante una escala de valoración para determinar el nivel de correspondencia son: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones, Recurso Humano, legal, Financiero y Servicios.

Posteriormente se presenta la guía de Gestión del Riesgo en donde se detallan los procesos y las actividades mediante productos de entrada, productos de salida, técnicas, prácticas y participantes responsables. Finalmente se ejecuta la guía a un proyecto de alcance Nacional y como resultado se muestra la información de todo el análisis de riesgos, las vulnerabilidades, amenazas e impactos; así como también los mecanismos de salvaguarda como procedimientos, políticas, planes y soluciones técnicas que pueden ser consideradas para futuros proyectos.

CAPITULO 1

INTRODUCCIÓN

El Gobierno Nacional ha delegado a las entidades gubernamentales, bajo el Plan Nacional para el Buen Vivir 2009 – 2013, impulsar programas y proyectos de tecnologías de información entre los cuales podemos mencionar educativos, de inclusión social, turísticos, de conservación y aumento de la productividad.

Luego del proceso de licitación, planificación e inicio de los proyectos, existen eventos o condiciones inciertas que producen efectos que pueden ser favorables o perjudiciales sobre al menos un objetivo del proyecto como tiempo, coste, alcance, calidad y uso eficiente de los recursos. Esto se debe ya que muchos de los administradores de contrato no consideran planes de gerencia, análisis de riesgos, monitoreo relacionado a proyectos, o porque no existe una política pública que asegure el cumplimiento de estándares.

En el mercado existen varios modelos que identifican y analizan los riesgos según aspectos relevantes de su área como por ejemplo en proyectos, desarrollo de software, comunicaciones, seguridad y alineamiento con el negocio. Por lo tanto, es necesario que los profesionales cuenten con una herramienta que integre todos los elementos de TI que analice y gestione el riesgo con un enfoque de proyectos de Tecnologías de Información y Comunicaciones.

Las contribuciones de este trabajo son: analizar los procesos de varios modelos y obtener una guía de gestión del Riesgo basada en mejores prácticas orientada a la ejecución de Proyectos de IT y que sea aplicable a diferentes entornos. Esto permitirá a las instituciones contar con una herramienta que maneje adecuadamente los riesgos desde la planeación hasta el cierre de los proyectos.

Este trabajo se estructura en cuatro capítulos. El capítulo 1 identifica los problemas existentes, presenta modelos en cuanto a la gestión del riesgo y formula un método de análisis para desarrollar la guía. En el capítulo 2 se ejecuta el método desarrollado para establecer la Guía de Gestión de Riesgos correspondiente a Proyectos de TI. En el Capítulo 3 se aplica la guía y se realiza

un análisis de riesgos al Proyecto Educativo “Plan Amanecer”, el cual cuenta con el aval de los Ministerios del Interior y Educación del Estado Ecuatoriano, cuyo fin es mejorar la infraestructura tecnológica de las instituciones educativas y aplicar procesos formativos con las TICs. El monto total del Plan Amanecer es de 30 millones de dólares americanos. Por último en el Capítulo 4 se encuentra la sección de conclusiones y recomendaciones.

El presente trabajo se enfoca en el análisis de la adquisición, implementación y operación de la infraestructura de TI implantada en el Plan Amanecer y no contempla el análisis de los efectos de la TI sobre la enseñanza y aprendizaje de los usuarios que fueron beneficiados con el equipamiento.

1.1 RIESGO Y GESTION DEL RIESGO

El Gobierno Nacional por medio de la Contraloría General del Estado, ha impulsado el control de la utilización de los recursos estatales mediante Normas Técnicas de Control Interno[1], apoyadas en leyes y reglamentos como la del Sistema Nacional de Contratación Pública en la administración de proyectos y contratos[2]. Por tal motivo los profesionales deben implementar estrategias efectivas de gestión para afrontar los riesgos y factores que pueden presentarse durante todo el ciclo de vida de un proyecto y cumplir con los objetivos esperados.

RIESGO:

Boehm (1989, citado por Bagnoud, 2002) define exposición al riesgo como ***“un valor compuesto, resultante de la multiplicación de la probabilidad de ocurrencia de un evento por la pérdida que la misma implica”.***

En base a la definición anterior, existen tres entidades básicas en el riesgo.

[1] Fecha de publicación: 14 de diciembre de 2009. Tipo de Norma: Acuerdo de la Contraloría General del Estado No.39, Registro Oficial Suplemento No.87, 410 Tecnología de la Información.

[2] Administradores de Contrato: Artículos 70 y 80 de la Ley Orgánica del Sistema Nacional de Contratación Pública y el Artículo 121 de su Reglamento General.

La Primera es que el riesgo implica **probabilidad**. Esta probabilidad se encuentra reflejada en eventos que pueden materializarse y se encuentran registradas como datos históricos, indicadores de mercado e información de expertos.

La segunda es que el riesgo implica **frecuencia**, es decir, el número de veces que una condición ha ocurrido. Esta también puede ser definida de manera cualitativa mediante condiciones como Frecuente, Normal o Poco Frecuente.

La tercera es que el riesgo es universal y el resultado son **consecuencias que impactan** a algún componente de un proyecto o de una actividad, siendo estos la programación, costos, calidad y alcance de los objetivos.

Por lo tanto, cuantitativamente el riesgo es definido mediante la siguiente fórmula:

Riesgo = Probabilidad * Impacto

Sobre la base de los puntos anteriores, a continuación se muestra un ejemplo de Riesgo:

> Mediante los registros de una organización, se ha detectado que en los últimos diez años se han producido cinco principios de incendio. En el caso de que se materialice un incendio, existen activos tecnológicos que pueden ser afectados manifestándose en pérdidas económicas valoradas en $20,000.00 USD.
>
> Para determinar el Riesgo es necesario conocer la probabilidad y el impacto en el caso de que acontezca un incendio.
>
> La probabilidad es la siguiente: 5 incendios/10 años, es decir, el 50%. El impacto es económico, siendo este $20,000.00 USD.
>
> Por lo tanto en el caso de que exista un incendio, aplicando la fórmula anterior tenemos un riesgo económico de $10,000.00 USD.

GESTIÓN DEL RIESGO

Según Connell (1997): La Gestión del Riesgo de un Proyecto **“*es identificar, estudiar y eliminar las fuentes de riesgo antes de que empiecen a amenazar la finalización satisfactoria de un proyecto*”**. Por su parte Galaway (2004)

define la Gestión de riesgos de un proyecto como ***"el arte y la ciencia de identificar, analizar, y responder a los riesgos a lo largo de la vida de un proyecto, con el propósito de lograr los objetivos del proyecto"***.

De los dos conceptos anteriores, para lograr éxito en los proyectos mediante la Gestión del Riesgo, existen tres procesos básicos: identificación, análisis (estudio) y respuesta (manejo) del riesgo.

En la **Identificación del Riesgo** se debe tomar en cuenta las fuentes que pueden incidir en la aparición de los riesgos las cuales pueden afectar a las actividades de los proyectos. Estos factores pueden ser económicos, sociales, de orden público, políticos, legales, cambios tecnológicos, estructura organizacional, sistemas de información, procesos y recursos económicos.

Para la identificación puede utilizarse diferentes fuentes de información de la organización tales como: registros históricos, opiniones de especialistas y expertos, informes de años anteriores, entrevistas, reuniones de trabajo, uso de diagramas de flujo, análisis y revisiones periódicas de factores económicos y tecnológicos, entre otros.

En el **Análisis del Riesgo** el objetivo es establecer una valoración y priorización de los riesgos a base de información obtenida en el proceso de identificación y de esta manera establecer el nivel de riesgo y las acciones que se van a implementar en el siguiente proceso. Para esto la probabilidad de ocurrencia y el impacto son valores necesarios que deben establecerse en escala de valoraciones sean estas cuantitativas o cualitativas.

La **Respuesta o Manejo del Riesgo** se refiere a la toma de decisiones entorno a las salvedades y salvaguardas para minimizar pérdidas. Existen riesgos que pueden ser aceptados y aquellos que no lo son, se los mitigará, transferirá o evitará mediante un análisis costo–beneficio y dentro de los parámetros técnico–legales.

La guía de PMBOK relaciona el concepto de Gestión del Riesgo con los procesos del ciclo de vida de un proyecto. PMBOK establece que existe mayor probabilidad de riesgo en la planificación del proyecto, ya que en esta etapa es en donde se

establece el contexto organizacional y se analiza eventos futuros para gestionarlos. En la etapa de Ejecución del proyecto es en donde se manifiestan mayormente los impactos, los cuales pueden ser representados por pérdidas o salvaguardas económicas, como muestra el siguiente gráfico.

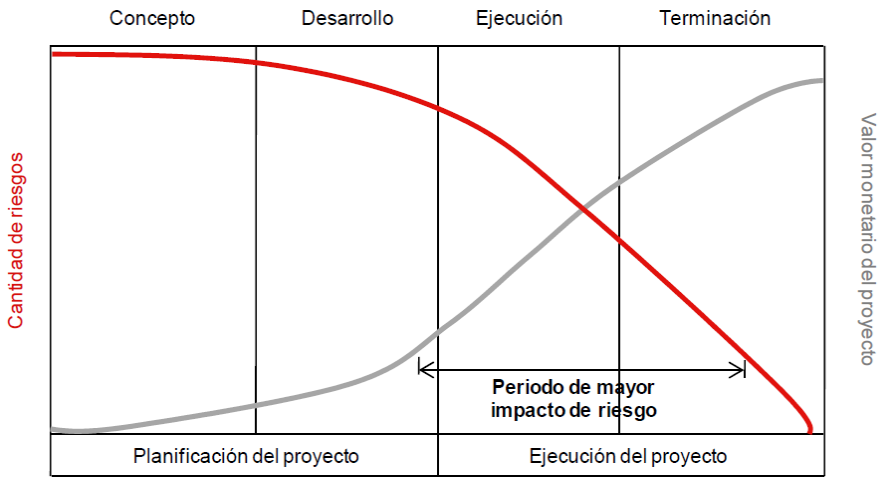


Figura 1. Relación Riesgo - Coste
Fuente: PMI-PMBOK 4th Edición

Tomando como referencia la Figura 1, los proyectos que se planean y ejecutan tienen riesgos, y al gestionarlos de forma proactiva se conseguirán mejores beneficios tanto para la organización como para el proyecto. La gestión del riesgo implica planificación y análisis; identificación y mitigación; control y disminución del impacto de eventos que afecten la ejecución de un proyecto.

Especialistas en el análisis y gestión del riesgo exponen los siguientes factores a tomar en cuenta:

Boehm[3]: problemas con el personal, planificación temporal y presupuestos poco realistas. Ropponen y Lyytinen[4]: mala planificación del tiempo y requerimientos funcionales incorrectos. Jones[5]: métricas inexactas, medición inadecuada (métricas que perturban y ralentizan el proceso) y excesiva presión en la planificación.

[3] Boehm, B. (1991): "Risk management". IEEE Software.

[4] Ropponen y Lyytinen (1993): "Can Software Risk Management Improve System Development: An Exploratory Study". European Journal of Information Systems

[5] Jack A. Jones (2005): "An Introduction to Factor Analysis of Information Risk". Risk Management Insight

1.1.1 GESTION DEL RIESGO: CAUSA - RIESGO - EFECTO

Otros factores que se deben tomar en cuenta para identificar, analizar y gestionar el riesgo es descubrir sus causas. El siguiente concepto proporcionado por por David Hillson (2006) menciona: ***"Debido a una o más causas, podría ocurrir un riesgo, lo que podría llevar a uno o más efectos".*** La guía de PMBOK (Project Management Institute, 4th Edition) indica que ***"Un riesgo puede tener una o más causas y, si sucede, uno o más impactos".***

Los conceptos anteriores contienen tres aspectos a tomar en cuenta, estos son: causas, riesgo y efectos (impactos).

Causas: "Son acontecimientos o circunstancias concretos que existen en el proyecto o su ambiente, y que producen incertidumbre." Ejemplos pueden ser la necesidad de usar una tecnología nueva no probada, la falta de personal especializado, un requisito, un supuesto, una restricción o una condición.

Riesgo: "Son incertidumbres que, si ocurriesen, tendrán un efecto positivo o negativo sobre uno o más objetivos del proyecto". Ejemplos incluyen la posibilidad de que las metas planificadas no se alcancen, dependencia de permisos de otras instituciones, condiciones climáticas, posibilidad de que requerimientos del cliente se entiendan mal, entre otras.

Efectos: "Son variaciones imprevistas en los objetivos del proyecto, que surgirían como consecuencia de que ocurran los riesgos." Ejemplos incluyen prórrogas o ampliaciones de plazo por no alcanzar las metas a tiempo, exceder un presupuesto autorizado o el dejar de alcanzar los objetivos convenidos en el contrato.

En base a lo anterior, para identificar un riesgo es importante analizar las causas que lo pueden producir. Este análisis demanda de revisión histórica, de evaluaciones de eventos anteriores con lo actual, de filtros de datos, entre otros. Estas causas pueden ser medios, circunstancias, factores, personas y condiciones que generan los riesgos.

Una técnica propuesta por Hillson (2006) para identificar causas que pueden producir incertidumbre es utilizando la siguiente frase: **"como resultado de este**

hecho, ¿qué riesgos inciertos podrían presentarse?". Esta técnica puede proporcionar una referencia para desarrollar respuestas adecuadas, asegurando que las acciones logren los resultados deseados de manera eficaz.

A continuación se presenta tres ejemplos que integran las causas, riesgo y efectos:

- En un proyecto en el que como requisito es necesario usar hardware nuevo (causa), errores inesperados en el sistema de integración pueden ocurrir (riesgo), que llevarían a un gasto excesivo en el proyecto (efecto en el presupuesto).

- Una vez que se ha asignado personal limitado para instalar la infraestructura de comunicaciones de un proyecto (causa), la instalación de equipos según la planificación puede ser afectada (riesgo), por lo que puede haber un impacto sobre el cronograma del proyecto (efecto en los plazos)

- Se necesita un permiso gubernamental de frecuencias (causa), si la entidad que otorga el permiso podría tardar más de lo previsto en emitir la autorización (riesgo), puede haber un impacto sobre el coste, el cronograma o el rendimiento del proyecto (efecto).

1.1.2 FUENTES DEL RIESGO

Según INTECO[6] los riesgos en un proyecto pueden tener diversos orígenes y entre las fuentes más típicas se encuentran los siguientes:

Riesgos conocidos, es decir, son riesgos que han sido identificados y analizados, y se puede tomar acciones al respecto. Para este tipo de riesgos el equipo de trabajo generalmente cuenta con planes de contingencia y de reserva para tratar cada riesgo en caso de que ocurriera. Entre estos riesgos está por ejemplo: el

[6] INTECO es un centro de desarrollo de carácter e interés público constituido como medio propio y servicio técnico de la Administración General del Estado Español. Se orienta a la aportación de valor, a la industria, a los usuarios, y a la difusión de las nuevas Tecnologías de la Información y gla Comunicación (TIC). www.inteco.es

aumento en la complejidad en el uso de un sistema de información, rendimiento o agresividad en las fechas de entrega.

En contraste con lo anterior, existen riesgos que pueden ser desconocidos, es decir, no pueden gestionarse de forma proactiva y pueden aparecer de manera imprevista. Una buena práctica para este tipo de riesgo es dejar una reserva de presupuesto y de tiempo por si apareciesen dificultades no esperadas.

Existen riesgos que tienen sus fuentes dentro de la organización y pueden catalogarse como internos. Estos pueden ser controlados por el equipo del proyecto. Por ejemplo la disponibilidad de los recursos y equipos, ambigüedades de contrato, estructura organizacional, niveles salariales, dirección de proyectos, entre otros.

Los riesgos externos, tienen sus fuentes fuera de la organización y no dependen de la gestión del equipo de trabajo. Por ejemplo desastres naturales, situación política del país, cambios constitucionales, inflación, entre otros.

Considerando los puntos anteriores, durante la ejecución de un proyecto Tecnológico existen actividades y eventos en las cuales se deben tomar decisiones, tanto por el responsable como por el resto del equipo (según sus funciones) para identificar, controlar y disminuir el impacto de eventos que afecten al proyecto.

1.1.3 MEJORES PRÁCTICAS: ENFOQUE EN LA GESTIÓN DE RIESGOS

Existen modelos y métodos que gestionan el riesgo, sin embargo, cada una de ellas se especializan en su área de aplicación. Los modelos que conciernen a esta investigación son: CMMI, SPICE, PMBOK, PRINCE2, COBIT, RISK IT, OCTAVE, NIST 800-30 y MAGERIT.

Estas mejores prácticas se caracterizan por lo siguiente:

CMMI (Capability Maturity Model Integration) *y* ***SPICE*** (Software Process Improvement and Capability dEtermination) son modelos orientados a la mejora de procesos y calidad del software, es decir, su ámbito de acción se relaciona con la Ingeniería y el ciclo de vida de un producto de software. Ambos modelos

Gestionan el Riesgo en el área de Proyectos haciendo mayor énfasis a la planificación y control de los proyectos de software. Estos recomiendan a las organizaciones inicialmente centrarse en identificar los riesgos para tener conocimiento de ellos y reaccionar cuando apareciesen.

PMBOK (Project Management Body of Knowledge), *y* ***PRINCE2*** (Projects IN Controlled Environments) son modelos de gestión sobre todo tipos de proyectos, no solamente para sistemas de información sino para otras aplicaciones de la ingeniería, como proyectos de construcción, eléctricos, químicos, educación, mecánicos, entre otros. Estos modelos pueden ser aplicados en su totalidad o utilizar procesos específicos según el tamaño y necesidades del proyecto.

COBIT (Control Objectives for Information and related Technology) y ***RISK IT*** se centran en el cumplimiento de los objetivos de la organización y constituyen un modelo aceptado a nivel mundial en materia de control y seguridad de la información. En conjunto hacen una descripción de las necesidades generales de los procesos, recursos y criterios de información para lograr objetivos de negocio, permitiendo a los ejecutivos de TI cubrir brechas entre los requerimientos de control, los aspectos técnicos y los riesgos de negocio.

A diferencia de los otros modelos que buscan eliminar los riesgos, *RISK IT* considera la posibilidad de tomar e ir en la búsqueda de riesgos que podrían beneficiar a la organización, siempre y cuando se encuentre el balance adecuado entre riesgo y costos.

Para entender el objetivo de RISK IT podemos utilizar el siguiente ejemplo: al momento de ejecutar algún proyecto relacionado con las TICs, es común que los representantes de áreas no informáticas o de tecnología de una organización soliciten que se les indique, como resultado del proyecto ¿Cuál es el nivel de riesgo que deben tomar para poder maximizar sus beneficios? La respuesta a este tipo de cuestionamientos se puede obtener adoptando *RISK IT* como modelo de gestión de riesgos.

Herramientas que analizan y gestionan el riesgo cuando se hacen uso de la tecnología de información son *OCTAVE, NIST 800-30* y *MAGERIT.*

NIST 800-30 Risk Management Guide for Information Technology Systems, es una metodología que analiza y gestiona el riesgo de la seguridad de la información[7]. Su principal característica basa en dividir su metodología en dos grandes procesos: Análisis de Riegos y Gestión de Riesgos. *NIST* cuenta con una serie de publicaciones especiales. La serie 800 se dedica a la seguridad de la información[8].

OCTAVE *(*Operationally Critical Threat, Asset, and Vulnerability Evaluation), al momento de gestionar el riesgo divide los activos en dos grupos: Sistemas (Hardware-Software-Datos) y Personas; por lo que al momento de identificar los riesgos y recursos importantes que afectan a la seguridad.

MAGERIT es una metodología que enfatiza en dividir los activos de la organización en variados grupos para identificar y analizar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente. Para esto *MAGERIT* cuenta con procesos que se encuentran estructurados en tres libros: 1. Método, 2. Catálogo de Elementos y 3. Guía de Técnicas.

MAGERIT cuenta con un producto de software acorde a su metodología denominado “PILAR” (de uso exclusivo en la administración pública española) y se lo puede adquirir o descargar[9] con una licencia de evaluación de 30 días. Cuenta con las versiones para Windows, Linux y Mac OS X.

Existen otras buenas prácticas que gestionan el riesgo, y se encuentran registradas en el ***Anexo A*** de este documento.

H. James Harrington (1993) respecto a la Gestión, sintetiza la importancia de valorar o medir: "la medición es el primer paso para el control y la mejora. Si algo no se puede medir, no se puede entender. Si no se entiende, no se puede controlar. Si no se puede controlar, no se puede mejorar.”

Sin embargo, el proceso de cálculo en nuestro caso para determinar la probabilidad y el impacto del riesgo en muchas ocasiones no es tan sencillo por el

[7] NIST 800-30, página 2

[8] http://csrc.nist.gov/publications/PubsSPs.html

[9] Zona de Descarga (Download): http://www.ar-tools.com/index.html?tools/pilar/index.html

desconocimiento del evento o simplemente porque sus variables de cálculo pertenecen a una ecuación indeterminada y por ende la valoración a realizar es subjetiva. Para estos casos el método recomendado es el *juicio de expertos*, en donde los especialistas en la materia expresan sus opiniones sobre la probabilidad, el impacto y el riesgo total asociado a ese determinado evento. Otras fuentes de información cuando los eventos son desconocidos pueden ser:

- Consultores
- Unidades dentro del proyecto o de la organización
- Interesados, incluyendo clientes, patrocinadores y ejecutores
- Asociaciones o Colegios de profesionales
- Grupos industriales

1.2 MÉTODO PARA DESARROLLAR LA GUIA DE GESTION DE RIESGOS PARA PROYECTOS DE TI

La guía de Gestión de Riesgos se desarrollará mediante un método que identifique los procesos y actividades de las mejores prácticas revisadas anteriormente con el objetivo de conocer ***qué*** hacen para gestionar el riesgo y a la vez conocer ***dónde*** y ***cómo*** aplican la gestión del riesgo en su área de especialidad y seleccionar los elementos de mayor correspondencia con los proyectos que involucran Tecnologías de Información y Comunicaciones.

1.2.1 JUSTIFICACIÓN

- Facilitar a las instituciones a través del análisis del riesgo el cumplimiento de los objetivos de los proyectos de TI, partiendo de la base del control estatal, de su razón de ser y de su compromiso con la sociedad.
- Mediante una Guía de Gestión de Riesgos de TI, gestionar los proyectos de forma proactiva y cumplir con los objetivos esperados tanto por contratantes y contratistas.

- Es necesario una Guía sistemática de Gestión de Riesgos de TI por los proyectos que ha impulsado el Gobierno del Ecuador según el Plan Nacional para el Buen Vivir 2009 – 2013.

1.2.2 OBJETIVOS

Objetivo General:

- Desarrollar y aplicar una guía de Gestión de Riesgos de TI mediante el análisis de metodologías y procesos de control generalmente aceptados a un proyecto que incorpora tecnologías de información y comunicaciones.

Objetivos Específicos:

- Identificar y seleccionar los procesos de las mejores prácticas que Gestionan el Riesgo mediante una evaluación de correspondencia con Proyectos de TI.
- Desarrollar una Guía de Gestión del Riesgo para Proyectos de alcance nacional que incorporan Tecnologías de Información y la Comunicación como aporte a la administración pública del estado ecuatoriano.
- Aplicar la guía propuesta y realizar el Análisis de Gestión del Riesgo al Proyecto del Mejoramiento de la Calidad de la Educación “Plan Amanecer”.

1.2.3 FASES DEL MÉTODO

El método se estructura en 5 fases y servirá para desarrollar la Guía de Gestión de Riesgos. Las fases son las siguientes:

1. **Disgregación:** Descomponer los modelos, metodologías y técnicas para determinar la característica[10] o características encargadas de la Gestión del Riesgo.
2. **Identificación:** Identificar los procesos y actividades encargadas de la Gestión de Riesgos para someterlos a evaluación.

[10] Característica: Se refiere a la Fase, Área, Dominio, Grupo o Macro-Proceso según denomine o nombre la Mejor Práctica.

3. **Evaluación:** Realizar una comparación y asignación cuantitativa y cualitativa de las actividades identificadas, bajo una escala de valoración con el objetivo de mostrar y estimar un nivel de correspondencia con los proyectos de TI.

4. **Selección:** Una vez obtenida la información de los resultados de la evaluación, se escogerá las actividades de mayor correspondencia (las que se encuentren dentro del rango de satisfacción de la escala de valoración) para integrarlos y crear un marco global para la Gestión de Riesgos para proyectos que incorporan TI.

5. **Definición:** Presentar la Guía de Gestión de Riesgos correspondientes a proyectos que involucran Tecnologías de Información y Comunicaciones.

Cada fase contará con entradas y salidas definidas, las cuales interactúan sistemáticamente produciendo resultados o información que será documentada. El proceso para desarrollar la guía se muestra a continuación:

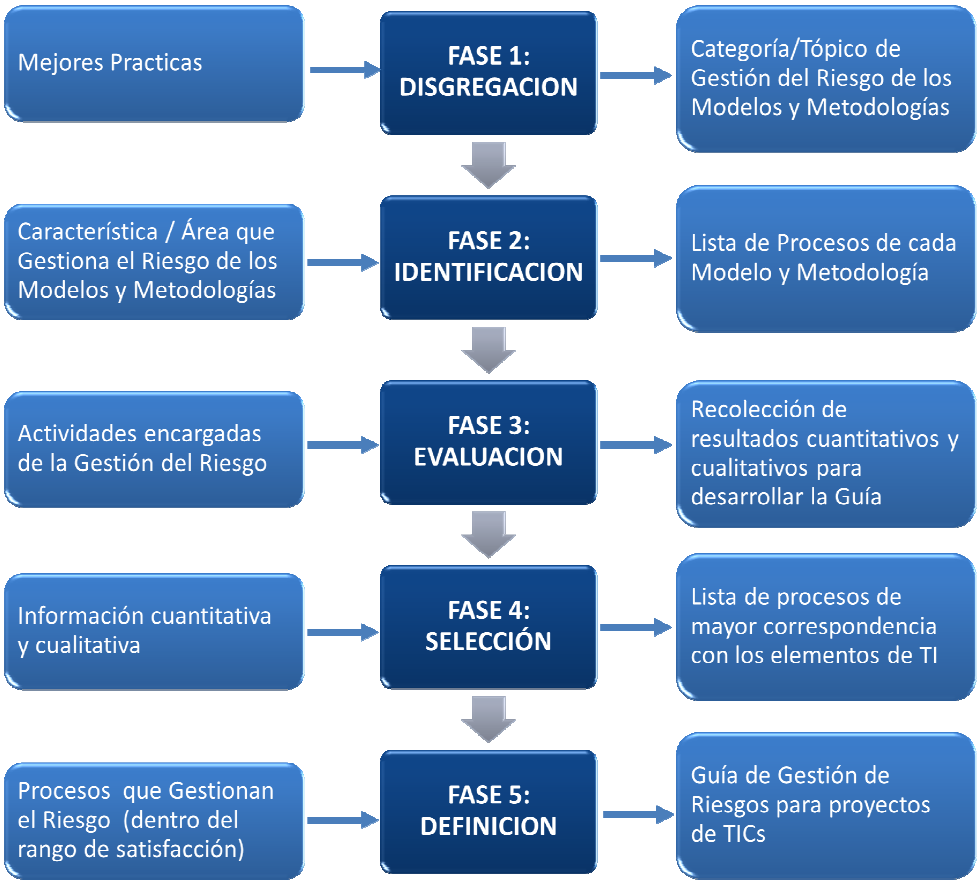


Figura 2. Proceso de Análisis para desarrollar la Guía de Gestión de Riesgos de TI

Como se puede observar en la figura anterior, el proceso inicia seleccionando las mejores prácticas segmentando el estudio al riesgo y a la identificación de procesos que se alinean con los proyectos de TI. Mediante un proceso de evaluación y análisis de resultados se definirá la guía por medio de un marco global a base de procesos y actividades.

Esto permitirá que la Guía de Gestión de Riesgos, objeto de esta investigación, tenga las siguientes características:

- Basada en estándares y mejores prácticas.
- Orientada a la ejecución de Proyectos de Tecnologías de Información y Comunicaciones
- Aplicable a diferentes entornos y proyectos de TI.

En la siguiente Tabla se presenta las mejores prácticas que servirán de base para desarrollar la guía:

MEJOR PRACTICA	DESCRIPCIÓN	ORGANIZACIÓN	PAIS
CMMI	Capability Maturity Model Integration	SEI (Software Engineering Institute)	Estados Unidos de América
SPICE	Software Process Improvement and Capability dEtermination	ISO (International Organization for Standardization)	Internacional (Suiza)
PMBOK	Project Management BOdy of Knowledge	PMI (Project Management Institute)	Estados Unidos de América
PRINCE2	Projects IN Controlled Environments	OGC (Office of Government Commerce)	Reino Unido
COBIT	Control OBjectives for Information and related Technology	ISACA (Information Systems Audit and Control Association) & ITGI (IT Governance Institute)	Estados Unidos de América
RISK IT	Risk IT Model	ISACA (Information Systems Audit and Control Association)	Estados Unidos de América
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Carnegie Mellon SEI (Software Engineering Institute) y CERT (Computer Emergency Response Team)	Estados Unidos de América
NIST 800-30	Risk Management Guide for Information Technology Systems	NIST (National Institute of Standards and Technology)	Estados Unidos de América
MAGERIT	Metodología de Análisis y GEstión de Riesgos de IT	MAP (Ministerio de Administraciones Públicas)	España

Tabla 1. Mejores Prácticas que Gestionan el Riesgo

1.2.4 ELEMENTOS DE TI Y ESCALA DE VALORACIÓN

Los elementos de TI a considerarse para desarrollar la guía, siguiendo las recomendaciones de las mejores prácticas y de los expertos, son los siguientes:

- Hardware [HW]
- Software [SW]
- Bases de Datos [BD]
- Redes y Telecomunicaciones [COM]
- Recurso Humano [RH]
- Legal [L]
- Financiero [F]
- Servicios [S]

En la siguiente tabla se describe cada elemento de TI a ser considerado para realizar la evaluación y el análisis de los procesos que Gestionan el Riesgo de las Mejores Prácticas.

ID	ELEMENTO DE TI	DESCRIPCION
HW	Hardware	Equipos informáticos. Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. También se incluyen dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo. Pueden ser o no portátiles. Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
SW	Software	Con varias denominaciones (programas, aplicativos, desarrollos, etc.) se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. NOTA: El denominado “código fuente” o programas que serán datos de interés comercial a valorar y proteger como tales, serán considerado como datos.
BD	Bases de Datos	Elementos de datos, información que, de forma singular o agrupada representan el conocimiento que se tiene de algo. Almacenados en equipos o soportes de información. Pueden ser transferidos de un lugar a otro por los medios de transmisión de datos. Informes, líneas de texto denominados código fuente (Source code, code base) escrito en un lenguaje de programación específico.

ID	ELEMENTO DE TI	DESCRIPCION
COM	Redes y Telecomunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
RH	Recurso Humano	Personas relacionadas con los sistemas de información. Equipo de TI. Usuarios Internos y externos. Operadores, Administradores.
L	Legal	Contratos, Licenciamiento, Derechos de Autor. Ley de Trabajo (Contratación de Personal), Ley de Servicio de Rentas Internas (Impuestos). Seguridad de la información. Normativa de la Información.
F	Financiero	Procesos involucrados en estimar, presupuestar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado. También involucra procesos de estimación y control en cuanto a entrega y recepción de productos (bienes y servicios).
S	Servicios	Función que satisface una necesidad de los usuarios. Servicios de información, servicios de comunicaciones, servicios de seguridad, servicios de capacitación. Servicios requeridos para el eficaz desempeño de la misión del proyecto/ organización.

Tabla 2. Elementos de TI

Para identificar el nivel de aceptación se plantea una escala cuantitativa y cualitativa dividida en cuatro rangos diferenciando el nivel de satisfacción.

