UNIVERSIDAD NACIONAL

Sistema de estudios de Posgrado

Maestría en Administración de Tecnología de la información (MATI)

Énfasis en Administración de Proyectos

Metodología de gestión de riesgos de operación para un servicio de TI

Marco Antonio Fonseca Aragón

Heredia, Costa Rica, Mayo 2015

26 de Mayo del año 2015

Universidad Nacional
Facultad de Ciencias Exactas y Naturales
Escuela de Informática
Posgrado en Gestión de la Tecnología de Información y Comunicación (ProGesTIC)

FORMULARIO DE DEPÓSITO LEGAL, AUTORIZACIÓN DE USO DE DERECHOS PATRIMONIALES DE AUTOR E INCORPORACIÓN A REPOSITORIOS INSTITUCIONALES DE INFORMACIÓN DE ACCESO PÚBLICO

La(s) persona(s) abajo firmantes, en nuestra condición de estudiantes de la maestría en Administración de Tecnología de la Información (MATI)

y autor(es) del Trabajo final de graduación titulado: “Metodología de gestión de riesgos de operación para un servicio de TI” para optar al grado académico de Máster en: Administración de Tecnología de la Información con énfasis en Administración de Proyectos, de conformidad con lo establecido en el documento de “Lineamientos generales para la realización del trabajo final de graduación” y demás normativa universitaria relacionada con estos trabajos de graduación, DECLARO(AMOS) BAJO FE DE JURAMENTO conociendo la responsabilidad civil, penal o administrativa en que podría(amos) incurrir al no decir la verdad, lo siguiente:

1. El documento, producto, obra audiovisual, software, resultado del trabajo final de graduación referido anteriormente es original, inédito y ha cumplido con todo el proceso de aprobación académico que confiere el grado académico postulado con esta obra.

2. El trabajo final de graduación referido anteriormente constituye una producción intelectual propia de la(s) persona(s) abajo firmantes y a esta fecha no ha sido divulgado a terceros(as) de forma pública, por ningún medio de difusión impreso o digital.

3. Autorizo(amos) el depósito de un ejemplar en formato impreso y otro en formato digital (entregado en soporte de disco compacto), en la colección de trabajos finales de graduación del ProGesTIC de la Universidad Nacional, así como la realización de copias electrónicas adicionales para fines exclusivos de seguridad y conservación de la información.

4. En caso de que el trabajo final de graduación haya sido elaborado como obra

en colaboración -bien se trate de obras en las que los autores(as) tienen el mismo grado de participación o aquellas en las que existe una persona autora principal y una o varias personas autoras secundarias-, todos(as) ellos(as) han contribuido intelectualmente en la elaboración del documento y en este acto, libero (amos) de responsabilidad a las autoridades del posgrado y a los funcionarios que custodian la colección del ProGesTIC, en relación con el reconocimiento que se realiza respecto de los niveles de participación asignados por los(as) propios autores(as) del proyecto.

5. En caso de que el trabajo final de graduación haya sido elaborado como obras en colaboración (conforme a lo dispuesto en el punto 4), los(as) autores(as) abajo firmantes designamos a Marco Antonio Fonseca Aragón como encargado(a) de recibir comunicaciones y representar con autoridad suficiente a los suscritos, en condición de agente autorizado(a) de los demás autores(as).

6. Reconozco(cemos) que la colección de trabajos finales del ProGesTIC no emite criterios ni valoraciones académicas sobre lo planteado en el producto final del trabajo de graduación y autorizo(amos) a esta dependencia para que proceda a poner a disposición del público la obra en mención, a través de los espacios físicos o virtuales que se posea, así como a través del Repositorio Institucional; a partir del cual los usuarios de dichas plataformas puedan acceder al documento y hacer uso de este en el marco de los fines académicos, no lucrativos y de respeto a la integridad del contenido del mismo así como la mención del autor o poseedor de sus derechos.

7. Manifiesto(amos) que todos los datos de citas dentro de texto y sus respectivas referencias bibliográficas, así como las tablas y figuras (ilustraciones, fotografías, dibujos, mapas, esquemas u otros) tienen la fuente y el crédito debidamente identificados y se han respetado los derechos de autor.

8. Autorizo(amos) la licencia gratuita no exclusiva de los derechos patrimoniales de autor para reproducir, traducir, distribuir y poner a disposición pública en formato electrónico, el documento depositado, para fines académicos, no lucrativos y por plazo indefinido en favor de la Universidad Nacional, que incluye además los siguientes actos:

a. La publicación y reproducción íntegra de la obra o parte de esta, tanto por medios impresos como electrónicos, incluyendo Internet y cualquier otra tecnología conocida o por conocer.

b. La traducción a cualquier idioma o dialecto de la obra o parte de esta.

c. La adaptación de la obra a formatos de lectura, sonido, voz y cualquier otra representación o mecanismo técnico disponible, que posibilite su acceso para personas no videntes parcial o totalmente, o con alguna otra forma de capacidades especiales que les impida su acceso a la lectura convencional del proyecto.

c. La distribución y puesta a disposición de la obra al público, de tal forma que el público pueda tener acceso a ella desde el momento y lugar que cada quien elija, a través de los mecanismos físicos o electrónicos de que disponga.

d. Cualquier otra forma de utilización, proceso o sistema conocido o por conocerse que se relacione con las actividades y fines académicos a los cuales se vincula la maestría, la colección de trabajos finales del ProGesTIC, la Escuela de Informática y la Universidad Nacional.

9. Reconozco(cemos) que la colección de trabajos del ProGesTIC manifiesta actuar con diligencia para evitar la existencia en su sitio web de contenidos ilícitos y en caso de que tenga conocimiento efectivo de la existencia de infracciones a los derechos de propiedad intelectual, se reserva el derecho de proceder a bloquear el acceso durante el trámite del debido proceso para comprobar el incumplimiento y en caso de verificarse la falta, retirar definitvamente el acceso al proyecto depositado.

10. Acepto(amos) que la publicación y puesta a disposición del público del trabajo final de graduación, así como la presente autorización de uso de la obra, se regirá por la normativa institucional de la Universidad Nacional y la legislación de la República de Costa Rica. Adicionalmente, en caso de cualquier eventual diferencia de criterio o disputa futura, acepto(amos) que esta se dirimirá de acuerdo con los mecanismos de Resolución Alterna de Conflictos y la Jurisdicción Costarricense.

Autor(a): Ing. Marco Antonio Fonseca Aragón.

Firma: _____

Fecha de entrega: _____

Correo electrónico: marcofonsecaa@gmail.com

Índice General

Índice General 6

Índice de Tablas 10

Índice de Figuras 11

Índice de Anexos 14

Dedicatoria 15

Resumen ejecutivo 16

CAPITULO I – El problema y su importancia 17

7.1. Tema 18

7.2. Justificación del tema 18

7.3. Formulación del problema 19

7.4. Objetivos de la investigación 21

7.4.1. Objetivo general 21

7.4.2. Objetivos específicos 21

7.5. Alcances y limitaciones 22

7.5.1. Alcances 22

7.5.2. Limitaciones 22

CAPITULO II – Marco teórico o conceptual 23

8.1. Marco referencial 24

8.2. Marco conceptual 26

8.2.1. Gestión de riesgos organizacional 31

8.2.2. Jerarquía de Riesgos 32

8.2.3. Estándares y marcos de trabajo para la gestión de riesgos 35

8.2.3.1. Marco de Trabajo ISACA Risk IT 37

8.2.3.2. Marco de Trabajo Gestión de riesgos PMBOK 40

8.2.3.3. Gestión de riesgos marco de trabajo ITIL V3 (ISO/IEC 20000) 43

8.2.4. Análisis de frecuencia de los riesgos 44

8.2.5. Análisis de costos de riesgos 49

8.2.5.1. Costos tangibles 51

8.2.5.2. Costos intangibles 51

CAPITULO III – Marco Metodológico 53
9.1. Enfoque de la investigación 54
9.2. Tipo de investigación 54
9.3. Sujetos y fuentes de información 54
9.3.1. Sujetos 54
9.3.2. Fuentes de Información 56
9.4. Población y muestra 58
9.4.1. Personal responsable de los procesos de gestión de riesgos 59
9.4.2. Personal ejecutor de la metodología de gestión de riesgos 59
9.5. Definición de variables 59
9.6. Descripción de instrumentos utilizados 64
9.6.1. Entrevistas 64
9.6.2. Encuesta 65
9.6.3. Análisis de contenido 65
CAPITULO IV – Diagnóstico y análisis de resultados 66
10.1. Metodología actual 67
10.1.1. Ciclo de Gestión de Riesgos Operativos 67
10.1.1.1. Método Identificación y Evaluación de Riesgos 68
10.1.1.1.1. Objetivo: 69
10.1.1.1.2. Insumos: 69
10.1.1.1.3. Ejemplo herramienta a documentar: 69
10.1.1.2. Método Mitigación de Riesgos 70
10.1.1.2.1. Objetivo 71
10.1.1.2.2. Insumos 71
10.1.1.2.3. Ejemplo herramienta a documentar: 71
10.2. Lineamientos y Procesos 73
10.3. Resultado de entrevistas a Mandos Medios del Proceso 75
10.4. Hallazgos relevantes de la encuesta 76
10.4.1. Marcos de trabajo de gestión de riesgos 76
10.4.2. Fortalezas de la metodología implementada 78
10.4.3. Oportunidades de mejora de la metodología implementada 80
10.4.4. Uso de características para la identificación de riesgos. 81
10.4.5. Nivel de eficiencia, efectividad y agilidad en la gestión de riesgos. 83
10.4.6. Características utilizadas para priorizar los riesgos. 85

10.4.7. Variables se cuantifican o traducen a términos económicos según el tiempo de afectación. 87
10.4.8. Elementos que se cuantifican para definir planes de mitigación. 90
10.5. Análisis final 92
CAPITULO V – Solución del Problema 94
11.1. Propuesta de solución 95
11.2. Desarrollo de la solución 103
11.2.1. Catálogo de escenarios de Riesgos 103
11.2.2. Herramienta de evaluación de Riesgos 110
11.2.2.1. Formulario para identificación de riesgos 110
11.2.2.2. Guía para la identificación de riesgos 124
11.2.3. Herramienta de respuesta a Riesgos 124
11.2.4. Indicadores de medición propuestos 134
11.3. Procedimiento de implementación 145
11.3.1. Alcance del plan piloto 145
11.3.2. Personal participante 145
11.3.3. Capacitación 146
11.3.4. Ejecución de un simulacro de identificación de riesgos y acciones de respuesta para el servicio de banca electrónica 147
11.4. Pruebas y resultados 150
11.4.1. Cantidad de riesgos documentados 150
11.4.2. Criticidad de los Riesgos 152
11.4.3. Estimación de impacto cuantitativo 153
11.4.4. Impacto cuantitativo por tipo de costo 154
11.4.5. Costo de los Planes 155
11.4.6. Estrategia de respuesta asignada a los riesgos 157
11.4.7. Indicadores de medición 158
11.4.7.1. Correlación de Riesgos vs Incidentes materializados 158
11.4.7.2. Nivel de satisfacción 160
11.4.7.3. Identificación de costos (tangibles / intangibles) asociados a los riesgos 163
11.4.7.4. Comparativo de indicadores metodología actual vs metodología propuesta 163
CAPITULO VI – Análisis financiero 165
12.1. Egresos 166
12.2. Ingresos 168

12.3. Flujo de caja 170
12.4. Indicadores de rentabilidad del proyecto 170
12.5. Conclusiones financieras 172
CAPITULO VII – Conclusiones y recomendaciones 174
13.1. Conclusiones 175
13.2. Recomendaciones 180
13.3. Acciones futuras 183
13.3.1. Acciones de corto plazo (< 6 meses) 183
13.3.2. Acciones a mediano plazo (6 a 24 meses) 185
13.3.3. Acciones a largo plazo (> 24 meses) 186
CAPITULO VIII – Análisis retrospectivo 188
Referencias Bibliográficas 193
ANEXOS 197

Índice de Tablas

Tabla 1 Escala de interpretación del índice de correlación de Pearson Fuente: http://www.monografias.com/trabajos85/coeficiente-correlacion-karl-pearson/coeficiente-correlacion-karl-pearson.shtml 49
Tabla 2 Cálculo índice correlación Riesgos vs Incidentes. Fuente Propia 49
Tabla 3 Personal responsable de la metodología de gestión de riesgos. Fuente Propia 55
Tabla 4 Personal ejecutor de la metodología de riesgos. Fuente Propia 55
Tabla 5 Fuentes de información utilizadas en la investigación. Fuente Propia. 58
Tabla 6 Lista de variables a analizar. Fuente Propia. 64
Tabla 7 Formato de entrevistas. Fuente Propia. 65
Tabla 8 Comparación Metodología actual vs Propuesta. Fuente Propia 102
Tabla 9 Taxonomía del catálogo de Riesgos. Fuente: Risk 109
Tabla 10 Secciones del formulario para identificación de riesgos. Fuente propia. 111
Tabla 11 Agrupaciones Información Análisis de Riesgo. Fuente Propia. 113
Tabla 12 Calificación de frecuencia de riesgos. Fuente Propia 114
Tabla 13 Variables críticas para estimación de costos. Fuente Propia 119
Tabla 14 Costo por transacción de utilizar canal sustituto. Fuente propia 120
Tabla 15 Distribución porcentual de volumen transaccional por tipo transacción. Fuente propia. 121
Tabla 16 Ejemplo cuantificación de costos individual vs general. Fuente Propia 122
Tabla 17 Campos Sección Respuesta a Riesgos. Fuente Propia. 126
Tabla 18 Estrategias para respuesta a Riesgos (Valdez, 2012) 128
Tabla 19 Parámetros para seleccionar la alternativa de respuesta a un riesgo. Fuente: Risk IT. 130
Tabla 20 Características que una respuesta a un riesgo debe cumplir. Fuente: Martínez 131
Tabla 21 Matriz de decisión para respuesta a riesgos. Fuente Risk IT. 133
Tabla 22 Comparación de Riesgos e incidentes según criticidad. Fuente propia. 138
Tabla 23 Resumen Indicadores metodología actual. Fuente propia. 144
Tabla 24 Personal participante del piloto según puesto. Fuente propia. 146
Tabla 25 Comparación Riesgos vs Incidentes según criticidad. Fuente Propia 159
Tabla 26 Comparativo de indicadores metodología actual vs metodología propuesta. Fuente propia. 164
Tabla 27 Resumen de egresos por período. Fuente propia. 168
Tabla 28 Ahorros estimados por implementar respuesta a riesgos. Fuente propia. 169
Tabla 29 Flujo de caja del proyecto. Fuente propia. 170
Tabla 30 Indicadores financieros del proyecto. Fuente propia. 171