Los datos **cualitativos** los denominamos ***Niveles de Puntuación (NP)*** y los datos **cuantitativos** decimos que se encuentran dentro de una ***Escala de Medición (EM)***.

A momento de seleccionar las actividades con mayor correspondencia, se ha determinado dos rangos de cumplimiento, es decir, **Satisfactorio (S)** e **Insatisfactorio (I)**.

A continuación se detalla la escala de valoración propuesta más los íconos de representación condicional:

ID	NIVEL DE PUNTUACION (NP)	ESCALA DE MEDICION (EM)	DESCRIPCION DE ALCANCE	RANGO DE SELECCIÓN	ÍCONOS DEL RANGO DE SELECCIÓN
N	NO CUMPLE	EM>=0 Y EM <0.5	Indica que existe poca o nula correspondencia con el elemento de TI evaluado.	INSATISFACTORIO (I)	
P	PARCIAL	EM>=0.5 Y EM <0.75	Muestra que existe aproximación pero algunas de las características con el elemento de TI no se dan.		
A	ADECUADO	EM>=0.75 Y EM <1	El proceso alcanza correspondencia con el elemento de TI evaluado pero difiere o requiere algún aspecto.	SATISFACTORIO (S)	
C	CUMPLE	EM=1	Existe evidencia de que el proceso evaluado alcanza completamente o supera el nivel de correspondencia.		

Tabla 3. Escala de Valoración

La herramienta para tabular, calcular e integrar las funciones lógicas de los datos recolectados serán hojas electrónicas (Microsoft Excel V.2010). Esta técnica nos permitirá la representación condicional (íconos de los niveles alcanzados) y también incorporar gráficos de la información para realizar un análisis integral de los resultados obtenidos y seleccionar los procesos para desarrollar la Guía.

En el nivel de puntuación **“No Cumple”**, abarca dos íconos de representación el cual considera que pueden existir valores igual a cero representados con el ícono vacío “ ”. De la misma manera existen dos íconos que representan el rango de selección **“Insatisfactorio”** puesto que este tiene dos puntuaciones que puede alcanzar siendo estos “no cumple” o “parcial.”

CAPITULO 2

GUIA DE GESTION DE RIESGOS PARA PROYECTOS DE TI

Para definir la guía, se lo realizará utilizando el método descrito en el punto 1.2 de esta investigación y que consta de cinco fases: Disgregación, Identificación, Evaluación, Selección y Definición.

Los modelos considerados y que servirán de base para desarrollar la guía son: CMMI, SPICE, PMBOK, PRINCE2, COBIT, RISK IT, OCTAVE, NIST 800-30 y MAGERIT.

Las entidades de evaluación para el análisis y/o comparación de resultados serán los elementos de TI considerados en la Tabla 2, siendo estos: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones, Recurso Humano, legal, Financiero y Servicios.

Para analizar los procesos que gestionan el riesgo de las mejores prácticas y determinar el nivel de correspondencia para desarrollar la guía se utilizará la escala de valoración de la Tabla 3.

Finalmente se presentará la guía de Gestión del Riesgo detallando los procesos y las actividades mediante productos de entrada, productos de salida, técnicas, prácticas y participantes responsables.

2.1 EJECUCION DEL MÉTODO

2.1.1 FASE 1: DISGREGACIÓN

Esta primera fase se encargará de descomponer las mejores prácticas para determinar la característica o características encargadas de la Gestión del Riesgo.

Los objetivos que persigue esta fase son:

a.) Enfocar el análisis en la Gestión del Riesgo.

b.) Seleccionar las características específicas encargadas de la Gestión del Riesgo.

La siguiente tabla, muestra un resumen de las mejores prácticas a analizar:

MODELOS			METODOLOGÍAS GESTION DE RIESGOS
PROCESOS Y CALIDAD	GESTION DE PROYECTOS	ALINEACION CON LA ORGANIZACIÓN	OCTAVE
CMMI	PMBOK	COBIT	NIST 800-30
SPICE	PRINCE2	RISK IT	MAGERIT

Tabla 4. Mejores Prácticas sometidas a Análisis para desarrollar la Guía de Gestión de Riesgos TI

Como se puede apreciar en la Tabla 4, se tiene un conjunto de mejores prácticas con diferentes áreas de conocimiento y características encargadas de la Gestión del Riesgo.

Por la diversidad de mejores prácticas, y con el fin de ser específicos, la ***Categoría*** puede ser el tópico, tema o capítulo. Mientras que la ***Característica*** se refiere a la Fase, Dominio, Grupo o Macro-Proceso según denomine el Modelo o la Metodología.

En la siguiente tabla se presenta los resultados de la Fase 1: Disgregación, de los modelos y las metodologías que son parte de esta investigación:

MEJOR PRACTICA	CATEGORÍA	CARACTERISTICA / AREA QUE GESTIONA EL RIEGO
CMMI	Gestión de Proyecto	RSKM- Gestión de Riesgos
SPICE	Procesos de Proyecto	MAN.5 Gestión de Riesgos
PMBOK	Gestión de un proyecto	Gestión de los Riesgos del Proyecto
PRINCE2	Temática	Gestión del riesgo
COBIT	Administración de Riesgos	• Planificar y Organizar (PO) • Entrega y Soporte (DS) • Mantener y Evaluar (ME)

MEJOR PRACTICA	CATEGORÍA	CARACTERISTICA / AREA QUE GESTIONA EL RIEGO
RISK IT	Dominio	1. Gobierno del riesgo (RG) 2. Evaluación de riesgo (RE) 3. Respuesta de riesgo (RR)
OCTAVE	Fase	1. Visión de la organización 2. Visión tecnológica 3. Planificación de las medidas y reducción de los riesgos
NIST 800-30	Proceso	1. Análisis de Riegos 2. Gestión de Riesgos
MAGERIT	Proyecto AGR (Análisis y Gestión de Riesgos)	Análisis y Gestión de Riesgos
TECNICAS[11]	Valoración	Cualitativa Cuantitativa

Tabla 5. Resultados Fase I: Disgregación - Característica/Área que Gestiona el Riesgo

2.1.2 FASE 2: IDENTIFICACIÓN

Sobre los resultados obtenidos en la Fase anterior, los objetivos que persigue esta Fase son los siguientes:

a.) Identificar los procesos encargados de la Gestión del Riesgo.

b.) Especificar las actividades y estrategias para Gestionar el Riesgo.

La siguiente tabla muestra las actividades que utilizan las mejores prácticas para Gestionar el Riesgo:

[11] La técnica a utilizarse en esta investigación es matemática/lógica, ésta permitirá determinar un valor esperado o estimado de las actividades que Gestionan el Riesgo.

MEJOR PRACTICA	CARACTERISTICA / AREA QUE GESTIONA EL RIEGO	OBJETIVOS / PROCESOS	ACTIVIDADES
CMMI	RSKM- Gestión de Riesgos	Definir una estrategia de gestión de riesgos, identificar y analizar los riesgos, manejar los riesgos identificados, incluyendo la implementación de planes de mitigación cuando sea necesario	**SG1 Prepararse para una gestión de riesgos** 1.1 Determinar recursos y categorías 1.2 Definir parámetros de riesgos 1.3 Establecer una estrategia de gestión de riesgos **SG2 Identificar y analizar los riesgos** 2.1 Identificar los riesgos 2.2 Evaluar, categorizar y priorizar riesgos **SG 3 Mitigar riesgos** 3.1 Desarrollar planes de mitigación de riesgos 3.2 Implementar planes de mitigación de riesgos
SPICE	MAN.5 Gestión de Riesgos	Identificar, analizar, tratar y monitorizar los riesgos de forma continua de un proyecto a lo largo de todo su ciclo de vida	5.1 Establecer el alcance de la gestión de riesgos 5.2 Definir estrategias de gestión de riesgos 5.3 Identificar riesgos 5.4 Analizar riesgos 5.5 Definir y realizar acciones de tratamiento de riesgos 5.6 Monitorizar los riesgos 5.7 Tomar acciones preventivas o correctivas
PMBOK	Gestión de los Riesgos del Proyecto	Describe los procesos involucrados en la identificación, análisis y control de los riesgos para el proyecto.	1. Planificar la Gestión de Riesgos 2. Identificar los Riesgos 3. Realizar Análisis Cualitativo de Riesgos 4. Realizar Análisis Cuantitativo de Riesgos 5. Planificar la Respuesta a los Riesgos 6. Dar seguimiento y Controlar los Riesgos

MEJOR PRACTICA	CARACTERISTICA / AREA QUE GESTIONA EL RIEGO	OBJETIVOS / PROCESOS	ACTIVIDADES
PRINCE2	Gestión del Riesgo	Análisis del riesgo y definición de estrategias para afrontarlo.	1. Identificar los Riesgos 2. Evaluar los Riesgos 3. Identificar los riesgos 4. Seleccionar/Respuesta a los Riesgos 5. Plan y Recursos 6. Monitorear / Comunicar
COBIT	• Planificar y Organizar (PO) • Adquirir e Implementar (AI) • Entrega y Soporte (DS) • Mantener y Evaluar (ME)	PO9. Evaluar y administrar riesgos de TI AI6. Administrar Cambios DS5. Asegurar la seguridad de los sistemas ME4. Proporcionar Gobierno de TI	1. Determinar la alineación de la administración de Riesgos 2. Entender los objetivos de negocio estratégicos relevantes 3. Entender los objetivos de los procesos de negocio relevantes 4. Identificar los objetivos internos de TI y establecer el contexto del riesgo 5. Identificar eventos asociados con objetivos 6. Asesorar el riesgo con los eventos 7. Evaluar y seleccionar respuestas a riesgos 8. Priorizar y planificar las actividades de control 9. Aprobar y garantizar la financiación de los planes de acción 10. Mantener y monitorizar el plan de acción de riesgos
RISK IT	1. Gobierno del riesgo (RG) 2. Evaluación de riesgo (RE) 3. Respuesta de riesgo (RR)	RG1 Establecer y mantener una vista de riesgo común. RG2 Integrar con ERM. RG3 Tomar decisiones conscientes de los riesgos del negocio. RE1 Recoger datos. RE2 Analizar los riesgos. RE3 Mantener perfil de riesgo. RR1 Riesgo articulado RR2 Manejar riesgos RR3 Reaccionar a acontecimientos	1. Definición de un universo de riesgos y ámbito de gestión de riesgo. 2. Apetito de riesgo y tolerancia al riesgo 3.Conciencia del riesgo, Comunicación y presentación de informes 4. Expresando y describiendo el riesgo 5. Escenarios de riesgo 6. Riesgo de respuesta y asignación de prioridades 7.Un flujo de trabajo de Análisis de Riesgo 8. Mitigación de Riesgos de TI Uso de COBIT y Val IT

MEJOR PRACTICA	CARACTERISTICA / AREA QUE GESTIONA EL RIEGO	OBJETIVOS / PROCESOS	ACTIVIDADES
OCTAVE	1. Visión de la organización 2. Visión tecnológica 3. Planificación de las medidas y reducción de los riesgos	Identificar los recursos importantes mediante encuestas y entrevistas. Realizar actividades de análisis de riesgo. Relacionar amenazas y vulnerabilidades. Crear estrategias de protección, planes de mitigación y diseñar políticas de seguridad.	1. Identificar la información (Gerencial-Operacional-Usuario Final) 2. Consolidar la Información y crear perfiles de amenaza 3. Identificación de componentes claves 4. Evaluación de componentes seleccionados 5. Análisis de riesgos de los recursos críticos 6. Desarrollo de estrategias de protección
NIST 800-30	1. Análisis de Riegos 2. Gestión de Riesgos	Análisis y Gestión de Riesgos de la seguridad de la Información, proporcionando controles de seguridad a un coste efectivo.	**1. Análisis** 1.1 Caracterización del sistema 1.2 Identificación de amenazas 1.3 Identificación de vulnerabilidades 1.4 Análisis de control Paso 1.5 Determinación de la probabilidad 1.6 Análisis de impacto 1.7 Determinación de riesgo 1.8 Recomendaciones de control 1.9 Documentación de resultados **2. Gestión** 2.1 Priorización de Acciones 2.2 Evaluación de Acciones de controles recomendados 2.3 Análisis Costo-Beneficio 2.4 Selección de Controles 2.5 Asignación de Responsabilidades 2.6 Desarrollo de plan de implantación de salvaguardas 2.7 Implantación de Controles seleccionados

MEJOR PRACTICA	CARACTERISTICA / AREA QUE GESTIONA EL RIEGO	OBJETIVOS / PROCESOS	ACTIVIDADES
MAGERIT	Análisis y Gestión de Riesgos	Para el Proyecto (Planificación): Formalizar las acciones a realizar a lo largo de un proyecto para ejecutar el Análisis y Gestión de Riesgos, estableciendo un marco normalizado de desarrollo. Para el Análisis: Determinar qué tiene la Organización y estimar lo que podría pasar. Para la Gestión: organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y a tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; haciendo que el riesgo llegue a un nivel residual que la Dirección asume.	**1. Planificación** 1.1 Estudio de oportunidad 1.2 Determinación del alcance del proyecto 1.3 Planificación del proyecto 1.4 Lanzamiento del proyecto **2. Análisis de riesgos** 2.1 Caracterización de los activos 2.2 Caracterización de las amenazas 2.3 Caracterización de las salvaguardas 2.4 Estimación del estado de riesgo **3. Gestión de riesgos** 3.1 Toma de decisiones 3.2 Plan de seguridad 3.3 Ejecución del plan

Tabla 6. Resultados Fase II: Identificación - Actividades que Gestionan el Riesgo

2.1.3 FASE 3: EVALUACIÓN

Una vez que las actividades que Gestionan el Riesgo han sido identificadas en la Fase anterior, los objetivos de la Fase de Evaluación son:

a) Efectuar un análisis integral de los procesos y de las actividades identificadas.

b) Realizar una asignación cuantitativa y cualitativa de las actividades de las mejores prácticas que gestionan el Riesgo.

c) Estimar un nivel de correspondencia con los elementos de TI.

d) Analizar los resultados obtenidos.

El campo ID de las tablas de estimación fueron definidas por el autor para facilidad de análisis en la siguiente fase.

2.1.3.1 CMMI

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
CM1.1	Determinar recursos y categorías	0.5	1	1	0.5	0	0	0.5	0.75	**0.53**	P	◑	I	🟡
CM1.2	Definir parámetros de riesgos	0.5	1	1	0.75	0.75	0	0	0.5	**0.56**	P	◑	I	🟡
CM1.3	Establecer una estrategia de gestión de riesgos	0.75	1	1	0.75	0.75	0.5	0.5	0.75	**0.75**	A	◕	S	🟢
CM2.1	Identificar los riesgos	0.5	1	1	0.5	0	0	0.5	0.75	**0.53**	P	◑	I	🟡
CM2.2	Evaluar, categorizar y priorizar riesgos	0.75	0.75	0.75	0.5	0.5	0	0	0.5	**0.47**	N	◔	I	🔴
CM3.1	Desarrollar planes de mitigación de riesgos	0.75	1	1	0.5	1	0.5	0.75	1	**0.81**	A	◕	S	🟢
CM3.2	Implementar planes de mitigación de riesgos	0.75	1	1	0.5	0.5	0	0.75	0.75	**0.66**	P	◑	I	🟡
	SUMA TOTAL DE VALORES ASIGNADOS	4.5	6.75	6.75	4	3.5	1	3	5	**4.31**	N/A	N/A	N/A	N/A
	NUMERO TOTAL DE ACTIVIDADES	7	7	7	7	7	7	7	7	7	N/A	N/A	N/A	N/A
	ESCALA DE MEDICION (EM)	**0.64**	**0.96**	**0.96**	**0.57**	**0.50**	**0.14**	**0.43**	**0.71**	0.62	P	◑	I	🟡
	NIVEL DE PUNTUACION (NP)	P	A	A	P	P	N	N	P					
		◑	◕	◕	◑	◑	○	◔	◑					
	RANGO DE SELECCIÓN	I	S	S	I	I	I	I	I					
		🟡	🟢	🟢	🟡	🟡	🔴	🔴	🟡					

Tabla 7. CMMI – Evaluación de Actividades que Gestionan el Riego

En cuanto a las actividades que gestionan el riesgo, CMMI se destaca en establecer una estrategia de Gestión de Riesgos y desarrollar planes que mitiguen esos riesgos. A nivel de elementos de TI alcanza un nivel adecuado de correspondencia con los Proyectos tanto en Software como en Bases de Datos (manejo de la información). Esto se debe ya que cada riesgo en el proceso de desarrollo, adquisición y mantenimiento de productos de software dispone de un registro que brinda información de la madurez alcanzada, su nombre y descripción; muestra su localización temporal a través de la fecha en la que fue documentado y las fases en las que el riesgo es susceptible de dispararse.

En la parte legal y manejo de Finanzas cuando CMMI trata de gestionar el riesgo en los proyectos, existe poca correspondencia puesto que en estas áreas el control y seguimiento de tareas se categorizan y priorizan enfocándose en el producto más no en el riesgo.

En la administración del Recurso Humano y Servicios, las tareas de estos dos elementos se enfocan en preparar a la gente en el área de desarrollo de software y prestación de funcionalidades, es decir, se enfocan en cómo el personal se tiene que comunicar, cómo tiene que pasar la información y producto terminado y quienes se encargan de la operación y mantenimiento, pero el riesgo como tal se lo gestiona según el nivel de madurez alcanzado.

El Modelo CMMI respecto a la Gestión del Riesgo, destaca sus procesos en la Gestión de Desarrollo de Software y Manejo de Información. En todo el proceso de producción del software se planifica y se documenta el riesgo en base a los requerimientos y explica cómo se pasa por la arquitectura, cómo se desarrolla, se construye, se prueba y se coloca en producción un producto.

2.1.3.2 SPICE

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
SP5.1	Establecer el alcance de la gestión de riesgos	0.5	1	0.75	0.5	0.5	0.5	1	0.75	**0.69**	P	◑	I	
SP5.2	Definir estrategias de gestión de riesgos	0.5	1	0.75	0.5	0.75	0	0.75	0.75	**0.63**	P	◑	I	
SP5.3	Identificar riesgos	1	1	1	0.75	0.5	0.5	0.75	1	**0.81**	A	◕	S	
SP5.4	Analizar riesgos	0.5	0.75	0.75	0.5	0.5	0	0.75	0.75	**0.56**	P	◑	I	
SP5.5	Definir y realizar acciones de tratamiento de riesgos	0.5	0.75	0.75	0.5	0.5	0.5	0.75	0.75	**0.63**	P	◑	I	
SP5.6	Monitorizar los riesgos	0.5	0.75	1	0.5	0.5	0.5	0.5	1	**0.66**	P	◑	I	
SP5.7	Tomar acciones preventivas o correctivas	0.5	0.75	1	0.5	0.5	0.5	0.75	0.75	**0.66**	P	◑	I	
	SUMA TOTAL DE VALORES ASIGNADOS	**4**	**6**	**6**	**3.75**	**3.75**	**2.5**	**5.25**	**5.75**	**4.63**	N/A	N/A	N/A	N/A
	NUMERO TOTAL DE ACTIVIDADES	7	7	7	7	7	7	7	7	7	N/A	N/A	N/A	N/A
	ESCALA DE MEDICION (EM)	**0.57**	**0.86**	**0.86**	**0.54**	**0.54**	**0.36**	**0.75**	**0.82**	0.66	P	◑	I	
	NIVEL DE PUNTUACION (NP)	P	A	A	P	P	N	A	A					
		◑	◕	◕	◑	◑	◔	◕	◕					
	RANGO DE SELECCIÓN	I	S	S	I	I	I	S	S					
		●	●	●	●	●	●	●	●					

Tabla 8. SPICE – Evaluación de Actividades que Gestionan el Riego

A nivel de actividad, SPICE, es un modelo que se enfoca en la identificación de riesgos tecnológicos basados en el proceso de ciclo de vida del software. Sin embargo, deja de lado elementos de vital importancia dentro de los proyectos como son el tema Legal y de Recurso Humano (Licenciamiento, Derechos de Autor y Contratación de Personal).

Podemos destacar que CMMI por su modelo de capacidad de procesos y guía para la mejora, respecto a la gestión del riesgo en los proyectos, confiere una estructura abierta y de seguimiento para cumplir con los servicios y con los requisitos de usuario e incluir procesos involucrados en estimar, presupuestar y controlar los costos.

Al momento de Gestionar el Riesgo, elementos de TI como el Hardware y las Redes & Telecomunicaciones alcanzan niveles parciales, sin embargo hay que destacar que se alcanza valores superiores al 50%, y esto es, dado que al momento de desarrollar un producto la arquitectura tecnológica es analizada para establecer un alcance acorde a las necesidades.

2.1.3.3 PMBOK

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
PB1.0	Planificar la Gestión de Riesgos	0.5	0.5	0.5	0.5	0.75	0	1	0.75	**0.56**	P	◑	I	🟡
PB2.0	Identificar los Riesgos	0.5	0.5	0.75	0.5	0.75	0	0.75	0.5	**0.53**	P	◑	I	🟡
PB3.0	Realizar Análisis Cualitativo de Riesgos	0.5	0.5	0.5	0.5	0.75	0	0.75	0.5	**0.50**	P	◑	I	🟡
PB4.0	Realizar Análisis Cuantitativo de Riesgos	0.5	0.5	0.5	0.5	0.75	0	0.75	0.5	**0.50**	P	◑	I	🟡
PB5.0	Planificar la Respuesta a los Riesgos	0.5	0.5	0.75	0.5	1	0	0.75	0.75	**0.59**	P	◑	I	🟡
PB6.0	Dar seguimiento y Controlar los Riesgos	0.5	0.5	0.5	0.5	1	0	0.75	0.5	**0.53**	P	◑	I	🟡
	SUMA TOTAL DE VALORES ASIGNADOS	**3**	**3**	**3.5**	**3**	**5**	**0**	**4.75**	**3.5**	**3.22**	N/A	N/A	N/A	N/A
	NUMERO TOTAL DE ACTIVIDADES	6	6	6	6	6	6	6	6	6	N/A	N/A	N/A	N/A
	ESCALA DE MEDICION (EM)	**0.50**	**0.50**	**0.58**	**0.50**	**0.83**	**0.00**	**0.79**	**0.58**	0.54	P	◑	I	🟡
	NIVEL DE PUNTUACION (NP)	P ◑	P ◑	P ◑	P ◑	A ◕	N ○	A ◕	P ◑					
	RANGO DE SELECCIÓN	I 🟡	I 🟡	I 🟡	I 🟡	S 🟢	I 🔴	S 🟢	I 🟡					

Tabla 9. PMBOK – Evaluación de Actividades que Gestionan el Riego

Una vez realizada la evaluación de este modelo de Administración de Proyectos, podemos destacar la actividad de *Planificación* que PMBOK propone al momento de Gestionar los Riesgos. Esta actividad estipula varios principios de la Gestión de Finanzas, Cronograma y de Recursos con el objetivo de finalizar el proyecto a tiempo. Sin embargo, dado que PMBOK es un modelo de gestión de todo tipo de proyectos, éste únicamente se relaciona con los Elementos de TI al momento de definir las *"Categorías de Proyecto",* las cuales las divide en: técnicos, externos, organizacional y de proyecto; dejando de lado un tema importante como el Legal.

Otra cualidad que podemos enfatizar de este modelo al momento de Gestionar el Riesgo es que propone Técnicas, Herramientas y la asignación de Responsabilidades del Recurso Humano para cada actividad, todo esto mediante un registro de riesgos para análisis, periodicidad de revisiones y si es el caso optar por una estrategia con el fin de dar respuesta inmediata a los impactos sobre los objetivos del proyecto.

El uso de Técnicas y Herramientas que el modelo plantea es una buena guía para los profesionales de TI, como por ejemplo: la Definición de Escalas de Impacto en función de los Objetivos del Proyecto, la Matriz probabilidad e impacto, acuerdo de formatos de informes, documentación de los procesos de gestión de riesgos, listas de control, técnicas de diagramación, distribuciones de probabilidad. Todas estas definidas en la Sección 11 de la guía de PMBOK.

Conviene mencionar que para todas las actividades que Gestionan el Riesgo de PMBOK, el juicio de expertos es significativo y deja abierta esta opción para actuar sobre riesgos específicos, en donde la experiencia relevante de un grupo o persona con conocimientos concretos pueden determinar el uso de técnicas y herramientas así como el manejo de datos. Todo esto en un marco de parcialidad de los expertos en este proceso.

2.1.3.4 PRINCE2

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
PC1.0	Identificar los Riesgos	0.5	0.5	0.5	0.5	0.75	0.5	0	0.75	**0.50**	P	◑	I	🟡
PC2.0	Evaluar los Riesgos	0.5	0.5	0.5	0.5	0.75	0	0	0.75	**0.44**	N	◔	I	🔴
PC3.0	Identificar los riesgos	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75	**0.53**	P	◑	I	🟡
PC4.0	Seleccionar/Respuesta a los Riesgos	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75	**0.53**	P	◑	I	🟡
PC5.0	Plan y Recursos	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75	**0.53**	P	◑	I	🟡
PC6.0	Monitorear / Comunicar	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75	**0.53**	P	◑	I	🟡
SUMA TOTAL DE VALORES ASIGNADOS		**3**	**3**	**3**	**3**	**3.5**	**2.5**	**2**	**4.5**	**3.06**	N/A	N/A	N/A	N/A
NUMERO TOTAL DE ACTIVIDADES		6	6	6	6	6	6	6	6	6	N/A	N/A	N/A	N/A
ESCALA DE MEDICION (EM)		**0.50**	**0.50**	**0.50**	**0.50**	**0.58**	**0.42**	**0.33**	**0.75**	**0.51**	P	◑	I	🟡
NIVEL DE PUNTUACION (NP)		P ◑	P ◑	P ◑	P ◑	P ◑	N ◔	N ◔	A ◕					
RANGO DE SELECCIÓN		I 🟡	I 🟡	I 🟡	I 🟡	I 🟡	I 🔴	I 🔴	S 🟢					

Tabla 10. PRINCE2 – Evaluación de Actividades que Gestionan el Riego

La estrategia de Gestión del riesgo que PRINCE2 transmite para ejecutar los proyectos es minimizar la incertidumbre, para esto y como objeto de nuestro

estudio en cuanto a los Elementos de TI, este modelo proporciona la generación del Product Breakdown Structure[12] (PBS), que básicamente es una estructura jerárquica de los componentes del producto a entregar.

Sin embargo, dado que PRINCE2 es un modelo de Gestión para cualquier tipo de Proyectos, el PBS es una herramienta que puede reducirse o ampliarse en función de las necesidades o experiencia del ejecutor. Esta característica es importante para incursionar en nuevas técnicas de análisis, pero negativa en cuanto a su generalidad ya que se pueden perder o no tomar en cuenta elementos neurálgicos al momento de desarrollar, adquirir, implantar o construir productos dentro de un Proyecto de TI.

Lo que podemos destacar de PRINCE2 en su doctrina de gestión de proyectos, es que el tema de la calidad de los productos al momento de su entrega es fundamental, todo esto bajo un esquema de una buena dirección y planificación. Así mismo cuenta con una serie de plantillas de documentación y registro para futuras revisiones y mejoramiento continuo de los bienes y servicios que van desde la iniciación del proyecto hasta su cierre.

Respecto a la correspondencia de los elementos de TI: Legal y Financiero, PRINCE2 desfallece porque es implícito al momento de determinar las técnicas de análisis financiero o presupuestario así como dar pautas en cuanto al manejo y control de contratos.

En cuanto a la Actividad PC2.0 de Gestión del Riesgo, *Evaluar*, PRINCE2 no especifica las técnicas a ejecutarse o si estas pueden ser cualitativas o cuantitativas. PRINCE2 deja a libertar del ejecutor o director de proyecto utilizar técnicas o herramientas para este proceso.

Una de las principales bondades que PRINCE2 presenta es el proceso continuo de Gestión del Riesgo en todas las fases del proyecto, expresado en la actividad Monitorear/Comunicar.

[12] PRINCE2 Manual, 3rd Edition, 2002: 280

2.1.3.5 COBIT

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
CB1.0	Determinar la alineación de la administración de Riesgos	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75	**0.78**	A	◕	S	●
CB2.0	Entender los objetivos de negocio estratégicos relevantes	1	1	1	1	1	0.75	0.75	0.75	**0.91**	A	◕	S	●
CB3.0	Entender los objetivos de los procesos de negocio relevantes	0.75	0.75	0.75	0.75	1	0.75	0.5	0.75	**0.75**	A	◕	S	●
CB4.0	Identificar los objetivos internos de TI y establecer el contexto del riesgo	0.75	0.75	0.75	0.75	0.75	0.75	0.5	0.75	**0.72**	P	◑	I	●
CB5.0	Identificar eventos asociados con objetivos	1	1	1	1	1	0.75	0.5	0.75	**0.88**	A	◕	S	●
CB6.0	Asesorar el riesgo con los eventos	1	1	1	1	1	0.75	0.5	0.75	**0.88**	A	◕	S	●
CB7.0	Evaluar y seleccionar respuestas a riesgos	1	1	1	1	1	0.75	0.75	0.75	**0.91**	A	◕	S	●
CB8.0	Priorizar y planificar las actividades de control	0.75	0.75	0.75	0.75	1	0.75	0.75	0.75	**0.78**	A	◕	S	●
CB9.0	Aprobar y garantizar la financiación de los planes de acción	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75	**0.78**	A	◕	S	●
CB10.0	Mantener y monitorizar el plan de acción de riesgos	1	1	1	1	1	1	0.75	1	**0.97**	A	◕	S	●
	SUMA TOTAL DE VALORES ASIGNADOS	**8.75**	**8.75**	**8.75**	**8.75**	**9.25**	**7.75**	**7**	**7.75**	**8.34**	N/A	N/A	N/A	N/A
	NUMERO TOTAL DE ACTIVIDADES	10	10	10	10	10	10	10	10	10	N/A	N/A	N/A	N/A
	ESCALA DE MEDICION (EM)	**0.88**	**0.88**	**0.88**	**0.88**	**0.93**	**0.78**	**0.70**	**0.78**	0.83	A	◕	S	●
	NIVEL DE PUNTUACION (NP)	A ◕	A ◕	A ◕	A ◕	A ◕	A ◕	P ◑	A ◕					
	RANGO DE SELECCIÓN	S ●	S ●	S ●	S ●	S ●	S ●	I ●	S ●					

Tabla 11. COBIT – Evaluación de Actividades que Gestionan el Riego

Realizada la evaluación a COBIT, este modelo presenta controles sobre la información que son la base en los requerimientos de calidad, legales y de seguridad, estableciendo una adecuada correspondencia con los Elementos de TI. Estos controles de la información son: Confidencialidad, Integridad, Disponibilidad, Efectividad, Eficiencia, Cumplimiento y Confiabilidad[13]. En el proceso PO09-Evaluar y Administrar los Riesgos de TI, los tres primeros controles

[13] COBIT 4.1, p. 10 - 11

de seguridad son catalogados por COBIT como primarios y los restantes como secundarios.

Así mismo, COBIT define en su marco de trabajo cuatro Recursos de TI[14] que deben ser gestionados al momento de Administrar los Riesgos: Aplicaciones, Información, infraestructura y Personas. Esto hace que el modelo en la mayoría de actividades satisfaga la correspondencia con los Proyectos de TI, según la Tabla 11.

Otra de las características que hace que COBIT sea sólido, es que su modelo es continuo al momento de Gestionar el Riesgo en los proyectos y sus procesos liga a los 4 dominios: Planear y Organizar (PO), Adquirir e Implantar (AI), Entregar y dar Soporte (DS), Mantener y Evaluar (ME); y estable roles clasificados para cada actividad, entre los principales tenemos: Director ejecutivo (CEO), Director Financiero (CFO), Director de Informática (CIO), Jefe de operaciones, Jefe de desarrollo, Arquitecto de TI, Jefe de administración de TI y la oficina o función de administración de proyectos (PMO).