Índice de Figuras

Figura 1 ISACA; Un marco de trabajo empresarial, 2012 ..... *29*
Figura 2 Fuente: ISACA; The Risk IT Framework, USA, 2009 ..... *32*
Figura 3 Fuente: ISACA; IT Governance Domain Practices and Competencies: Information Risks: Whose Business are they?, USA, 2005 ..... *33*
Figura 4 Fuente: ISACA; The Risk IT Framework, USA, 2009 ..... *36*
Figura 5 Criterios de elección de Marcos de Trabajo para este análisis *37*
Figura 6 Fuente: ISACA, Risk IT Framework, USA, 2009 ..... *38*
Figura 7 Fuente: PMBOK 5ta edición; Impacto de variables basado en el tiempo del proyecto *41*
Figura 8 Fuente: Libro ITIL Service Transition; OGC *42*
Figura 9 Escala logarítmica. Fuente: http://www.scribd.com/doc/145713459/Escala-logaritmica#scribd *44*
Figura 10 Escala Richter de un sismo. http://www.artinaid.com/2013/04/escala-richter-de-un-sismo/ *45*
Figura 11 Comparación de escalas de presión acústica. http://hysiunidad4.weebly.com/contaminacioacuten-por-ruido.html *45*
Figura 12 Correlación Riesgos/Incidentes Panamá *46*
Figura 13 Correlación Riesgos/Incidentes Costa Rica *46*
Figura 14 Correlación Riesgos/Incidentes El Salvador *47*
Figura 15 Correlación Riesgos/Incidentes Guatemala *47*
Figura 16 Ejemplos de índices de correlación de Pearson Fuente: http://www.monografias.com/trabajos85/coeficiente-correlacion-karl-pearson/coeficiente-correlacion-karl-pearson.shtml *48*
Figura 17 Ciclo de Gestión de Riesgos Operativos. Fuente: Metodología Riesgos Operativos BAC *67*
Figura 18 Identificación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *68*
Figura 19 Evaluación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *69*
Figura 20 Herramienta identificación de riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *70*
Figura 21 Herramienta evaluación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *70*
Figura 22 Mitigación de riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *71*
Figura 23 Herramienta Identificación y evaluación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *71*
Figura 24 Herramienta Mitigación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *72*
Figura 25 Herramienta Mitigación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC *72*

Figura 26 Respuestas Pregunta 1 – Encuesta personal ejecutor y responsable de la metodología de gestión de riesgos *77*
Figura 27 Respuestas Pregunta 2 – Encuesta a personal responsable y ejecutor sobre las fortalezas de la gestión de riesgos *79*
Figura 28 Respuestas Pregunta 3 – Encuesta a personal responsable y ejecutor sobre las oportunidades de la gestión de riesgos *80*
Figura 29 Respuestas Pregunta 4 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre las características utilizadas para la identificación de riesgos. *82*
Figura 30 Respuestas Pregunta 4 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre las características utilizadas para la identificación de riesgos. *82*
Figura 31 Respuestas Pregunta 5 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre las características sobre nivel de eficiencia, efectividad y agilidad. *84*
Figura 32 Respuestas Pregunta 5 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre las características sobre nivel de eficiencia, efectividad y agilidad. *84*
Figura 33 Respuestas Pregunta 6 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre las características utilizadas para la priorización de riesgos. *86*
Figura 34 Respuestas Pregunta 6 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre las características utilizadas para la priorización de riesgos. *86*
Figura 35 Respuestas Pregunta 7 – Encuesta a personal responsable de la metodología de gestión de riesgos las variables que se cuantifican o traducen a términos económicos *88*
Figura 36 Respuestas Pregunta 7 – Encuesta a personal ejecutor de la metodología de gestión de riesgos las variables que se cuantifican o traducen a términos económicos. *89*
Figura 37 Respuestas Pregunta 8 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre los elementos que se cuantifican y documentan. *91*
Figura 38 Respuestas Pregunta 8 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre los elementos que se cuantifican y documentan. *91*
Figura 39 Fuente: ISACA, Risk IT Framework, USA, 2009 ..... *95*
Figura 40 Fuente: Propia, Basado en Risk IT Framework, USA, 2009 ..... *96*
Figura 41 Fuente: The Risk IT Practitioner Guide. Componentes de un escenario de Riesgo de TI *99*
Figura 42 Fuente: The Risk IT Practitioner Guide. Flujo de Respuesta y Priorización para Riesgos *99*
Figura 43 Fuente: The Risk IT Practitioner Guide. Flujo de Respuesta y Priorización para Riesgos *100*
Figura 44 Ciclo de Gestión de Riesgos Operativos. Fuente: Metodología Riesgos Operativos BAC *101*
Figura 45 Escala logarítmica. Fuente: http://www.scribd.com/doc/145713459/Escala-logaritmica#scribd *113*
Figura 46 Evaluación de Riesgos Cualitativos. Fuente Propia *116*
Figura 47 Mapa de calor para asignar impacto económico. Fuente propia. *117*
Figura 48 Flujo de Respuesta y Priorización para Riesgos Fuente: The Risk IT Practitioner Guide *129*

Figura 49 Fuente: The Risk IT Practitioner Guide. Flujo de Respuesta y Priorización para Riesgos..... 132
Figura 50 Cantidad de riesgos identificados por metodología actual según criticidad. Fuente propia. 136
Figura 51 Composición de riesgos identificados por metodología actual según criticidad. Fuente propia. 137
Figura 52 Cantidad de incidentes según criticidad 2014. Fuente propia. 138
Figura 53 Comparación de incidentes 2014 vs riesgos identificados. Fuente propia. 139
Figura 54 Resultados encuesta de satisfacción con metodología de gestión de riesgos actual realizada a gerentes. Fuente propia. 140
Figura 55 Índice de satisfacción Gerentes con metodología actual por variable. Fuente propia. 141
Figura 56 Resultados encuesta de satisfacción con metodología de gestión de riesgos actual realizada a usuarios del piloto. Fuente propia. 142
Figura 57 Índice de satisfacción usuarios del piloto con metodología actual por variable. Fuente propia. 143
Figura 58 Comparación cantidad de riesgos documentados Metodología actual vs Metodología propuesta. Fuente propia 150
Figura 59 Distribución calificación general riesgos por criticidad. Fuente propia..... 152
Figura 60 Porcentaje riesgos con estimación de impacto cuantitativo. Fuente Propia. 153
Figura 61 Distribución de riesgos con impacto cuantitativo asignado por tipo de costo. Fuente propia... 154
Figura 62 Distribución de riesgos con acciones de repuestas asociadas. Fuente propia. 155
Figura 63 Distribución de riesgos con planes de acción definidos. Fuente propia. 156
Figura 64 Distribución de riesgos según estrategia de respuesta asignada. Fuente propia. 157
Figura 65 Comparación de incidentes vs riesgos identificados en el piloto. Fuente propia 159
Figura 66 Resultados encuesta de satisfacción con piloto realizada a usuarios. Fuente propia. 161
Figura 67 Comparativo índice de satisfacción usuarios con metodología actual vs piloto. Fuente propia. 162
Figura 68 Porcentaje de riesgos identificados en el piloto con estimación de impacto cuantitativo. Fuente propia. 163
Figura 69 Recuperación de la inversión por período. Fuente propia. 172

Índice de Anexos

Anexo 1 – Minutas entrevistas

Anexo 2 – Encuesta Evaluación Metodología Gestión de Riesgos TI BAC

Anexo 3 – Resultados Encuesta

Anexo 4 – Encuesta Nivel de Satisfacción Usuarios con la Metodología Actual

Anexo 5 – Catálogo de escenarios de riesgos

Anexo 6 – Prototipo formulario para ingreso de nuevos riesgos

Anexo 7 – Guía para la identificación de Riesgos

Anexo 8 – Reporte de Violación de Datos Personalizado 253

Anexo 9 – Ejemplos de Pantallas de la herramienta diseñada en Sharepoint utilizada para el Piloto

Anexo 10 - Campos Sección I – Resumen del Riesgo

Anexo 11 – Campos Sección II – Descripción del Riesgo

Anexo 12 – Niveles de afectación para cada dimensión

Anexo 13 – Mapa de calor Riesgos

Anexo 14 – Indicadores de medición propuestos

Dedicatoria

El presente trabajo no habría sido posible lograrlo sin el apoyo incondicional que recibí por parte de grandes personas que Dios puso en mi vida, las cuales quiero recordar a continuación y dedicarles esta tesis.

A mis compañeros de trabajo, colegas y colaboradores por sus palabras de aliento y el tiempo que dedicaron a apoyar mi propuesta.

A Jorge Betancourth por su apoyo, consejo pero principalmente por el tiempo que siempre me brindó, a pesar de sus múltiples responsabilidades, para asesorarme y guiarme a través del desarrollo del proyecto.

A mi padre que, con su ejemplo, siempre me motivó a seguir adelante. Y que hoy, a pesar de su enfermedad, sigue siendo un luchador que me inspira para seguir creciendo e igualar sus éxitos académicos. A mi madre por darme la vida, pero principalmente inculcarme disciplina, una buena formación, tenacidad y educación.

A mis hermanas (María Vilma, Carolina y Josselyn) que siempre estuvieron para motivarme a seguir adelante y darme su apoyo incondicional compartiendo responsabilidades.

A mis hijos, Andy y Lala, que son una gran fuente de motivación en mi vida, a quienes quiero dejarles un ejemplo de superación y sacrificio.

Finalmente a Jessica, que siempre estuvo presente para apoyarme y alentarme a seguir adelante cada vez que me quería rendir. Gracias por tu paciencia, sabio consejo e ideas que contribuyeron muchísimo al éxito de mi proyecto.

> ***"He llegado hasta aquí y me rehusé a renunciar porque toda mi vida siempre he terminado la carrera"*** Louis Zamperini

Resumen ejecutivo

El presente trabajo está enfocado en el análisis y mejora de una metodología existente para la gestión de riesgos de operación, poniendo énfasis en la reducción de pérdidas económicas causados por la interrupción de un servicio de banca electrónica dentro de una institución financiera.

Se realizó un diagnóstico de situación actual, encontrando como principales oportunidades de mejora: la herramienta utilizada actualmente por la organización y la cuantificación en términos económicos de los riesgos identificados.

Posterior a realizar un estudio del estado del arte en gestión de riesgos de tecnología, se propuso una metodología de gestión de riesgos basada en Risk IT de ISACA. A dicha metodología se le incorporó un modelo de estimación de costos (tangibles e intangibles), propuesto por el investigador, con el fin de simplificar y hacer más predecible la evaluación y priorización de los riesgos.

La metodología propuesta se puso en práctica mediante la aplicación de un piloto. Dentro de los resultados más relevantes posterior a la aplicación del piloto, se logró aumentar el nivel de satisfacción de los clientes a un 67% y un importante incremento en la identificación de costos tangibles e intangibles asociados a los riesgos (64% del total de riesgos identificados contaban con dichas variables).

Al analizar la rentabilidad de la metodología propuesta, se encontró que la implementación de la misma lograría cubrir sus costos como mínimo al siguiente año de implementación, lo cual la hace muy atractiva para la organización.

A raíz de lo anterior, se recomienda a la organización adoptar la metodología e implementarla de manera inicial en el sistema donde fue probada para luego ampliar su uso hacia otros sistemas y diferentes áreas de tecnología ubicadas en los diferentes países donde tiene presencia la organización.

CAPITULO I – El problema y su importancia

7.1. Tema

El presente trabajo está enfocado en el análisis y mejora de una metodología existente para la gestión de riesgos, poniendo énfasis en la reducción de pérdidas económicas y daños a la reputación causados por la interrupción de un servicio de misión crítica dentro de una institución financiera.

7.2. Justificación del tema

Para una institución bancaria que ofrece servicios centralizados para varios países de la región centroamericana, México y Panamá, la gestión de riesgos de operación y su frecuente actualización se torna un elemento crítico para la oportuna toma de decisiones a nivel ejecutivo.

Es a través de una adecuada gestión de riesgos operativos y un plan de respuesta apropiado que se puede lograr minimizar cualquier interferencia a la ejecución de la estrategia empresarial.

Interrupciones no planificadas en un servicio crítico, a causa de eventos o incidentes no hayan sido anticipados y planificados, podrían comprometer la estrategia afectando la imagen o el cumplimiento regulatorio de la organización, con las pérdidas directas o indirectas que este tipo de eventos pueden causar.

Por esta razón, proponemos desarrollar y/o robustecer una metodología que facilite la identificación, análisis y gestión de riesgos de operación que comprometan la continuidad de servicios críticos, como herramienta esencial para dar soporte a las decisiones organizacionales e inversiones para la prevención de riesgos.

Con el desarrollo de este proyecto el cliente recibirá como beneficios:

1) Lograr un entendimiento de las debilidades del proceso actual.
2) Identificar las brechas existentes comparando sus prácticas actuales versus las mejores prácticas para la gestión de riesgos disponibles en la industria.

3) Recibir un conjunto de recomendaciones asociadas a la mejora de los procesos actuales.

7.3. Formulación del problema

La red financiera BAC Credomatic Network, con presencia en varios países de la región (desde México hasta Panamá), brinda a sus clientes un servicio de Banca Electrónica a través de Internet. Con una antigüedad cercana a los trece años, el servicio se ha consolidado como un canal muy importante, no únicamente por el volumen transaccional y monetario que se transa a través del mismo, sino también por el soporte que brinda a la estrategia de medios de pago de la organización.

Aunque si bien la aplicación está diseñada para dar servicio tanto a personas físicas como jurídicas, su fortaleza principal es la habilidad de funcionar como una solución integrada de manejo de tesorería para las empresas que tienen presencia en los diferentes países de la región. Esto se ha convertido en un elemento diferenciador, comparado con el resto de ofrecimientos que otras entidades bancarias tienen, y ha generado que la criticidad del servicio aumente considerando la alta dependencia que ahora tienen múltiples empresas, incluyendo sus proveedores y colaboradores, para recibir sus pagos y salarios a través de esta aplicación de banca electrónica.

Mediante el servicio de banca electrónica, se pueden realizar diversas transacciones bancarias como por ejemplo: consultas de saldo, consultas de estados de cuenta, pagos de planilla y proveedores, transferencias de fondos (locales, interbancarias e internacionales), pagos de servicios públicos, pagos de tarjetas de crédito, inversiones, entre otros.

A través de los años, el servicio de banca electrónica ha venido evolucionando y aumentando su madurez consecuente al incremento en la criticidad del servicio. Esto se ha facilitado gracias a la inversión realizada por la empresa en gente, procesos y tecnología. Lo anterior ha permitido que las métricas de calidad de servicio (tiempos de respuesta, consistencia y disponibilidad) se hayan mejorado

significativamente permitiendo controlar eventos e incidentes recurrentes. Sin embargo, existe preocupación por parte de la administración sobre la capacidad de asegurar la continuidad del servicio y su calidad ante incidentes mayores o desastres naturales. Dichas preocupaciones están fundamentadas en fuertes dependencias del personal técnico encargado de la gestión del servicio que deben ser evaluadas y mitigadas.

El canal de banca electrónica, hoy en día, es un habilitador de transacciones de autoservicio para el cliente. Dichas transacciones están disponibles en un horario 24x7 y el tiempo que el cliente espera para su ejecución es mínimo (prácticamente tiempo real). Por otro lado, algunas de las operaciones únicamente se encuentran disponibles a través de este canal. Esto significa que no necesariamente están accesibles para la totalidad de los clientes en los demás canales de servicio (agencias, kioscos, banca telefónica, banca móvil, backoffice, etc.). Por otro lado, las operaciones que si están habilitadas en estos otros canales, representan un costo mayor para la organización y el tiempo de respuesta para los clientes es mayor.

Por esta razón, una falla prolongada que interfiera con el uso del servicio de banca electrónica afectaría a todos los clientes de los distintos países que dependen de esta plataforma de servicio y además conlleva implicaciones fuertes en la imagen de la empresa, exposiciones a nivel regulatorio y un aumento en los costos de operación debido al incremento en el costo de las transacciones realizadas a través de otros canales de mayor costo por transacción.

Considerado los antecedentes anteriores, la administración de TI consideró necesario someter a un estudio el proceso y métodos utilizados actualmente para la gestión de los riesgos operacionales de este servicio, con el fin de poder identificar y aplicar mejoras que den como resultado un mayor control sobre dichos imprevistos.

7.4. Objetivos de la investigación

7.4.1. Objetivo general

Realizar un análisis y proponer mejoras a la metodología de gestión de riesgos de operación utilizada actualmente por la organización para el servicio de banca electrónica con el fin de innovar, simplificar y enriquecer los instrumentos utilizados para hacer un uso más eficiente y efectivo de los recursos de la organización.

7.4.2. Objetivos específicos

1) Analizar las prácticas actuales de gestión de riesgos en la organización para determinar las brechas que existen en comparación con las mejores prácticas de gestión de riesgos de la industria.
2) Realizar un estudio del estado del arte en gestión de riesgos de tecnología para identificar las oportunidades de mejora de los procesos actuales.
3) Proponer una metodología de gestión de riesgos de operación y continuidad de servicio con el fin definir claramente las diferentes etapas y establecer un ciclo de revisión periódica.
4) Proponer los instrumentos necesarios (o complementar los existentes) con el fin de enriquecer el proceso actualmente ejecutado por la organización para identificación y valoración de riesgos.
5) Estandarizar la herramienta utilizada para el registro de nuevos riesgos, incorporando las variables económicas necesarias para facilitar el cálculo de costos y la priorización con el fin de simplificar y hacer más predecible la evaluación de los riesgos
6) Crear un catálogo de escenarios de riesgos que permita reducir la ambigüedad y hacer más estructurado el proceso de identificación de riesgos con el fin de proveer mayor orientación a los usuarios en la documentación de nuevos riesgos.
7) Realizar un piloto de la metodología propuesta desarrollando una herramienta automatizada (Sharepoint) para medir la mejoría en la efectividad y nivel de satisfacción con la metodología de gestión de riesgos propuesta.

8) Realizar un análisis de factibilidad financiera de implementar la metodología propuesta contrastando los costos y el retorno de la inversión para validar que la inversión que la organización realizará justifica los beneficios económicos que recibirá a cambio.

7.5. Alcances y limitaciones

7.5.1. Alcances

Dentro del alcance del presente trabajo se considerará el análisis y mejoras al proceso de gestión de riesgos, en sus diferentes fases, que afecten la continuidad o disponibilidad de un servicio crítico de TI.

No está bajo el alcance de este análisis las gestión de riesgos laborales (accidentes, sanitarios, patológicos, etc.) o riesgos financieros (crédito liquidez, mercado, operacional) que no tengan relación con la continuidad de un servicio de tecnología.

Adicionalmente, dado el enfoque del proyecto, el cual definimos en la continuidad de servicios de tecnología, limitamos el alcance del diagnóstico de situación actual, únicamente al personal de tecnología que tiene relación directa con el proceso de gestión de riesgos. No considerando al personal de áreas de negocio o usuarios finales de la herramienta.

7.5.2. Limitaciones

Debido a restricciones de tiempo, el trabajo se enfocará en analizar como mejores prácticas únicamente a los marcos de trabajo propuestos por ISACA y Basilea, específicamente CRISC, CGEIT y COSO.

Seleccionamos los marcos de trabajo anteriores, debido a que son los más comúnmente utilizados por la industria financiera, basado en la retroalimentación brindada por el patrocinador del proyecto.

CAPITULO II – Marco teórico o conceptual

8.1. Marco referencial

Esta investigación se desarrolla dentro de la organización BAC Credomatic Network, una institución financiera con presencia en la región centroamericana, México y Panamá.

El grupo BAC Credomatic fue fundado originalmente en Nicaragua en el año 1952 como la primera empresa de tarjetas de crédito en ese país. Actualmente Credomatic es el líder en emisión de tarjetas de crédito, y extiende sus soluciones financieras y de pago a través de Centroamérica y Panamá. Credomatic se fusionó con BAC (Banco de América Central) formando el grupo BAC Credomatic. La organización mantiene una posición relevante en el mercado centroamericano; en Julio 2013 alcanzó US$14 billones en activos. Tiene una sólida historia en el mercado de 62 años y un buen historial de indicadores de rentabilidad comparado con sus homólogos en la región.

Según la información publicada en el sitio web www.bac.net, la misión del grupo es:

> "Facilitar con excelencia el intercambio y financiamiento de bienes y servicios, a través de sistemas de pago y soluciones financieras innovadoras y rentables que contribuyan a generar riqueza, a crear empleo y a promover el crecimiento económico sostenible y solidario de los mercados donde operamos."

La misma fuente indica que la visión del grupo es:

> "Ser la organización financiera preferida de las comunidades que atendemos por nuestro liderazgo en medios de pago, por nuestra solidez, confiabilidad, avanzada tecnología y conectividad con personas y empresas, a quienes les simplificamos la vida facilitándoles la realización de sus sueños y el logro de sus metas."

Los valores de la organización consideran: Excelencia, Integridad, Innovación, Responsabilidad y Respeto.

El grupo financiero brinda los servicios a sus clientes, a través de una combinación de servicios locales y regionales. Es decir, algunos servicios informáticos forman parte del portafolio de aplicaciones que se gestionan localmente. Sin embargo, existe un grupo de servicios que se operan de forma centralizada para beneficio de todos los clientes ubicados en los diferentes países.

El trabajo a desarrollar está dirigido hacia la metodología de gestión de riesgos de los servicios que se prestan de forma centralizada. Estos servicios son administrados por el personal de TI corporativo de la organización conocido como DICA (Dirección Regional de Informática), dichos colaboradores se encuentran localizados en Costa Rica.

El área de Riesgos está compuesta por 4 colaboradores y forman parte de la Gerencia de Riesgos y Seguridad de Sistemas, quien a su vez le reporta al Chief de Informática (CIO).

A partir de este proyecto, la maestría recibirá un marco de trabajo que servirá como punto de partida para definir una metodología para el análisis formal de riesgos de operación de cualquier servicio tecnológico que una organización ponga a disposición de sus clientes.

Para el desarrollo de este proyecto se considerarán los siguientes componentes de tecnología y áreas de conocimiento de la maestría:

1) Investigación y desarrollo de TI (Innovación tecnológica)
    - A través de la investigación del estado del arte en la gestión de riesgos operacionales de tecnología se buscará elevar la madurez actual que la organización posee en esta área y enriquecer sus procesos y conocimiento.
2) Gestión de la TI

- Al revisar los procesos actuales y su apego a mejores prácticas de la industria realizaremos aportes con propuestas de mejora a la administración de la tecnología y servicios.

3) Administración del cambio
    - Modificaciones al estatus quo de cómo se manejan actualmente los riesgos requerirán una adecuada gestión del cambio con el fin de que las mejoras sean aceptadas con beneplácito por parte de todos los stakeholders.
4) Administración de proyectos como especialidad del proyecto.
    - Toda la planificación y ejecución del proyecto será gestionada a través de una metodología de Administración de Proyectos que permita cumplir las expectativas en tiempo, costo y calidad.

Adicionalmente, con el desarrollo de este proyecto, se espera:

1) Adquirir conocimientos y experiencias en el análisis y gestión de riesgos.
2) Adquirir conocimientos en administración de un servicio y variables críticas de operación.
3) Aplicar técnicas y herramientas modernas en la gestión de riesgos.
4) Poner en práctica la creatividad para buscar soluciones prácticas y costo/efectivas a las debilidades que se detecten dentro del proceso de gestión implementado actualmente.

8.2. Marco conceptual

Esta investigación se centra el análisis y reforzamiento de una metodología para la gestión de riesgos de operación y continuidad, es por ello que debemos definir bajo el contexto de este análisis, qué entendemos por cada uno de los conceptos que vamos a abordar.

Dentro de este estudio vamos a considerar el siguiente glosario de definiciones:

1. Riesgo: “Es la posibilidad de que un evento ocurra, el cual tendrá impacto en el alcance de los objetivos y típicamente se mide en términos de probabilidad e impacto.” (ISACA, 2013).

   Según el marco de trabajo ISO 31000, además “riesgo es el efecto de la incertidumbre sobre los objetivos. La incertidumbre considera eventos (los cuales pueden o no ocurrir) y también incertidumbre causada por la ambigüedad o falta de información. Adicionalmente se consideran impactos no únicamente negativos sino también los positivos sobre los objetivos.” (Purdy, GPURDY, 2010).

2. Riesgo Operacional: “Se define como el riesgo incurrido por las actividades internas de una organización. Los riesgos operacionales se enfocan en los riesgos que se generan a partir de las personas, tecnologías y procesos a través de los cuales una compañía opera. También puede incluir otras clases de riesgos, como riesgos de fraudes, riesgos legales, riesgos ambientales y riesgos físicos.” (Fondo Monetario Internacional, 2011, pp. 2-3) Una definición ampliamente utilizada para riesgo operacional es la contenida dentro de las regulaciones de Basilea II. Esta definición afirma que “el riesgo operacional es el riesgo de pérdida resultante de un sistema, gente o proceso interno inadecuado o fallido o por eventos externos.” (Basel Committee on Banking Supervision, 2001).

3. ISACA: Es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información. “ISACA actualmente atiende a unos 115,000 electores (miembros y profesionales con certificaciones ISACA) en unos 180 países”. Dentro de las actividades de la organización se encuentra que son los custodios del marco de trabajo COBIT, creadores del ITGI (IT Governance Institute) y desarrolladores de cuatro certificaciones profesionales: (ISACA, 2014)

a. CISA - Certified Information Systems Auditor, certificación de auditores de sistemas de información. Existen cerca de 103,000 personas certificadas;
b. CISM - Certified Information Security Manager, certificación de gestores de seguridad. Existen cerca de 22,500 personas certificadas;
c. CGEIT - Certified in the Governance of Enterprise IT, certificación de gestores del gobierno empresarial de TI. Existen cerca de 5,600 personas certificadas;
d. CRISC - Certified in Risk and Information Systems Control, certificación de gestores de control de riesgos en sistemas de información. Existen cerca de 16.800 personas certificadas.

4. COBIT: Objetivos de Control para Información y Tecnologías Relacionadas ("COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentado como marco de trabajo ("framework" en inglés), dirigida al control y supervisión de tecnología de la información (TI). Tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un marco de trabajo, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión. En su cuarta edición, COBIT 4.1 tiene 34 procesos que cubren 210 objetivos de control (específicos o detallados) clasificados en cuatro dominios (Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, Supervisión y Evaluación) (ITIL ORG).

5. COBIT 5: ISACA lanzó el 10 de abril del 2012 la nueva edición de este marco de referencia. COBIT 5 es la última edición del marco de trabajo mundialmente aceptado, el cual proporciona una visión empresarial del Gobierno de TI que tiene a la tecnología y a la información como protagonistas en la creación de valor para las empresas. COBIT 5 se basa en COBIT 4.1, y a su vez lo amplía mediante la integración de otros

importantes marcos y normas como Val IT y Risk IT, Information Technology Infrastructure Library (ITIL ®) y las normas ISO relacionadas. en esta norma (ISACA).

En la siguiente figura detallamos la evolución que ha tenido COBIT a lo largo del tiempo y el enfoque que ha tenido en cada una de sus versiones. Aunque si bien COBIT 5 fue liberado al público en el 2012, integrando y mejorando varios estándares, actualmente las entidades financieras continúan siendo evaluadas y supervisadas bajo el alcance de COBIT 4.1. Por esta razón, es que la presente investigación tomará en consideración la normativa y definiciones vigentes para COBIT 4.1.