Cabe destacar que COBIT en todo su proceso de Gobierno de TI, y en nuestro caso, la Gestión del Riesgo (PO09), presenta una serie de métricas para medir el cumplimiento de las principales actividades de control de los dominios. Estas métricas tienen su propio plan de implementación y el mismo es gradual y depende de la criticidad del proceso a medir.

Aunque uno de los objetivos de COBIT al momento de Evaluar y Administrar los Riesgos de TI, es "expresar en términos financieros a las partes interesadas para permitirles alinear el riesgo a un nivel de tolerancia aceptable"[15], el CFO participa activamente en dos de las diez actividades que Gestionan el Riesgo y en las demás se mantiene al margen o simplemente es informado y/o consultado. Esto hace que las inversiones y/o manejo de fondos dentro de un proyecto en ejecución sea un cuello de botella en la Identificación, Evaluación, Control y Mitigación de Riesgos.

[14] COBIT 4.1, p.12
[15] COBIT 4.1, p. 63

2.1.3.6 RISK IT

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
RIT1.0	Definición de un universo de riesgos y ámbito de gestión de riesgo	1	1	1	1	0.75	0.75	0.5	0.75	**0.84**	A	◕	S	●
RIT2.0	Apetito de riesgo y tolerancia al riesgo	1	1	1	1	0.75	0.5	1	1	**0.91**	A	◕	S	●
RIT3.0	Conciencia del riesgo, Comunicación y presentación de informes	0.75	0.75	1	0.75	0.5	0.75	0.5	0.75	**0.72**	P	◑	I	●
RIT4.0	Expresando y describiendo el riesgo	1	1	1	1	0.75	0.75	0.5	0.75	**0.84**	A	◕	S	●
RIT5.0	Escenarios de riesgo	1	1	1	1	0.75	0.5	0.5	0.75	**0.81**	A	◕	S	●
RIT6.0	Riesgo de respuesta y asignación de prioridades	0.75	0.75	1	0.75	0.75	1	0.5	1	**0.81**	A	◕	S	●
RIT7.0	Un flujo de trabajo de Análisis de Riesgo	0.75	0.75	0.75	0.75	0.75	0.5	0.5	0.75	**0.69**	P	◑	I	●
RIT8.0	Mitigación de Riesgos de TI Uso de COBIT y VAL IT	1	1	1	1	1	0.75	0.75	1	**0.94**	A	◕	S	●
SUMA TOTAL DE VALORES ASIGNADOS		**7.25**	**7.25**	**7.75**	**7.25**	**6**	**5.5**	**4.75**	**6.75**	**6.56**	N/A	N/A	N/A	N/A
NUMERO TOTAL DE ACTIVIDADES		8	8	8	8	8	8	8	8	8	N/A	N/A	N/A	N/A
ESCALA DE MEDICION (EM)		**0.91**	**0.91**	**0.97**	**0.91**	**0.75**	**0.69**	**0.59**	**0.84**	0.82	A	◕	S	●
NIVEL DE PUNTUACION (NP)		A ◕	A ◕	A ◕	A ◕	A ◕	P ◑	P ◑	A ◕					
RANGO DE SELECCIÓN		S ●	S ●	S ●	S ●	S ●	I ●	I ●	S ●					

Tabla 12. RISK IT – Evaluación de Actividades que Gestionan el Riego

La relación entre los riesgos de negocio y la Tecnología de Información es lo que Risk IT propone a las organizaciones, con el fin de identificar, gobernar y administrar los riesgos asociados al negocio. Para esto, este modelo cuenta con ocho actividades relacionadas con tres dominios (Gobierno, Evaluación y Respuesta).

Para Gestionar el Riesgo, Risk IT presenta una estructura que incluye prácticas y lineamientos gerenciales, metas y métricas así como modelos de madurez de los procesos. Sin embargo para que todo este sistema funcione Risk IT mantiene una

relación directa en todos sus procesos con COBIT y Val IT, es decir, COBIT se encarga de gestionar todas las actividades relacionadas con TI en la organización y Val IT describe cómo maximizar el retorno de la inversión cuando se identifican las oportunidades de cambios del negocio relacionados con TI.

Podemos destacar que Risk IT define roles, responsabilidades y rendición de cuentas al momento de Gestionar el Riesgo. La función que destaca es la creación del CRO (del Inglés Chief Risk Officer) o Director de Riesgos, quien supervisa todos los aspectos de la gestión del riesgo tanto de TI como de la organización.

En cuanto a las actividades R3.0 y R7.0 de la Tabla 12, encontramos un nivel de correspondencia parcial ya que el nivel de fluyo de trabajo y de comunicación entre el CEO, CFO, CIO y CRO es limitada respecto a temas de coordinación valor, riesgo y beneficios que la organización o proyecto obtiene a través de sus iniciativas de TI.

Respecto al tema financiero y legal, Risk IT en sus procesos es soportado por Val IT y estos dos modelos trabajan juntos en este aspecto para identificar, documentar y administrar los riesgos relacionados con TI. Conviene mencionar que respecto al tema legal existe parcial correspondencia puesto que existen pocos lineamientos respecto a contratos, licenciamiento y tributación.

Risk IT no se no se limita a la seguridad de la información sino que también considera temas de Retrasos en la entrega de proyectos, cumplimiento, arquitectura de TI, problemas en la entrega de servicios de TI, entre otros.

2.1.3.7 OCTAVE

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
OC1.0	Identificar la información (Gerencial-Operacional-Usuario Final)	0.75	0.75	0.75	0.75	1	0.5	0	0	**0.56**	P	◑	I	🟡
OC2.0	Consolidar la Información y crear perfiles de amenaza	0.75	0.75	0.75	1	1	0.75	0	0.75	**0.72**	P	◑	I	🟡
OC3.0	Identificación de componentes claves	1	1	1	1	0.5	0.5	0.5	1	**0.81**	A	◕	S	🟢
OC4.0	Evaluación de componentes seleccionados	1	1	1	1	0.75	0	0.75	1	**0.81**	A	◕	S	🟢
OC5.0	Análisis de riesgos de los recursos críticos	1	1	1	1	0.75	0.5	0.5	0.75	**0.81**	A	◕	S	🟢
OC6.0	Desarrollo de estrategias de protección	1	1	1	1	0.5	0.5	0.5	0.75	**0.78**	A	◕	S	🟢
SUMA TOTAL DE VALORES ASIGNADOS		**5.5**	**5.5**	**5.5**	**5.75**	**4.5**	**2.75**	**2.25**	**4.25**	**4.50**	N/A	N/A	N/A	N/A
NUMERO TOTAL DE ACTIVIDADES		6	6	6	6	6	6	6	6	6	N/A	N/A	N/A	N/A
ESCALA DE MEDICION (EM)		**0.92**	**0.92**	**0.92**	**0.96**	**0.75**	**0.46**	**0.38**	**0.71**	0.75	A	◕	S	🟢
NIVEL DE PUNTUACION (NP)		A ◕	A ◕	A ◕	A ◕	A ◕	N ◔	N ◔	P ◑					
RANGO DE SELECCIÓN		S 🟢	S 🟢	S 🟢	S 🟢	S 🟢	I 🔴	I 🔴	I 🟡					

Tabla 13. OCTAVE - Evaluación de Actividades que Gestionan el Riego

Una vez realizada la evaluación de la Gestión del Riesgo de la Metodología OCTAVE, podemos destacar que la principal herramienta que utiliza para estructurar la información es mediante entrevistas. Este proceso lo realiza en varios niveles de la organización obteniendo datos del personal y de los componentes que conforman la tecnología de información. Esto permite la comprensión del manejo de los recursos, la identificación y la evaluación de los riesgos que afectan la seguridad.

Algo que caracteriza a OCTAVE es la definición del perfil de Riesgos mediante una herramienta denominada “árbol” de amenaza, que no es más que la identificación de componentes claves y críticos más la valoración del impacto y niveles de aceptación del riesgo.

OCTAVE es una metodología de Gestión de Riesgos que se enfoca en identificar, medir, y proveer un plan para la administración de riesgos[16]. Temas como el legal financiero y criterios de calidad de servicio son áreas que no lo fortalecen, sin embargo, OCTAVE recalca la necesidad del control como un propósito de comunicación y recuperación.

El buen nivel de correspondencia con los cuatro primeros elementos de TI que alcanza OCTAVE (Tabla 13) es por la construcción de los perfiles de amenazas basados en activos y la identificación de la infraestructura de vulnerabilidades.

Dado que OCTAVE es una Metodología de Seguridad de la Información los atributos de Confidencialidad, Integridad y Disponibilidad[17] son elementos clave para Gestionar el Riesgo.

Adicionalmente a esto OCTAVE proporciona herramientas de registro como formularios, formatos y documentos tipo “check list” para registrar toda la información en el proceso de Gestión del Riesgo.

[16] OCTAVE Method Implementation Guide Version 2.0 – Vol. 1, 2001: I-7

[17] OCTAVE Criteria, Version 2.0, Security Requirements for Critical Assets, 2001: 41

2.1.3.8 NIST 800-30

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
NT1.1	1.1 Caracterización del sistema	1	1	1	1	1	0.5	0.5	1	**0.88**	A	◕	S	●
NT1.2	1.2 Identificación de amenazas	1	1	1	1	1	0.5	0.5	1	**0.88**	A	◕	S	●
NT1.3	1.3 Identificación de vulnerabilidades	1	1	1	1	0.75	0.75	0.75	0.75	**0.88**	A	◕	S	●
NT1.4	1.4 Análisis de control Paso	0.75	0.75	1	0.75	0.75	0.5	0.75	1	**0.78**	A	◕	S	●
NT1.5	1.5 Determinación de la probabilidad	1	1	1	1	0.75	0.5	0.75	1	**0.88**	A	◕	S	●
NT1.6	1.6 Análisis de impacto	1	1	1	1	0.75	0.75	0.75	1	**0.91**	A	◕	S	●
NT1.7	1.7 Determinación de riesgo	1	1	1	1	0.75	0.5	0.75	0.5	**0.81**	A	◕	S	●
NT1.8	1.8 Recomendaciones de control	1	1	1	1	0.5	1	0.5	1	**0.88**	A	◕	S	●
NT1.9	1.9 Documentación de resultados	1	1	1	1	1	0.5	0.5	1	**0.88**	A	◕	S	●
NT2.1	2.1 Priorización de Acciones	0.75	0.75	1	0.75	0.75	0.75	0.75	0.75	**0.78**	A	◕	S	●
NT2.2	2.2 Evaluación de Acciones de controles recomendados	1	1	1	1	1	0	0	1	**0.75**	A	◕	S	●
NT2.3	2.3 Análisis Costo-Beneficio	0.75	0.75	0.75	0.75	0.75	0.75	1	1	**0.81**	A	◕	S	●
NT2.4	2.4 Selección de Controles	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75	**0.78**	A	◕	S	●
NT2.5	2.5 Asignación de Responsabilidades	0.75	0.75	0.75	0.75	1	0	1	1	**0.75**	A	◕	S	●
NT2.6	2.6 Desarrollo de plan de implantación de salvaguardas	1	1	1	1	1	0.75	0.75	0.75	**0.91**	A	◕	S	●
NT2.7	2.7 Implantación de Controles seleccionados	1	1	1	1	1	0.75	0.75	0.75	**0.91**	A	◕	S	●
	SUMA TOTAL DE VALORES ASIGNADOS	**14.8**	**14.8**	**15.3**	**14.75**	**13.5**	**9.25**	**11**	**14.3**	**13.44**	N/A	N/A	N/A	N/A
	NUMERO TOTAL DE ACTIVIDADES	16	16	16	16	16	16	16	16	16	N/A	N/A	N/A	N/A
	ESCALA DE MEDICION (EM)	**0.92**	**0.92**	**0.95**	**0.92**	**0.84**	**0.58**	**0.69**	**0.89**	0.84	A	◕	S	●
	NTVEL DE PUNTUACION (NP)	A ◕	A ◕	A ◕	A ◕	A ◕	P ◑	P ◑	A ◕					
	RANGO DE SELECCIÓN	S ●	S ●	S ●	S ●	S ●	I ●	I ●	S ●					

Tabla 14. NIST 800-30 - Evaluación de Actividades que Gestionan el Riego

Una vez realizada la evaluación de las actividades que Gestionan el Riesgo de la metodología NIST 800-30, podemos observar (a base de la Tabla 14) que existe una importante correspondencia con los elementos de TI considerados en esta investigación. El proceso que la publicación 800-30 de NIST utiliza para Gestionar el Riesgo se encuentra dividido en dos fases: Análisis de Riesgos y

Gestión de Riesgos (identificadas las actividades en la Tabla 14 con ID NT1.X y NT2.X respectivamente).

En la primera fase: Análisis, la metodología determina e identifica los componentes y recursos de TI para ejecutar la evaluación del riesgo, todo esto con el uso de técnicas como la preparación de cuestionarios, establecimiento entrevistas en el sitio y herramientas automatizadas, por ejemplo el mapeo de Red. En esta fase también se identifican las posibles fuentes de amenaza y vulnerabilidades destacándose la lista relacionadas con las personas, sus motivaciones y acciones a tomar; todo esto con el fin de ser adaptadas a cada organización.

Así mismo la metodología NIST 800-30 describe las principales funciones del personal que debe apoyar y participar en el proceso de análisis y gestión de riesgos, es decir, la planificación, ejecución de actividades, presupuestos y desempeño van de la mano con la gestión del recurso humano.

Los objetivos de seguridad como la integridad, disponibilidad y confidencialidad[18] son la base para el análisis de impacto en la metodología definiéndose listas de comprobación de Requerimientos de Seguridad en todos los activos (personal, hardware, software y la información) agrupadas en tres áreas: Gerencial, Operacional y Técnica. Todo esto hace que el nivel de correspondencia con los elementos de TI de esta investigación sea adecuado, alcanzando el nivel de aceptación.

En la segunda fase: Gestión, consiste en la estrategia para combatir y mitigar el Riesgo asegurando que los sistemas informáticos almacenen, procesen y transmitan la información organizacional, tomando en cuenta el control, análisis de costos y riesgos residuales.

Podemos destacar en este punto el proceso de análisis de amenazas[19] para determinar el nivel de aceptación y evitación de las vulnerabilidades y riesgos. Así mismo la metodología presenta una arquitectura de controles y técnicas[20] que se

[18] NIST 800-30 Risk Management Guide for Information Technology Systems (RMGITS), 2001: 9
[19] NIST 800-30 RMGITS - Risk Mitigation Action Points, 2002: 28
[20] NIST 800-30 RMGITS - Technical Security Controls, 2002: 33

relacionan entre ellos para mitigar el riesgo, entre ellas podemos mencionar: identificación única de usuarios, procesos y recursos; criptografía, administración segura, protección de los sistemas mediante privilegios; autenticación, autorización, control de acceso, No repudio, protección de las comunicaciones; auditoría, detección de intrusos y de contención, restauración, virus y erradicación de software instalado.

Sin embargo, temas como el legal y las finanzas están orientados técnicamente al cumplimiento normativo y de auditoría así como al análisis costo beneficio.

2.1.3.9 MAGERIT

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
MG1.1	Estudio de oportunidad	0.75	0.75	0.75	0.75	1	0.5	0.75	1	**0.78**	A	◕	S	●
MG1.2	Determinación del alcance del proyecto	0.75	0.75	0.75	0.75	1	0.5	1	1	**0.81**	A	◕	S	●
MG1.3	Planificación del proyecto	0.75	0.75	0.75	0.75	1	0.75	0.75	1	**0.81**	A	◕	S	●
MG1.4	Lanzamiento del proyecto	1	1	1	1	1	0.75	0.75	0.75	**0.91**	A	◕	S	●
MG2.1	Caracterización de los activos	1	1	1	1	0.75	0.75	0.75	1	**0.91**	A	◕	S	●
MG2.2	Caracterización de las amenazas	1	1	1	1	0.75	1	0.75	1	**0.94**	A	◕	S	●
MG2.3	Caracterización de las salvaguardas	1	1	1	1	0.75	1	1	1	**0.97**	A	◕	S	●
MG2.4	Estimación del estado de riesgo	1	1	1	1	0.75	1	1	1	**0.97**	A	◕	S	●
MG3.1	Toma de decisiones	1	1	1	1	0.75	1	0.75	1	**0.94**	A	◕	S	●
MG3.2	Plan de seguridad	1	1	1	1	0.75	1	1	1	**0.97**	A	◕	S	●
MG3.3	Ejecución del plan	1	1	1	1	0.75	1	1	1	**0.97**	A	◕	S	●
	SUMA TOTAL DE VALORES ASIGNADOS	**10.3**	**10.3**	**10.3**	**10.25**	**9.25**	**9.25**	**9.5**	**10.8**	**9.97**	N/A	N/A	N/A	N/A
	NUMERO TOTAL DE ACTIVIDADES	11	11	11	11	11	11	11	11	11	N/A	N/A	N/A	N/A
	ESCALA DE MEDICION (EM)	**0.93**	**0.93**	**0.93**	**0.93**	**0.84**	**0.84**	**0.86**	**0.98**	**0.91**	A	◕	S	●
	NTVEL DE PUNTUACION (NP)	A ◕	A ◕	A ◕	A ◕	A ◕	A ◕	A ◕	A ◕					
	RANGO DE SELECCIÓN	S ●	S ●	S ●	S ●	S ●	S ●	S ●	S ●					

Tabla 15. MAGERIT - Evaluación de Actividades que Gestionan el Riego

MAGERIT divide su metodología en tres fases: Planificación, Análisis y Gestión del Riesgo. Para nuestra investigación las actividades de cada fase fueron

identificadas como MG1.X, MG2.X, MG3.X respectivamente, como se muestra en la Tabla 15.

MAGERIT se encuentra estructurado por tres libros de la siguiente manera:

- Libro I: Método (Descripción de la Metodología, fases y tareas a ejecutar).
- Libro II: Catálogo de Elementos (Especificación de términos y criterios técnicos).
- Libro III: Guía de Técnicas (Explicación de las técnicas cuantitativas y cualitativas en el Análisis y Gestión del Riesgo).

Estos tres libros se encuentran enlazados por conceptos que son puntuales en el desarrollo, por ejemplo: *Análisis coste-beneficio (ver "Guía de Técnicas" 3.1)* o *Catálogos de amenazas (ver "Catálogo de Elementos", capítulo 5)*[21].

Una de las características que presenta MAGERIT en la fase de Planificación es que su meta es concientizar a los Directivos sobre la importancia de contar con una herramienta que Gestione el Riesgo Tecnológico y que ésta se encuentre alineada con la Planificación Estratégica de la Organización. Así mismo en esta primera fase MAGERIT proporciona una serie de actividades y tareas para estructurar y definir un "Proyecto" de Análisis y Gestión de Riesgos (AGR)[22], tomando en cuenta el perfil y responsabilidad del recurso humano participante en todo el proceso, alcance del Proyecto AGR, recursos necesarios para la ejecución y criterios de evaluación dependiendo de los activos.

En la segunda fase, Análisis, MAGERIT se orienta en la identificación de los activos, amenazas y salvaguardas, todo esto para obtener información necesaria y realizar estimaciones de riesgo. Cabe indicar las estimaciones de riesgo en toda la metodología son expresadas en valores económicos, y por consiguiente las decisiones que deban tomarse y que tengan que ser validadas por los Directivos estarán fundamentadas y serán argumentadas desde un punto de vista financiero.

[21] MAGERIT V2.0 Libro I, 2006: 46 y 63

[22] MAGERIT V2.0 Libro I, 2006: 32

Para analizar el Riesgo MAGERIT toma en cuenta las denominadas dimensiones de seguridad que hacen valioso un activo[23], estas son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad[24]. Estas características se identifican con los activos para valorar la materialización de amenazas e impactos para posteriormente gestionarlos.

Finalmente, en la tercera fase, Gestión, MAGERIT procesa los resultados de riesgos de la fase anterior para asumirlos o afrontarlos. Para afrontar los riesgos que se consideren inaceptables se llevará a cabo un plan de seguridad, que ordene y organice las acciones encaminadas a llevar el estado de riesgo a un punto aceptable y aceptado por la Dirección.

A diferencia de los otros modelos y metodologías MAGERIT en su Libro III, explica y detalla las técnicas más utilizadas en los proyectos, se puede encontrar varios tipos de análisis de datos, entre los más importantes podemos mencionar: análisis mediante matrices, análisis algorítmico, árboles de ataque, análisis coste-beneficio, diagramas de flujos de datos, diagrama de procesos, diagramas Gantt y diagramas PERT

Podemos destacar que para MAGERIT el marco legal es trascendental[25] y presenta una serie de Leyes, reglamentos y procedimientos administrativos, así como también contratación de personal y compromisos contractuales. También la metodología detalla leyes sobre manejo de información clasificada, Firma Electrónica y Seguridad de las redes de Información. Todo esto en el contexto de la Gestión del Riesgo para sustentarlo y para ser de utilidad en un proyecto AGR.

Si bien las leyes y normativas que se especifican en la metodología aplican a España y los países europeos, pueden servir como referencia para su análisis y uso en los ámbitos que aplique. La documentación actualizada puede encontrarse en las páginas web del SSISTAD[26] y del CSAE[27] del Gobierno de España: http://www.csi.map.es/

[23] MAGERIT V2.0 Libro II, 2006: 16
[24] Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. MAGERIT V2.0 Libro II, 2006: 17
[25] MAGERIT V2.0 Libro I, 2006: Apéndice 3
[26] SSITAD: Seguridad de los Sistemas de Información y Protección de Datos Personalizados Automatizados

2.1.2.3.10 RECOLECCION DE RESULTADOS

MEJOR PRACTICA	ELEMENTO DE TI							
	HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS
CMMI	◑	◕	◕	◑	◑	○	◔	◑
SPICE	◑	◕	◕	◑	◑	◔	◕	◕
PMBOK	◑	◑	◑	◑	◕	○	◕	◑
PRINCE2	◑	◑	◑	◑	◑	◔	◔	◕
COBIT	◕	◕	◕	◕	◕	◕	◑	◕
RISK IT	◕	◕	◕	◕	◕	◑	◑	◕
OCTAVE	◕	◕	◕	◕	◕	◔	◔	◑
NIST 800-30	◕	◕	◕	◕	◕	◑	◑	◕
MAGERIT	◕	◕	◕	◕	◕	◕	◕	◕

LEYENDA: ○ No Cumple ◔ ◑ Parcial ◕ Adecuado ● Completo

Tabla 16. Comparativa de Mejores Prácticas que Gestionan el Riesgo – Nivel de Puntuación (NP)

En la Tabla 16, se presentan los resultados macro del nivel de puntuación alcanzado por cada mejor práctica.

A continuación se presenta una tabla comparativa de los modelos y metodologías del Rango de Selección alcanzado por cada Elemento de TI:

[27] CSAE: Consejo Superior de Administración Electrónica

MEJOR PRACTICA	ELEMENTO DE TI							
	HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS
CMMI	🟡	🟢	🟢	🟡	🟡	🔴	🔴	🟡
SPICE	🟡	🟢	🟢	🟡	🟡	🔴	🟢	🟢
PMBOK	🟡	🟡	🟡	🟡	🟢	🔴	🟢	🟡
PRINCE2	🟡	🟡	🟡	🟡	🟡	🔴	🔴	🟢
COBIT	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢
RISK IT	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢
OCTAVE	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟡
NIST 800-30	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢
MAGERIT	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢

LEYENDA: 🔴 Insatisfactorio 🟡 🟢 Satisfactorio

Tabla 17. Comparativa de Mejores Prácticas que Gestionan el Riesgo – Rango de Selección

Los resultados cuantitativos de todo el proceso de evaluación se muestran en la siguiente figura:

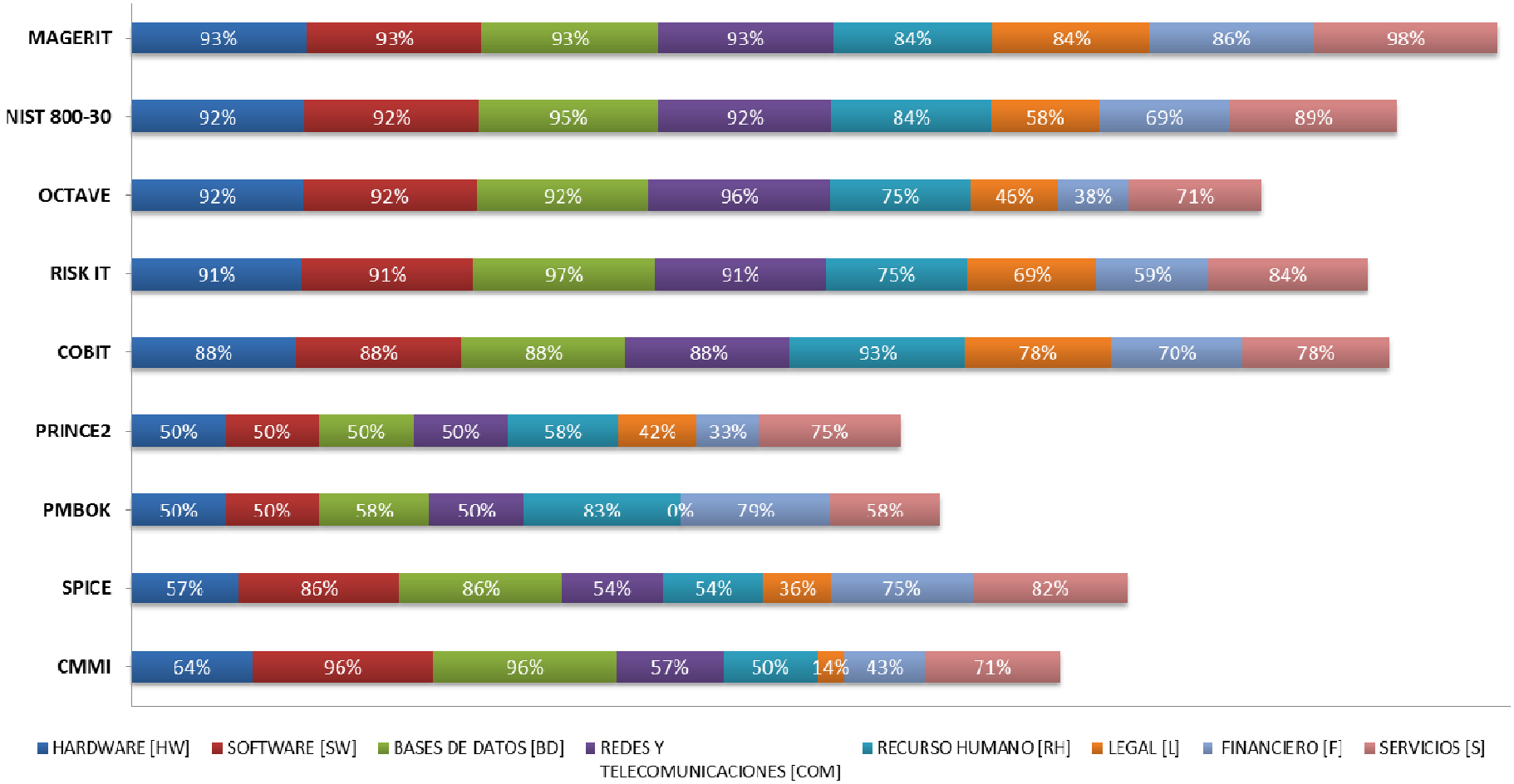


Figura 3. Comparativa de Mejores Prácticas que Gestionan el Riesgo – Escala de Medición (EM)

A base de la Tabla 16, 17 y Figura 3, podemos destacar que COBIT, RISK IT, OCTAVE, NIST 800-30 y MAGERIT alcanzan niveles de correspondencia satisfactorios al momento de Gestionar el Riesgo con respecto al: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones. De igual manera CMMI y SPICE alcanzan el nivel satisfactorio cuando se trata de la Gestión del ciclo de vida del Software y Bases de Datos.

Aquellas buenas prácticas que podemos recalcar al momento de Administrar el Recurso Humano son PMBOK, COBIT, NIST 800-30 y MAGERIT. Estos modelos y metodologías al Gestionar el Riesgo matizan su acción definiendo un equipo de trabajo con perfiles y competencias para los proyectos, con su respectiva asignación de funciones y responsabilidades apoyadas por una matriz RACI[28] dando respuesta inmediata a los impactos sobre los objetivos del proyecto.

Respecto al tema Legal, COBIT y MAGERIT encabezan la lista cubriendo temas de Seguridad y Normativa de la Información. Sin embargo, una de las bondades que presenta MAGERIT es que la alineación de las leyes y normativas se basan según requerimientos técnicos-gubernamentales cubriendo temas que no tratan otras buenas prácticas como: Contratos, Licenciamiento, Derechos de Autor, Contratación de Personal, Impuestos, Protección de datos de carácter personal, entre otros que pueden servir como referencia según el área de aplicabilidad y ejercicio.

El trato con las finanzas, es un tema que las buenas prácticas evaluadas en esta investigación adolecen con la excepción de PMBOK y MAGERIT que sobrepasan el umbral definido en este documento (75% para obtener niveles adecuados de correspondencia). Un caso particular es COBIT y RISK IT los cuales son apoyados directamente por Val IT.

En cuanto a la correspondencia de los Servicios, cada modelo y metodología se orienta según su doctrina y ámbito de aplicación, por ejemplo CMMI y SPICE al desarrollo de aplicaciones y soluciones automatizadas, PMBOK y PRINCE2 a la

[28] RACI, del inglés: Responsible, Accountable, Consulted, Informed (Responsable, Aprobador, Consultado, Informado)

gestión del proyecto como tal; COBIT y RISK IT en la alineación de los objetivos de la organización con la Tecnología de la Información; OCTAVE, NIST 800-30 y MAGERIT en el Análisis y Gestión del Riesgo cuando se hace uso de la TI.

A base de lo anterior, se analiza cada uno de los modelos y metodologías:

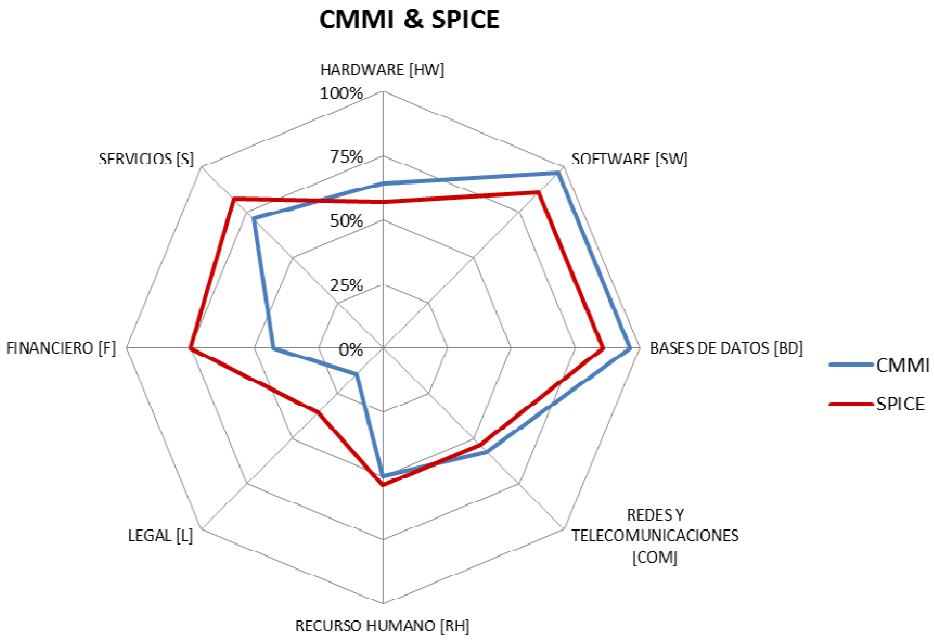


Figura 4. CMMI & SPICE - Gestión del Riesgo de TI

Según la Figura 4, en la Gestión del Riesgo CMMI y SPICE son herramientas que brindan soporte adecuado en proyectos que implican Ingeniería de Software (SW, BD y S), considerando que los procesos de gestión y organizativos buscan un mayor nivel de madurez o capacidad. En la Administración de Proyectos ambos modelos gestionan sus actividades en un marco de actividades para cumplir los requerimientos de usuario y servicios de información siendo la base la arquitectura tecnológica.