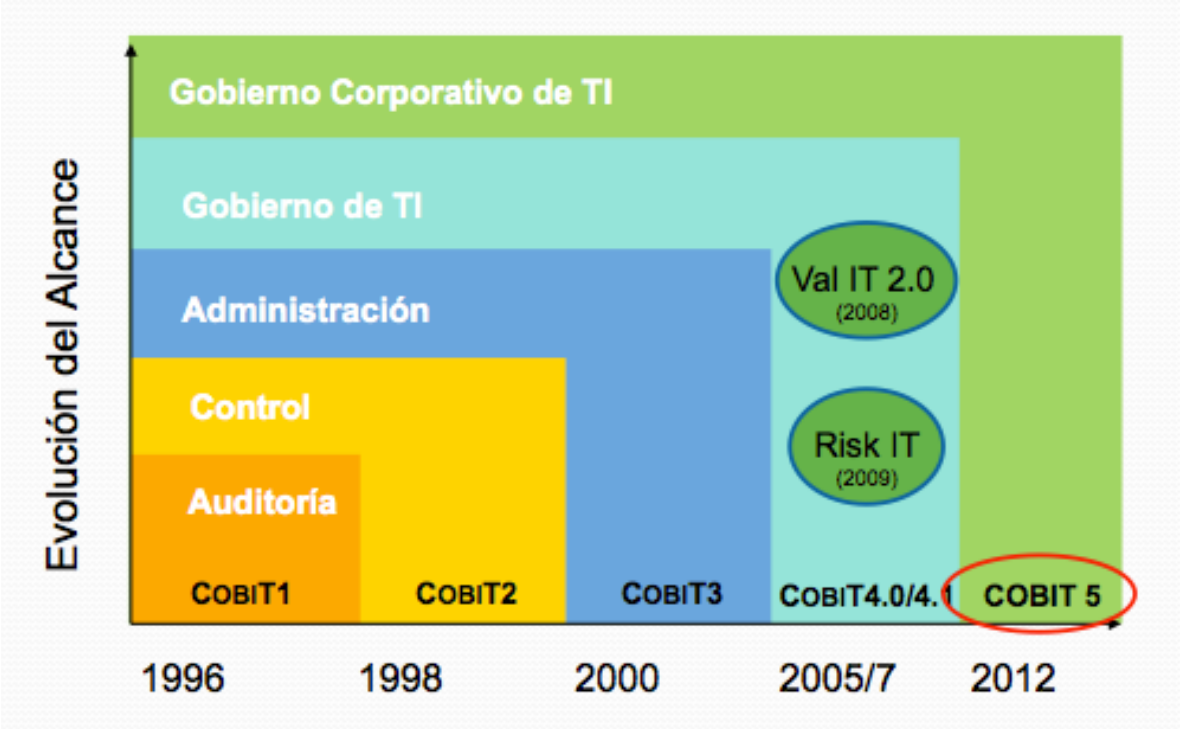


Figura 1 ISACA; Un marco de trabajo empresarial, 2012

6. CRISC: “Certified in Risk and Information Systems Control” (CRISC) es una certificación reconocida por ISACA para profesionales de Tecnologías de Información con experiencia en la gestión de riesgos de TI. Para ganar esta certificación, los candidatos deben aprobar un examen escrito y tener por lo menos ocho años de experiencia en tecnología de información o el negocio,

con un mínimo de tres años de experiencia laboral en por lo menos tres dominios del CRISC. La intención de la certificación es proveer un cuerpo común de conocimiento para la gestión de riesgos de TI o sistemas y reconocer el conocimiento adquirido en riesgos organizacionales y de TI, así como también la capacidad de implementar y mantener controles de sistemas de información para mitigar riesgos de sistemas de información o tecnología de información. La certificación CRISC requiere demostrar conocimiento en cinco áreas funcionales o dominios de la gestión de riesgos de TI: (ISACA)

   a. Identificación, estimación y evaluación de riesgos
   b. Respuesta a riesgos
   c. Monitoreo de riesgos
   d. Diseño e implementación de controles de sistemas de información
   e. Monitoreo y mantenimiento de controles de sistemas de información

7. CGEIT: “Certified in the Governance of Enterprise IT (CGEIT) es una certificación otorgada por ISACA que reconoce a los profesionales su conocimiento y aplicación de prácticas y principios de gobierno de TI empresarial. La certificación permite un abordaje holístico al gobierno de la tecnología para proveer un mayor valor a la organización. Las áreas enfoque corresponden a: (ISACA)

   a. Marco de Trabajo para el gobierno de la TI empresarial
   b. Administración Estratégica
   c. Realización de beneficios
   d. Optimización de riesgos
   e. Optimización de recursos

8. Basilea II: Es el segundo de los acuerdos de Basilea, los cuales son recomendaciones sobre la legislación y regulación bancaria emitidas por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II es crear un estándar internacional que sirva de referencia para los reguladores bancarios, con el fin de controlar cuanto capital tienen que reservar los

bancos para protegerse contra los diferentes tipos de riesgos financieros y operacionales que afrontan tanto los bancos como la economía (González, 2008). Basilea II se apoya en tres pilares: (Basel Committee on Banking Supervision, 2001)

a. Pilar I: el cálculo de los requisitos mínimos de capital, es en este punto donde los riesgos operativos juegan un importante papel por cuanto afecta la reserva que el banco debe realizar para manejar imprevistos.
b. Pilar II: el proceso de supervisión de la gestión de los fondos propios.
c. Pilar III: la disciplina de mercado.

Para efectos de esta investigación, se rescata de Basilea II la relevancia que otorga a la gestión de riesgos a nivel general en los sistemas financieros a nivel mundial. Sin embargo, no aporta respecto a la gestión de riesgos operativos de Tecnología de Información que se considera dentro del alcance de este trabajo.

8.2.1. Gestión de riesgos organizacional

El riesgo de una organización o negocio es afectado por factores ambientales del negocio (estilo de administración o cultura, apetito de riesgo y factores de sector de la industria como la competencia, reputación, regulaciones nacionales o internacionales) y consecuentemente los riesgos de TI pueden ser afectados de manera similar. (ISACA, 2013).

La necesidad universal de mostrar un adecuado gobierno empresarial a los accionistas y clientes es el principal impulsor de una creciente cantidad de actividades alrededor de la gestión de riesgos. Existen muchos tipos de riesgos empresariales además del riesgo financiero. Las entidades regulatorias están específicamente concentradas en los riesgos operacionales y sistémicos. Precisamente en estas dos últimas áreas es donde los riesgos de tecnología y seguridad de información son relevantes. La administración de riesgos es la piedra angular del gobierno de TI, asegurando que los objetivos estratégicos del negocio

no se vean amenazados por fallas en la tecnología. Los riesgos asociados con fallas tecnológicas están cada vez más formando parte de las agendas de las juntas directivas debido a que una falla de TI puede tener consecuencias devastadoras (ISACA, 2013).

8.2.2. Jerarquía de Riesgos

Es importante considerar los riesgos de TI dentro de todo el contexto del negocio, en los niveles operacional, de portafolio, de programas, de proyectos y estratégico. Existen varios estándares y marcos de trabajo de riesgos publicados, la mayoría de los cuales refleja que los riesgos de TI son parte de una jerarquía de riesgos, tal y como se muestra en la Figura 2.

Figura 2 Fuente: ISACA; The Risk IT Framework, USA, 2009

Para el caso del "framework" conocido como Management of Risk (M_o_R), el cual pertenece a la UK Office of Goverment Commerce (OGC), se definen cuatro niveles de riesgos para asegurarse que los riesgos se consideren a los niveles ejecutivos desde el nivel estratégico hasta el nivel operacional, como se observa en la Figura 3 (ISACA, 2013).

Figura 3 Fuente: ISACA; IT Governance Domain Practices and Competencies: Information Risks: Whose Business are they?, USA, 2005

El enfoque de esta investigación estará centrado en los riesgos de operación y entrega de servicios de TI o el Nivel Operacional, según se identifica en las dos figuras anteriores.

Los riesgos asociados al nivel operacional comprenden riesgos relacionados a las personas, aspectos técnicos, costos, tiempos, recursos, soporte operacional, calidad, fallas de proveedores, seguridad, fallas de infraestructura, continuidad del negocio y relaciones con los clientes, entre otros. (ISACA, 2013).

El énfasis al nivel operacional está centrado en objetivos a corto plazo que aseguren la continuidad ininterrumpida de los servicios de negocio. (ISACA, 2013).

El contexto de la administración de riesgos varía significativamente desde el nivel estratégico hasta el nivel de operaciones de TI. Como mínimo los riesgos deberían analizarse; aunque no se tomen ninguna acción inmediata, la conciencia del riesgo influenciará las decisiones estratégicas para buscar mejoría. Usualmente, los

riesgos de TI más dañinos no son bien comprendidos. Al nivel estratégico, es necesario entender que la aceptación de riesgos es un elemento esencial de los negocios hoy en día y el éxito llega a aquellas empresas que logran detectar, identificar y gestionar riesgos de la manera más efectiva. A este nivel, la administración de riesgos se involucra respondiendo al impacto real en el negocio, identificado los problemas relevantes y asegurándose que los riesgos reales e importantes sean tratados o resueltos (ISACA, 2013).

El enfoque en el nivel operacional de TI es la entrega de servicios de TI en cumplimiento con los niveles gestión de servicios esperados. La administración de riesgos es vista en términos de la desviación de estos niveles de servicio y su impacto al negocio asociado. El enfoque orientado a procesos utilizado en los marcos de trabajo ITIL (Information Technology Infrastructure Library) y COBIT ha ganado terreno en los años recientes. Tomar un enfoque orientado a procesos asegurará que los dueños de procesos sean encargados de conocer y administrar el riesgo inherente en los procesos que tienen bajo su responsabilidad. Esto genera una administración de riesgos proactiva, en la cual la responsabilidad y corrección de los riesgos es parte de la práctica estándar (ISACA, 2013).

Los riesgos conocidos son aquellos que han sido identificados y analizados, haciendo posible planificar respuestas a los mismos. A los riesgos conocidos que no podemos administrar de manera proactiva, se les debería asignar una reserva de contingencia. Lo mismo sucede con los riesgos desconocidos los cuales no se pueden gestionar proactivamente y por ello se les debe asignar una reserva para su administración (PMI, 2013).

Las organizaciones perciben los riesgos como el efecto de la incertidumbre en los proyectos, los servicios y los objetivos organizacionales. Las organizaciones están dispuestas a aceptar diferentes niveles de riesgos dependiendo de su actitud hacia el riesgo. Estas actitudes pueden verse influenciadas por un conjunto de factores que se pueden clasificar en tres temas: (PMI, 2013).

1) Apetito de riesgo: Es el grado de incertidumbre que una entidad está dispuesta a aceptar en anticipación a cambio de una recompensa.
2) Tolerancia a riesgo: Es el grado, cantidad o volumen de riesgo que una organización o individuo puede resistir.
3) Umbral de riesgo: Se refiere a medidas a lo largo del nivel de incertidumbre o el nivel de impacto en el cual un participante podría tener un interés particular. Debajo de ese umbral, la organización aceptará el riesgo. Por encima del umbral, la organización no tolerará el riesgo

Cada organización es diferente, por lo que los niveles anteriores pueden ser definidos en niveles distintos y esto hará que su plan de respuesta a dichos riesgos sea diferente si se llegaran a comparar. (PMI, 2013, p. 310).

Las personas y grupos adoptan posiciones diferentes alrededor de los riesgos, lo cual influencia la manera que responden a ellos. Estas posiciones están dirigidas por percepciones, tolerancias, inclinaciones y prejuicios, todo esto debe hacerse explícito hasta donde sea posible. De ahí que, la comunicación de cada riesgo y las medidas acordadas para su manejo, debe ser abierta y transparente. Las respuestas a los riesgos reflejan el balance percibido de una organización entre la toma de riesgos y la prevención de riesgos (PMI, 2013, p. 310).

8.2.3. Estándares y marcos de trabajo para la gestión de riesgos

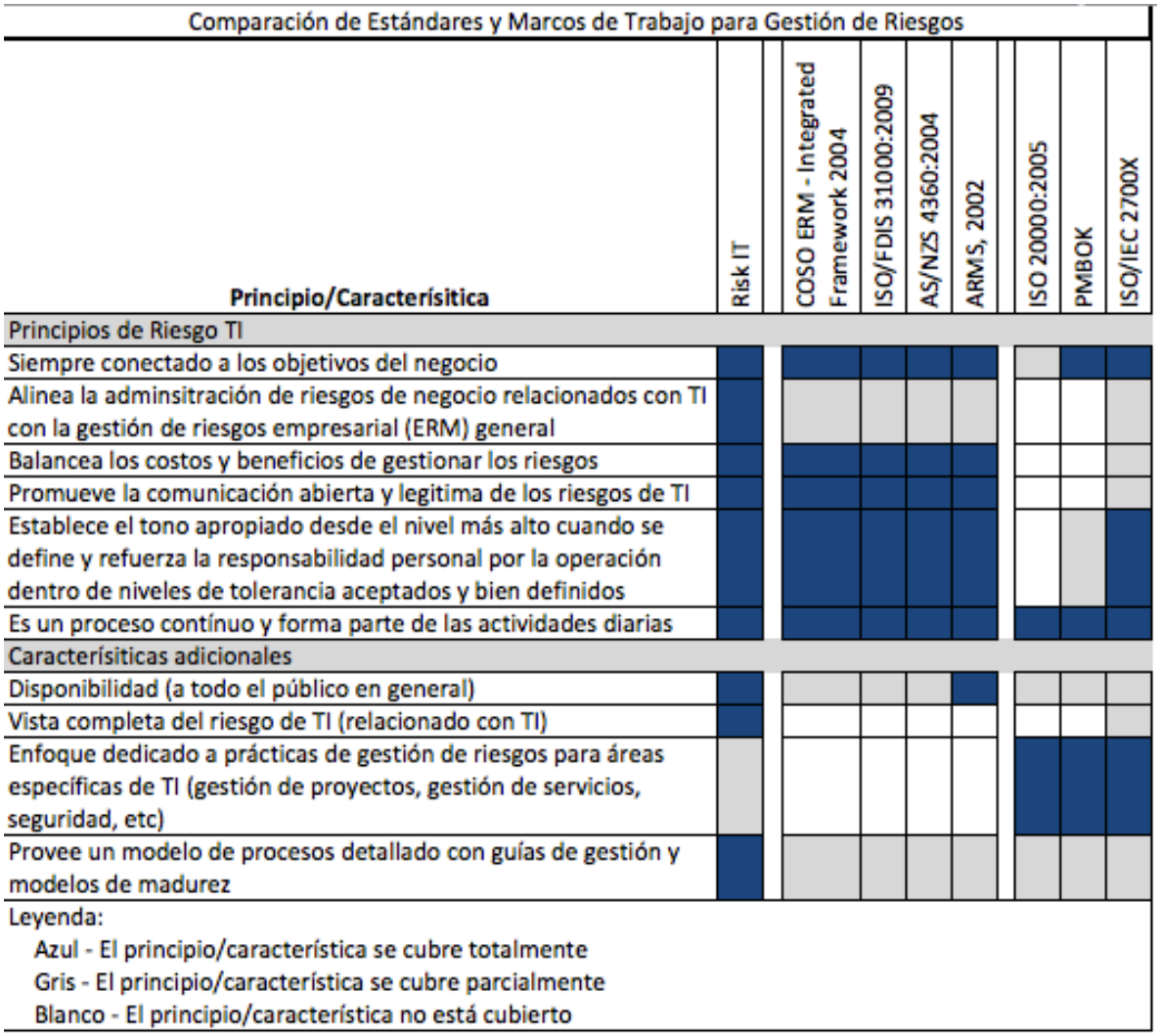
Existen un conjunto de estándares y marcos de trabajo de riesgos, los cuales proveen guía para la aplicación de gestión de riesgos, los cuales tienen múltiples orígenes.

Algunos de los más importantes/conocidos son:

1. Risk IT Framework de ISACA
2. ERM (Enterprise Risk Management) Framework de COSO
3. ISO 31000:2009 Principios y Reglas para implementación de Gestión de Riesgos de ISO
4. M_o_R Framework de la OGC

5. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) de la Universidad de Carnegie Mellon
6. ISO/IEC 27000 Familia de estándares de Seguridad de Información de ISO
7. ISO/IEC 20000 Estándar internacional para gestión de servicios de TI
8. ITIL M_o_R Guía para Profesionales

A continuación, en la Figura 4 se presenta un comparativo de algunos de los diferentes estándares y marcos de trabajo mencionados anteriormente:



Comparación de Estándares y Marcos de Trabajo para Gestión de Riesgos

Principio/Caracterísitica	Risk IT	COSO ERM - Integrated Framework 2004	ISO/FDIS 31000:2009	AS/NZS 4360:2004	ARMS, 2002	ISO 20000:2005	PMBOK	ISO/IEC 2700X
Principios de Riesgo TI								
Siempre conectado a los objetivos del negocio	■	■	■	■	■	▒	■	■
Alinea la adminsitración de riesgos de negocio relacionados con TI con la gestión de riesgos empresarial (ERM) general	■	▒	▒	▒	▒			▒
Balancea los costos y beneficios de gestionar los riesgos	■	■	■	■	■			▒
Promueve la comunicación abierta y legitima de los riesgos de TI	■	■	■	■	■			▒
Establece el tono apropiado desde el nivel más alto cuando se define y refuerza la responsabilidad personal por la operación dentro de niveles de tolerancia aceptados y bien definidos	■	■	■	■	■		▒	■
Es un proceso contínuo y forma parte de las actividades diarias	■	■	■	■	■	■	■	■
Caracterísiticas adicionales								
Disponibilidad (a todo el público en general)	■	▒	▒	▒	■	▒	▒	▒
Vista completa del riesgo de TI (relacionado con TI)	■							▒
Enfoque dedicado a prácticas de gestión de riesgos para áreas específicas de TI (gestión de proyectos, gestión de servicios, seguridad, etc)	▒					■	■	■
Provee un modelo de procesos detallado con guías de gestión y modelos de madurez	■	▒	▒	▒	▒	▒	▒	▒

Leyenda:
Azul - El principio/característica se cubre totalmente
Gris - El principio/característica se cubre parcialmente
Blanco - El principio/característica no está cubierto

Figura 4 Fuente: ISACA; The Risk IT Framework, USA, 2009

La figura anterior muestra las diferencias entre las características evaluadas de los diferentes marcos de trabajo a nivel general y tomando en cuenta la gestión

integral de todos los riesgo. Pero para efectos del alcance de esta investigación, enfocada en riesgos de operación de un servicio de TI y considerando el tiempo disponible, se tomaron en consideración únicamente los siguientes marcos de trabajo: ISACA Risk IT, el PMBOK e ITIL V3 (base de ISO 20000).

Para efectos de sustentar la elección de estos marcos de trabajo se consideró:

1. Disponibilidad y accesibilidad a documentación y material bibliográfico.
2. Relación directa con la gestión de tecnología de información (operación de servicios/proyectos)
3. Apego a las actividades de entidades financieras
4. Enfoque dedicado a operación/servicios de TI

A continuación se detalla una tabla comparativa de dichos criterios:

Criterios de elección de Estándares y Marcos de Trabajo para Gestión de Riesgos

Criterios de elección	Risk IT	COSO ERM - Integrated Framework 2004	ISO/FDIS 31000:2009	AS/NZS 4360:2004	ARMS, 2002	ISO 20000:2005	PMBOK	ISO/IEC 27000X
Disponibilidad y accesibilidad a documentación y material bibliográfico	■					■	■	
Relación directa con la gestión de tecnología de información (operación de servicios/proyectos)	■					■	■	■
Apego a actividades de entidades financieras	■	■	■	■	■	■	■	■
Enfoque dedicado a servicios/operaciones de TI						■		
TOTAL	3	1	1	1	1	4	3	2

Leyenda:
Azul - El principio/característica se cubre
Blanco - El principio/característica no está cubierto

Figura 5 Criterios de elección de Marcos de Trabajo para este análisis

8.2.3.1. *Marco de Trabajo ISACA Risk IT*

El Marco de trabajo Risk IT, alineado con COBIT, está diseñado para ayudar a implementar gobierno de TI y mejorar la gestión de riesgos relacionados con

tecnología. Está compuesto por un conjunto de principios, dominios y procesos, como se muestra en la figura 6.

Figura 6 Fuente: ISACA, Risk IT Framework, USA, 2009

La utilización de este marco de trabajo, busca que las organizaciones puedan tomar decisiones apropiadas basadas en el conocimiento de sus riesgos. El marco de trabajo trata de atender muchos de los retos que las empresas enfrentan hoy en día, en necesidades como: (ISACA, 2013, p. 113).

- Una vista precisa de los riesgos significativos actuales y futuros, en el corto plazo, relacionados con TI a través de toda la organización y la efectividad con que la empresa los está atendiendo.
- Una guía de extremo a extremo en cómo administrar riesgos relacionados con TI, más allá de únicamente métricas de control técnicas y seguridad.

- Entendimiento de cómo capitalizar una inversión realizada en un sistema de control interno de TI para administrar los riesgos relacionados con tecnología.
- Entendimiento de cómo una gestión efectiva de riesgos de TI habilita la eficiencia en los procesos de negocio, mejora la calidad y reduce los costos y el desperdicio.
- Integrando las estructuras corporativas de riesgo y cumplimiento dentro de la organización cuando se valoran y gestionen los riesgos de TI.
- Un marco de trabajo común o lenguaje para facilitar la comunicación y entendimiento a través de la administración del negocio, TI, riesgo y auditoria.
- Promoción de la responsabilidad del riesgo y su aceptación a través de toda la organización.
- Un perfil completo de riesgos para un mejor entendimiento de la exposición total de la organización, para facilitar la mejor utilización de los recursos de la organización.

El marco de trabajo de Risk IT posiciona los riesgos de TI como un componente de todo el universo de riesgos de la organización. Existen tres dominios: (ISACA, 2013, p. 114)

1. Gobierno de Riesgos: El objetivo de este dominio es asegurarse que las prácticas de gestión de riesgo relacionadas con Tecnología de información estén implementadas en la organización, permitiendo asegurar un retorno óptimo ajustado a los riesgos. El mismo está conformado de tres procesos: Integración con el ERM (Enterprise Risk Management), Establecimiento y mantenimiento de una vista común de riesgos y Toma de decisiones de negocio consciente de los riesgos.
2. Evaluación de Riesgos: El objetivo de este dominio es asegurarse que las oportunidades y riesgos asociados a la TI sean identificados, analizados y presentados en términos de negocio. Este dominio está

compuesto de tres procesos: Análisis de riesgos, Recolección de datos y mantenimiento del perfil de riesgos.

3. Respuesta a Riesgos: El objetivo de este dominio es asegurarse que los problemas, oportunidades y eventos relacionados con riesgos de TI sean tratados de manera costo/efectiva y alineados con las prioridades del negocio. Este dominio está compuesto de tres procesos: Gestión de riesgos, articulación de riesgos y reacción a riesgos.

8.2.3.2. *Marco de Trabajo Gestión de riesgos PMBOK*

El PMBOK en su versión 5 incorpora un apartado relacionado con la gestión de riesgos de proyecto, la cual incorpora seis procesos diferentes:

1) Planificar la gestión de riesgos
2) Identificar Riesgos
3) Realizar análisis de riesgos cualitativos
4) Realizar análisis de riesgos cuantitativos
5) Planificar las respuestas a los riesgos
6) Controlar los Riesgos

Los proyectos comienzan con un alto grado de incertidumbre y riesgos que conforme avanza el proyecto tienden a disminuir, tal y como se observa en la siguiente figura 7 (PMI, 2013, p. 40).

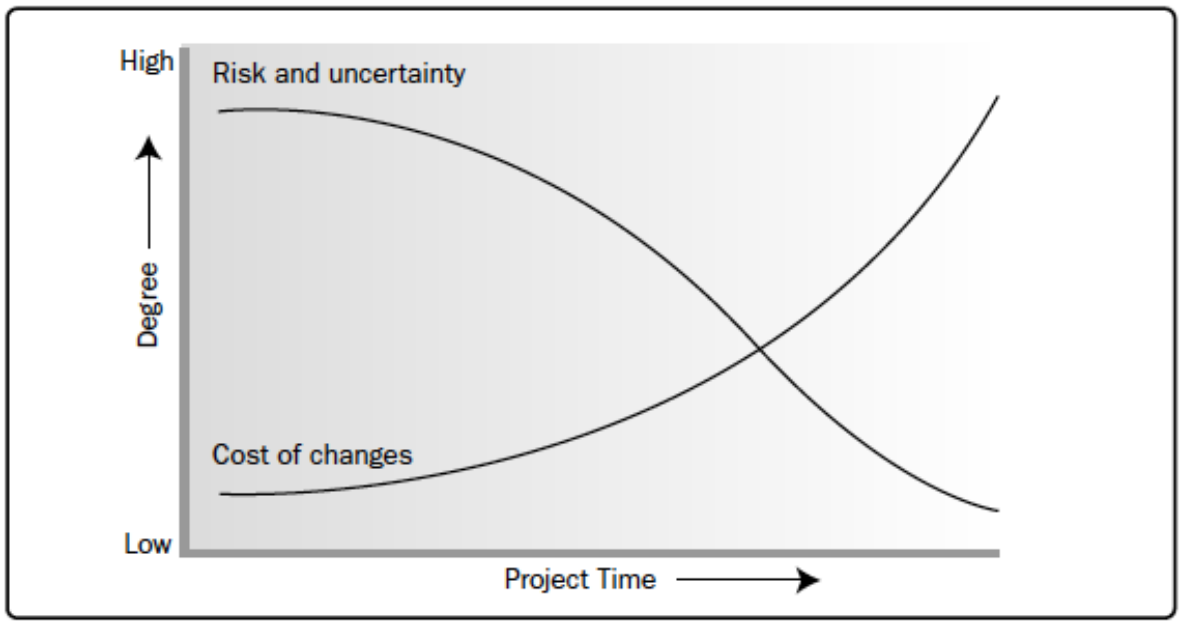


Figura 7 Fuente: PMBOK 5ta edición; Impacto de variables basado en el tiempo del proyecto

Una situación diferente encontramos en un servicio de tecnología de información, considerado operación en marcha, dado que nuevos riesgos pueden aparecer en el tiempo conforme los factores externos van cambiando y las amenazas externas evolucionan, como por ejemplo el software malicioso, la obsolescencia del hardware/software o la obsolescencia del conocimiento. Asimismo los riesgos aumentan su impacto y crecen de manera exponencial conforme pasa el tiempo, si los mismos permanecen sin gestionarse, como se observa en la figura 8. Siendo entonces que un riesgo que no causa hoy día alguna pérdida significativa, tampoco se espera que aumente significativamente en el tiempo (OGC, 2007).