Estos modelos son buenas referencias para planificar, gestionar, controlar y mejorar procesos de adquisición, desarrollo, operación, soporte y mantenimiento de productos para el comercio internacional de software.

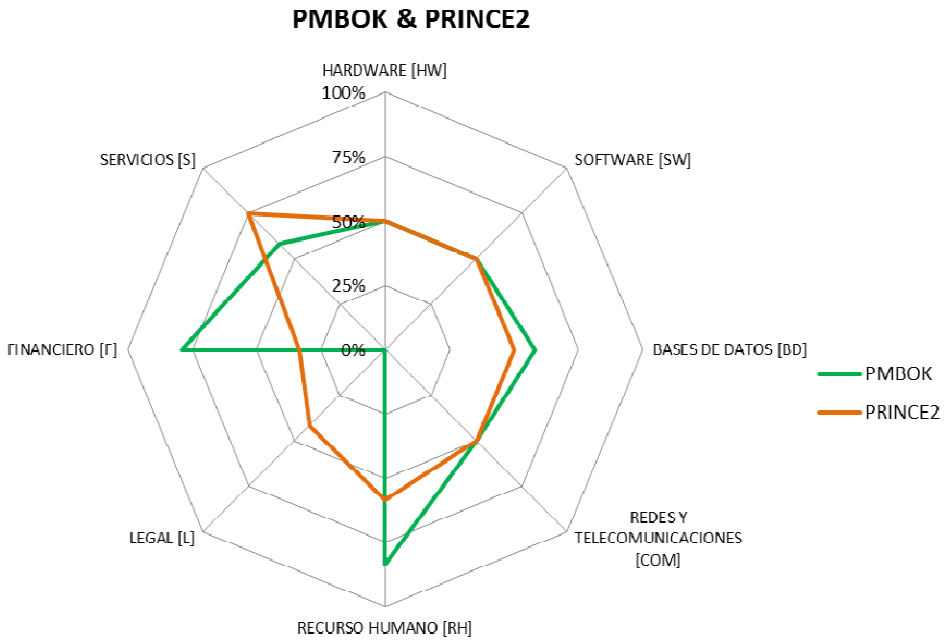


Figura 5. PMBOK & PRINCE2 - Gestión del Riesgo de TI

La Gestión del Riesgo según la Figura 5, PMBOK y PRINCE2 establece una orientación de cumplimiento de objetivos y de productos a base de la administración de los Servicios, Recurso Humano y Finanzas; destacándose PMBOK en este último aspecto. Por ser herramientas para cualquier tipo de proyecto, alcanzan niveles parciales de correspondencia con los Elementos Técnicos de TI (HW, SW, BD y COM).

El tema legal se encuentra direccionado al cumplimiento de productos más sin embargo los dos modelos dejan la brecha abierta para que el juicio de expertos sea quien direccione la toma de decisiones.

La Administración del Recurso Humano (RH) es uno de los aspectos que fortalecen a PMBOK y PRINCE2, ambos modelos definen con detalle los roles y responsabilidades dentro del proyecto y la organización con el objetivo de tener un equipo que sepa lo que tiene que hacer y pueda tomar las decisiones que le corresponden en el alcance, tiempo y costos.

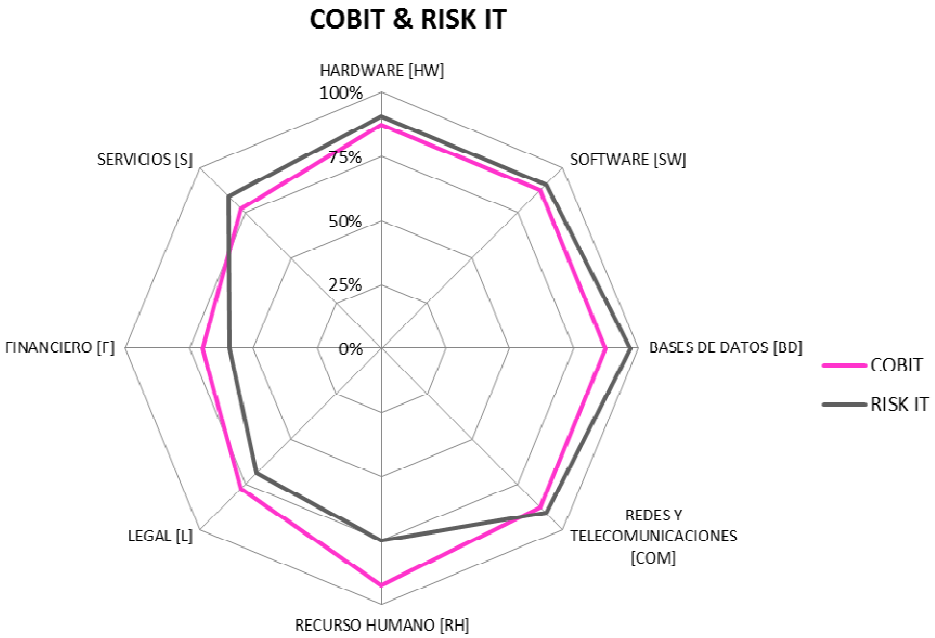


Figura 6. COBIT & RISK IT - Gestión del Riesgo de TI

En la Figura 6, podemos observar que COBIT y RISK IT son modelos que cubren gran parte del área al momento de Gestionar los Riesgos en proyectos que involucran Tecnologías de información y Comunicaciones.

En estos dos modelos que pertenecen a la misma familia existe un balance característico en los elementos técnicos/administrativos, COBIT en el aspecto Financiero, Legal y del Recurso Humano alcanza niveles superiores; RISK IT por su parte con los elementos de tecnología (HW, SW, BD y COM) y Servicios.

Esto no quiere decir que el uno sea superior al otro puesto que existen varios acápites de dependencia entre RISK IT y COBIT. Es importante mencionar que al momento de realizar esta investigación ISACA ha evolucionado el concepto de gobernanza sobre TI anunciando la elaboración de la versión 5 de COBIT[29], que integrará los siguientes Framewoks[30]: COBIT, Val IT, RISK IT, ITAF[31] y BMIS[32].

[29] www.isaca.org/cobit5
[30] COBIT 5: The Framework Exposure Draft, 2011: 10
[31] ITAK: IT Assurance Framewok (Marco de Aseguramiento de TI. Proporciona orientación y asistencia a las empresas.)
[32] BMIS: Business Model for Information Security (Modelo de Negocio para la Seguridad de la Información)

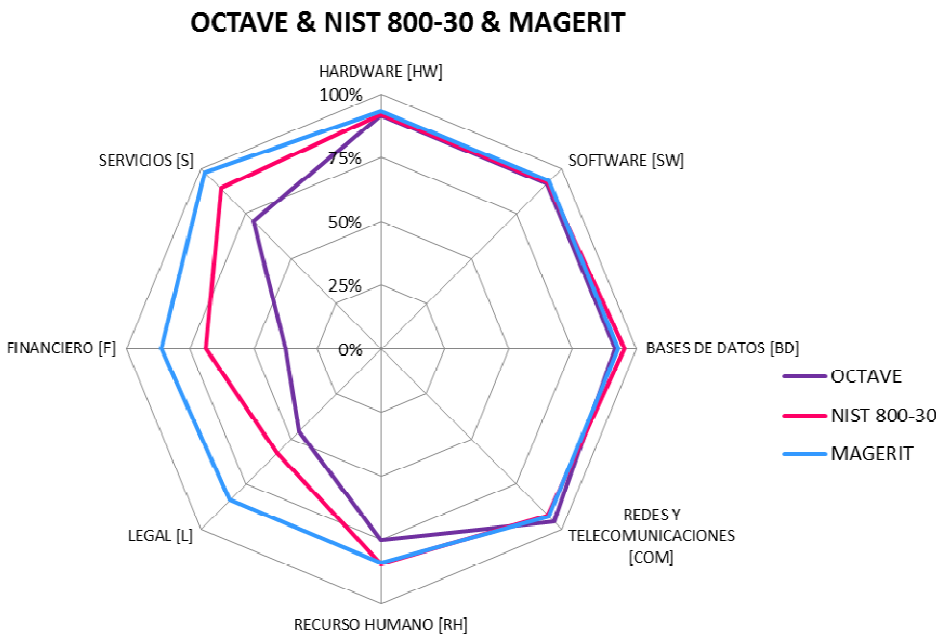


Figura 7. OCTAVE & NIST 800-30 & MAGERIT - Gestión del Riesgo de TI

El alto nivel alcanzado, Figura 7 de los Elementos de TI: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones; se debe a que estas tres metodologías inician la Gestión del Riesgo identificando los activos involucrados dentro de un proyecto u organización, es decir, se inicia examinando todos los recursos tecnológicos, administrativos, de operación y de usuario involucrados en transmitir y proporcionar información con el fin de conocer su función y tener un "inventario" de todos los elementos para realizar un análisis y caracterización de amenazas y vulnerabilidades .

Podemos destacar que la definición de las funciones, responsabilidades y roles del equipo de trabajo (en el proyecto u organización) son definidas bajo el contexto de la Gestión del Riesgo de TI para entregar servicios y productos a tiempo y acorde a las especificaciones requeridas para el eficaz desempeño de la empresa o institución.

En cuanto al área Financiera y Legal, MAGERIT alcanza valores aceptables de correspondencia y la metodología describe las técnicas utilizadas en los proyectos de análisis y Gestión de Riesgos sin ser exhaustivas. Los profesionales de TI pueden profundizar cada área según su interés.

Los criterios de seguridad que son la base para realizar el análisis y valorar la materialización de amenazas e impactos sobre los Elementos de TI se muestran en la siguiente tabla:

CRITERIO	COBIT	OCTAVE	NIST 800-30	MAGERIT
CONFIDENCIALIDAD	✓	✓	✓	✓
INTEGRIDAD	✓	✓	✓	✓
DISPONIBILIDAD	✓	✓	✓	✓
AUTENTICIDAD	✗	✗	✗	✓
TRAZABILIDAD	✗	✗	✗	✓
EFECTIVIDAD	✓	✗	✗	✗
EFICIENCIA	✓	✗	✗	✗
CUMPLIMIENTO	✓	✗	✗	✗
CONFIABILIDAD	✓	✗	✗	✗

Tabla 18. Mejores Prácticas - Criterios de Seguridad de la Información

2.1.4 FASE 4: SELECCIÓN

Una vez que tenemos la información cualitativa y cuantitativa de las actividades de las Mejores Prácticas que Gestionan el Riesgo, los objetivos de la Fase de Selección son:

a) Procesar los datos adquiridos en la Fase de Evaluación para disgregar información según la escala de valoración.

b) Obtener una lista de procesos de mayor correspondencia con los Elementos de TI: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones, Recurso Humano, Legal, Financiero y Servicios.

c) Seleccionar las actividades que se alineen con los Elementos de TI en Proyectos que involucran Tecnologías de Información y Comunicaciones

En el ***Anexo B*** de este documento, se adjunta la información de la evaluación de todas las actividades que gestionan el Riesgo de las Mejores Prácticas tratadas en esta investigación.

Según la Escala de Valoración de la Tabla 3, los valores considerados como satisfactorios son aquellos que alcanzan un valor igual o superior al 75%. A continuación se presenta una ***consolidación integral*** de resultados:

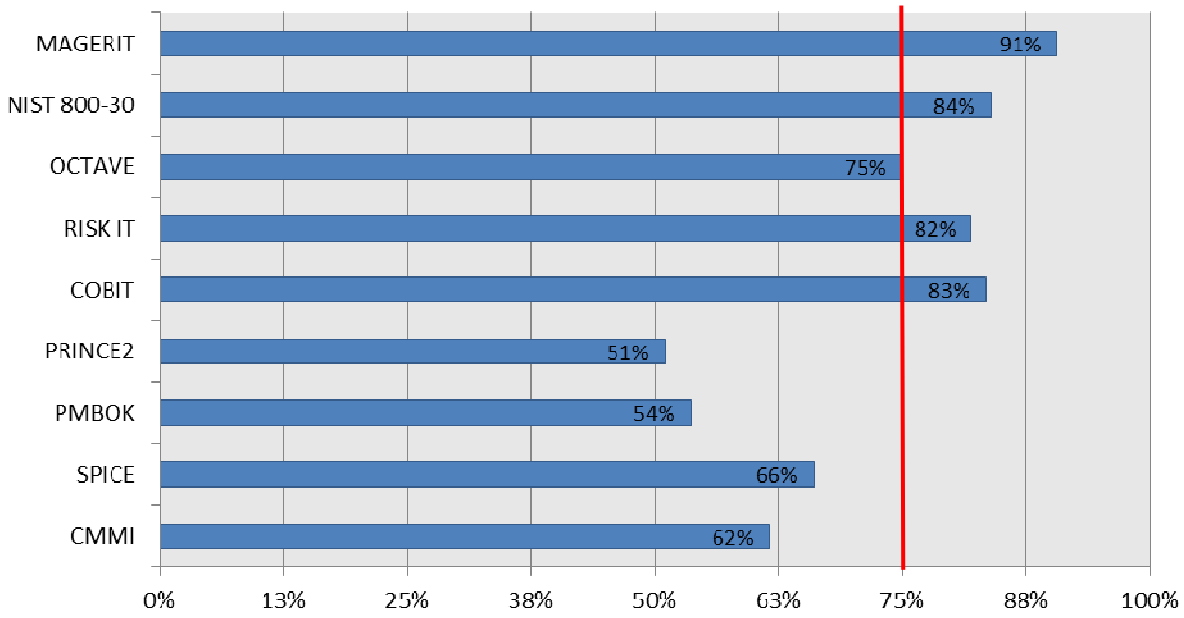


Figura 8. Mejores Prácticas que Gestionan el Riesgo - Consolidación de Resultados

La sumarización de los datos obtenidos es el resultado de la aplicación de la siguiente ecuación:

$$EscalaDeMedición_{Mejor\ Práctica} = \frac{1}{np}\sum_{i=1}^{n} Xi$$

Dónde n: es el Número Total de actividades que Gestionan el Riesgo

Xi: representa cada uno de los valores asignados

p: Elementos de TI ([HW], [SW], [BD], [COM], [RH], [L], [F], [S]), constante=8

Gráficamente, todas las actividades se presentan a continuación:

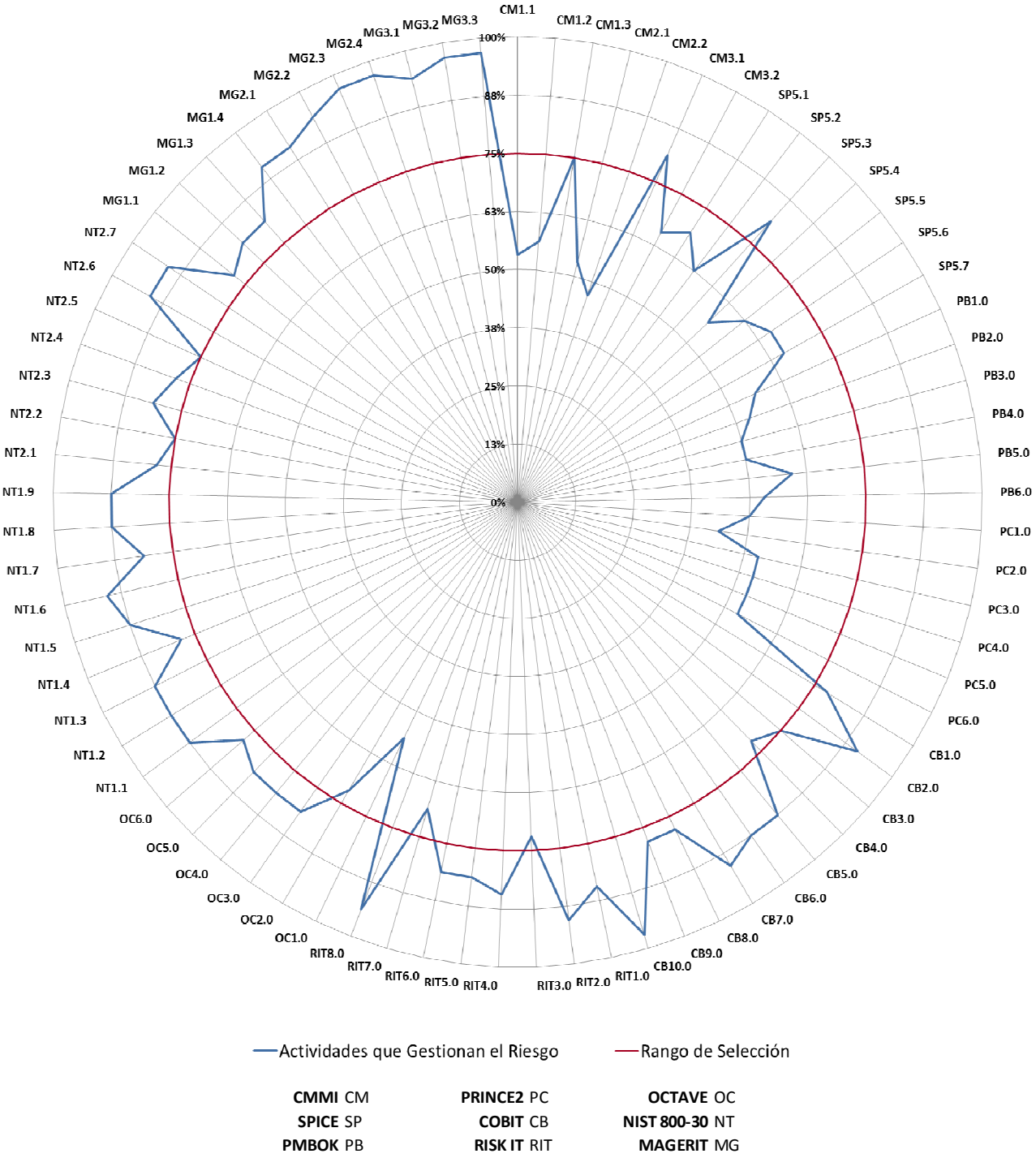


Figura 9. Mejores Prácticas - Actividades que Gestionan el Riesgo – Rango de Selección

Para realizar el cálculo de correspondencia y determinar el valor de la escala de medición de cada actividad utilizamos la siguiente fórmula:

$$EscalaDeMedición_{Actividad} = \frac{1}{p}\sum_{i=1}^{p} Xi$$

Dónde p: Elementos de TI ([HW], [SW], [BD], [COM], [RH], [L], [F], [S]), constante=8

Xi: representa cada uno de los valores asignados

Las Actividades que alcanzan el nivel satisfactorio son las siguientes:

MEJOR PRACTICA	ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ESCALA DE MEDICION (EM)
			HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	
CMMI	**CM1.3**	Establecer una estrategia de gestión de riesgos	0.75	1	1	0.75	0.75	0.5	0.5	0.75	**0.75**
CMMI	**CM3.1**	Desarrollar planes de mitigación de riesgos	0.75	1	1	0.5	1	0.5	0.75	1	**0.81**
SPICE	**SP5.3**	Identificar riesgos	1	1	1	0.75	0.5	0.5	0.75	1	**0.81**
COBIT	**CB1.0**	Determinar la alineación de la administración de Riesgos	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75	**0.78**
COBIT	**CB2.0**	Entender los objetivos de negocio estratégicos relevantes	1	1	1	1	1	0.75	0.75	0.75	**0.91**
COBIT	**CB3.0**	Entender los objetivos de los procesos de negocio relevantes	0.75	0.75	0.75	0.75	1	0.75	0.5	0.75	**0.75**
COBIT	**CB5.0**	Identificar eventos asociados con objetivos	1	1	1	1	1	0.75	0.5	0.75	**0.88**
COBIT	**CB6.0**	Asesorar el riesgo con los eventos	1	1	1	1	1	0.75	0.5	0.75	**0.88**
COBIT	**CB7.0**	Evaluar y seleccionar respuestas a riesgos	1	1	1	1	1	0.75	0.75	0.75	**0.91**
COBIT	**CB8.0**	Priorizar y planificar las actividades de control	0.75	0.75	0.75	0.75	1	0.75	0.75	0.75	**0.78**
COBIT	**CB9.0**	Aprobar y garantizar la financiación de los planes de acción	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75	**0.78**
COBIT	**CB10.0**	Mantener y monitorizar el plan de acción de riesgos	1	1	1	1	1	1	0.75	1	**0.97**
RISKIT	**RIT1.0**	Definición de un universo de riesgos y ámbito de gestión de riesgo	1	1	1	1	0.75	0.75	0.5	0.75	**0.84**
RISKIT	**RIT2.0**	Apetito de riesgo y tolerancia al riesgo	1	1	1	1	0.75	0.5	1	1	**0.91**
RISKIT	**RIT4.0**	Expresando y describiendo el riesgo	1	1	1	1	0.75	0.75	0.5	0.75	**0.84**
RISKIT	**RIT5.0**	Escenarios de riesgo	1	1	1	1	0.75	0.5	0.5	0.75	**0.81**
RISKIT	**RIT6.0**	Riesgo de respuesta y asignación de prioridades	0.75	0.75	1	0.75	0.75	1	0.5	1	**0.81**
RISKIT	**RIT8.0**	Mitigación de Riesgos de TI Uso de COBIT y VAL IT	1	1	1	1	1	0.75	0.75	1	**0.94**
OCTAVE	**OC3.0**	Identificación de componentes claves	1	1	1	1	0.5	0.5	0.5	1	**0.81**
OCTAVE	**OC4.0**	Evaluación de componentes seleccionados	1	1	1	1	0.75	0	0.75	1	**0.81**
OCTAVE	**OC5.0**	Análisis de riesgos de los recursos críticos	1	1	1	1	0.75	0.5	0.5	0.75	**0.81**
OCTAVE	**OC6.0**	Desarrollo de estrategias de protección	1	1	1	1	0.5	0.5	0.5	0.75	**0.78**
NIST 800-30	**NT1.1**	1.1 Caracterización del sistema	1	1	1	1	1	0.5	0.5	1	**0.88**
NIST 800-30	**NT1.2**	1.2 Identificación de amenazas	1	1	1	1	1	0.5	0.5	1	**0.88**
NIST 800-30	**NT1.3**	1.3 Identificación de vulnerabilidades	1	1	1	1	0.75	0.75	0.75	0.75	**0.88**
NIST 800-30	**NT1.4**	1.4 Análisis de control Paso	0.75	0.75	1	0.75	0.75	0.5	0.75	1	**0.78**
NIST 800-30	**NT1.5**	1.5 Determinación de la probabilidad	1	1	1	1	0.75	0.5	0.75	1	**0.88**
NIST 800-30	**NT1.6**	1.6 Análisis de impacto	1	1	1	1	0.75	0.75	0.75	1	**0.91**

MEJOR PRACTICA	ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI								ESCALA DE MEDICION (EM)
			HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	
NIST 800-30	**NT1.7**	1.7 Determinación de riesgo	1	1	1	1	0.75	0.5	0.75	0.5	**0.81**
NIST 800-30	**NT1.8**	1.8 Recomendaciones de control	1	1	1	1	0.5	1	0.5	1	**0.88**
NIST 800-30	**NT1.9**	1.9 Documentación de resultados	1	1	1	1	1	0.5	0.5	1	**0.88**
NIST 800-30	**NT2.1**	2.1 Priorización de Acciones	0.75	0.75	1	0.75	0.75	0.75	0.75	0.75	**0.78**
NIST 800-30	**NT2.2**	2.2 Evaluación de Acciones de controles recomendados	1	1	1	1	1	0	0	1	**0.75**
NIST 800-30	**NT2.3**	2.3 Análisis Costo-Beneficio	0.75	0.75	0.75	0.75	0.75	0.75	1	1	**0.81**
NIST 800-30	**NT2.4**	2.4 Selección de Controles	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75	**0.78**
NIST 800-30	**NT2.5**	2.5 Asignación de Responsabilidades	0.75	0.75	0.75	0.75	1	0	1	1	**0.75**
NIST 800-30	**NT2.6**	2.6 Desarrollo de plan de implantación de salvaguardas	1	1	1	1	1	0.75	0.75	0.75	**0.91**
NIST 800-30	**NT2.7**	2.7 Implantación de Controles seleccionados	1	1	1	1	1	0.75	0.75	0.75	**0.91**
MAGERIT	**MG1.1**	Estudio de oportunidad	0.75	0.75	0.75	0.75	1	0.5	0.75	1	**0.78**
MAGERIT	**MG1.2**	Determinación del alcance del proyecto	0.75	0.75	0.75	0.75	1	0.5	1	1	**0.81**
MAGERIT	**MG1.3**	Planificación del proyecto	0.75	0.75	0.75	0.75	1	0.75	0.75	1	**0.81**
MAGERIT	**MG1.4**	Lanzamiento del proyecto	1	1	1	1	1	0.75	0.75	0.75	**0.91**
MAGERIT	**MG2.1**	Caracterización de los activos	1	1	1	1	0.75	0.75	0.75	1	**0.91**
MAGERIT	**MG2.2**	Caracterización de las amenazas	1	1	1	1	0.75	1	0.75	1	**0.94**
MAGERIT	**MG2.3**	Caracterización de las salvaguardas	1	1	1	1	0.75	1	1	1	**0.97**
MAGERIT	**MG2.4**	Estimación del estado de riesgo	1	1	1	1	0.75	1	1	1	**0.97**
MAGERIT	**MG3.1**	Toma de decisiones	1	1	1	1	0.75	1	0.75	1	**0.94**
MAGERIT	**MG3.2**	Plan de seguridad	1	1	1	1	0.75	1	1	1	**0.97**
MAGERIT	**MG3.3**	Ejecución del plan	1	1	1	1	0.75	1	1	1	**0.97**

Tabla 19. Mejores Prácticas – Lista de Actividades - Rango de Selección Satisfactorio

2.1.5 FASE 5: DEFINICIÓN

El objetivo de esta Fase es presentar la Guía de Gestión de Riesgos en el proceso de adquisición e implantación de bienes y servicios correspondientes a proyectos de gran envergadura que involucran Tecnologías de Información y Comunicaciones.

Esta guía contempla que el proyecto ha superado las etapas de licitación y aprobación existiendo responsabilidad contractual para el desarrollo, ejecución y entrega del producto final definido en las bases del concurso o pliegos así como en el alcance del proyecto, del tiempo, del costo y de la calidad requerida.

2.1.5.1 GUÍA DE GESTION DE RIESGOS

Para definir la Guía de Gestión de Riesgos se contempla las actividades que alcanzaron el nivel satisfactorio obtenido en la Fase anterior (Selección).

La Guía se encuentra sistematizada en el siguiente diagrama:

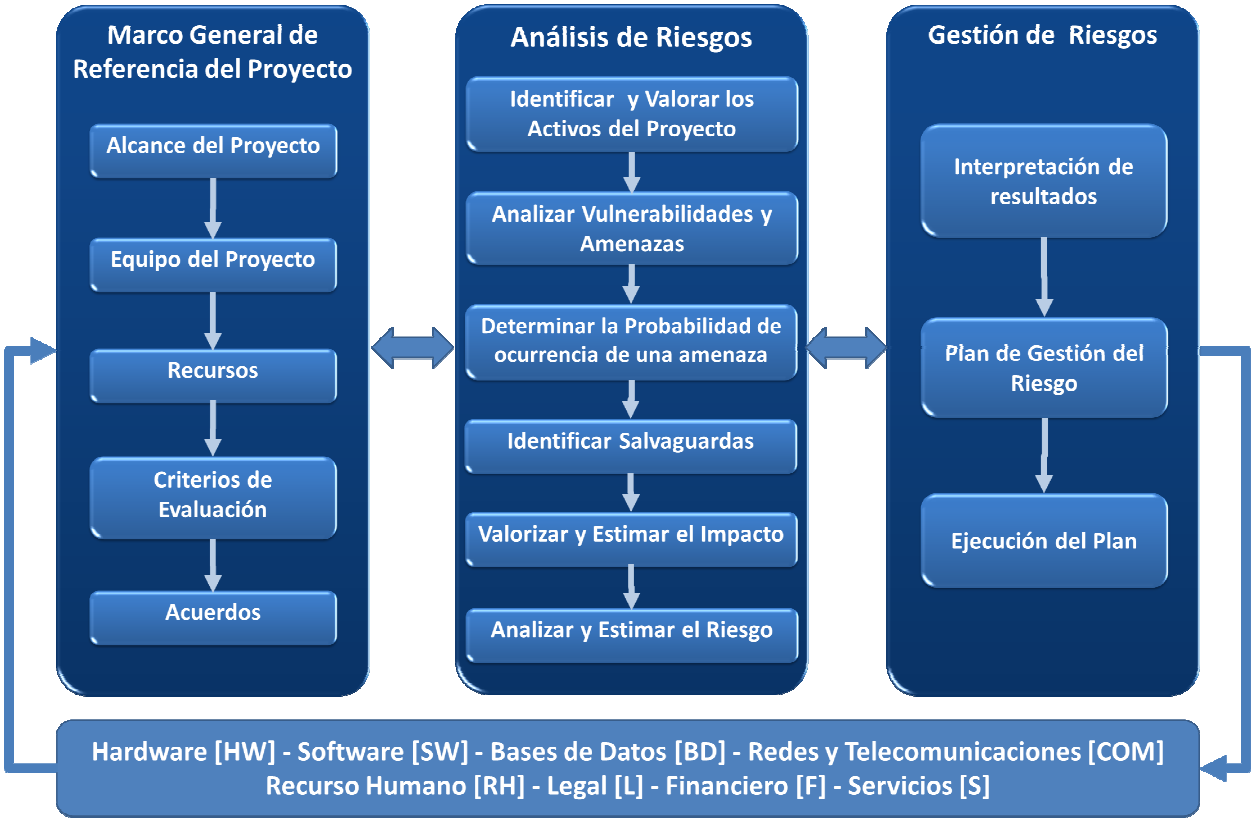


Figura 10. Modelo de Guía de Gestión de Riesgos correspondiente a Proyectos TI

La Guía especifica que el Marco General del Proyecto, el Análisis y la Gestión de Riesgos debe considerarse un ciclo en el que las tres etapas se enfocan en gestionar el riesgo dentro de un proyecto de TICs y se sitúan en una nueva iteración que permite obtener la evolución de los procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas; y de esta forma reajustar permanentemente el nivel de riesgo a los requerimientos del proyecto.

A base de la Figura 10, el documento de la Guía se estructura siguiendo el siguiente proceso:

1. Marco General de Referencia del Proyecto
    1.1 Alcance del Proyecto
    1.2 Establecer el Contexto Organizacional y áreas críticas
    1.3 Equipo del Proyecto
    1.4 Recursos
    1.5 Criterios de Evaluación
    1.6 Acuerdos
2. Análisis de Riesgos
    2.1 Identificar y Valorar los Activos de la Organización.
    2.2 Analizar Vulnerabilidades y Amenazas
    2.3 Determinar la Probabilidad de ocurrencia de una amenaza.
    2.4 Identificar Salvaguardas
    2.5 Valorizar y Estimar el Impacto
    2.6 Analizar, Estimar y Priorizar el Riesgo
3. Gestión del Riesgo
    3.1 Interpretación de los Resultados
    3.2 Plan de Gestión del Riesgo
    3.3 Ejecución del Plan

2.1.5.1.1Especificación de la Guía

La siguiente información se proporciona para lograr que los profesionales de TI puedan utilizar esta herramienta de manera ágil y que las técnicas que actualmente se aplican en la Gestión de Riesgos sean presentadas en función de las mejores prácticas.