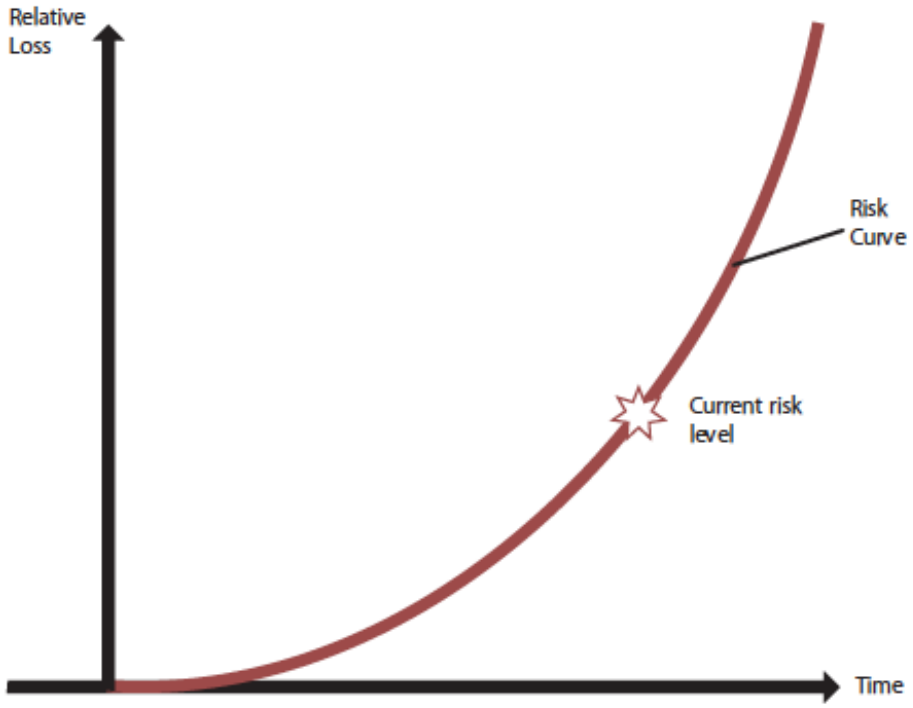


Figura 8 Fuente: Libro ITIL Service Transition; OGC

A pesar de que existen estas diferencias, como elementos comunes podemos encontrar que la materialización de los riesgos negativos se convierten en incidentes que impactan los objetivos, ya sea de un servicio de Tecnología de Información o de un proyecto (costo, tiempo, calidad, alcance, rendimiento) (PMI, 2013, p. 310).

El PMBOK realiza un aporte interesante al análisis de riesgos, separando el análisis en dos procesos diferentes: análisis cuantitativo y análisis cualitativo.

El análisis cualitativo de riesgos es el proceso de priorizar los riesgos para un análisis o acción posterior estimando y combinando su probabilidad de ocurrencia e impacto. El principal beneficio de este proceso es que permite a los responsables reducir el nivel de incertidumbre y enfocarse en los riesgos de mayor prioridad (PMI, 2013, p. 328).

El análisis cuantitativo de riesgos es el proceso de analizar numéricamente los efectos de los riesgos identificados en los objetivos generales de un proyecto/servicio. El principal beneficio de este proceso es que produce información cuantitativa para soportar la toma de decisiones para efectos de reducir la incertidumbre (PMI, 2013, p. 333).

Posteriormente estaremos considerando el análisis cuantitativo para efectos de poder considerar cuantificar monetariamente el impacto económico que una afectación de servicio puede generar de manera directa (costos tangibles) pero también indirecta (costos intangibles).

Como se demostró en la Figura 4, el proceso de gestión de riesgos PMBOK está centrado en un área específica de TI que es la gestión de proyectos, la cual no forma parte del alcance de la presente investigación. Adicionalmente las fases sugeridas guardan mucha similitud con los demás marcos de trabajo. Por ello consideraremos las herramientas y técnicas sugeridas para efectos de enriquecer la propuesta de solución que se estará sugiriendo.

8.2.3.3. *Gestión de riesgos marco de trabajo ITIL V3 (ISO/IEC 20000)*

Aunque si bien a través de los diferentes procesos de ITIL V3, se menciona la necesidad de evaluar y gestionar los riesgos, no existe un proceso formal dedicado a la gestión de riesgos dentro del compendio de mejores prácticas. ITIL llama a estas invocaciones “ejercicios coordinados de evaluación de riesgos” (IT Process Maps).

A nivel de la certificación en ITIL, también existen discrepancias respecto a cuáles son los procesos de ITIL que incorporan actividades de gestión de riesgos, lo cual ha ocasionado que se eviten preguntas asociadas a la gestión de riesgos (Odin, 2009).

Por esta razón, dentro de la fase “Diseño de Servicio” se sugiere implementar un proceso básico de gestión de Riesgos o bien incorporar un marco de trabajo más integral (Enterprise Risk Management). Los libros de ITIL recomiendan el marco de trabajo M_o_R. (OGC, 2007).

Considerando que la certificación ISO 20000 orientada a empresas está fundamentada sobre ITIL V3 con algunas diferencias en cuanto a su orientación, se concluyó que tampoco incorpora procesos detallados de gestión de riesgos al igual que ITIL V3 (Gaughan, 2010).

8.2.4. Análisis de frecuencia de los riesgos

La frecuencia de los riesgos está enmarcada dentro de una escala logarítmica que clasifica las veces que cada evento puede ocurrir en un período de un año.

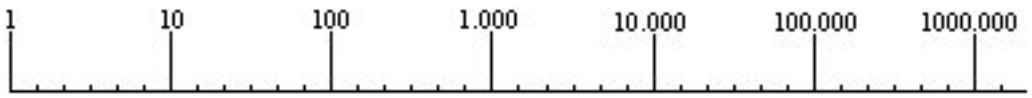


Figura 9 Escala logarítmica. Fuente: http://www.scribd.com/doc/145713459/Escala-logaritmica#scribd

La razón por la cual se considera dicha escala se debe a que típicamente los eventos de menor magnitud tienden a ocurrir con mayor frecuencia, a diferencia de los eventos de mayor impacto o impacto crítico, los cuales ocurren con una frecuencia mucho menor.

Se puede encontrar varias situaciones en la naturaleza que nos confirman este comportamiento como por ejemplo, la escala Richter utilizada para medir la intensidad de los eventos sísmicos o la unidad empleada en acústica llamada decibeles.

Ambas métricas utilizan escalas logarítmicas debido a que su impacto aumenta un 100% por cada unidad aritmética.

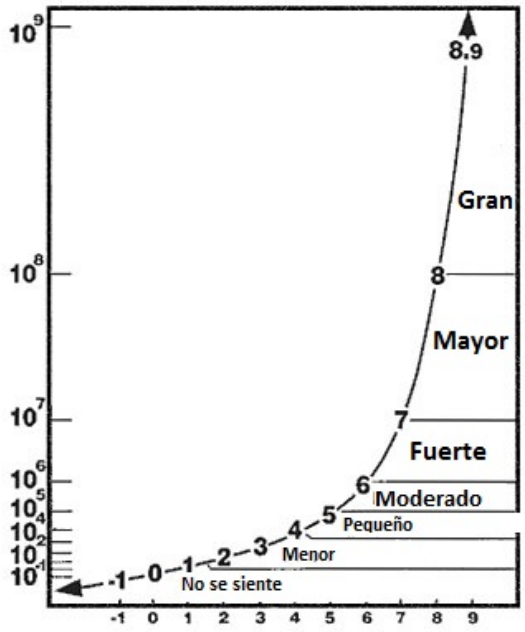


Figura 10 Escala Richter de un sismo. http://www.artinaid.com/2013/04/escala-richter-de-un-sismo/

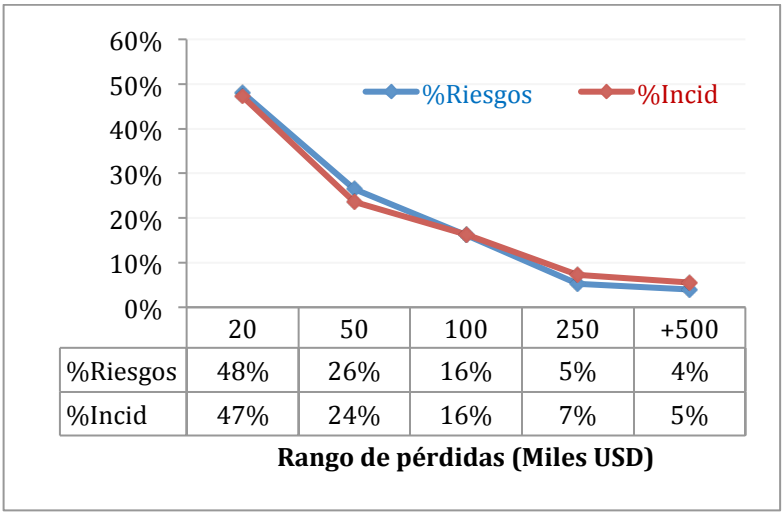
Presión acústica (µPa)	Nivel de presión acústica (dB)	Ambiente típico
200.000.000	140	Dolor
20.000.000	120	Avión al despegue
2.000.000	100	Martillo neumático
200.000	80	Tráfico intenso
20.000	60	Oficina
2.000	40	Biblioteca
200	20	Campiña
20	0	Umbral de audición

Figura 11 Comparación de escalas de presión acústica. http://hysiunidad4.weebly.com/contaminacioacuten-por-ruido.html

Adicionalmente, dentro de la institución se han realizado estudios, donde el área encargada de riesgos operativos ha logrado demostrar que se puede establecer una correlación entre la cantidad y magnitud de incidentes registrados comparado con la cantidad y criticidad de los riesgos identificados.

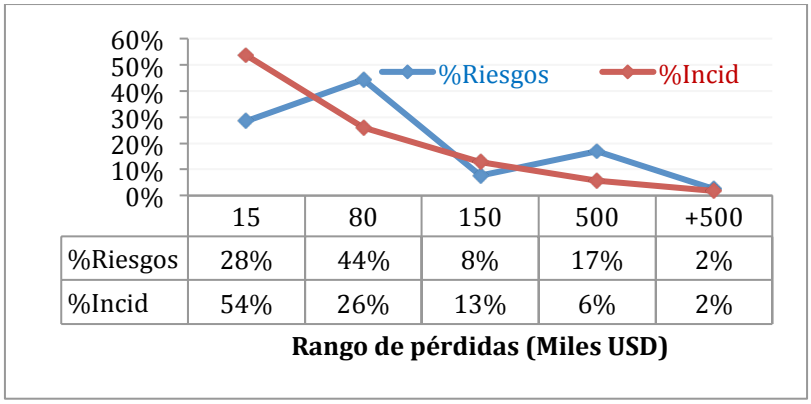
A continuación se incluyen algunos ejemplos de países como Panamá, Costa Rica, El Salvador y Guatemala donde se realizó la correlación entre ambas variables. La escala en el eje “x” expresa los rangos de pérdidas en miles de

dólares a la que expone el riesgo o bien el incidente. En el eje “y” se detalla el porcentaje de riesgos o incidentes que se agrupan bajo cada uno de los rangos.



	20	50	100	250	+500
%Riesgos	48%	26%	16%	5%	4%
%Incid	47%	24%	16%	7%	5%

Figura 12 Correlación Riesgos/Incidentes Panamá



	15	80	150	500	+500
%Riesgos	28%	44%	8%	17%	2%
%Incid	54%	26%	13%	6%	2%

Figura 13 Correlación Riesgos/Incidentes Costa Rica

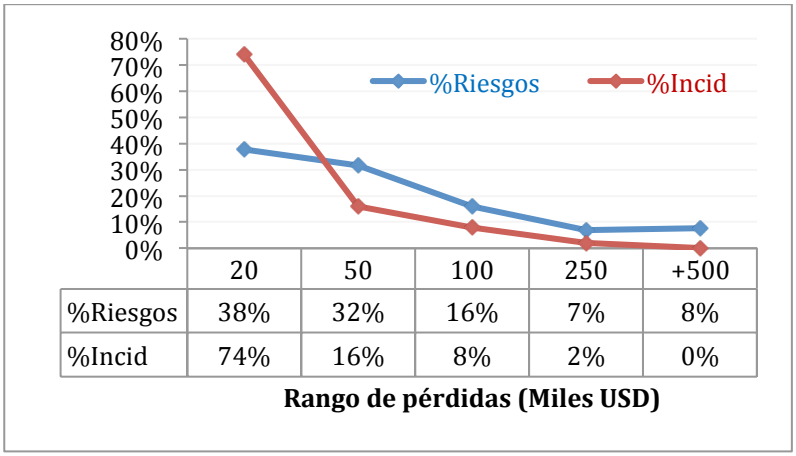


Figura 14 Correlación Riesgos/Incidentes El Salvador

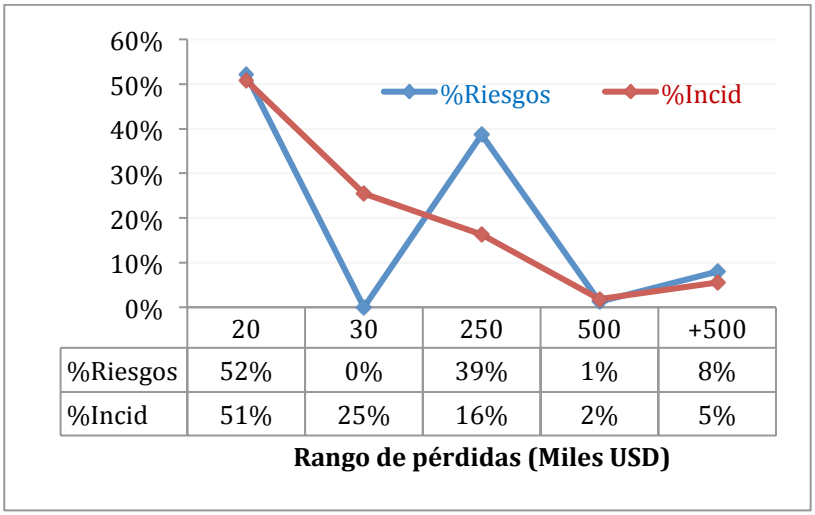


Figura 15 Correlación Riesgos/Incidentes Guatemala

A partir del análisis anterior, se consideró viable e interesante proponer un indicador basado en el índice de correlación de Pearson. Esta es una medida que permite establecer la relación lineal entre dos variables aleatorias cuantitativas, para las cuales es indiferente la escala de medidas de ambas variables. En otras palabras, el coeficiente de correlación de Pearson es como un índice que puede utilizarse para medir el grado de relación de dos variables siempre y cuando sean cuantitativas. (Universidad de Sevilla, p. 2)

El coeficiente es un número que varía entre los límites de +1 y -1. Su magnitud indica el grado de relación existente entre las dos variables y en qué medida se

relacionan. El valor de cero indica que no existe relación entre las variables; el valor 1 indica que hay una correlación perfecta positiva (al crecer “x”, crece “y” ó al decrecer “x”, decrece “y”); el valor -1 implica que hay una correlación perfecta negativa (al crecer “x”, decrece “y” ó al decrecer “x”, crece “y”). (Monografías)

Un valor negativo implica que las variables actúan inversamente proporcionales.