Es importante indicar que en el **Anexo C** de este documento se adjunta un CD con los manuales de todos los modelos y metodologías tratadas en esta investigación.

Proceso 1: Marco General de Referencia del Proyecto

Objetivos:

Determinar los objetivos del proyecto

Determinar las pautas generales que se imponen sobre el proyecto

Formalizar las acciones a realizar a lo largo de un proyecto

Producto de Entrada:

Recopilación de la documentación pertinente del proyecto

Producto de Salida:

Especificación detallada de los objetivos del proyecto, recursos y equipo de trabajo.

Técnicas, prácticas y pautas:

Entrevistas (Ver MAGERIT Libro III – Guía de Técnicas, 3.6.1, p. 64)

Reuniones (Ver MAGERIT Libro III – Guía de Técnicas, 3.6.2, p. 65)

Participantes:

Comité de Proyecto[33]

Director de Riesgos (CRO)

Actividad 1.1: Alcance del Proyecto

Comunicar y entender los objetivos del proyecto, su dominio, sus límites y cronograma. Se realiza una lista de todos los productos y se analiza el proceso de entrega recepción a base de los procesos contractual y financiero definidos previamente (Ver MAGERIT Libro I – Método, 3, p. 32). Se debe tener en cuenta la posible existencia de otros planes contractuales por ejemplo: Planes de Ejecución, Plan Operativo, Plan Estratégico, Plan de Seguridad, Plan de Sistemas de Información, entre otros.

La adquisición, instalación y operación es un proceso que se tiene que especificar, es decir, si las tres instancias anteriores son de tipo internacional, nacional o mixta. Esta información es un producto para la siguiente fase.

[33] El Comité de Proyecto representa los niveles directivos de Negocio, Usuario y Proveedor interesados en el proyecto. Sus miembros deberán poseer cierta autoridad, ya que son los que tomarán decisiones y serán responsables del compromiso de los recursos. (PRINCE2 Manual, 3rd Edition, 2002: 195)

Actividad 1.2: Establecer el Contexto Organizacional y áreas críticas

Entender y conocer los procesos de la organización que ejecutará el proyecto, es decir, poner en contexto los Procesos de negocio y de soporte, que son los definidos para cumplir los objetivos de Proyecto para asegurar el funcionamiento las actividades en la Gestión de Riesgos (Ver COBIT 4.1 - P09. Evaluar y Administrar los Riesgos de TI – Directrices Gerenciales, p. 65)

Actividad 1.3: Equipo del Proyecto

Establecer el grupo de personas que realizará los trabajos del proyecto con la particularidad de tener conocimientos específicos en una determinada área para contribuir con el cumplimiento de objetivos, tiempo y coste. En este punto se debe tratar la definición de roles, matriz RACI, modalidades de contrato (según permita la ley) e inducción de los objetivos y metas del proyecto.

En el **Anexo D** de este documento se adjunta una propuesta del equipo de trabajo que gestionará el riesgo en los Proyectos de TI.

Es importante también tomar en cuenta unidades de trabajo externas relacionadas con el desarrollo del proyecto, por ejemplo: Aseguradoras, Auditores Externos, Organismos de control gubernamental, Consultorías, entre otras. (Ver RISK IT - Role Definitions, p. 39; PMBOK 4th Edition – 2.3 Project Stakeholder; Human Resource Management, Chapter 9; NIST 800-30 – Key Roles, 2.3, p.6)

Actividad 1.4: Recursos

Determinar y estimar el costo de los materiales, equipos, software y suministros para ejecutar cada actividad. Se pueden aplicar técnicas como el análisis coste-beneficio (ver MAGERIT Libro III - Guía de Técnicas, 3.1, p. 26) y Planificación de proyectos (ver MAGERIT Libro III - Guía de Técnicas, 3.5, p. 60). Es importante indicar que la valoración del coste del proyecto se realiza estimando los tiempos (cronograma) y perfiles de personal asignado a las etapas del proyecto dimensionado anteriormente. Así mismo se debe tomar en cuenta que existirán costos de las Salvaguardas a identificar.

Actividad 1.5: Criterios de Evaluación

Definir el modo de evaluar el control y seguimiento del proyecto para Analizar y Gestionar el Riesgo. Para esto se puede establecer métricas y variables tanto para el proyecto como para el riesgo como: avance, cumplimiento, madurez, dimensiones de seguridad y cumplimiento contractual. En este punto es importante definir la escala de valoración tanto para los datos cualitativos y cuantitativos (ver MAGERIT Libro II – Catalogo de Elementos, 4, p.19), metas y métricas (Ver COBIT 4.1 - P09. Evaluar y Administrar los Riesgos de TI, p.65)

En el **Anexo E** de este documento a base del análisis de las mejores prácticas se presenta las dimensiones de seguridad y nivel de madurez de la implantación para proyectos de TI.

Actividad 1.6: Acuerdos

Establecer formatos en cuanto a documentos y comunicaciones siendo estos oficios, emails, actas, cuestionarios tipo y plantillas de registro para formalizar la recogida de la información y realizar el análisis de riesgos que pueden adaptarse a las necesidades según el proyecto u organización.

Proceso 2: Análisis de Riesgos

Objetivos:

Identificar todos los activos y componentes del Proyecto

Determinar Vulnerabilidades y Amenazas así como la probabilidad de ocurrencia.

Identificar Salvaguardas y valorizar el posible impacto priorizando el mayor riesgo

Determinar el Riesgo

Producto de Entrada:

Documentación del Contexto Organizacional y áreas críticas del proyecto.

Producto de Salida:

Caracterización de los activos

Análisis de Riesgos

Técnicas, prácticas y pautas:

Herramientas y técnicas para Gestionar el Riesgo en Proyectos, Juicio de Expertos (Ver PMBOK 4th Edition – Management Risk, Chapter 11)

Técnicas Específicas y Generales para Gestionar el Riesgo (Ver MAGERIT Libro III – Guía de Técnicas, 2 y 3)

Participantes:

Director de Riesgos (CRO)

Director de control/seguimiento[34] (PCM)

Director Ejecutivo (CEO)

Director de proyecto (PM)

Actividad 2.1: Identificar y Valorar los Activos de la Organización.

Clasificar los activos por área de Gestión según el Proyecto de TI, siendo estos: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones, Recurso Humano, Legal, Financiero y Servicios. En el **Anexo F** de este documento se encuentra un detalle de activos según la clasificación que hemos considerado. Otra clasificación acorde a nuestros propósitos se encuentra en el Manual de NIST (Ver NIST 800-30, System Characterization, 3.1, p. 10).

Actividad 2.2: Analizar Vulnerabilidades y Amenazas

Especificar (a base de la información de los activos) las debilidades que se pueden presentar de manera accidental o intencionalmente así como la posibilidad de que se produzca un daño en los activos o procesos del proyecto. Estos pueden ser: Humanos, Naturales, Técnicos, Industriales, y Regulatorios. (Ver NIST 800-30, Fase 2 y 3, 3.2 – 3.3, p.12-19 y MAGERIT, Libro I – Método, 2.1.2, p. 22)

Para tener una mejor visualización de la relación Activo-Vulnerabilidad-Amenaza, se presenta la siguiente Figura:

[34] Director de control/seguimiento: Fiscalización, también conocido como Project Control Manager (PCM)

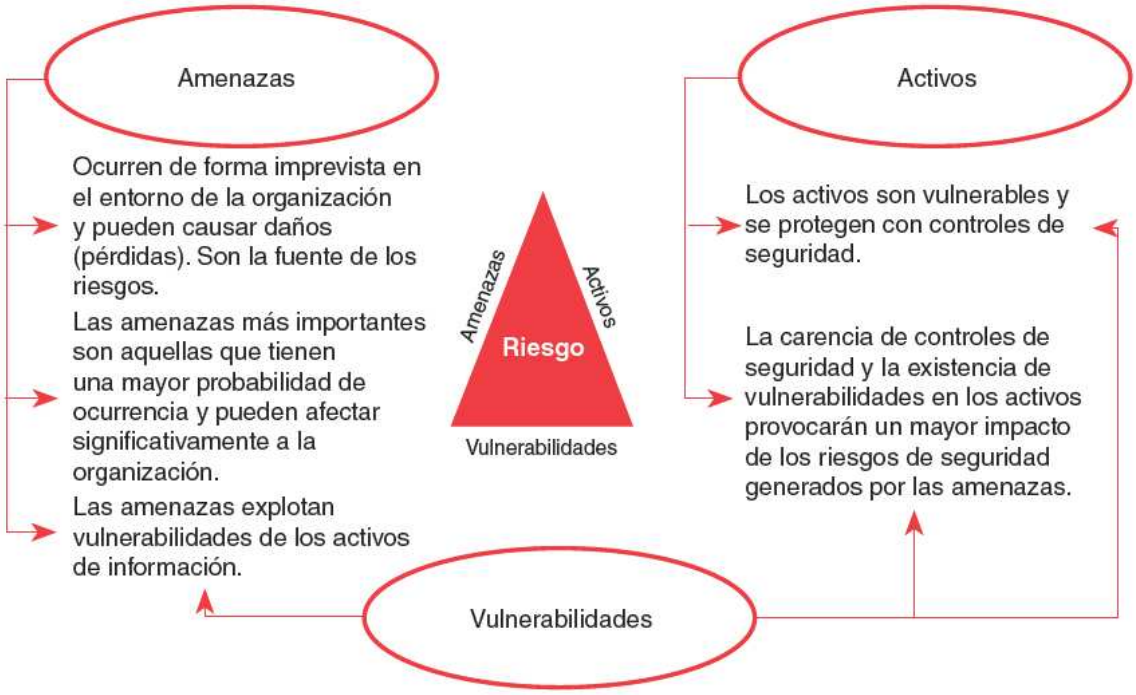


Figura 11. Relación Activo-Amenaza-Vulnerabilidad
Fuente: Instituto Nacional de Tecnologías de la Información INTECO - España

Actividad 2.3: Determinar la Probabilidad de ocurrencia de una amenaza.

Establecer a base de datos históricos, indicadores de mercado o juicio de expertos la probabilidad de que se produzca una amenaza. La probabilidad de ocurrencia puede ser según el análisis de riesgo cuantitativo o cualitativo.

Cuando se realiza un análisis cuantitativo el valor de la probabilidad se encuentra entre 0 y 1 (cero y uno), mientras que cuando se realiza un análisis cualitativo se establece una escala de valoración, por ejemplo: Muy Frecuente, Frecuente, Normal y Poco Frecuente.

Para elegir una de estas alternativas, revisemos las características más relevantes de estos dos tipos de análisis:

Característica	Cuantitativo	Cuantitativo
Cálculos	Numéricos	No Numéricos
Aplicable	No siempre	Siempre
Análisis Costo/Beneficio	Concreto	Subjetivo
Objetividad	Alta	Baja
Comprensible por la dirección	Mayor	Menor

Tabla 20. Características de Análisis Cuantitativo y Cuantitativo

El análisis de datos mediante tablas, análisis algorítmico, y árboles de ataque lo detalla la metodología MAGERIT (Ver MAGERIT, Libro III – Guía de Técnicas, 2.1; 2.2 y 2.3).

Actividad 2.4: Identificar Salvaguardas

Identificar los mecanismos de salvaguarda asociadas a cada activo. Es una buena práctica que en el plan de Gestión de Riesgos se obtenga información del coste del mantenimiento de tales salvaguardas, esto ayudará a saber el costo neto de protección para reducir el riesgo. Los mecanismos de salvaguarda pueden ser procedimientos, políticas de personal, soluciones técnicas, dispositivos, físicos o lógicos que reducen el riesgo (Ver MAGERIT, Libro II – Catálogo de Elementos, 6, p. 49).

Actividad 2.5: Valorizar y Estimar el Impacto

Valorar el impacto sobre un activo debido a una amenaza, es decir, conocer el alcance de daño o grado de cambio sobre un activo. Para estimar el impacto, se lo calcula por la degradación del activo mediante un porcentaje de su valor expresado en formato monetario o duración (segundos/minutos/hora/días/semanas/meses).

Cualitativamente el impacto se lo puede expresar mediante una escala de valores, por ejemplo: Muy Alto, Alto, Medio, Bajo y Muy Bajo. (Ver NIST 800-30, Fase 6 Impact Analysis, p. 21)

Actividad 2.6: Analizar, Estimar y Priorizar el Riesgo

Una vez que se ha obtenido toda la información de las actividades anteriores, se procede a analizar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para el proyecto.

$$\textbf{Riesgo}_{\text{Activo}} = \textbf{Probabilidad}_{\text{Ocurrencia Amenaza}} * \textbf{Impacto}_{\text{Activo}}$$

A continuación se presenta los siguientes ejemplos para determinar la probabilidad de ocurrencia:

Ejemplo Cuantitativo:

CARACTERISTICA	INFORMACIÓN
ACTIVO:	Servidor de aplicaciones
VALOR DEL ACTIVO:	$10,000 USD
VULNERABILIDAD:	Material inflamable en el Centro de Procesamiento de Datos
AMENAZA:	Incendio
PROBABILIDAD DE OCURRENCIA:	Datos Históricos: En los últimos 10 años se han producido 5 principios de incendio en la organización (0.5).
SALVAGUARDA:	Sistema de detección / extinción de incendios
IMPACTO:	Degradación Baja, 20% del valor del activo ($2,000 USD)

Riesgo = 0.5 * $2,000 = $1,000

El riesgo de que un incendio afecte al servidor de aplicaciones asciende a $1,000 USD al año.

Ejemplo Cualitativo:

Escalas de Valoración Cualitativa:

VALOR DEL ACTIVO	
MUY ALTO	MA
ALTO	A
MEDIO	ME
BAJO	B
MUY BAJO	MB

VALOR DEL IMPACTO	
MUY ALTO	MA
ALTO	A
MEDIO	ME
BAJO	B
MUY BAJO	MB

PROBABILIDAD DE OCURRENCIA	
MUY FRECUENTE	MF
FRECUENTE	F
NORMAL	N
POCO FRECUENTE	PF

RIESGO	
MUY ALTO	MA
ALTO	A
MEDIO	ME
BAJO	B
MUY BAJO	MB

IMPACTO		DEGRADACION		
		10%	50%	100%
MUY ALTO	MA	ME	A	MA
ALTO	A	B	ME	A
MEDIO	ME	MB	B	ME
BAJO	B	MB	MB	B
MUY BAJO	MB	MB	MB	MB

RIESGO		PROBABILIDAD DE OCURRENCIA			
IMPACTO		MF	F	N	PF
MUY ALTO	MA	MA	MA	A	ME
ALTO	A	MA	A	ME	B
MEDIO	ME	A	ME	B	B
BAJO	B	M	B	MB	MB
MUY BAJO	MB	B	MB	MB	MB

CARACTERISTICA	INFORMACIÓN
ACTIVO:	Servidor de Base de Datos
VALOR DEL ACTIVO:	Muy Alto (MA)
VULNERABILIDAD:	Antivirus Desactualizado
AMENAZA:	Virus
PROBABILIDAD DE OCURRENCIA:	Indicadores de mercado: Los ataques de Virus son Frecuentes (F)
SALVAGUARDA:	Software de detección de actividades anormales en la red y servidores
IMPACTO:	Si el valor de impacto es Muy Alto (MA) y la Degradación es al 100% entonces el impacto terminal será Muy Alto (MA).

Riesgo = Frecuente (F) * Muy Alto (MA) = Muy Alto

El riesgo de que un virus infecte al Servidor de Base de Datos es Muy Alto.

Proceso 3: Gestión del Riesgo

Objetivos:

Interpretar los Resultados de las actividades de Análisis de Riesgos

Presentar la estructura de un Plan de Gestión del Riesgo

Producto de Entrada:

Análisis de Gestión del riesgo

Producto de Salida:

Estrategia de Gestión del Riesgo mediante controles de mitigación, aceptación, transferencia y evitación.

Técnicas, prácticas y pautas:

Reuniones (Ver MAGERIT Libro III – Guía de Técnicas, 3.6.2, p. 65)

Análisis de riesgos (Ver proceso 2)

Planificación de proyectos (Ver MAGERIT Libro III - Guía de Técnicas, 3.5, p. 60)

Análisis Coste - Beneficio (Ver MAGERIT Libro III - Guía de Técnicas, 3.1, p. 26; NIST 800-30, Cost-Benefit Analysis, 4.5, p.37)

Participantes:

Director de Riesgos (CRO)

Director Ejecutivo (CEO)

Comité de Proyecto

Actividad 3.1 Interpretación de los Resultados

Procesar los impactos y riesgos identificados en el proceso anterior, y definir los umbrales de riesgo considerados como aceptables o inaceptables. Es importante indicar que el miembro del equipo de trabajo en definir el umbral de riesgo es el Director de Riesgos del Proyecto, y este debe informar y acordar con la Dirección Ejecutiva, y en reunión de trabajo comunicar al resto del Equipo. La Dirección Ejecutiva por su parte comunicará al Comité de Proyecto.

Esta cadena de comunicación permitirá que todos los involucrados tengan un conocimiento suficiente del entorno, situación y organización del proyecto para aumentar la eficacia y eficiencia de los miembros.

Los Riesgos que han sido declarados como inaceptables se los tratará de la siguiente manera:

a.) Mitigación: Implementar controles/salvaguardas que reduzcan el Riesgo sea en la probabilidad de ocurrencia o en el impacto. Para aquello la realización de un análisis coste-beneficio es fundamental ya que evidenciará si conviene asumir el costo del control/salvaguarda. Entre los principales costos a considerar son los siguientes:

- Costo de Adquisición
- Costo de Transporte
- Costo de Seguro
- Costo de Instalación y puesta a punto
- Costo de Mantenimiento
- Costo de Administración

b.) **Aceptación:** Asumir los riesgos que se encuentran fuera del nivel aceptable del proyecto. Esta decisión lo tomará la máxima autoridad, es decir, el Comité de Proyecto. Es necesario definir un documento/acta en donde se plasmen los acuerdos, la responsabilidad y el alcance de aceptación; con el único objetivo de tener respaldos de compromiso dentro del proyecto.

c.) **Transferencia:** Compartir parte del Riesgo con terceras partes

d.) **Evitación:** Eliminar la actividad que crea el riesgo (cuando esto sea practicable), de manera que el mismo ya no exista

El juicio de expertos en esta actividad es importante y el manejo de resultados debe ser transparente (Ver NIST 800-30, Results Documentation, Fase 9, p.26). El Análisis de decisiones a base de la teoría de Probabilidad y Estadística es otra de las técnicas a tomar en cuenta en esta fase (Ver MAGERIT Libro III - Guía de Técnicas, 3.7.3.1, p. 70).

Actividad 3.2 Plan de Gestión del Riesgo

A base del análisis de las mejores prácticas, la estructura del documento del Plan de Gestión del Riesgo que proponemos es la siguiente:

1. Introducción
2. Marco de Referencia
3. Objetivo
   - 3.1 Objetivo General
   - 3.2 Objetivos Específicos.
4. Alcance
5. Responsabilidades
6. Salvaguardas a implantar
7. Presupuesto
8. Plazos de Ejecución

Al momento de desarrollar el Plan de gestión de Riesgos se debe detallar:

- En la Introducción: Un breve antecedente de los resultados del análisis de riesgos y la interpretación de resultados.
- El Marco de Referencia debe tratar puntos neurálgicos del Proyecto de TI, sus objetivos, los productos a obtener y los plazos a cumplir.
- Los objetivos: deben ser determinados enfocados en el tratamiento de los riesgos que se encuentran fuera del nivel de aceptación.
- El Alcance: delimitar la administración del manejo de impacto y del riesgo que afrontan los activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo
- Responsabilidades: Unidad Responsable de la Ejecución acompañada de objetivos de cumplimiento.
- Las Salvaguardas a implantar: Tareas y actividades para mitigar el riesgo.
- Presupuesto: Estimación de costes: admirativos, técnicos, de operación, adquisición, implantación, mantenimiento, capacitación, de desarrollo, entre otros.
- Plazos de Ejecución: desde su arranque hasta su puesta en operación.

Actividad 3.3 Ejecución del Plan

Puesta en marcha el Plan de Gestión del Riesgo por parte de los responsables designados. Se debe tomar en cuenta que el plan es un proceso continuo y que puede ser mejorado o cambiado según las necesidades del proyecto. Por tal razón la distribución, comunicación, gestión de versiones y cambios del documento es un proceso que se encuentra dentro de los parámetros de gestión.

CAPITULO 3

APLICACIÓN DE LA GUÍA Y ANÁLISIS DE RESULTADOS

Una vez definida la Guía de Gestión de Riesgos en el capítulo anterior, se procederá a aplicar la guía a un Proyecto que integre las Tecnologías de Información y las Comunicaciones considerando los Elementos IT definidos, es decir, Hardware [HW], Software [SW], Bases de Datos [BD], Redes y Telecomunicaciones [COM], Recurso Humano [RH], Legal [L], Financiero [F] y Servicios [S].

3.1 MARCO GENERAL DE REFERENCIA DEL PROYECTO

Las metas de esta Fase es determinar los objetivos del proyecto, establecer las pautas generales que se imponen sobre el proyecto y determinar de manera formal las acciones a realizar a lo largo del proyecto. Para tal efecto y como productos de entrada contaremos con la documentación del proyecto (especificaciones, pliegos, oferta, entre otros) y como producto de salida obtendremos la especificación del proyecto, recursos y equipo de trabajo.

3.1.1 ALCANCE DEL PROYECTO

Nombre del Proyecto:

Mejoramiento de la calidad de la Educación particular popular y de la comunicación social comunitaria “Plan Amanecer”.

Sponsor y Monto:

Ministerio de Gobierno y Ministerio de Educación de la República del Ecuador. Monto: $30’000,000 (Treinta millones de dólares americanos)

Alcance y Beneficiados:

Cubre a las 24 provincias del Ecuador (Especificaciones ver en Productos, pág. 91). Escuelas fisco-misionales dirigidas por la Conferencia Episcopal Ecuatoriana.

Tiempo de Ejecución:

Dos (2) años

Empresa Ejecutora:

Consorcio Eductrade – Santillana

- Oficinas Centrales Dirección: Calle Asunción Castell, 13 28020 Madrid-España
- Oficina en Ecuador: República de El Salvador N35-33 y Portugal Edificio Gabriela, Oficina 404. Quito-Ecuador

Objetivos[35]:

- Fortalecer la gestión a través del equipamiento de las instituciones educativas y el desarrollo de contenidos y métodos adecuados.
- Acceder a nuevos recursos por medio de infraestructura tecnológica, al alcance de todos.
- Mejorar las competencias docentes con un plan de capacitación continua basado en cuatro ámbitos de contenidos: tecnológico, pedagógico, metodológico y humanístico.
- Integrar fines educativos con las necesidades sociales a través del trabajo directo con las familias y la dotación de talleres y laboratorios para el desarrollo de las comunidades.
- Fortalecer la formación de padres, profesores y alumnos, como personas libres y responsables, capaces de conocer la realidad y comprometerse con ella.

Productos:

- 428 Aulas virtuales (66 de 5 puestos, 338 de 10 puestos, 23 de 16 puestos y 1 de 20 plazas)

[35] http://plataforma.planamanecer.com/

- 1,132 Equipos Individuales (Computador + impresora)
- Software Educativo (7 CDs para primaria [de primero a séptimo de básica] + 1 CD para secundaria [Historia y Geografía]). Número de Copias: 2,000/CD, Total 14,000.
- Redes y Comunicaciones (Internet para las 428 aulas y 1,132 equipos individuales mediante equipos satelitales y GSM)
- Planificar, Organizar y Administrar la infraestructura Tecnológica y Equipo de Trabajo del Plan Amanecer, incluido el Centro de Operaciones de Red y Servicios (NOC) para la entrega y soporte de servicios de IT.
- Instalación de Software Base, herramientas y utilitarios para aulas, equipos individuales y Centro de Operaciones (NOC).
- Enlace de Comunicaciones (Autorización del uso de frecuencias y servicio portador para la operación de la infraestructura de comunicaciones del Plan Amanecer)
- Colaboración virtual y capacitaciones mediante Videoconferencias.
- Instalar equipos de IT a 102 laboratorios técnicos artesanales (Electrónica, Electricidad y Mecánica); 139 laboratorios de Ciencias (Física, Química y Biología) y 16 Radios.
- Desarrollo de un Portal Educativo
- Desarrollo de una Plataforma para la Educación Virtual (e-learning)
- Generación de Planes, Programas y Servicios en: Sensibilización (Comunicación, promoción y difusión del proyecto); Formación (Capacitación y transferencia de conocimiento/tecnología a todo el Equipo que conforma el proyecto) y Evaluación (Informe de progreso, sistema de indicadores y Transferencia)

Proceso Entrega Recepción:

El proceso ha sido definido según las normas gubernamentales ecuatorianas de entrega recepción, tal y como se muestra en la siguiente figura:

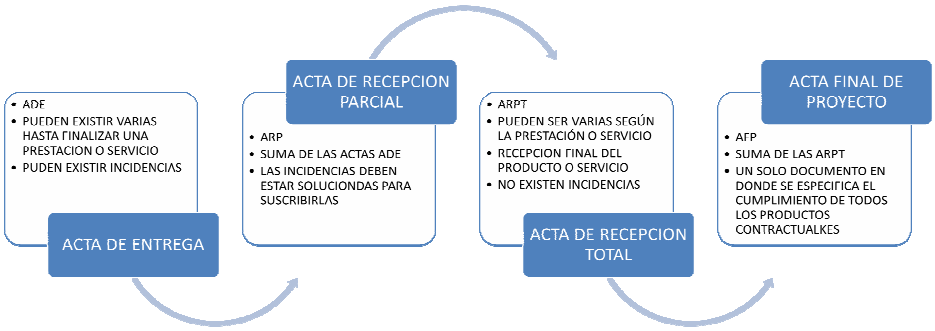


Figura 12. Proceso Contractual Entrega-Recepción de Productos y Servicios
Fuente: Plan Amanecer

Planes Contractuales:

- Plan de Ejecución: Acciones y nivel de prioridad para cumplir los objetivos.
- Plan Operativo: Conjunto de actividades de carácter administrativo, operativo y logístico en el que se especifican los responsables y los fondos para alcanzar las metas planteadas según el cronograma del proyecto.

Adquisición, Instalación y Operación:

El equipamiento completo será adquirido (por acuerdo gubernamental y de crédito entre Ecuador y España) en Europa, sin embargo, si algún elemento, equipo y/o suministro que sea necesario para cumplir con los objetivos del proyecto y que tenga mejores prestaciones, se lo podrá adquirir en el Ecuador. El ejecutor realizará el cambio tecnológico debidamente justificado a la Unidad de Control del Proyecto.

3.1.2 ESTABLECER EL CONTEXTO ORGANIZACIONAL Y ÁREAS CRÍTICAS

La organización que ejecutará el proyecto será un Consorcio (Eductrade y Santillana) de nacionalidad española, con oficinas y personal Directivo en Quito.

Adicional al equipo de España la empresa ha dispuesto que su personal especialista de Argentina se radique en Quito, para establecer lineamientos de capacitación, soporte y estrategia para la entrega-recepción y operación del equipamiento tecnológico y de comunicaciones del proyecto.

Por su parte el Gobierno de la República del Ecuador, ha dispuesto la organización de un equipo de trabajo coordinado por los Ministerios de Gobierno y Educación para el control, fiscalización y Dirección del personal. La Dirección

Ejecutiva del Proyecto será dirigida por el ente gobernante en las instituciones beneficiadas fisco-misionales, Conferencia Episcopal Ecuatoriana.

En el Anexo G de este documento se encuentra una tabla resumen del marco legal del proyecto Plan Amanecer.

El Consorcio ejecutor del Proyecto deberá entregar como hitos de inicio de proyecto los siguientes documentos:

- Cronograma de Proyecto
- Plan estratégico de TI
- Plan de Gestión de Riesgos
- Plan de Gestión de proveedores
- Directrices de administración y acciones correctivas de riesgos relacionados con TI.

3.1.3 EQUIPO DEL PROYECTO

En el Anexo D de este documento se detalla el equipo de trabajo que se ha definido en la Guía. Sin embargo se debe tomar en cuenta que por razones de estructura organizacional puede cambiar, y es criterio del Responsable de la Gestión del Riesgo determinar a manera de matriz RACI las funciones y definiciones de cada miembro del equipo de proyecto.

A continuación se presenta la distribución del personal del Proyecto Plan Amanecer, a nivel de área:

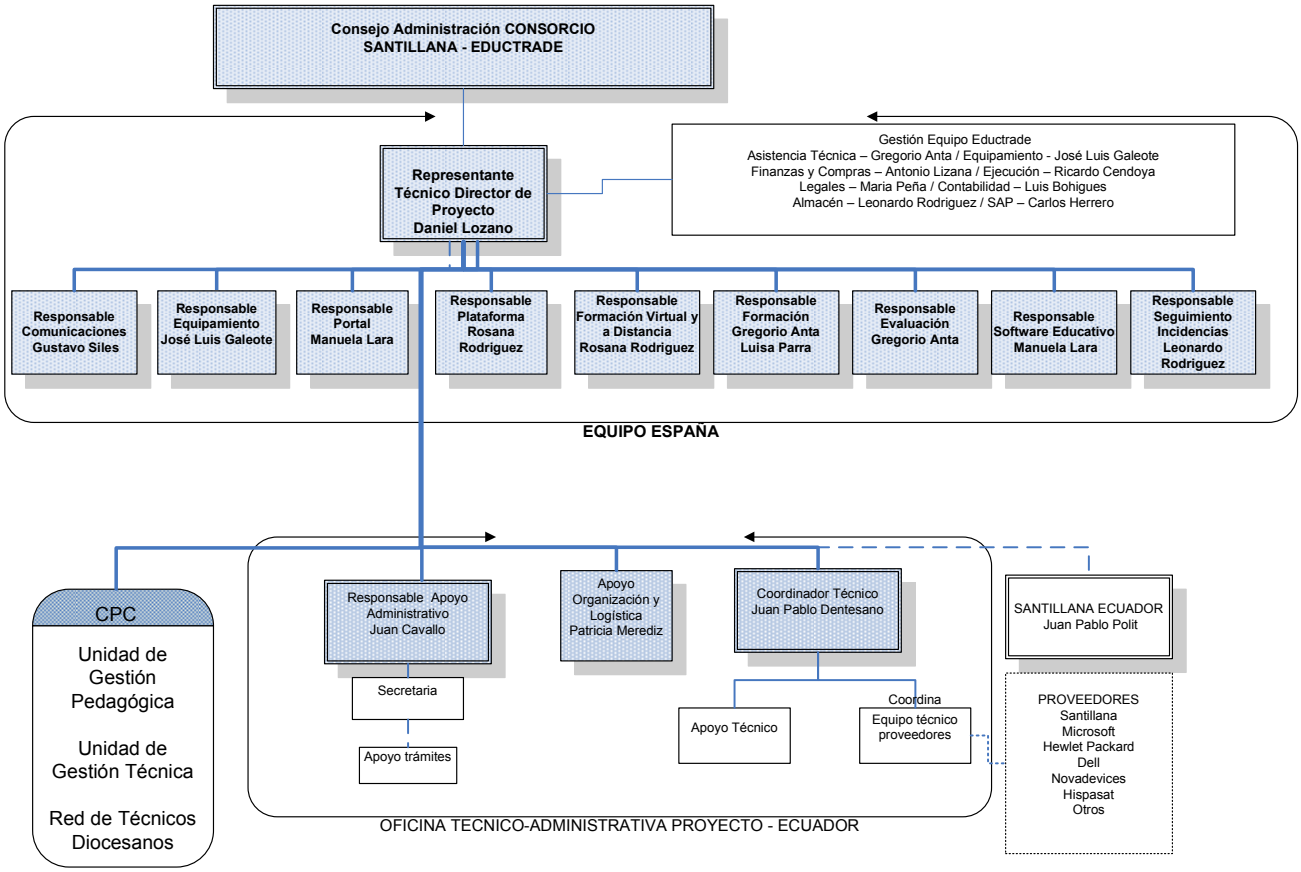
Personal	Área	Servidor (LOSEP)
Consejo de Administración (Comité)	Proyecto	N/A
Director de Proyecto	Proyecto	4NJS
Director Unidad Ejecutora	Proyecto	4NJS
Project Control Manager	Proyecto	Servidor Público 14
Analista de TI - Fiscalizador	Proyecto	Servidor Público 5
Especialista Web	Portal	Servidor Público 8
Especialista de Comunicaciones	Redes y Comunicaciones	Servidor Público 8
Especialista de E-learning	Plataforma	Servidor Público 8
Especialista de Formación	Capacitación	Servidor Público 8

Personal	Área	Servidor (LOSEP)
Especialista Equipamiento	Bienes y Servicios	Servidor Público 8
Especialista Animación	Software Educativo	Servidor Público 8
Especialista Administrativo	Finanzas, logística	Servidor Público 8
Coordinador Técnico	Coordinación Proyecto	Servidor Público 14

Tabla 21. Equipo de Proyecto

Las modalidades de contrato de cada miembro del equipo, a excepción del Director de Proyecto, son por servicios ocasionales durante un año, con opción a renovación. Esto según la ley orgánica del Servicio Público LOPSEP.

El equipo que realizará los trabajos del proyecto se presenta a continuación:



3.1.4 RECURSOS

Esta actividad se refiere a determinar y estimar el costo de los materiales, equipos, software y suministros, en este caso para ejecutar el proyecto durante 24 meses.

Ítem	Cantidad	Descripción	Costo Unitario	Tiempo de Vida	Tiempo Proyecto	Prorrateo (meses de proyecto / tiempo vida)	Valor (cantidad* costo unitario *prorrateo)
Adquisición de PCs	20	Estación de Trabajo	1,500.00	24	24	1	30,000.00
Adquisición de Laptops	10	Portátiles para Directivos	1,200.00	24	24	1	12,000.00
Adquisición de software	30	Licenciamiento SO, Ofimática, Proyectos	22,500.00	24	24	1	675,000.00
Gastos de mantenimiento de hardware y software anteriores.	1	Mantenimiento anual	10,000.00	12	24	2	20,000.00
Gastos de comunicaciones	1	Líneas, teléfono, correo, Internet, etc.	13,200.00	12	24	2	26,400.00
Gastos de instalación	1	Acondicionamiento de oficinas y materiales, gastos de viaje, logística, etc.	50,000.00	12	24	2	100,000.00
Recursos Humanos	20	Personal de Operativo del Proyecto (Directores y especialistas dentro del rubro de Proyecto)	1,500.00	12	24	2	60,000.00
Gastos de consultoría	20	En caso de requerirse algún consultor externo en cualquier etapa del proyecto.	5,000.00	12	24	2	200,000.00
Gastos de formación	10	De todo tipo (Desarrolladores, Operadores, Implantadores, Usuario Final,etc.).	1,500.00	12	24	2	30,000.00
Gastos de material	8	Papel, toner, material de oficina, etc.	60.00	24	24	1	480.00
Costes derivados de la curva de aprendizaje	20	De todo el personal involucrado: Desarrolladores, Instaladores, especialistas	1,000.00	24	24	1	20,000.00
Costes financieros salvauardas a identificar	1	Proyección en funión del costo total del proyecto (1%)	300,000.00	24	24	1	300,000.00
TOTAL							**1,473,880.00**

Tabla 22. Resumen de Costos de Recursos para Ejecutar el Proyecto

Fuente: Plan Amanecer

3.1.5 CRITERIOS DE EVALUACIÓN

Los criterios de Evaluación para ejecutar el análisis de riesgos serán:

- Valor económico del activo
- Probabilidad de ocurrencia de una amenaza

- Porcentaje de degradación del activo
- Impacto
- Riesgo

3.1.6 ACUERDOS

Los formatos en cuanto a documentos y comunicaciones serán los siguientes:

<table>
<tr><th>Tipo</th><th>Descripción</th><th>Formato Numeración</th><th>Ejemplo</th></tr>
<tr><td rowspan="3">Oficios</td><td>De Director a Unidad Ejecutora</td><td>#-DP-año</td><td>01-DP-2011, siendo # un número secuencial</td></tr>
<tr><td>De Unidad Ejecutora a Consorcio</td><td>#-PA-año</td><td>01-PA-2011, siendo # un número secuencial</td></tr>
<tr><td>De Project Control Manager a Unidad Ejecutora a Consorcio</td><td>#-PA/FIS-año</td><td>01-PA/FIS-2011, siendo # un número secuencial</td></tr>
<tr><td></td><td>Referencia del Oficio</td><td>REF: Categoría - Actividad</td><td>REF: CAT01 - Antivirus</td></tr>
<tr><td>Email</td><td>Envío</td><td>De:
Para:
Asunto: Codificación Categoría - Actividad</td><td>De: director.proyecto@eductrade.com
Para: director.ejecutivo@planamanecer.com
Asunto: CAT01 - Instalación Aulas</td></tr>
<tr><td>Actas</td><td>Definiciones, Negociaciones y Acuerdos en Reuniones de Trabajo</td><td>Lugar:
Fecha:
Objeto:
Orden del día:
Asisten:</td><td>Lugar: Plan Amanecer
Fecha: 09 de Noviembre de 2011
Objeto: Estado Financiero
Orden del día: Análisis verificación mes de Octubre de 2011
Asisten: Nombre1, Nombre2, Nombre 3</td></tr>
<tr><td>Tablas de Riesgos</td><td>Valores para cada tipo de Riesgo - datos Cualitativos

Para información se agrega este campo. Es importante indicar que si el análisis es cuantitativo este campo no aplica.</td><td>Valor del Activo, Valor de Impacto, probabilidad, impacto y riesgo.</td><td>
<table>
<tr><th colspan="2" rowspan="2">IMPACTO</th><th colspan="3">DEGRADACION</th></tr>
<tr><th>10%</th><th>50%</th><th>100%</th></tr>
<tr><td>MUY ALTO</td><td>MA</td><td>ME</td><td>A</td><td>MA</td></tr>
<tr><td>ALTO</td><td>A</td><td>B</td><td>ME</td><td>A</td></tr>
<tr><td>MEDIO</td><td>ME</td><td>MB</td><td>B</td><td>ME</td></tr>
<tr><td>BAJO</td><td>B</td><td>MB</td><td>MB</td><td>B</td></tr>
<tr><td>MUY BAJO</td><td>MB</td><td>MB</td><td>MB</td><td>MB</td></tr>
</table>
<table>
<tr><th colspan="2" rowspan="2">RIESGO</th><th colspan="4">PROBABILIDAD DE OCURRENCIA</th></tr>
<tr><th colspan="2">IMPACTO</th><th>MF</th><th>F</th><th>N</th><th>PF</th></tr>
<tr><td>MUY ALTO</td><td>MA</td><td>MA</td><td>MA</td><td>A</td><td>ME</td></tr>
<tr><td>ALTO</td><td>A</td><td>MA</td><td>A</td><td>ME</td><td>B</td></tr>
<tr><td>MEDIO</td><td>ME</td><td>A</td><td>ME</td><td>B</td><td>B</td></tr>
<tr><td>BAJO</td><td>B</td><td>M</td><td>B</td><td>MB</td><td>MB</td></tr>
<tr><td>MUY BAJO</td><td>MB</td><td>B</td><td>MB</td><td>MB</td><td>MB</td></tr>
</table>
</td></tr>
</table>

Tipo	Descripción	Formato Numeración	Ejemplo
Riesgos	Riesgo Cualitativo (Si los activos son más de 10, estandarizar mediante tablas)	Característica: Activo: Valor del activo: Vulnerabilidad: Amenaza: Probabilidad de ocurrencia: Salvaguarda: Impacto:	Característica: información Activo: Servidor de Aplicaciones Valor del activo: $10,000 USD Vulnerabilidad: Material inflamable en el centro de procesamiento de datos Amenaza: Incendio Probabilidad de ocurrencia: Datos históricos: en los últimos 10 años se han producido 5 principios de incendio en la organización (0.5). Salvaguarda: Sistema de detección / extinción de incendios Degradación: 20% del valor del activo Impacto: $2,000 USD Riesgo: Probabilidad * Impacto Riesgo= 0.5*$2,000=$1,000 USD
	Riesgo Cuantitativo (Si los activos son más de 10, estandarizar mediante tablas) Para información se agrega este campo. Es importante indicar que si el análisis es cuantitativo este campo no aplica.	Característica: Activo: Valor del activo: Vulnerabilidad: Amenaza: Probabilidad de ocurrencia: Salvaguarda: Impacto:	Característica: información Activo: Servidor de base de datos Valor del activo: Muy alto (MA) Vulnerabilidad: Antivirus desactualizado Amenaza: Virus Probabilidad de ocurrencia: Indicadores de mercado: los ataques de virus son frecuentes (F) Salvaguarda: Software de detección de actividades anormales en la red y servidores Degradación: 100% Impacto: Sobre la base de la tabla anterior, si el valor de impacto es muy alto (MA) y la degradación es al 100% entonces el impacto terminal será muy alto (MA). Riesgo= Probabilidad * Impacto Riesgo= Frecuente*Muy Alto = Muy Alto

Tabla 23. Acuerdos de Formatos para ejecutar Proyectos

3.2 ANALISIS DE RIESGOS

Las metas que persigue esta Fase es identificar todos los activos y componentes del Proyecto, determinar Vulnerabilidades y Amenazas así como la probabilidad de ocurrencia e identificar Salvaguardas y valorizar el posible impacto priorizando el mayor riesgo para determinarlo cuantitativamente. Los productos de entrada son la documentación del contexto organizacional y áreas críticas del proyecto. Como productos de salida se obtendrá la caracterización de los activos y el Análisis de Riesgos.

3.2.1 IDENTIFICAR Y VALORAR LOS ACTIVOS DE LA ORGANIZACIÓN

Los activos serán clasificados por los siguientes elementos de TI, tomando en cuenta que de aquí en adelante se cubrirán las fases *adquisición e implantación* de equipamiento y servicios de tecnologías de información y comunicaciones:

- Hardware [HW]
- Software [SW]
- Bases de Datos [BD]
- Redes y Telecomunicaciones [COM]
- Recurso Humano [RH]
- Legal [L]
- Financiero [F]
- Servicios [S]

Por la cantidad de información generada, una vez identificado los activos de TI del Proyecto Plan Amanecer, todos los datos se encuentran en el CD adjunto a esta investigación (**ANEXO C**).

La siguiente Tabla muestra un extracto de la información para que el lector pueda identificar los parámetros considerados:

AREA DE GESTION	No. ACTIVO	ACTIVO	CANT. TOTAL	DESCRIPCION ACTIVO	MARCA	MODELO	VALOR UNITARIO	VALOR TOTAL
HARDWARE	1	COMPUTADOR PERSONAL	1132	COMPUTADOR PERSONAL	DELL	OPTIPLEX GX520	943.71	1,068,279.72
HARDWARE	3		7	ESTACION DE TRABAJO Y HELP DESK TECNICO	DELL	PRECISION 690	2,968.10	20,776.70
HARDWARE	43	MONITORES	4098	MONITOR 17"	NOVADEVICES	L-7D	113.06	463,319.88
……								
SOFTWARE	49	OFIMÁTICA	28	OFFICE 2007	MICROSOFT	OFFICE 2007 PRO	140.45	3,932.60
SOFTWARE	50		5713	OFFICE 2007	MICROSOFT	OFFICE 2007 ESTÁNDAR	118.07	674,533.91
SOFTWARE	55	SISTEMA OPERATIVO	4098	WINDOWS	MICROSOFT	WINDOWS VISTA STD	130.55	534,993.90
……								
BASES DE DATOS	92	DATOS DE GESTIÓN INTERNA	1	GESTION DE PROYECTO	N/A	N/A	201.76	201.76
BASES DE DATOS	102	DATOS DE CONFIGURACIÓN	1	PROTOCOLO INSTALACION CPC	N/A	N/A	64.20	64.20
……								
REDES Y TELECOMUNICACIONES	132	REDES LOCALES	1	CPD (CENTRO DE PROCESAMIENTO DE DATOS)	N/A	N/A	11,713.82	11,713.82
……								
RECURSO HUMANO	139	ADMINISTRADORES DE SISTEMAS	2	PERSONAL CPC	N/A	N/A	30,418.82	60,837.64
RECURSO HUMANO	140	ADMINISTRADORES DE REDES Y COMUNICACIONES	5	PERSONAL CPC	N/A	N/A	12,167.53	60,837.64
……								
LEGAL	151	GARANTÍA GARANTÍAS	4098	GARANTIAS COMPUTADOR ESTUDIANTE TIPO THIN CLIENT	NOVADEVICES	KYPUS THIN CLIENT	303.09	1,242,070.22
LEGAL	152		428	GARANTIAS SERVIDOR DE APLICACIONES	DELL	POWER EDGE SC440	2,543.34	1,088,549.52
……								
FINANCIERO	168	ACTAS DE ENTREGA Y ACTAS DE RECEPCIÓN	11,500	ACTAS DE ENTREGA RECEPCION	N/A	N/A	5.10	58,650.00
……								
SERVICIOS	171	SOPORTE TÉCNICO	1	SOPORTE TECNICO EXTERNOS E INTERNOS	N/A	N/A	156,721.41	156,721.41
SERVICIOS	180	SERVICIO NOC (NETWORK OPERATIONS CENTER)	1	NOC (NETWORK OPERATIONS CENTER)	N/A	N/A	78,360.70	78,360.70
……								

Tabla 24. Síntesis: Identificación y Valorización de Activos – Plan Amanecer

Fuente: Plan Amanecer - Alcance Económico

3.2.2 ANALIZAR VULNERABILIDADES Y AMENAZAS

A base de la información de los activos se analiza las debilidades que se pueden presentar de manera accidental o intencionalmente así como la posibilidad de que se produzca un daño en los activos o procesos del proyecto.

Por la cantidad de información generada, una vez identificado las vulnerabilidades y amenazas de los activos de TI del Proyecto Plan Amanecer, toda la Información se encuentra en el CD adjunto de esta investigación (**ANEXO C**).

La siguiente Tabla muestra un extracto del contenido para que el lector pueda identificar los datos generados.

No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	VULNERABILIDAD	AMENAZA
1	COMPUTADOR PERSONAL	1132	INFRAESTRUCTURA INSTALACIONES INADECUADAS DIMENSIONAMIENTO DE HW DEFECTO DE FABRICACIÓN ANTIVIRUS DESACTUALIZADO	ROBO ATAQUE FISICO AVERÍA VIRUS
4	SERVIDOR DE APLICACIONES	428	INSTALACIONES INADECUADAS CONTRASEÑAS DÉBILES FALTA DE USO DE CRIPTOGRAFÍA EN LA COMUNICACIÓN COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC EMPLEADOS DESCONTENTOS, DELICUENTES AUSENCIA DE IDENTIFICACIÓN DE PERSONAS Y DE LOCALES, ETC INFRAESTRUCTURA DIMENSIONAMIENTO DE HW DEFECTO DE FABRICACIÓN ANTIVIRUS DESACTUALIZADO	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA. SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS ATAQUE FISICO AVERÍA VIRUS
…….				
60	PLATAFORMA E-LEARNING	1	CONTRASEÑAS DÉBILES, FALTA DE USO DE CRIPTOGRAFÍA EN LA COMUNICACIÓN, COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC. USO INCORRECTO LA AUSENCIA DE SISTEMAS DE CIFRADO (ENCRIPTACIÓN) EN LAS COMUNICACIONES QUE PUDIERAN PERMITIR QUE PERSONAS AJENAS A LA ORGANIZACIÓN OBTENGAN INFORMACIÓN PRIVILEGIADA. LA MALA ELECCIÓN DE SISTEMAS DE COMUNICACIÓN PARA ENVÍO DE MENSAJES DE ALTA PRIORIDAD DE LA EMPRESA PUDIERA PROVOCAR QUE NO ALCANZARAN EL DESTINO ESPERADO O BIEN SE INTERCEPTARA EL MENSAJE EN SU TRÁNSITO. CAMBIO DE LA NORMATIVA/LEYES NUEVA POLITICA	SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN ACCESO NO PERMITIDO A LA BASE DE DATOS CAMBIO DE REQUISITOS
……..				

No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	VULNERABILIDAD	AMENAZA
110	PORTAL EDUCATIVO	1	INSTALACIONES INADECUADAS CONTRASEÑAS DÉBILES FALTA DE USO DE CRIPTOGRAFÍA EN LA COMUNICACIÓN COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC EMPLEADOS DESCONTENTOS, DELICUENTES AUSENCIA DE IDENTIFICACIÓN DE PERSONAS Y DE LOCALES, ETC INFRAESTRUCTURA DIMENSIONAMIENTO DE HW DEFECTO DE FABRICACIÓN	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ROBO DESTRUCCIÓN ACCESO NO PERMITIDO A LA BASE DE DATOS
…….				
133	ENLACES SATELITALES	428	INFRAESTRUCTURA INCAPAZ DE RESISTIR A LAS MANIFESTACIONES DE LA NATURALEZA COMO TERREMOTOS, MAREMOTOS, HURACANES ETC. REDUNDANCIA TECNOLÓGICA HW-SW-COM LA AUSENCIA DE SISTEMAS DE CIFRADO (ENCRIPTACIÓN) EN LAS COMUNICACIONES QUE PUDIERAN PERMITIR QUE PERSONAS AJENAS A LA ORGANIZACIÓN OBTENGAN INFORMACIÓN PRIVILEGIADA. LA MALA ELECCIÓN DE SISTEMAS DE COMUNICACIÓN PARA ENVÍO DE MENSAJES DE ALTA PRIORIDAD DE LA EMPRESA PUDIERA PROVOCAR QUE NO ALCANZARAN EL DESTINO ESPERADO O BIEN SE INTERCEPTARA EL MENSAJE EN SU TRÁNSITO. INTRUCION DE PERSONAS NO AUTORIZADAS LOS SISTEMAS OPERATIVOS CONECTADOS A UNA RED CONTRASEÑAS DÉBILES, FALTA DE USO DE CRIPTOGRAFÍA EN LA COMUNICACIÓN, COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC.	DISPONIBILIDAD DE SERVICIO ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN MODIFICACIÓN DE DATOS MALINTENCIONADA SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS HACKING INGENIERÍA SOCIAL INTRUSIONES AL SISTEMA
…..				
140	PERSONAL CPC	5	CONTRASEÑAS DÉBILES FALTA DE USO DE CRIPTOGRAFÍA EN LA COMUNICACIÓN COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC EMPLEADOS DESCONTENTOS, DELICUENTES	ACCESO NO AUTORIZADO CURIOSIDAD INGENIERÍA SOCIAL GANANCIA MONETARIA ERRORES NO INTENCIONALES ESPIONAJE DE INFORMACIÓN CONFIDENCIAL FRAUDE
……				
151	GARANTIAS COMPUTADOR ESTUDIANTE TIPO THIN CLIENT	4098	CAPACIDAD DEL PROVEEDOR EN EL CUMPLIMIENTO DE UNA OBLIGACIÓN O PAGO DE UN ACTIVO	CUMPLIMIENTO DE LA NORMATIVA INTERNA CUMPLIMIENTO DE LA NORMATIVA EXTERNA DEFECTOS PROVOCADOS POR EL MAL USO DEL PRODUCTO
…….				
169	TRASLADO EQUIPAMIENTO	1	INFRAESTRUCTURA INSTALACIONES INADECUADAS RESOLUCION POLITICA CAMBIO EN LA ECONOMIA MANIFESTACIONES DE LA NATURALEZA COMO TERREMOTOS, MAREMOTOS, HURACANES, ETC CAMBIO DE LA NORMATIVA / SEGUROS	ROBO HUELGA TERREMOTO INUNDACION CIERRE DE VIAS (POR HUELGA, MANTENIMIENTO) PERMISOS ESPECIALES (NORMATIVA) INCREMENTO DE COSTES
…….				
180	NOC (NETWORK OPERATIONS CENTER)	1	INFRAESTRUCTURA INCAPAZ DE RESISTIR A LAS MANIFESTACIONES DE LA NATURALEZA COMO TERREMOTOS, MAREMOTOS, HURACANES ETC. REDUNDANCIA TECNOLÓGICA HW-SW-COM LA AUSENCIA DE SISTEMAS DE CIFRADO (ENCRIPTACIÓN) EN LAS COMUNICACIONES QUE PUDIERAN PERMITIR QUE PERSONAS AJENAS A LA ORGANIZACIÓN OBTENGAN INFORMACIÓN PRIVILEGIADA. LA MALA ELECCIÓN DE SISTEMAS DE COMUNICACIÓN PARA ENVÍO DE MENSAJES DE ALTA PRIORIDAD DE LA EMPRESA PUDIERA PROVOCAR QUE NO ALCANZARAN EL DESTINO ESPERADO O BIEN SE INTERCEPTARA EL MENSAJE EN SU TRÁNSITO. SISTEMA DE SOPORTE NO DISPONIBLE	DISPONIBILIDAD DE SERVICIO SOPORTE TECNICO

Tabla 25. Síntesis: Análisis de Vulnerabilidades y Amenazas – Plan Amenecer

3.2.3 DETERMINAR LA PROBABILIDAD DE OCURRENCIA DE UNA AMENAZA.

Para establecer la probabilidad de ocurrencia existen dos posibilidades: cuantitativa o cualitativa. Para esta investigación la determinación de la probabilidad será cuantitativa a base de las características definidas en la Tabla 20 de este documento. Por lo tanto, los valores estarán comprendidos entre 0 y 1(cero y uno).

En virtud de lo anterior, los valores establecidos para cada activo serán parte de datos históricos y del juicio de expertos que participaron en el del proyecto Plan Amanecer (Director de Proyecto y Director de Control de Proyecto).

Por la cantidad de información generada, los datos de la probabilidad de ocurrencia de las amenazas identificadas se encuentran en el CD adjunto de esta investigación (**ANEXO C**).

La siguiente la Tabla muestra un extracto del contenido para que el lector pueda identificar los datos generados:

AREA DE GESTION	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	AMENAZA	PROBABILIDAD DE OCURRENCIA
HARDWARE	1	COMPUTADOR PERSONAL	1132	ROBO ATAQUE FISICO AVERÍA VIRUS	0.15
HARDWARE	4	SERVIDOR DE APLICACIONES	428	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA. SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS ATAQUE FISICO AVERÍA VIRUS	0.05
……..					
SOFTWARE	60	PLATAFORMA E-LEARNING	1	SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN ACCESO NO PERMITIDO A LA BASE DE DATOS CAMBIO DE REQUISITOS	0.05
…….					
BASES DE DATOS	110	PORTAL EDUCATIVO	1	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ROBO DESTRUCCIÓN	0.05

AREA DE GESTION	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	AMENAZA	PROBABILIDAD DE OCURRENCIA
				ACCESO NO PERMITIDO A LA BASE DE DATOS	
……..					
REDES Y TELECOMUNICACIONES	133	ENLACES SATELITALES	428	DISPONIBILIDAD DE SERVICIO ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN MODIFICACIÓN DE DATOS MALINTENCIONADA SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS HACKING INGENIERÍA SOCIAL INTRUSIONES AL SISTEMA	0.35
…….					
RECURSO HUMANO	140	PERSONAL CPC	5	ACCESO NO AUTORIZADO CURIOSIDAD INGENIERÍA SOCIAL GANANCIA MONETARIA ERRORES NO INTENCIONALES ESPIONAJE DE INFORMACIÓN CONFIDENCIAL FRAUDE	0.15
……..					
LEGAL	151	GARANTIAS COMPUTADOR ESTUDIANTE TIPO THIN CLIENT	4098	CUMPLIMIENTO DE LA NORMATIVA INTERNA CUMPLIMIENTO DE LA NORMATIVA EXTERNA DEFECTOS PROVOCADOS POR EL MAL USO DEL PRODUCTO	0.15
……..					
FINANCIERO	169	TRASLADO EQUIPAMIENTO	1	ROBO HUELGA TERREMOTO INUNDACION CIERRE DE VIAS (POR HUELGA, MANTENIMIENTO) PERMISOS ESPECIALES (NORMATIVA) INCREMENTO DE COSTES	0.6
……..					
SERVICIOS	180	NOC (NETWORK OPERATIONS CENTER)	1	DISPONIBILIDAD DE SERVICIO SOPORTE TECNICO	0.02
…..					

Tabla 26. Síntesis: Probabilidad de ocurrencia de Amenazas – Plan Amanecer

3.2.4 IDENTIFICAR SALVAGUARDAS

Para cada activo se identificará los mecanismos de salvaguarda asociadas a las amenazas. Se ha considerado como mecanismos de salvaguarda procedimientos, políticas, planes, soluciones técnicas y dispositivos físicos o lógicos.

Por la cantidad de información generada, los salvaguardas identificados se encuentran en el CD adjunto de esta investigación (**ANEXO C**).

En la siguiente tabla se muestra una síntesis del contenido para que el lector pueda identificar los datos generados:

TIPO ACTIVO	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	AMENAZA	SALVAGUARDA
HARDWARE	1	COMPUTADOR PERSONAL	1132	ROBO ATAQUE FISICO AVERÍA VIRUS	PROTECCIÓN DEL EQUIPO EN EL SITIO LIMITACIÓN DE ACCESO A LAS INSTALACIONES DE LA ORGANIZACIÓN MANTENIMIENTO COPIAS DE RESPALDO SOFTWARE DE DETECCIÓN DE ACTIVIDADES ANORMALES EN LA RED Y SERVIDORES
HARDWARE	4	SERVIDOR DE APLICACIONES	428	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA. SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS ATAQUE FISICO AVERÍA VIRUS	LIMITACIÓN DE ACCESO AL SISTEMA Y NORMAS DE SEGURIDAD ACCESO A LOS DATOS SIEMPRE A TRAVÉS DEL SISTEMA IDENTIFICACIÓN POR USUARIO Y CONTRASEÑA SISTEMAS CON CARACTERÍSTICAS BIOMÉTRICAS DATOS DE APOYO PROTECCIÓN DEL EQUIPO EN EL SITIO LIMITACIÓN DE ACCESO A LAS INSTALACIONES DE LA ORGANIZACIÓN MANTENIMIENTO COPIAS DE RESPALDO SOFTWARE DE DETECCIÓN DE ACTIVIDADES ANORMALES EN LA RED Y SERVIDORES
.....					
SOFTWARE	60	PLATAFORMA E-LEARNING	1	SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN ACCESO NO PERMITIDO A LA BASE DE DATOS CAMBIO DE REQUISITOS	IDENTIFICACIÓN POR USUARIO Y CONTRASEÑA DATOS DE APOYO RECONOCIMIENTO DE DESTINO, SI EL DESTINO NO ES CONOCIDO NO SE BORRAN LOS DATOS. COMPROBACIÓN DE PERMISOS COPIAS DE RESPALDO SEÑALES DE DISPOSITIVOS LISTOS, FUNCIONAMIENTO DE TRANSACCIÓN (UN FALLO ANULA LA TRANSFERENCIA ENTERA) IDENTIFICACIÓN POR USUARIO Y CONTRASEÑA SISTEMAS CON CARACTERÍSTICAS BIOMÉTRICAS LIMITACIÓN DE ACCESO AL SISTEMA Y NORMAS DE SEGURIDAD (ACCESO A LOS DATOS SIEMPRE A TRAVÉS DEL SISTEMA) PLAN DE GESTION DE CAMBIOS
.....					
BASES DE DATOS	110	PORTAL EDUCATIVO	1	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ROBO DESTRUCCIÓN ACCESO NO PERMITIDO A LA BASE DE DATOS	LIMITACIÓN DE ACCESO AL SISTEMA Y NORMAS DE SEGURIDAD ACCESO A LOS DATOS SIEMPRE A TRAVÉS DEL SISTEMA DATOS DE APOYO RECONOCIMIENTO DE DESTINO, SI EL DESTINO NO ES CONOCIDO NO SE BORRAN LOS DATOS. COMPROBACIÓN DE PERMISOS COPIAS DE RESPALDO PROTECCIÓN DEL EQUIPO EN EL SITIO LIMITACIÓN DE ACCESO A LAS INSTALACIONES DE LA ORGANIZACIÓN CONTRATACION DE SEGUROS GESTIÓN DE PRIVILEGIOS IDENTIFICACIÓN POR USUARIO Y CONTRASEÑA
.....					

TIPO ACTIVO	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	AMENAZA	SALVAGUARDA
REDES Y TELECOMUNICACIONES	133	ENLACES SATELITALES	428	DISPONIBILIDAD DE SERVICIO ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN MODIFICACIÓN DE DATOS MALINTENCIONADA SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS HACKING INGENIERÍA SOCIAL INTRUSIONES AL SISTEMA	REDUNDANCIA FISICA / LOGICA PLAN DE CONTINUIDAD ACCESO A LOS DATOS SIEMPRE A TRAVÉS DEL SISTEMA SEÑALES DE DISPOSITIVOS LISTOS, FUNCIONAMIENTO DE TRANSACCIÓN (UN FALLO ANULA LA TRANSFERENCIA ENTERA) IDENTIFICACIÓN POR USUARIO Y CONTRASEÑA SISTEMAS CON CARACTERÍSTICAS BIOMÉTRICAS DATOS DE APOYO CIFRADO PROTECCIÓN FRENTE A CÓDIGO DAÑINO: VIRUS, TROYANOS, PUERTAS TRASERAS, ETC CONTROL DE ACCESO POLITICAS DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN SISTEMAS CON CARACTERÍSTICAS BIOMÉTRICAS LIMITACIÓN DE ACCESO AL SISTEMA Y NORMAS DE SEGURIDAD
.....					
RECURSO HUMANO	140	PERSONAL CPC	5	ACCESO NO AUTORIZADO CURIOSIDAD INGENIERÍA SOCIAL GANANCIA MONETARIA ERRORES NO INTENCIONALES ESPIONAJE DE INFORMACIÓN CONFIDENCIAL FRAUDE	SISTEMAS CON CARACTERÍSTICAS BIOMÉTRICAS CONTROL DE ACCESO POLÍTICA DE CÓDIGO DE ÉTICA POLITICAS DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN REGISTRO DE ACTUACIONES FORMACIÓN CONTINUA CONTROL DE ACCESO: ENTRADA Y SALIDA DE PERSONAS, EQUIPOS, SOPORTES DE INFORMACIÓN, ETC SISTEMAS CON CARACTERÍSTICAS BIOMÉTRICAS LIMITACIÓN DE ACCESO AL SISTEMA Y NORMAS DE SEGURIDAD (ACCESO A LOS DATOS SIEMPRE A TRAVÉS DEL SISTEMA) CONTROL DE ACCESO: ENTRADA Y SALIDA DE PERSONAS, EQUIPOS, SOPORTES DE INFORMACIÓN, ETC FIRMA ELECTRÓNICA
.....					
LEGAL	151	GARANTIAS COMPUTADOR ESTUDIANTE TIPO THIN CLIENT	4098	CUMPLIMIENTO DE LA NORMATIVA INTERNA CUMPLIMIENTO DE LA NORMATIVA EXTERNA DEFECTOS PROVOCADOS POR EL MAL USO DEL PRODUCTO	CAPACITACION ACUERDOS MANUAL DE USUARIO MANUAL DE INSTALACION MANUAL TÉCNICO
.....					
FINANCIERO	169	TRASLADO EQUIPAMIENTO	1	ROBO HUELGA TERREMOTO INUNDACION CIERRE DE VIAS (POR HUELGA, MANTENIMIENTO) PERMISOS ESPECIALES (NORMATIVA) INCREMENTO DE COSTES	PROTECCIÓN DEL EQUIPO EN EL SITIO LIMITACIÓN DE ACCESO A LAS INSTALACIONES DE LA ORGANIZACIÓN PLAN DE SEGURIDAD PLAN DE CONTINGENCIAS PROCEDIMIENTOS DE ESCALADO Y RESOLUCIÓN DE INCIDENCIAS RUTAS ALTERNATIVAS
.....					
SERVICIOS	180	NOC (NETWORK OPERATIONS CENTER)	1	DISPONIBILIDAD DE SERVICIO SOPORTE TECNICO	REDUNDANCIA FISICA / LOGICA PLAN DE CONTINUIDAD APLICACIÓN DE CONEXIÓN REMOTA EMAIL CHAT
.....					