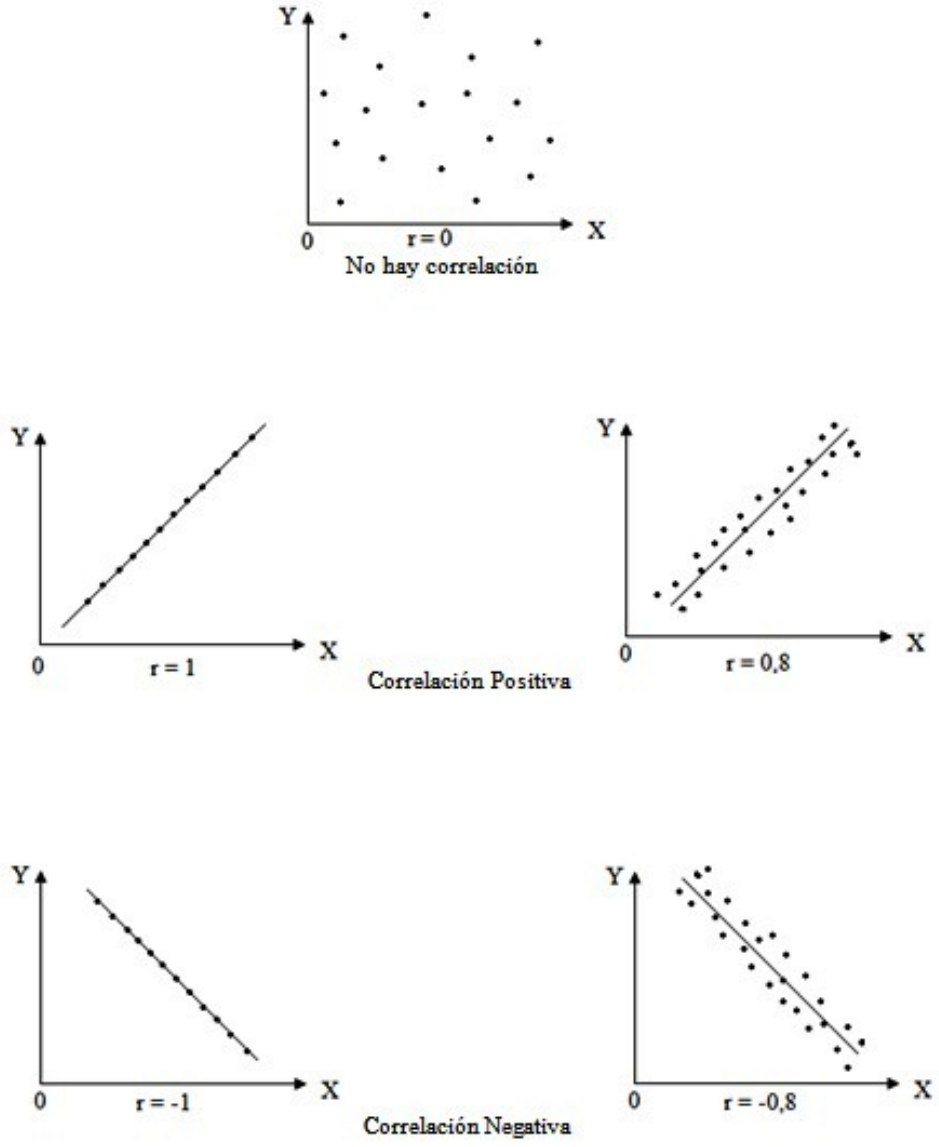


Figura 16 Ejemplos de índices de correlación de Pearson Fuente: http://www.monografias.com/trabajos85/coeficiente-correlacion-karl-pearson/coeficiente-correlacion-karl-pearson.shtml

Valor	Significado
-1	Correlación negativa grande y perfecta
-0,9 a -0,99	Correlación negativa muy alta
-0,7 a -0,89	Correlación negativa alta
-0,4 a -0,69	Correlación negativa moderada
-0,2 a -0,39	Correlación negativa baja
-0,01 a -0,19	Correlación negativa muy baja
0	Correlación nula
0,01 a 0,19	Correlación positiva muy baja
0,2 a 0,39	Correlación positiva baja
0,4 a 0,69	Correlación positiva moderada
0,7 a 0,89	Correlación positiva alta
0,9 a 0,99	Correlación positiva muy alta
1	Correlación positiva grande y perfecta

Tabla 1 Escala de interpretación del índice de correlación de Pearson Fuente: http://www.monografias.com/trabajos85/coeficiente-correlacion-karl-pearson/coeficiente-correlacion-karl-pearson.shtml

Aplicando el coeficiente de correlación de Pearson a los ejemplos brindados anteriormente se obtienen los siguientes resultados.

Figura y País	Índice de Correlación de Pearson
Figura 12 - Panamá	0.9965
Figura 13 - Costa Rica	0.6240
Figura 14 - El Salvador	0.8340
Figura 15 - Guatemala	0.7104

Tabla 2 Cálculo índice correlación Riesgos vs Incidentes. Fuente Propia

8.2.5. Análisis de costos de riesgos

A partir de este apartado introducimos la importancia del análisis de costo en la evaluación de los riesgos debido a que es un elemento clave para efectos de poder focalizar los esfuerzos de la organización en atención de los riesgos más relevantes.

Independientemente de la metodología o marco de trabajo que se utilice, uno de los aspectos más importantes que toda gestión de riesgos debe incorporar es un mecanismo para poder priorizar la atención de los riesgos identificados y analizados, que además superen el apetito de riesgo de la organización. Es necesario contar con un esquema de priorización para la atención de los riesgos debido a que los recursos de toda organización son limitados y sería optimista pretender que se contará con todo el tiempo, el dinero o el personal necesario para resolver o mitigar todos los riesgos identificados.

Existen múltiples variables que se pueden considerar para efectos de priorizar los riesgos, por ejemplo (ISACA, 2009, p. 38):

1. Frecuencia o probabilidad de ocurrencia del riesgo
2. Impacto en la ventaja competitiva (porcentaje de participación de mercado)
3. Productividad - Pérdida de ingresos (porcentaje de ingresos expuestos)
4. Respuesta - Costo de la respuesta
5. Reputación - Satisfacción del cliente (encuesta de satisfacción anual)
6. Reputación - Percepción externa (cobertura negativa en medios de comunicación masivos como prensa, televisión, revistas, redes sociales, etc.)
7. Legal - Incumplimiento regulatorio o no cumplimiento (Prisión, condena personal, pérdidas financieras, revocación de licencias para operar, multas)

Algunas de las variables mencionadas anteriormente tienen un impacto tangible en términos económicos (Costo de Respuesta, Pérdida de Ingresos, etc.). Otros son variables no aparecen cuantificadas en términos monetarios (e.g. Satisfacción del cliente, percepción externa, etc.).

El impacto de un riesgo materializado sobre un servicio de tecnología de información se puede cuantificar analizando los costos tangibles y los costos intangibles.

8.2.5.1. *Costos tangibles*

“Los costos tangibles o costos explícitos son aquellos que se pueden calcular con criterios convencionales de costos, normalmente siguiendo principios de contabilidad generalmente aceptados” (Oficina de Calidad de los Servicios Secretaria General de la Gobernación de Salta, p. 24).

Por lo general estos costos consideran, básicamente costos de personal, materias primas y materiales. Sin embargo, tratándose de un servicio de TI de una entidad financiera debemos considerar que este impacto se traduce a un costo de oportunidad por transacción no efectuada.

Esto significa que el impacto monetario tangible de las transacciones no realizadas durante un período de no disponibilidad de un sistema se puede calcular fácilmente a partir del costo unitario de cada transacción.

Es importante diferenciar entre transacciones monetarias (e.g. pagos de servicios, transferencias) y no monetarias (e.g. estados de cuenta, consultas de saldo) al momento de calcular el costo por transacción. Esto se debe a que las transacciones monetarias generan mayor rentabilidad para las instituciones financieras por las cuotas que cobran por este tipo de servicios (e.g. transferencias de fondos).

8.2.5.2. *Costos intangibles*

“Los costos intangibles, también denominados costos implícitos, son aquellos que se calculan con criterios subjetivos y que no son registrados como costos en los sistemas de contabilidad. La mayoría de los costos intangibles se sitúan en la categoría de costos de fallos externos, como por ejemplo la pérdida de imagen de la organización. No obstante también pueden aparecer cuando la Organización incurre en fallos internos, como por ejemplo la desmotivación de su personal, los conflictos, etc.” (Oficina de Calidad de los Servicios Secretaria General de la Gobernación de Salta, p. 25).

En términos cuantitativos, la importancia relativa de los costos intangibles es mayor que la de los costos tangibles. Esto fundamentado en estudios estadísticos que han logrado demostrar que: (Oficina de Calidad de los Servicios Secretaria General de la Gobernación de Salta, p. 26)

1. Por cada $1 que se invierte en evaluación, la Organización logra disminuir en $9 los fallos externos.
2. Por cada $1 que se invierte en prevención, la Organización logra disminuir en $15 las pérdidas por fallos Internos.

Con base a lo anterior, se considera que el análisis de costos intangibles y su traducción a términos monetarios son altamente recomendables cuando se evalúan los riesgos para efectos de priorizar su atención.

CAPITULO III – Marco Metodológico

El propósito del presente capítulo consiste en detallar el procedimiento empleado para elaborar el marco teórico y el análisis de la situación actual. Ambos componentes son claves de esta investigación y apoyarán las propuestas de solución a plantear durante el avance del proyecto.

9.1. Enfoque de la investigación

Se empleará adicionalmente un enfoque cuantitativo el cual se apoya en la recolección de datos para sintetizarlos, con base a la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías. (Hernández, 2006)

Para objeto de esta investigación, no se planteará una hipótesis, pero nos apoyaremos en un conjunto de herramientas propias del paradigma cuantitativo.

Considerando este enfoque, se realizará la recolección de datos mediante el uso de encuestas y entrevistas. La información capturada con los anteriores instrumentos serán analizados estadísticamente para lograr concluir de forma cuantitativa la situación actual de la gestión de riesgos.

9.2. Tipo de investigación

La investigación a realizar se desarrollará bajo el enfoque no experimental, lo cual significa que las variables independientes no se manipulan porque ya han sucedido. Las inferencias sobre las relaciones entre variables se realizan sin intervención y se observan tal y como se han dado en su contexto natural.

9.3. Sujetos y fuentes de información

9.3.1. Sujetos

El objetivo de esta investigación es analizar la metodología de gestión de riesgos actualmente empleada por la organización objeto de la investigación, para plantear mejoras relacionadas con la focalización de los esfuerzos de mitigación en los riesgos que representen el mayor impacto negativo en términos económicos y de imagen para la organización.

Los sujetos a considerar dentro de este estudio corresponden al personal de la Gerencia Regional de Riesgos y Seguridad de Información responsables de controlar y dirigir la ejecución de los procesos relacionados con la gestión de riesgos tecnológicos y operativos. En total, son cuatro personas distribuidas de la siguiente manera:

Puesto	Colaboradores
Gerente Regional de Riesgos y Seguridad de Información	1
Supervisor Regional de Riesgos	1
Gestor Regional de Riesgos	2

Tabla 3 Personal responsable de la metodología de gestión de riesgos. Fuente Propia

Adicionalmente se considerará a los clientes de la metodología que la ejecutan en las diferentes Gerencias de la Dirección Regional de Informática, bajo la dirección de los Gestores Regionales de Riesgos. A estos clientes se les conoce internamente como líderes de riesgo y han sido involucrados por los respectivos Gerentes de área con el objetivo de que participen en las reuniones de seguimiento de riesgos y coordinen las actividades relacionadas con el proceso a lo interno de cada gerencia.

Al momento de desarrollar esta investigación se identificaron a 12 colaboradores que están plenamente involucrados y capacitados para desempeñarse como líderes de riesgo. A continuación se detalla la composición del personal según puesto desempeñado:

Puesto	Colaboradores
Jefes de departamento	7
Ingenieros de Procesos	2
Oficial Cumplimiento	1
Supervisor	1
Gestor administrativo	1

Tabla 4 Personal ejecutor de la metodología de riesgos. Fuente Propia

9.3.2. Fuentes de Información

La información utilizada para esta investigación proviene de diferentes fuentes, por lo tanto utilizaremos la técnica de recolección de datos mixta. Realizando un estudio de fuentes documentales como normativas, lineamientos, procesos, metodologías, estándares, libros y documentos pero también recolectando información con un trabajo de campo. Para la recolección de los datos se aplicará una encuesta al personal involucrado en la gestión de riesgos y entrevistas con el personal clave que tiene la visión integral y ejecutiva de la metodología, además que conocen las oportunidades de mejora que observan en dichos procesos y su ejecución.

Las fuentes primarias son documentos que presentan resultados de estudios y análisis, tales como: Documentos originales, minutas, entrevistas, investigaciones, conferencias, seminarios y discursos.

Las fuentes secundarias son textos basados en hechos reales, analiza e interpreta las fuentes primarias como por ejemplo: Libros de texto, artículos de revistas, crítica literaria y comentarios.

A continuación se listan las fuentes de información clasificadas según las definiciones anteriores:

Tipo Fuente de información	Título	Autor
Primaria	*CGEIT Review Manual 2013 (Certified in the Governance of Enterprise IT).*	ISACA. (2013).
Primaria	*History of ISACA*. Retrieved 03 de 2014 from http://www.isaca.org: http://www.isaca.org/about-isaca/history/pages/default.aspx	ISACA. (03 de 2014).
Primaria	*COBIT 5 Introducción.* Retrieved 03 de 2014 from http://www.isaca.org: http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt	ISACA. (n.d.).