Tabla 27. Síntesis: Identificación de Salvaguardas – Plan Amanecer

3.2.5 VALORIZAR Y ESTIMAR EL IMPACTO

Sobre la base de la guía establecida en este documento, para valorar el impacto de un activo debido a una amenaza, se lo calculará por la degradación del activo mediante un porcentaje de su valor económico, es decir, mediante la siguiente fórmula:

$$\textbf{Impacto} = \%\textbf{Degradación}_{\text{Activo}} * \textbf{Valor}_{\text{Económico}}$$

La degradación de los activos para este análisis, se lo ha establecido de la siguiente manera:

DEGRADACIÓN	% VALOR DE ACTIVO
Total	100%
Alta	90%
Media	50%
Baja	20%
Nula	0%

Tabla 28. Escala de valores de Degradación para los activos

Los valores de Impacto para el proyecto se encuentran en el CD adjunto de esta investigación (**ANEXO C**).

La siguiente Tabla muestra una síntesis del contenido para que el lector identifique los datos generados:

TIPO ACTIVO	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	VAL.TOTAL (USD)	AMENAZA	% DEGRADACIÓN	IMPACTO= %DEGRADACIÓN * VAL.TOTAL (USD)
HARDWARE	1	COMPUTADOR PERSONAL	1132	1,068,279.72	ROBO ATAQUE FISICO AVERÍA VIRUS	20%	213,655.94
HARDWARE	4	SERVIDOR DE APLICACIONES	428	1,088,549.52	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA. SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS ATAQUE FISICO AVERÍA VIRUS	20%	217,709.90
……							

TIPO ACTIVO	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	VAL.TOTAL (USD)	AMENAZA	% DEGRADACIÓN	IMPACTO= %DEGRADACIÓN * VAL.TOTAL (USD)
SOFTWARE	60	PLATAFORMA E-LEARNING	1	263,480.82	SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN ACCESO NO PERMITIDO A LA BASE DE DATOS CAMBIO DE REQUISITOS	20%	52,696.16
……							
BASES DE DATOS	130	CATEGORIAS PROYECTO	1	50,000	ACCESO NO PERMITIDO MODIFICACIÓN DE DATOS MALINTENCIONADA INTRODUCCIÓN DE DATOS INCORRECTOS DESCARGA DE DATOS EN DESTINO INAPROPIADO BORRADO DE DATOS ROBO DESTRUCCIÓN ACCESO NO PERMITIDO A LA BASE DE DATOS	20%	10,000.00
……							
REDES Y TELECOMUNICACIONES	133	ENLACES SATELITALES	428	772,711.20	DISPONIBILIDAD DE SERVICIO ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN MODIFICACIÓN DE DATOS MALINTENCIONADA SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS HACKING INGENIERÍA SOCIAL INTRUSIONES AL SISTEMA	20%	154,542.24
……							
RECURSO HUMANO	140	PERSONAL CPC	5	60,837.64	ACCESO NO AUTORIZADO CURIOSIDAD INGENIERÍA SOCIAL GANANCIA MONETARIA ERRORES NO INTENCIONALES ESPIONAJE DE INFORMACIÓN CONFIDENCIAL FRAUDE	20%	12,167.53
……							
LEGAL	151	GARANTIAS COMPUTADOR ESTUDIANTE TIPO THIN CLIENT	4098	1,242,070.22	CUMPLIMIENTO DE LA NORMATIVA INTERNA CUMPLIMIENTO DE LA NORMATIVA EXTERNA DEFECTOS PROVOCADOS POR EL MAL USO DEL PRODUCTO	90%	1,117,863.20
……							

TIPO ACTIVO	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	VAL.TOTAL (USD)	AMENAZA	% DEGRADACIÓN	IMPACTO= %DEGRADACIÓN * VAL.TOTAL (USD)
FINANCIERO	168	ACTAS ENTREGA RECEPCION	11,500	58,650.00	ROBO HUELGA TERREMOTO INUNDACION CIERRE DE VIAS (POR HUELGA, MANTENIMIENTO) PERMISOS ESPECIALES (NORMATIVA) INCREMENTO DE COSTES	20%	11,730.00
……							
SERVICIOS	180	NOC (NETWORK OPERATIONS CENTER)	1	78,360.70	DISPONIBILIDAD DE SERVICIO SOPORTE TECNICO	50%	39,180.35
……							

Tabla 29. Síntesis: Estimación de Impacto – Plan Amanecer

3.2.6 ANALIZAR, ESTIMAR Y PRIORIZAR EL RIESGO

Una vez obtenido toda la información requerida, en esta actividad se estimará el riesgo. Para este análisis la prioridad del riesgo se establecerá en función del costo, es decir, mayor costo-mayor priorización. Es importante indicar que existen activos con valor económico cero, esto no quiere decir que no tienen un valor si no más bien que es complemento de otro activo identificados como una sub-prioridad, por ejemplo:

PRIORIDAD	TIPO ACTIVO	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	VAL.TOTAL	AMENAZA	PROBABILIDAD DE OCURRENCIA	% DEGRADACIÓN	IMPACTO = %DEGRADACIÓN * VAL.TOTAL	RIESGO = PROBABILIDAD OCURRENCIA AMENAZA * IMPACTO
21	SERVICIOS	182	VIDEO CONFERENCIA (428 PUNTOS)	1	628,931.30	DISPONIBILIDAD DE SERVICIO SOPORTE TECNICO	0.15	20%	125,786.26	18,867.94
21.1	LEGAL	164	VIDEO CONFERENCIA	1	0.00	ALINEAMIENTO AL CONTRATO CUMPLIMIENTO SLA DISPONIBILIDAD	0.55	20%	0.00	0.00
Riesgo Total Video Conferencia										**$18,867.94**

El valor del Riesgo de cada activo para el proyecto Plan Amanecer se encuentran en el CD adjunto de esta investigación (**ANEXO C**). Para el cálculo del riesgo utilizaremos la siguiente fórmula:

$$\textbf{Riesgo}_{\textbf{Activo}} = \textbf{Probabilidad}_{\textbf{Ocurrencia Amenaza}} * \textbf{Impacto}_{\textbf{Activo}}$$

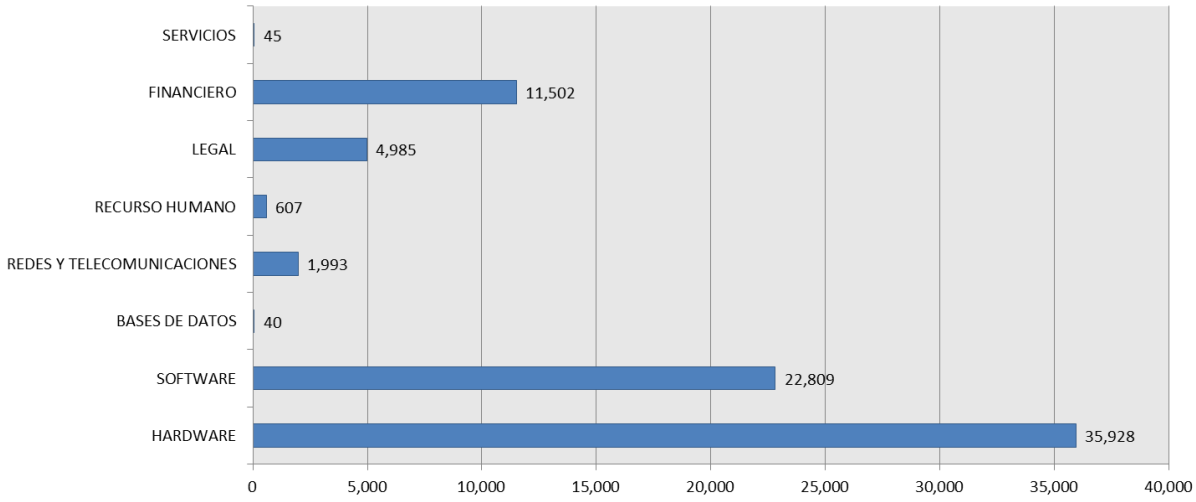
En la siguiente tabla se muestra una síntesis del contenido para que el lector identifique los datos generados:

PRIORIDAD	TIPO ACTIVO	No. ACTIVO	DESCRIPCION ACTIVO	CANT. TOTAL	VAL. TOTAL	AMENAZA	PROBABILIDAD DE OCURRENCIA	% DEGRADACIÓN	IMPACTO = %DEGRADACIÓN * VAL.TOTAL	RIESGO = PROBABILIDAD OCURRENCIA AMENAZA * IMPACTO
1	SOFTWARE	50	OFFICE 2007	5713	674,533.91	LICENCIAMIENTO INSTALACION INCOMPLETA MODIFICACIÓN DE CONFIGURACION	0.25	100%	674,533.91	168,633.48
2	LEGAL	151	GARANTIAS COMPUTADOR ESTUDIANTE TIPO THIN CLIENT	4098	1,242,070.22	CUMPLIMIENTO DE LA NORMATIVA INTERNA CUMPLIMIENTO DE LA NORMATIVA EXTERNA DEFECTOS PROVOCADOS POR EL MAL USO DEL PRODUCTO	0.15	90%	1,117,863.20	167,679.48
3	HARDWARE	11	COMPUTADOR ESTUDIANTE TIPO THIN CLIENT	4098	3,867,323.58	ROBO ATAQUE FISICO AVERÍA VIRUS MODIFICACIÓN DE CONFIGURACION	0.2	20%	773,464.72	154,692.94
…….										
7	SERVICIOS	176	GESTION DE CAMBIOS	1	1,175,410.57	CUMPLIMIENTO DEL PROCESO	0.45	20%	235,082.11	105,786.95
8	REDES Y TELECOMUNICACIONES	133	ENLACES SATELITALES	428	772,711.20	DISPONIBILIDAD DE SERVICIO ACCESO NO PERMITIDO A LA COMUNICACIÓN ERROR EN LA COMUNICACIÓN MODIFICACIÓN DE DATOS MALINTENCIONADA SUPLANTACIÓN DE IDENTIDAD INTRODUCCIÓN DE DATOS INCORRECTOS HACKING INGENIERÍA SOCIAL INTRUSIONES AL SISTEMA	0.35	20%	154,542.24	54,089.78
…….										
19	RECURSO HUMANO	146	PERSONAL FISCALIZACION	10	2,400,000	CONTRASEÑAS DÉBILES FALTA DE USO DE CRIPTOGRAFÍA EN LA COMUNICACIÓN COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC EMPLEADOS DESCONTENTOS, DELICUENTES	0.05	20%	480,000.00	24,000.00
…….										
47	BASES DE DATOS	130	CATEGORIAS PROYECTO	1	50,000.00	LUGAR DE ALMACENAMIENTO EN LOCALES INSALUBRES O CON ALTO NIVEL DE, HUMEDAD, MAGNETISMO O ESTÁTICA, MOHO, ETC. LOCALES PRÓXIMOS A RÍOS PROPENSOS A INUNDACIONES INFRAESTRUCTURA INCAPAZ DE RESISTIR A LAS MANIFESTACIONES DE LA NATURALEZA COMO TERREMOTOS, MAREMOTOS, HURACANES ETC AUSENCIA DE RECURSOS PARA EL COMBATE A INCENDIOS INSTALACIONES INADECUADAS CONTRASEÑAS DÉBILES COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC.	0.3	20%	10,000.00	3,000.00
……										
65	FINANCIERO	168	ACTAS ENTREGA RECEPCION	11500	58,650.00	INSTALACIONES INADECUADAS CONTRASEÑAS DÉBILES FALTA DE USO DE CRIPTOGRAFÍA EN LA COMUNICACIÓN COMPARTIMIENTO DE IDENTIFICADORES TALES COMO NOMBRE DE USUARIO O CREDENCIAL DE ACCESO, ETC EMPLEADOS DESCONTENTOS, DELICUENTES AUSENCIA DE IDENTIFICACIÓN DE PERSONAS Y DE LOCALES, ETC	0.15	20%	11,730.00	1,759.50
……										

Tabla 30. Síntesis: Estimación y Priorización del Riesgo

Es necesario indicar que cada activo representa un valor del riesgo, y sobre la base del juicio de los expertos muchos de ellos son relegados según el criterio de aceptación definido en el Plan de Riesgos[36].

Siendo el Plan Amanecer un proyecto de alcance nacional y siendo uno de sus objetivos estratégicos acceder a nuevos recursos por medio de infraestructura tecnológica para fortalecer la gestión de las instituciones educativas, en la siguiente figura se muestra la cantidad de activos del proyecto, correspondientes a cada área o elemento de Gestión de Tecnologías de Información.



Para cada activo, la probabilidad de ocurrencia de una amenaza fue establecida cuantitativamente instituida por datos históricos y del juicio de expertos que participaron en el Plan Amanecer (Director de Proyecto y Director de Control de Proyecto).

En la siguiente figura se muestra la probabilidad acumulada para cada área de Gestión:

[36] El Plan de Riesgos corresponde a la actividad 3.2 de la Gestión del Riesgo.

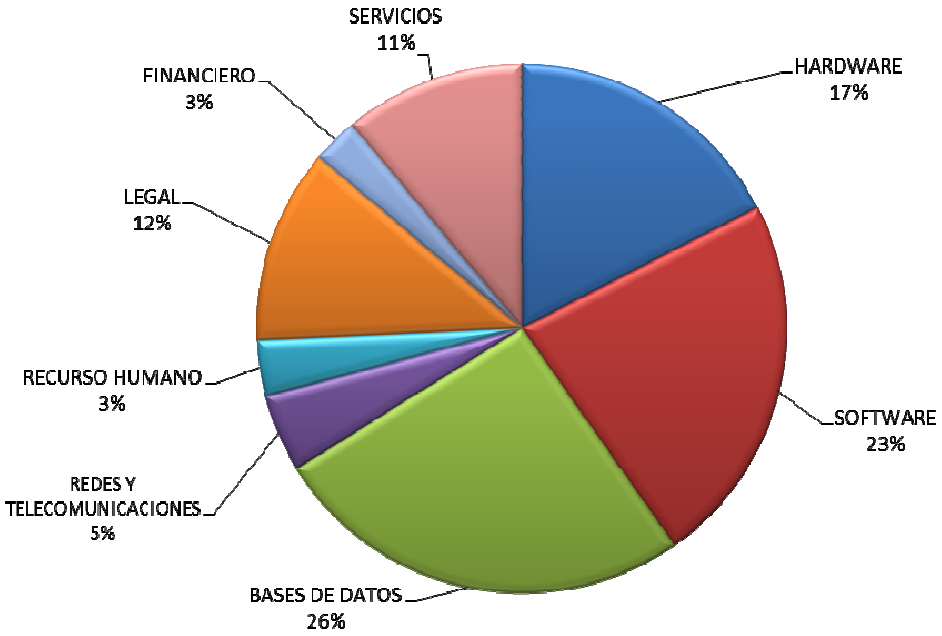


Figura 14. Probabilidad Acumulada por área de Gestión de TI – Plan Amanecer

Dentro de un proyecto de TI de gran envergadura a base de la Figura 14, en el caso de que suceda una amenaza producido por vulnerabilidades, los datos y manejo de información corren mayor probabilidad de ocurrencia; seguido por el Software y Hardware. Esto sucede ya que existen procesos de almacenaje digital y físico manejados por personas y soportados tanto por software y por hardware.

En el CD adjunto de esta investigación (**ANEXO C**) se especifican las vulnerabilidades y amenazas existentes, sin embargo, la alta probabilidad existente en software, hardware, servicios y demás elementos se debe principalmente a amenazas como:

- Robo
- Ataque físico
- Avería
- Destrucción
- Cambio de requisitos
- Virus
- Terremoto
- Huelga
- Inundación
- Cierre de vías (huelga-mantenimiento)
- Permisos especiales (normativa)
- Cumplimiento cronograma
- Incremento de costes
- Ingeniería social

En contraste con lo anterior, los mecanismos salvaguardas de las amenazas determinan que aumente o disminuya el impacto tomando como factor el porcentaje de degradación de un activo.

El porcentaje de degradación de un activo puede estar dentro de una escala tal como muestra la Tabla 28 de este documento, sin embargo dependiendo de la cantidad de activos y valor económico de estos, el analista de Riesgos puede definir la escala de ponderación y plantear los niveles de degradación.

En la siguiente figura se muestra el impacto acumulado en los elementos de Gestión de TI para el Proyecto Plan Amanecer:

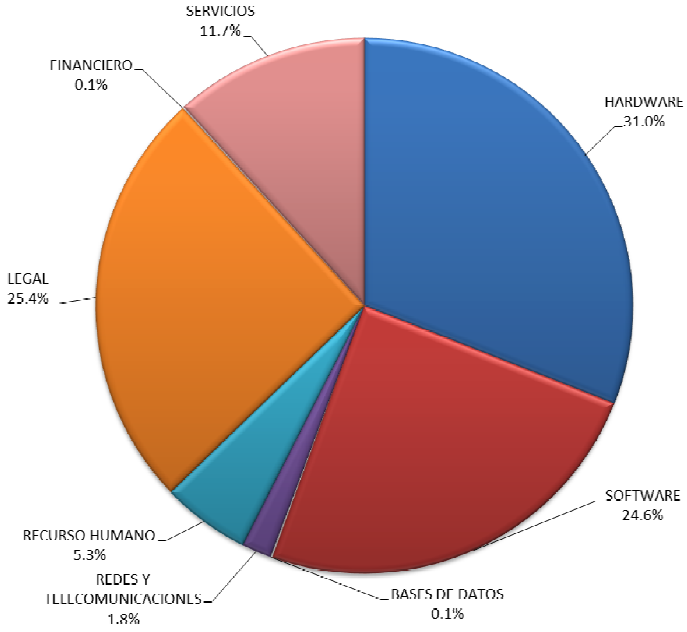


Figura 15. Impacto Acumulado por área de Gestión de TI – Plan Amanecer

Dado que el Riesgo es producto de la probabilidad de que ocurra una amenaza por un impacto (económico o de tiempo), la siguiente figura muestra el resultado para el proyecto sujeto de análisis:

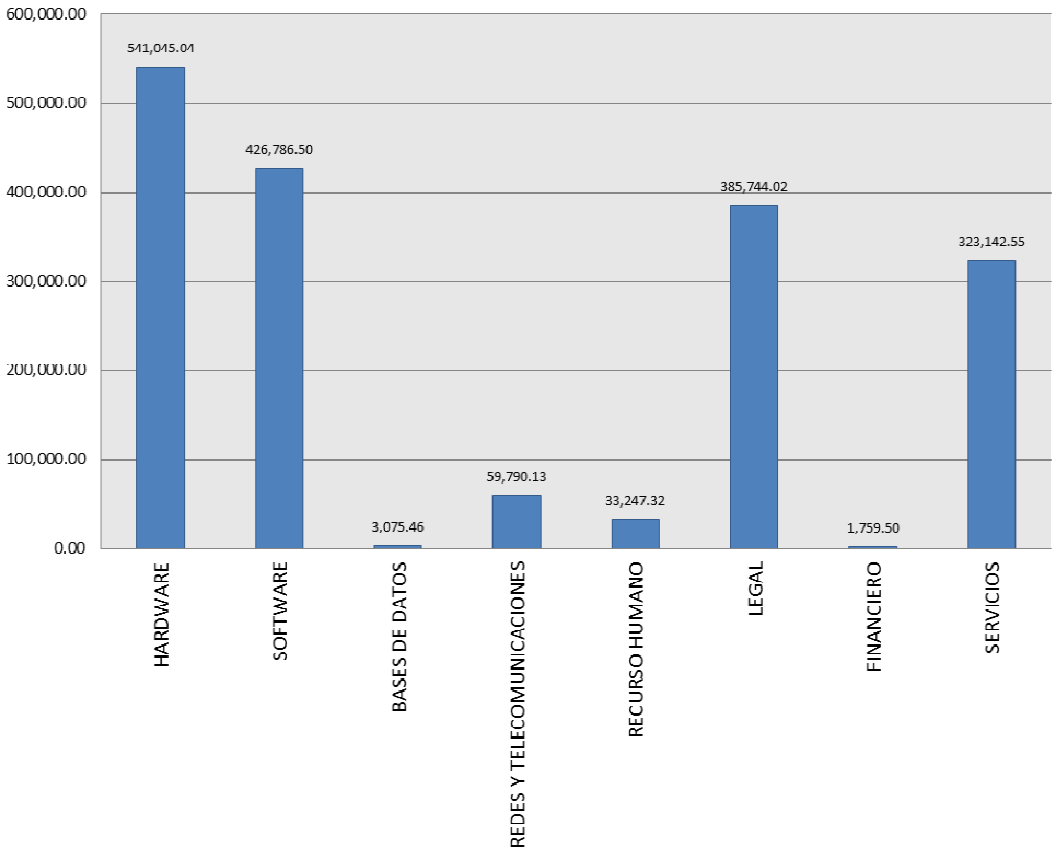


Figura 16. Riesgo acumulado por Área de Gestión de TI – Plan Amanecer

Finalmente, la figura 16 muestra los resultados cuantitativos de riesgo de cada elemento de TI o área de gestión.

El Riesgo acumulado es 1’774,590.53 USD, valor que representa el 6% del total del proyecto.

Es indispensable mencionar que a nivel macro los profesionales que desarrollan y ejecutan proyectos de TI en instituciones públicas deben tomar en cuenta: capacidad del proveedor, cronograma, permisos gubernamentales, conocimientos básicos de compras públicas y asignación de personal calificado y capacitado.

Una vez que hemos cumplido los objetivos de esta investigación pasaremos a puntualizar las actividades que se deben ejecutar en la Gestión del Riesgo.

3.3 GESTION DEL RIESGO

Una vez que se ha procesado los datos de probabilidad de ocurrencia, degradación del activo, impactos y riesgo; es el tiempo de definir el umbral de

aceptación. La aceptación de un riesgo varía según el criterio del Director de Riesgos.

Según datos del proyecto (Director Ejecutivo) para el Plan Amanecer se ha catalogado como un riesgo aquellos que sobrepasan los mil dólares americanos (1,000 USD).

Sobre la base de la guía presentada en esta investigación, los Riesgos que han sido declarados como inaceptables tienen 4 posibilidades de tratamiento: se los mitigará, aceptará, transferirá o evitará; teniendo en cuenta una estrategia técnica-económica-contractual.

Tal como lo especifica la Guía de este documento, en esta fase intervienen conceptos y teorías de decisiones a base de la Probabilidad y Estadística para definir un Plan de Gestión del Riesgo.

En la guía definida en este documento se presenta la estructura del Plan de Gestión del Riesgo (Actividad 3.2 Plan de Gestión del Riesgo).

La ejecución del Plan de Riesgo debe ser un proceso continuo, actualizado y que puede ser mejorado o alterado según las necesidades.

Finalmente, la monitorización y evolución de indicadores en la Gestión de Riesgo es un proceso que se lo debe documentar y analizar con el fin de mostrar avance de gestión tanto en probabilidad de ocurrencia, impacto y riesgo.

Una vez alcanzado todo lo anterior, se puede definir el Nivel de madurez de la implantación del Plan de Gestión de Riesgos, es decir, se puede establecer en qué medida se puede confiar del funcionamiento adecuado de las salvaguardas que se han impuesto a los activos.

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Los modelos que se destacan al momento de gestionar el riesgo y alcanzan niveles satisfactorios en Hardware, Software, Bases de Datos, Redes y Telecomunicaciones son COBIT, RISK IT, OCTAVE, NIST 800-30 y MAGERIT; ya que en su estructura se encuentran criterios de seguridad que son la base para realizar el análisis y valorar la materialización de amenazas e impactos sobre los Elementos de TI, siendo los comunes entre estos la confidencialidad, integridad y disponibilidad. En Software y Bases de Datos se destacan CMMI y SPICE por el soporte en la adquisición, desarrollo, operación y mantenimiento de productos de software. Respecto a la Administración del Recurso Humano PMBOK, COBIT, NIST 800-30 y MAGERIT alcanzan niveles satisfactorios, puesto que estos modelos gestionan el riesgo definiendo un equipo de trabajo con perfiles y competencias para los proyectos con su respectiva asignación de funciones y responsabilidades.

- La administración de Normativa y de la Seguridad de la información respecto a la Gestión del Riesgo la encabezan COBIT y MAGERIT. Esto es principalmente ya que COBIT cubre requerimientos de normas y seguridad mediante sus objetivos de control en base a las buenas prácticas a través de un marco de trabajo de dominios y procesos. MAGERIT por su parte se alinea con las leyes y normativas técnicos-gubernamentales (españoles), cubriendo temas que no tratan otras buenas prácticas como: contratos, licenciamiento, derechos de autor, contratación de personal, impuestos y protección de datos de carácter personal; siendo estos puntos referenciales para que los profesionales de TI puedan desarrollar el análisis de vulnerabilidades y amenazas en un proyecto al momento de Gestionar el Riesgo.

- La Gestión del Riesgo al momento de administrar las finanzas, es un elemento que las buenas prácticas evaluadas en esta investigación adolecen por los resultados obtenidos, con la excepción de PMBOK y MAGERIT puesto que en

su estructura tienen capítulos encargados de la planificar, estimar, presupuestar y administrar los costos de un proyecto. Un caso particular en este tema es COBIT y RISK IT ya que son apoyados directamente por Val IT. En cuanto a la correspondencia de la Gestión del Riesgo de los Servicios de TI, cada modelo y metodología tratada en esta investigación se orienta según su doctrina y ámbito de aplicación, por ejemplo CMMI y SPICE al desarrollo de aplicaciones y soluciones automatizadas, PMBOK y PRINCE2 a la gestión del proyecto; COBIT y RISK IT en alinear las metas de negocio con las metas de Tecnología de la Información; OCTAVE, NIST 800-30 y MAGERIT en el Análisis y Gestión del Riesgo cuando se hace uso de la TI.

- La contribución de esta investigación es la Guía de Análisis y Gestión del Riesgo la cual considera un proceso cíclico que permite obtener la evolución de las actividades, activos, recursos, vulnerabilidades, amenazas y salvaguardas; permitiendo reajustar permanentemente el nivel de riesgo, brindando un mejoramiento continuo a los requerimientos del proyecto considerando todas las áreas de TI como son el Hardware, Software, Bases de Datos, Redes/Telecomunicaciones, Recurso Humano, legal, Financiero y Servicios.

- La guía desarrollada en esta investigación fue aplicada a un proyecto gubernamental de alcance nacional y se pudo determinar que los mecanismos salvaguardas de las amenazas determinan que aumente o disminuya el impacto tomando como factor el porcentaje de degradación de un activo. En el CD adjunto a este documento se muestra la información de todo el análisis de riesgos, las vulnerabilidades, amenazas e impactos; así como también los mecanismos de salvaguarda como procedimientos, políticas, planes y soluciones técnicas que pueden ser consideradas para futuros proyectos.

4.2 RECOMENDACIONES:

- Al momento de identificar las vulnerabilidades y amenazas de un activo, se recomienda examinar las condiciones de los activos que van desde lo físico hasta lo lógico y que puedan ser catalogados como debilidades y/o afectaciones que pueden ser perjudiciales para el proyecto, ya que de esta manera se tendrá un marco lógico de antecedentes y de estado de cada activo.

Así mismo para establecer la probabilidad de ocurrencia de una amenaza es recomendable buscar o investigar datos históricos tomando en cuenta registros, publicaciones y observaciones del juicio de expertos. Las salvaguardas pueden ser uno o varios para un activo, sin embargo en la fase de Gestión del Riesgo es importante realizar un análisis costo-beneficio de cada salvaguarda y estimar si es conveniente o no considerar la solución.

- Los proyectos estatales demandan una serie de requisitos tanto técnicos como legales, por lo tanto, se recomienda a los profesionales que desarrollan y ejecutan proyectos de TI adquirir conocimientos básicos de la ley de contratación pública, normas de control interno de la Contraloría, negociación, administración, finanzas, y conocimientos básicos de permisos gubernamentales (según el área de aplicación). Esto permitirá agilitar y desarrollar de manera eficiente los proyectos dentro de los parámetros y alternativas que las entidades públicas deben seguir.

- El control de la utilización de los recursos estatales y la consecución de los objetivos de las instituciones es una política en ejecución que comanda la Contraloría General del Estado, por tal motivo, se recomienda conformar un equipo de trabajo especialista planteado en este documento y continuar con esta línea de investigación para que la Gestión de Tecnologías de Información y Comunicaciones contenga técnicas de control y seguimiento elaboradas y propuestas por profesionales que se encuentran en el campo de acción y que con el apoyo de la alta dirección sean consideradas para incorporarlas en el interior de las entidades como una política de gestión.

- Ya que las Actas de Entrega acreditan el cumplimiento a satisfacción de un producto y generan transacción financiera de acuerdo a las cláusulas contractuales (porcentajes de pago), se recomienda por seguridad del administrador y de la institución que las actas contengan por lo menos la siguiente información: antecedentes, condiciones generales de ejecución, condiciones operativas, liquidación económica, liquidación de plazos, constancia de la recepción mediante un check list de productos, cumplimiento de las obligaciones contractuales, reajustes de precios pagados, o pendientes de pago y si es necesario cualquier otra circunstancia que se estime necesaria.

REFERENCIAS BIBLIOGRAFICAS

[1]. Project Management Institute, 4th Edition. A Guide to the Project Management Body of Knowledge PMBOK.

[2]. Office of Government Commerce. Projects IN Controlled Environments, PRINCE2 Manual. 3rd Edition. Londres, 2002.

[3]. NIST, National Institute of Standards and Technology Special Publication 800-30. Risk Management Guide for Information Technology Systems. July 2002.

[4]. MAGERIT – Versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, Libro II Catálogo de elementos, Libro III Guía de Técnicas. Junio 2006.

[5]. OCTAVE, Operationally Critical Threat Asset and Vulnerability Evaluation. Method Implementation Guide Version 2.0. June 9, 2003.

[6]. ISACA, Information Systems Audit and Control Association . Control objectives for information and related technology COBIT 4.1. 2007.

[7]. ISACA, Information Systems Audit and Control Association. The Risk IT Framework. 2009.

[8]. ISO, International Organization for Standardization. Software Process Improvement and Capability dEtermination, SPICE (ISO 15504).

[9]. Software Engineering Institute. CMMI. Capability Maturity Model Integrated. [disponible en línea] 2002. http://www.sei.cmu.edu/cmmi/index.cfm.

[10]. INTECO, Instituto Nacional de Tecnologías de la Comunicación. Guía Avanzada del Riesgo. España, Diciembre 2008.

[11]. Galaway, Lionel. Quantitative Risk Analysis for Project Management: A critical review. s.l. : RAND Corporation working paper, February 2004.

[12]. Ropponen y Lyytinen, “Can Software Risk Management Improve System Development: An Exploratory Study”. European Journal of Information Systems, 1993

[13]. Kindinger, John P. y Darby, John L. Risk Factor Analysis- A New Qualitative Risk Management Tool. Proceedings of the Project Management Institute Annual Seminars & Symposium. Houston, Texas. USA, September 7 – 16, 2000.

[14]. Connell, S. Desarrollo y Gestión de Proyectos Informáticos, McGraw-Gill, 1997.

ANEXOS

ANEXO A. OTRAS MEJORES PRACTICAS QUE GESTIONAN EL RIESGO

A más de las mejores prácticas descritas en este documento, existen otras que no se han analizado porque se han considerado de menor relevancia por no ser populares o no muy utilizadas en nuestro país. Algunas de las mejores prácticas descartadas por estos motivos son las siguientes:

- PARA (Practical Application of Risk Analysis)
- Austrian IT Security Handbook (sólo disponible en alemán)
- Dutch A&K Analysis (sólo disponible en holandés)
- Ebios (Expression des Besoins et Identification des Objectifs de Sécurité), publicada por la Administración Pública francesa. Incorpora una herramienta de soporte.
- FRAP/FRAAP (Facilitated Risk Analysis –and Assessment - Process), basada en la realización de ejercicios de brainstorming (lluvia de ideas) por parte de un grupo de participantes de distintos perfiles complementarios. Desarrollada por Peltier Associates.
- CORA (Cost-Of-Risk Analysis)
- ISRAM (Information Security Risk Analysis Method)
- IT-Grundschutz (IT Baseline Protection Manual), publicada por la Administración Pública alemana. Soportado por la herramienta GSTool.
- MEHARI publicada por el Club Francés de Seguridad de la Información. Dispone de una herramienta de soporte (Risicare).
- ARiES (Aerospace Risk Evaluation System)
- STIR (Simple Technique for Illustrating Risk)

Existe un elevado número de mejores prácticas **propietarias soportadas por productos comerciales**. Estas mejores prácticas no se han considerado en la realización de esta investigación. Algunas de las metodologías comerciales más relevantes son:

- Acuity Stream
- Amenaza IT Threat Tree Modeling System
- Callio
- Casis
- COBRA (Consultative Objective & Bi-functional Risk Analysis)
- Countermeasures
- GxSGSI
- ISAMM (Information Security Assessment & Monitoring Method)
- MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale)
- Modulo Risk Manager
- Proteus
- Ra2
- Real ISMS
- ResolverBallot y Resolver Risk
- RiskPAC
- Riskwatch
- RM Studio
- SBA
- Security Risk Management Toolkit
- The Buddy System

ANEXO B. EVALUACION DE ACTIVIDADES DE MEJORES PRACTICAS QUE GESTIONAN EL RIESGO

MEJOR PRACTICA	ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI							
			HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS
CMMI	**CM1.1**	Determinar recursos y categorías	0.5	1	1	0.5	0	0	0.5	0.75
CMMI	**CM1.2**	Definir parámetros de riesgos	0.5	1	1	0.75	0.75	0	0	0.5
CMMI	**CM1.3**	Establecer una estrategia de gestión de riesgos	0.75	1	1	0.75	0.75	0.5	0.5	0.75
CMMI	**CM2.1**	Identificar los riesgos	0.5	1	1	0.5	0	0	0.5	0.75
CMMI	**CM2.2**	Evaluar, categorizar y priorizar riesgos	0.75	0.75	0.75	0.5	0.5	0	0	0.5
CMMI	**CM3.1**	Desarrollar planes de mitigación de riesgos	0.75	1	1	0.5	1	0.5	0.75	1
CMMI	**CM3.2**	Implementar planes de mitigación de riesgos	0.75	1	1	0.5	0.5	0	0.75	0.75
SPICE	**SP5.1**	Establecer el alcance de la gestión de riesgos	0.5	1	0.75	0.5	0.5	0.5	1	0.75
SPICE	**SP5.2**	Definir estrategias de gestión de riesgos	0.5	1	0.75	0.5	0.75	0	0.75	0.75
SPICE	**SP5.3**	Identificar riesgos	1	1	1	0.75	0.5	0.5	0.75	1
SPICE	**SP5.4**	Analizar riesgos	0.5	0.75	0.75	0.5	0.5	0	0.75	0.75
SPICE	**SP5.5**	Definir y realizar acciones de tratamiento de riesgos	0.5	0.75	0.75	0.5	0.5	0.5	0.75	0.75
SPICE	**SP5.6**	Monitorizar los riesgos	0.5	0.75	1	0.5	0.5	0.5	0.5	1
SPICE	**SP5.7**	Tomar acciones preventivas o correctivas	0.5	0.75	1	0.5	0.5	0.5	0.75	0.75
PMBOK	**PB1.0**	Planificar la Gestión de Riesgos	0.5	0.5	0.5	0.5	0.75	0	1	0.75
PMBOK	**PB2.0**	Identificar los Riesgos	0.5	0.5	0.75	0.5	0.75	0	0.75	0.5
PMBOK	**PB3.0**	Realizar Análisis Cualitativo de Riesgos	0.5	0.5	0.5	0.5	0.75	0	0.75	0.5
PMBOK	**PB4.0**	Realizar Análisis Cuantitativo de Riesgos	0.5	0.5	0.5	0.5	0.75	0	0.75	0.5
PMBOK	**PB5.0**	Planificar la Respuesta a los Riesgos	0.5	0.5	0.75	0.5	1	0	0.75	0.75
PMBOK	**PB6.0**	Dar seguimiento y Controlar los Riesgos	0.5	0.5	0.5	0.5	1	0	0.75	0.5
PRINCE2	**PC1.0**	Identificar los Riesgos	0.5	0.5	0.5	0.5	0.75	0.5	0	0.75
PRINCE2	**PC2.0**	Evaluar los Riesgos	0.5	0.5	0.5	0.5	0.75	0	0	0.75
PRINCE2	**PC3.0**	Identificar los riesgos	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75
PRINCE2	**PC4.0**	Seleccionar/Respuesta a los Riesgos	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75
PRINCE2	**PC5.0**	Plan y Recursos	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75
PRINCE2	**PC6.0**	Monitorear / Comunicar	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.75
COBIT	**CB1.0**	Determinar la alineación de la administración de Riesgos	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75
COBIT	**CB2.0**	Entender los objetivos de negocio estratégicos relevantes	1	1	1	1	1	0.75	0.75	0.75

MEJOR PRACTICA	ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI							
			HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS
COBIT	**CB3.0**	Entender los objetivos de los procesos de negocio relevantes	0.75	0.75	0.75	0.75	1	0.75	0.5	0.75
COBIT	**CB4.0**	Identificar los objetivos internos de TI y establecer el contexto del riesgo	0.75	0.75	0.75	0.75	0.75	0.75	0.5	0.75
COBIT	**CB5.0**	Identificar eventos asociados con objetivos	1	1	1	1	1	0.75	0.5	0.75
COBIT	**CB6.0**	Asesorar el riesgo con los eventos	1	1	1	1	1	0.75	0.5	0.75
COBIT	**CB7.0**	Evaluar y seleccionar respuestas a riesgos	1	1	1	1	1	0.75	0.75	0.75
COBIT	**CB8.0**	Priorizar y planificar las actividades de control	0.75	0.75	0.75	0.75	1	0.75	0.75	0.75
COBIT	**CB9.0**	Aprobar y garantizar la financiación de los planes de acción	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75
COBIT	**CB10.0**	Mantener y monitorizar el plan de acción de riesgos	1	1	1	1	1	1	0.75	1
RISKIT	**RIT1.0**	Definición de un universo de riesgos y ámbito de gestión de riesgo	1	1	1	1	0.75	0.75	0.5	0.75
RISKIT	**RIT2.0**	Apetito de riesgo y tolerancia al riesgo	1	1	1	1	0.75	0.5	1	1
RISKIT	**RIT3.0**	Conciencia del riesgo, Comunicación y presentación de informes	0.75	0.75	1	0.75	0.5	0.75	0.5	0.75
RISKIT	**RIT4.0**	Expresando y describiendo el riesgo	1	1	1	1	0.75	0.75	0.5	0.75
RISKIT	**RIT5.0**	Escenarios de riesgo	1	1	1	1	0.75	0.5	0.5	0.75
RISKIT	**RIT6.0**	Riesgo de respuesta y asignación de prioridades	0.75	0.75	1	0.75	0.75	1	0.5	1
RISKIT	**RIT7.0**	Un flujo de trabajo de Análisis de Riesgo	0.75	0.75	0.75	0.75	0.75	0.5	0.5	0.75
RISKIT	**RIT8.0**	Mitigación de Riesgos de TI Uso de COBIT y VAL IT	1	1	1	1	1	0.75	0.75	1
OCTAVE	**OC1.0**	Identificar la información (Gerencial-Operacional-Usuario Final)	0.75	0.75	0.75	0.75	1	0.5	0	0
OCTAVE	**OC2.0**	Consolidar la Información y crear perfiles de amenaza	0.75	0.75	0.75	1	1	0.75	0	0.75
OCTAVE	**OC3.0**	Identificación de componentes claves	1	1	1	1	0.5	0.5	0.5	1
OCTAVE	**OC4.0**	Evaluación de componentes seleccionados	1	1	1	1	0.75	0	0.75	1
OCTAVE	**OC5.0**	Análisis de riesgos de los recursos críticos	1	1	1	1	0.75	0.5	0.5	0.75
OCTAVE	**OC6.0**	Desarrollo de estrategias de protección	1	1	1	1	0.5	0.5	0.5	0.75
NIST	**NT1.1**	1.1 Caracterización del sistema	1	1	1	1	1	0.5	0.5	1

MEJOR PRACTICA	ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTO DE TI							
			HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS
NIST	**NT1.2**	1.2 Identificación de amenazas	1	1	1	1	1	0.5	0.5	1
NIST	**NT1.3**	1.3 Identificación de vulnerabilidades	1	1	1	1	0.75	0.75	0.75	0.75
NIST	**NT1.4**	1.4 Análisis de control Paso	0.75	0.75	1	0.75	0.75	0.5	0.75	1
NIST	**NT1.5**	1.5 Determinación de la probabilidad	1	1	1	1	0.75	0.5	0.75	1
NIST	**NT1.6**	1.6 Análisis de impacto	1	1	1	1	0.75	0.75	0.75	1
NIST	**NT1.7**	1.7 Determinación de riesgo	1	1	1	1	0.75	0.5	0.75	0.5
NIST	**NT1.8**	1.8 Recomendaciones de control	1	1	1	1	0.5	1	0.5	1
NIST	**NT1.9**	1.9 Documentación de resultados	1	1	1	1	1	0.5	0.5	1
NIST	**NT2.1**	2.1 Priorización de Acciones	0.75	0.75	1	0.75	0.75	0.75	0.75	0.75
NIST	**NT2.2**	2.2 Evaluación de Acciones de controles recomendados	1	1	1	1	1	0	0	1
NIST	**NT2.3**	2.3 Análisis Costo-Beneficio	0.75	0.75	0.75	0.75	0.75	0.75	1	1
NIST	**NT2.4**	2.4 Selección de Controles	0.75	0.75	0.75	0.75	0.75	0.75	1	0.75
NIST	**NT2.5**	2.5 Asignación de Responsabilidades	0.75	0.75	0.75	0.75	1	0	1	1
NIST	**NT2.6**	2.6 Desarrollo de plan de implantación de salvaguardas	1	1	1	1	1	0.75	0.75	0.75
NIST	**NT2.7**	2.7 Implantación de Controles seleccionados	1	1	1	1	1	0.75	0.75	0.75
MAGERIT	**MG1.1**	Estudio de oportunidad	0.75	0.75	0.75	0.75	1	0.5	0.75	1
MAGERIT	**MG1.2**	Determinación del alcance del proyecto	0.75	0.75	0.75	0.75	1	0.5	1	1
MAGERIT	**MG1.3**	Planificación del proyecto	0.75	0.75	0.75	0.75	1	0.75	0.75	1
MAGERIT	**MG1.4**	Lanzamiento del proyecto	1	1	1	1	1	0.75	0.75	0.75
MAGERIT	**MG2.1**	Caracterización de los activos	1	1	1	1	0.75	0.75	0.75	1
MAGERIT	**MG2.2**	Caracterización de las amenazas	1	1	1	1	0.75	1	0.75	1
MAGERIT	**MG2.3**	Caracterización de las salvaguardas	1	1	1	1	0.75	1	1	1
MAGERIT	**MG2.4**	Estimación del estado de riesgo	1	1	1	1	0.75	1	1	1
MAGERIT	**MG3.1**	Toma de decisiones	1	1	1	1	0.75	1	0.75	1
MAGERIT	**MG3.2**	Plan de seguridad	1	1	1	1	0.75	1	1	1
MAGERIT	**MG3.3**	Ejecución del plan	1	1	1	1	0.75	1	1	1

ANEXO C. CONTENIDO DEL CD ADJUNTO DE ESTA INVESTIGACIÓN

CD contiene:

A. MANUALES Y DOCUMENTOS DE MEJORES PRÁCICAS

- PMBOK, A Guide to the Project Management Body of Knowledge, PMI, 4th Edition
- PRINCE2, Manual, 3rd Edition, 2002
- COBIT 4.1, ISACA - IT Governance Institute. 2007
- RISK IT, ISACA - IT Governance Institute. 2009
- OCTAVE, Method Implementation Guide Versión 2.0, 2003
- NIST 800-30, Risk Management Guide for Information Technology Systems, 2002
- MAGERIT, Libro I Método - Libro II Catálogo de elementos - Libro III Guía de Técnicas, Versión 2.0, 2006

B. ANÁLISIS DE RIESGOS

- 3.2.1. Identificar y Valorar los Activos de la Organización.doc
- 3.2.2 Analizar Vulnerabilidades y Amenazas.doc
- 3.2.3 Determinar la Probabilidad de ocurrencia de una amenaza.doc
- 3.2.4 Identificar Salvaguardas.doc
- 3.2.5 Valorizar y Estimar el Impacto.doc
- 3.2.6 Analizar, Estimar y Priorizar el Riesgo.doc

ANEXO D: EQUIPO DE TRABAJO QUE GESTIONARÁ EL RIESGO EN LOS PROYECTOS DE TI

Actividades que Gestionan el Riesgo	EQUIPO DEL PROYECTO									
	Comité de Proyecto	Director Ejecutivo (CEO)	Director de Informática (CIO)	Director de Riesgos (CRO)	Director Financiero (CFO)	Director de Recursos Humanos (CHR)	Director de Proyecto (PM)	Director de Control de Proyecto (PCM)	Asesor Legal	Organismos de control gubernamental
1. Marco General de Referencia del Proyecto	A/R			R						
1.1 Alcance del Proyecto	A	R	R	R	R	R	R	R	R	C/I
1.2 Establecer el Contexto Organizacional y áreas críticas	A	R	R	R	R	R	R	R	R	
1.3 Equipo del Proyecto	A	R	R	R	C	R	C	C	C	
1.4 Recursos	A	C	C	R	R	R	R	R	C	
1.5 Criterios de Evaluación		C	R	R	C	C	R	R	R	C
1.6 Acuerdos	A	R	R	R	R	C	R	R	R	C
2. Análisis de Riesgos		R		A/R			R	R		
2.1 Identificar y Valorar los Activos de la Organización.		I	A/R	R	R	R	C	C	R	
2.2 Analizar Vulnerabilidades y Amenazas		I	R	A/R	R	R	C	C	R	
2.3 Determinar la Probabilidad de ocurrencia de una amenaza.		I	R	A/R	R	R	C	C	R	C
2.4 Identificar Salvaguardas		A	R	R	R	R	R	R	R	
2.5 Valorizar y Estimar el Impacto		I	R	A/R	R	R	R	R	R	
2.6 Analizar, Estimar y Priorizar el Riesgo		I	R	A/R	R	R	R	R	R	
3. Gestión del Riesgo	A/R	R		R						
3.1 Interpretación de los Resultados	A	C/I	I	R	I	I	I	I	C	
3.2 Plan de Gestión del Riesgo	I	A	R	R	R	R	R	R	C	
3.3 Ejecución del Plan	I	I	R	R	R	R	R	R	C	

MATRIZ RACI

EQUIPO DE PROYECTO

Función	Definición
Comité de Proyecto	Grupo de más altos ejecutivos de la organización que son responsables de la gestión del proyecto. Puede representar al usuario y tienen el control total de sus recursos.
Director Ejecutivo (CEO)	Máxima autoridad de la gestión y dirección administrativa del proyecto.
Director de Informática (CIO)	El más alto ejecutivo de la organización que es responsable de la adquisición, instalación y operación de TI. Su función tiene alcance para alinear las TI con las estrategias organizacionales y de proyectos. Tiene que planificar las acciones necesarias para brindar servicios de TI a tiempo cumpliendo las características de seguridad de la información. Generalmente tiene un equipo de trabajo especialistas en las áreas de TI.
Director de Riesgos (CRO)	Es el encargado de supervisar todos los aspectos de la Gestión de Riesgos de TI en todo el proyecto. Debe presentar al Comité de proyecto información para una correcta toma de decisiones en cuanto al manejo del riesgo al que se ve enfrentado el proyecto.
Director Financiero (CFO)	Realiza la Planificación financiera de todo el proyecto, relaciones con los proveedores, riesgos financieros. Mantiene comunicación directa con el CEO y CRO.
Director de Recursos Humanos (CHR)	Planifica las políticas con respecto a todos los recursos humanos del proyecto.
Director de Proyecto (PM)	Encargado de alcanzar los objetivos del proyecto de TI en el tiempo establecido, costos planificados y recursos designados. Dar seguimiento y juntamente con el CRO responder a los riesgos.
Director de Control de Proyecto (PCM)	Realiza tareas de supervisión, inspección y control para garantizar el cabal cumplimiento de los productos del proyecto según las bases fijadas y de las obligaciones contractuales adquiridas.
Asesor Legal	Asesora, en el ámbito de su competencia al equipo del proyecto y si se requiere al comité del proyecto sobre aspectos jurídicos y contractuales, entrega – recepción, licenciamiento, derechos de autor, entre otros. Elabora, revisa y asesora en las negociaciones que se puedan dar en el transcurso del proyecto de TI.
Organismos de control gubernamental	Entidades de estado que se encargan del control de la utilización de los recursos, prestación de los servicios de telecomunicaciones y auditoría. Para el caso de Proyectos de TI, Contraloría General del Estado, Superintendencia de Telecomunicaciones, Ministerio de Telecomunicaciones, Ministerio de Finanzas.

ANEXO E. DIMENSIONES DE SEGURIDAD Y NIVEL DE MADUREZ PARA PROYECTOS DE TI

En aras de la adaptabilidad, la Guía no define un conjunto de requerimientos de seguridad cerrado a utilizar, que deberá definirse para cada análisis. Se proponen los siguientes requerimientos de seguridad considerando la Tabla 18 de este documento que pueden valorarse al definir los requerimientos a considerar, procedentes de diversos modelos y metodologías:

Dimensiones de Seguridad	Modelo y Metodología
Confidencialidad	Generalmente Aceptado
Integridad	Generalmente Aceptado
Disponibilidad	Generalmente Aceptado
Autenticidad	MAGERIT V2.0
Trazabilidad	MAGERIT V2.0
Efectividad	COBIT 4.1
Eficiencia	COBIT 4.1
Cumplimiento	COBIT 4.1
Confiabilidad	COBIT 4.1

Conviene destacar que los distintos requerimientos de seguridad no son totalmente independientes entre sí, existiendo algunos requerimientos para los que se espera una elevada correlación. Algunos ejemplos[37] de estas correlaciones son:

Dimensiones de Seguridad	Nivel	Requiere Alta	Argumento
Confidencialidad	ELEVADO	TRAZABILIDAD	Debido a la necesidad de identificar accesos no autorizados a la información.
	ELEVADO	AUTENTICIDAD DE USUARIOS	Por la necesidad de garantizar la identidad de las personas que acceden a la información.
Integridad	ELEVADO	TRAZABILIDAD	Debido a la necesidad de identificar modificaciones no autorizadas de la información.
	ELEVADO	AUTENTICIDAD DE USUARIOS	Por la necesidad de garantizar la identidad de las personas que modifican la información.
	ELEVADO	AUTENTICIDAD DE DATOS	Debido a que el impacto de utilizar datos no fiables y utilizar datos no auténticos será, en muchos casos, similar.

[37] Análisis de riesgos de Seguridad de la Información, Juan Manuel Matalobos, 2009:106

Dimensiones de Seguridad	Nivel	Requiere Alta	Argumento
Disponibilidad	ELEVADO	INTEGRIDAD	Debido a que el impacto entre no disponer de información para la ejecución de un proceso y que la información disponible no sea fiable, será generalmente similar.

El Nivel de madurez de la implantación, se refiere cuando el Plan de Gestión de Riesgos se encuentra en marcha y define en qué medida se puede confiar en el funcionamiento adecuado de la salvaguarda de los activos según sus especificaciones. En la determinación del nivel de madurez se considera el modelo CMMI (Capability Maturity Model Integration), que define los siguientes niveles de madurez aplicables a cualquier proceso o control:

Nivel	Descripción
Nivel 0 (Inexistente)	La salvaguarda no se ha implantado.
Nivel 1 (Inicial)	La implantación de la salvaguarda depende de la iniciativa de personas individuales, por lo que no se puede garantizar su aplicación de forma consistente ni en todos los casos.
Nivel 2 (Repetible)	La salvaguarda se aplica de forma generalizada debido al conocimiento de todos los interesados de su necesidad y de su funcionamiento, pero no se ha llevado a cabo una formalización que asegure la aplicación de forma consistente ni que la aplicación de la medida se mantendrá a lo largo del tiempo al cambiar las personas responsables.
Nivel 3 (Formalizado)	La aplicación de la salvaguarda está formalmente documentada en políticas, procedimientos, guías, estándares, cuadernos de carga, definiciones de puestos, etc. Esta formalización asegura que la salvaguarda se aplicará de forma generalizada y consistente y se mantendrá independientemente de las personas responsables.
Nivel 4 (Gestionado)	La aplicación de la salvaguarda se monitoriza y se revisa periódicamente. Esta monitorización y revisión permite detectar cualquier desviación en la aplicación de la salvaguarda, garantizando su funcionamiento permanente.
Nivel 5 (Optimizado)	La monitorización y la revisión de la salvaguarda se utilizan para introducir mejoras que permitan aumentar la eficacia a lo largo del tiempo.

ANEXO F. ACTIVOS DE PROYECTOS DE TI

HARDWARE	
Computador personal	Antenas
Servidores	Equipo de Videoconferencia
Laptop	Pizarra Electrónica
Thin Clients	Proyector
Sistemas de alimentación ininterrumpida	Almacenamiento y Respaldo: Disco Duro, CD, DVD, Dispositivos USB, Cintas
Impresora Multifuncion (Scaner-Copiadora-Impresora)	Switch
Módems	Punto de acceso Wireless
Agendas Electrónicas	Centralita Telefónica
Firewall	Fuentes de alimentación
Periféricos	Equipos de climatización
Generadores eléctricos	Cableado Eléctrico
Teléfonos inteligentes	Monitores
Mobiliario: armarios, etc	Routers
Equipos de Videovigilancia	Cajas fuertes
Equipos de destrucción de soportes de información	Equipo de detección/extinción de incendios
Cableado Estructurado	Impresora

SOFTWARE	
Ofimática	Software de terminales
Anti virus	Navegador web
Drivers	Gestor de Proyectos
Sistema operativo	Sistema de alarma
Sistema de backup	Sistema de gestión de bases de datos
Sistema de video vigilancia	Sistemas de Gestión de la Red
Sistemas de control de acceso	Sistema de detección/extinción de incendios
Sistema Financiero	Software para Servidores

Software Educativo	Software Empresarial
Software de Diseño Gráfico	Software de Cálculo Numérico
Software de Correspondencia: Email	Desarrollo de Software propio
Software para Videoconferencia	Desarrollo de Software
Sistema de detección de intrusiones	Virtualización
BASES DE DATOS	
Datos de gestión interna	Voz
Datos de configuración	Datos de prueba
Multimedia	Código fuente
Registro de actividad (log)	Código ejecutable
Informes	Datos de Avance
Seguimiento y Control	Inventarios
Datos de Finanzas	Actualizaciones Tecnológicas
REDES Y TELECOMUNICACIONES	
Redes locales	Internet
Enlaces de telecomunicaciones	red MAN (metropolitana)
Redes inalámbricas	Red WAN
Red Satelital	Red privada virtual
Intranet	Red telefónica
RECURSOS HUMANO	
Administradores de sistemas	Usuarios externos
Administradores de redes y comunicaciones	Usuarios internos
Administradores de Bases de Datos	Operadores
Desarrolladores	Clientes
Proveedores	Subcontratas
Directivos	Reguladores/supervisores
LEGAL	
Contrato	Ley de comercio electrónico
Garantías	Acuerdo de nivel de servicio o Service

	Level Agreement
Actas y Acuerdos	Ley de Servicio de Rentas Internas
Licenciamiento	Manejo Datos de Carácter Personal
Derechos de Autor	Administración Pública (si corresponde)
Ley de Trabajo	Normativa de la Seguridad de la Información
FINANCIEROS	
Actas de Entrega y Actas de Recepción[38]	Viáticos
Multas y Sanciones por incumplimiento de la ley u obligaciones contractuales	Costo de reposición: adquisición e instalación
Seguros	
SERVICIOS	
Servicios y Funciones de la Organización	Servicios del Proyecto
Soporte Técnico	Servicio de Seguridad (Instalaciones)
Aplicaciones que procesan datos	Servicio de prevención y detección de intrusiones
Capacitación	Gestión de Incidentes
Gestión de Cambios	Instalaciones: Site Operation
ISP (Internet Service Provider)	Servicios de Transporte en la Recepción y Entrega
Servicio de Email	Servicio de directorio
Acceso remoto a cuenta local	Transferencia de ficheros
Servicio NOC (Network Operations Center)	Servcios Profesionales (Consultorías)
CPD (Centro de Procesamiento de Datos)	Mensajes Instantáneos
Servicio de Conferencia de audio, video, web	Servicios de voz de IP
Web Hosting	Telefonía Tradicional
Intercambio electrónico de datos	Outsourcing

[38] Actas de Entrega y Actas de Recepción: Documentos que acreditan el cumplimiento a satisfacción de un producto y generan transacción financiera de acuerdo a las cláusulas contractuales (porcentajes de pago).

ANEXO G. RESUMEN MARCO LEGAL PROYECTO "PLAN AMANECER"

1. MARCO LEGAL GENERAL

DOCUMENTO	FECHA	OBJETO
Convenio suscrito entre el Reino de España y la República del Ecuador	29-SEPT-1997	Financiar exportaciones de bienes de origen español para proyectos de desarrollo.
Decreto Ejecutivo No. 691, Registro Oficial No. 148	24-AGOS-2000	Autoriza a los Ministerios de Gobierno y, de Educación, a suscribir convenio con la Conferencia Episcopal Ecuatoriana, a fin de que este organismo sea la Unidad Ejecutora del Proyecto.

2. MARCO LEGAL CONSORCIO EDUCTRADE S. A. – SANTILLANA EDUCACIÓN S. L. GRUPO SANTILLANA DE EDICIONES S. L

DOCUMENTO	FECHA	OBJETO
Contrato entre la CEE y el Consorcio Eductrade– Santillana. US$ 30´000.000		Implementación del proyecto "Mejoramiento de la Calidad de la Educación Particular Popular y Comunicación Social Comunitaria
Acta de Negociación, suscrita entre la CEE y el Consorcio Eductrade–Santillana.	29-MAYO-2006	Recoge propuesta de actualización y mejora tecnológica propuesta por el Consorcio.
Decreto Ejecutivo No 732, Registro Oficial 141 de 9 noviembre de 2005,	09-NOVIE-2005	Autoriza al Ministro de Economía y Finanzas, a suscribir contratos con el Banco Bilbao Vizcaya Argentaria S.A. y con el Instituto de Crédito Oficial del Reino de España, ICO.
Convenio de Crédito, entre el Banco Bilbao Vizcaya Argentaria S. A. (BBVA) y la República del Ecuador, US $15´000.000	18 ENERO 2006	Financiar el proyecto "Mejoramiento de la Calidad de la Educación Particular y Comunicación Social Comunitaria",
Convenio de Crédito, entre el Instituto de Crédito Oficial del Reino de España, ICO, y la República del Ecuador, US $15´000.000	18 ENERO 2006	Financiar el proyecto "Mejoramiento de la Calidad de la Educación Particular y Comunicación Social Comunitaria",
Entrega del anticipo por parte del BBVA y del ICO	03-OCTUB-2006	Puesta en vigor del Contrato
Incio del Proyecto		Incio de Actividades y procedimientos para implantar el equipamiento y procesos de capacitación y transferencia de tecnología y de conocimiento.
Fin de Actividades	30-SEPT-2010	Fin del proceso Entrega-Recepción
Fin de Proyecto	31-DICIEM-2010	Cierre de Acta de Recepción Total
Sostenibilidad	CONTINUO	Tiempo de producción, capacitación y de mantenimiento de todos los bienes y servicios del proyecto.

GLOSARIO DE TÉRMINOS

Activo: Cualquier recurso de Software, Hardware, datos, administrativo, físico, de personal o de comunicaciones.

Amenaza: La Amenaza es la posibilidad de que se produzca una determinada vulnerabilidad de forma satisfactoria, es decir, una amenaza es una circunstancia o evento con la capacidad de causar daño a un sistema, entendiendo como daño una forma de destrucción, revelación o modificación de datos.

Bienes: Es un recurso tangible para suplir necesidades y son susceptibles de apropiación, sea privada o pública.

CMMI: Capability Maturity Model Integration, es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software que cubren el ciclo de vida del producto.

COBIT: Control Objectives for Information and related Technology, es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información

Impacto: El impacto es la materialización de un riesgo; una medida del grado de daño o cambio sobre un activo, entendiendo como riesgo la probabilidad de que un evento desfavorable ocurra y que tendría un impacto negativo si se llegase a materializar.

MAGERIT: responde a "Metodología de Análisis y Gestión de Riesgos de IT", elaborada por el Ministerio de Administraciones Públicas (MAP) del Reino de España

NIST 800-30: Risk Management Guide for Information Technology Systems, es una metodología basada en los conceptos generales presentados en el Instituto Nacional de los Estándares y la Tecnología (NIST, National Institute of Standards and Technology).

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation; es una metodología de evaluación y de gestión de los riesgos para garantizar la seguridad del sistema informático

PMBOK: Project Management Body of Knowledge, es un modelo en la Administración de proyectos desarrollado por el Project Management Institute (PMI).

PRINCE2: Projects IN Controlled Environments, es un modelo estructurado para la gestión de proyectos

Proactividad: <<pro>>, que significa ‘antes de’, y «actividad», que significa ‘facultad de obrar’, es decir, la toma de iniciativa en el desarrollo de acciones creativas y audaces para generar mejoras antes que sucedan.

Producto: Son bienes o servicios que satisfacen un deseo o una necesidad y generan valor o capacidad.

Proyecto: Es un conjunto de actividades coordinadas y controladas, con fechas de inicio y fin definidas, encaminado a la creación de un bien o servicio único y conforme a unos requisitos específicos, incluyendo limitaciones de tiempo, coste y recursos.

RISK IT*:* Riesgos de Tecnologías de Información, se constituyó a partir de los componentes de riesgo relacionados dentro de los marcos de COBIT y Val IT

Rol: Una función definida que debe realizar un miembro del equipo del proyecto, como evaluar, archivar, inspeccionar, analizar o codificar.

Servicios: Conjunto de actividades o mecanismos para responder a necesidades específicas. La presentación de un servicio no resulta en posesión, y así es como un servicio se diferencia de proveer un bien físico.

SPICE: Software Process Improvement and Capability dEtermination, también conocido como modelo ISO/IEC 15504

Vulnerabilidad: Una vulnerabilidad es una debilidad que puede ser ‘activada’ de forma accidental o intencionadamente.