Primaria	*Certified in Risk and Information Systems Control (CRISC) Fact Sheet*. Retrieved 03 de 2014 from Sitio Web de ISACA.ORG: http://www.isaca.org/About-ISACA/Press-room/Pages/CRISC-Fact-Sheet.aspx	ISACA. (n.d.).
Primaria	*Certified in the Governance of Enterprise IT (CGEIT) Fact Sheet*. Retrieved 03 de 2014 from Sitio de ISACA.ORG: http://www.isaca.org/About-ISACA/Press-room/Pages/CGEIT-Fact-Sheet.aspx	ISACA. (n.d.).
Primaria	*Libro ITIL V3 Service Design.* Londres, Reino Unido: TSO.	OGC. (2007).
Primaria	*Libro ITIL V3 Service Transition.* Londres, Reino Unido: TSO.	OGC. (2007).
Primaria	*Which ITIL processes include risk analysis and management activities?* . Retrieved 03 de 2014 from IT Service Management Oasis: http://askme4itsm.blogspot.com/2009/10/which-itil-processes-include-risk.html	Odin. (12 de 12 de 2009).
Primaria	*ITIL Gestion del Riesgo.* Retrieved 03 de 2014 from IT Process Maps: http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_del_Riesgo	IT Process Maps. (n.d.).
Secundaria	*Comparing ISO/IEC 20000 Part 1 Requirements to ITIL V3 Processes and Functions.* Retrieved 03 de 2014 from PA&E Global: http://www.paeglobal.com/library/Comparison_of_ISO_20K_to_ITIL_V3.pdf	Gaughan, T. (2010).
Primaria	*METODOLOGÍA DELA INVESTIGACIÓN.* Mexico, Mexico: MCGRAW-HILL.	Sampieri, R. H. (1997).
Primaria	*Metodología de la investigación.* México: McGraw - Hill.	Hernández, S. R. (2006).
Primaria	*The Risk IT Practitioner Guide.* Rolling Meadows, Illinois, EEUU.	ISACA. (2009).
Secundaria	*Operational Risk in the Basil II framework.* From http://www.bis.org: http://www.bis.org/publ/bcbsca07.pdf	Basel Committee on Banking Supervision. (01 de 2001).
Secundaria	*ISO 31000:2009—Setting a New Standard for Risk Management.* Retrieved 03 de 2014 from http://www.broadleaf.com.au/: http://www.broadleaf.com.au/pdfs/articles/art_riskanalysis_iso31000.pdf	Purdy, G. (2010).
Secundaria	*What is COBIT - Overview*. Retrieved 03 de 2014 from Sitio Web de itil.org: http://www.itil.org/en/vomkennen/cobit/ueberblick/index	ITIL ORG. (n.d.).

	.php	
Secundaria	*A Guide to the Project Management Body of Knowledge (PMBOK Guide 5th edition).* Pennsylvania, EEUU: PMI Publications.	PMI. (2013).
Secundaria	From http://en.wikibooks.org/wiki/ITIL_v3_%28Information_Technology_Infrastructure_Library%29/Service_Design	WikiBooks. (n.d.).
Secundaria	*Algunas nociones sobre los costos de la No Calidad.* Retrieved 03 de 2014 from Gobierno de la Provincia de Salta: http://www.salta.gov.ar/descargas/archivos/ocspdfs/ocs_algunas_nociones_sobre_los_costos_de_la_no_calidad.pdf	Oficina de Calidad de los Servicios Secretaria General de la Gobernación de Salta. (n.d.).

Tabla 5 Fuentes de información utilizadas en la investigación. Fuente Propia.

9.4. Población y muestra

Con base a lo indicado en el apartado 3.3.1 Sujetos, la población de este estudio estará enfocado en el personal de la Dirección Regional de Informática que tiene relación directa con la metodología de gestión de riesgos. Se justifica esta elección considerando que son el personal que tiene el conocimiento general de los procesos e involucramiento directo en su ejecución, por otro lado son las personas que tienen relación con los riesgos tecnológicos y operativos de la tecnología de información, lo cual es congruente con el alcance que tiene la presente investigación.

Considerando que una población es el conjunto de todos los casos que cumplen con una especificación (Hernández, 2006), bajo esa definición las 16 personas mencionadas en el apartado 3.3.1 son las que se tomarán en cuenta como población para esta investigación.

La muestra es un subconjunto de un grupo o individuos y se obtienen con la finalidad de inferir características de la totalidad de la población.

Considerando que el tamaño de la población es pequeño, para efectos de recolectar los datos, se analizará la información tomando de la población indicada anteriormente dos muestras distintas.

El objetivo de contar con dos muestras diferentes es el de poder comparar las percepciones de quienes controlan y dirigen el proceso y las personas que lo están ejecutando. A partir de las similitudes o diferencias que se encuentren, se estarán definiendo las acciones o recomendaciones a seguir.

Las muestras que se utilizarán son del tipo no probabilística, la cual es una técnica donde las muestras se recogen en un proceso que no brinda a todos los individuos de la probación iguales oportunidades de ser seleccionados. Con esto, buscamos seleccionar a individuos que tienen un conocimiento profundo del tema bajo estudio y consideramos que la información aportada por esas personas es vital para la toma de decisiones.

9.4.1. Personal responsable de los procesos de gestión de riesgos

Se considerará de manera de manera separada al personal que controla y dirige la ejecución de los procesos de gestión de riesgos. La muestra está conformada por las 4 personas que laboran directamente para la Gerencia Regional de Seguridad y Riesgo que están a cargo de la gestión de riesgos.

9.4.2. Personal ejecutor de la metodología de gestión de riesgos

Se considerará de manera de manera separada al personal que ejecuta e implementa la ejecución de los procesos de gestión de riesgos. Bajo esa definición, se considerarán al menos 8 de las 12 personas mencionadas en el apartado 3.3.1 que cumplen con este criterio. Esto con el fin de lograr al menos un 66% de representación.

9.5. Definición de variables

Una variable estadística es cada una de las características o cualidades que poseen los individuos de una población y que estamos interesados en analizar.

Según la influencia que asignemos a unas variables sobre las otras, podemos clasificar dos tipos, independientes o dependientes. Las variables independientes son aquellas que se conocen al inicio del proceso y cuyo valor no depende de otra

variable y las variables dependientes son las que se crean como resultado del estudio y pueden estar influidas por los valores de las variables independientes.

Para efectos de esta investigación lo que buscamos es encontrar las relaciones causales entre actividades de la gestión de riesgos y sus impactos en una serie de variables dependientes.

A continuación se listan las variables a analizar dentro de esta investigación:

Nombre	Definición
Conocimiento de opciones de marcos de trabajo de riesgos de TI	Medir el nivel de conocimiento de la organización sobre los marcos de trabajo correspondientes a la gestión de riesgos de TI. Se evaluará el nivel de conocimiento del personal involucrado al seleccionar opciones validas o inválidas de múltiples marcos de trabajo y estándares existentes.
Uso de los marcos de trabajo utilizados en la gestión de riesgo para la implementación de procesos.	Conocer cuáles son los marcos de trabajo más utilizados en los procesos claves y la gestión de riesgos. Siendo los siguientes conceptos mencionados: COBIT ITIL CISA Basilea II PMBOK ISACA CGEIT CRISC Risk IT COSO ERM ISO 31000:2009 M_o_R OCTAVE CMMi ISO/IEC 27000 ISO 20000
Fortalezas de la gestión de riesgos existente en la	Identificar las 2 principales fortalezas de la gestión de riesgos de la organización.

organizacional	
Oportunidades de mejora de la gestión de riesgos existente en la organización.	Identificar las 2 principales debilidades de la gestión de riesgos de la organización.
Características documentadas cuando se identifican los riesgos asociados a servicios de TI.	Medir la frecuencia con que se capturan algunas características cuando se identifican riesgos asociados a servicios de TI. Las características principales comprenden: ✓ Impacto medido en costos intangibles (pe pérdidas por mala reputación e imagen) ✓ Volumen transaccional ✓ Impacto en imagen (no cuantificado monetariamente) ✓ Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas) ✓ Criticidad del componente involucrado ✓ Probabilidad de ocurrencia ✓ Impacto regulatorio ✓ Severidad ✓ Vulnerabilidad ✓ Criticidad del servicio del servicio involucrado ✓ Frecuencia con que ocurre ✓ Apetito de Riesgo
Nivel de eficiencia, efectividad y/o agilidad de algunas variables asociadas	Conocer y medir la percepción del nivel de eficiencia, efectividad y/o agilidad de las siguientes variables para la gestión de riesgos:

a la gestión de riesgos de la organización	✓ Herramientas ✓ Mecanismos para aumentar el compromiso del personal. ✓ Indicadores claves de gestión. ✓ Procesos de la gestión de riesgos. ✓ Conocimiento y experiencia del personal participante del proceso. ✓ Patrocinio de los gerentes y directores.
Características utilizadas para priorizar la atención de los riesgos identificados.	Medir la frecuencia con que se utilizan ciertas características (monetarias e intangibles) para priorizar la atención de los riesgos identificados. Las principales características: ✓ Impacto en imagen (no cuantificado monetariamente) ✓ Volumen transaccional ✓ Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas) ✓ Impacto medido en costos intangibles (pe pérdidas por mala reputación e imagen) ✓ Probabilidad de ocurrencia ✓ Frecuencia con que ocurre ✓ Vulnerabilidad ✓ Criticidad del componente involucrado ✓ Severidad ✓ Apetito de Riesgo ✓ Criticidad del servicio del servicio involucrado ✓ Impacto regulatorio
Variables intangibles cuantificadas en	Identificar las variables cuantificadas en términos económicos que se documentan cuando se identifican

términos económicos que se documentan cuando se identifican riesgos.	riesgos que puedan afectar la disponibilidad de un servicio. Principales Variables: ✓ Incumplimiento regulatorio o legal (Prisión, pérdidas financieras, revocación de licencias para operar, multas, etc.) ✓ Impacto en Satisfacción del cliente ✓ Impacto en percepción externa (cobertura negativa en medios de comunicación masivos como prensa, televisión, revistas, redes sociales, etc.) ✓ Impacto en Productividad ✓ Costo de la respuesta al riesgo (Planes) ✓ Impacto en ventaja competitiva ✓ Impacto en participación de mercado
Elementos que se cuantifican y documentan cuando se definen planes de mitigación de riesgos.	Identificar principales elementos que se cuantifican, documentan y consideran al momento de definir planes de mitigación de riesgos. Los principales elementos: ✓ Costo de la respuesta/plan definido para atender el riesgo (Evitar/Mitigar/Transferir) ✓ Ahorros tangibles por evitar un riesgo ✓ Ahorros intangibles (imagen, reputación, etc.) por reducción/mitigación del impacto del riesgo con los planes indicados ✓ Ahorros intangibles (imagen, reputación, etc.) por evitar un riesgo

	✓ Ahorros tangibles por reducción/mitigación del impacto del riesgo con los planes indicados

Tabla 6 Lista de variables a analizar. Fuente Propia.

9.6. Descripción de instrumentos utilizados

En este apartado se describen y presentan los diferentes instrumentos empleados para la recolección de datos, de forma tal que nos permitan contar con una base de información para el análisis cuantitativo a realizar posteriormente.

9.6.1. Entrevistas

Para recolectar información relevante sobre la situación actual de la gestión de riesgos en la organización se realizarán entrevistas a los mandos medios propietarios de estos procesos.

Se considera únicamente a los mandos medios del área de Riesgo para el instrumento de entrevista debido a que son quienes tienen una visión más integral y ejecutiva del proceso, así como el conocimiento formal sobre el tema de estudio. Adicionalmente el resultado de esta investigación será de interés principalmente de este personal.

El formato de las entrevistas realizadas considera la recolección de información en los siguientes temas:

Tema	Resultado esperado
Visión del Participante	Entender situación actual desde las perspectiva del entrevistado
Áreas de enfoque para el trabajo a realizar	Entender Preocupaciones, necesidades, debilidades y recomendaciones que el participante aporta
Organización actual	Obtener descripción del personal involucrado, roles y responsabilidades

	de los involucrados
Mejoras en proceso	Entender las mejoras que se están llevando a cabo actualmente para tomarlas en consideración en esta investigación.
Métricas del proceso	Entender los Indicadores Claves del Proceso, y contribución a la mejora continua a la gestión de riesgos actual.
Incentivos que contribuyan a la gestión de riesgos.	Conocer los incentivos que tiene la organización para aumentar la cultura de Gestión de Riesgos.

Tabla 7 Formato de entrevistas. Fuente Propia.

9.6.2. Encuesta

Para la recolección de los datos asociados a las variables de interés para este estudio, en la muestra establecida, se utilizó el formulario de encuesta que se encuentra en el anexo 2 de este documento.

9.6.3. Análisis de contenido

Para efectos de analizar la situación actual se considerará dentro del análisis principalmente la documentación de los procesos y formularios oficiales publicados actualmente por la organización en el sistema de documentación que soporta la certificación de ISO 9000.

La documentación relevante a esta investigación considera la siguiente documentación:

1. Lineamiento de Gestión de Riesgos Operativos
2. Proceso “Evaluar y administrar los Riesgos (PO9)
3. Proceso “Evaluación y gestión de Riesgos Tecnológicos (PO9)”

CAPITULO IV – Diagnóstico y análisis de resultados

En este capítulo resumiremos el estado actual de los métodos y herramientas implementados por la organización para la gestión de riesgos y la retroalimentación que el personal involucrado directamente en su implementación brinda acerca sobre su efectividad a través de los instrumentos planteados en el marco metodológico.

10.1. Metodología actual

10.1.1. Ciclo de Gestión de Riesgos Operativos

A nivel general, la metodología utilizada por la organización actualmente se resume en el siguiente el siguiente ciclo.

Figura 17 Ciclo de Gestión de Riesgos Operativos. Fuente: Metodología Riesgos Operativos BAC

En el ciclo de gestión de riesgos operativos se identifican seis etapas diferentes:

1. Identificación, evaluación y monitoreo de riesgos
2. Mitigación de Riesgos Principales
3. Evaluación de Controles
4. Medición de Riesgos & Reporte de Incidentes
5. Gestión de Ambiente de Control
6. Generación de reportes

Cada etapa propone a los usuarios un método para efectos de poder desarrollar las diferentes actividades de manera tal que les permita cumplir con los objetivos de dicha etapa.

Para efectos de esta investigación, mantendremos el enfoque en las dos primeras etapas. A continuación se enumeran los diferentes métodos propuestos para las dos etapas de interés:

10.1.1.1. *Método Identificación y Evaluación de Riesgos*

Para cumplir con la identificación de riesgos, el ciclo propone las siguientes actividades:

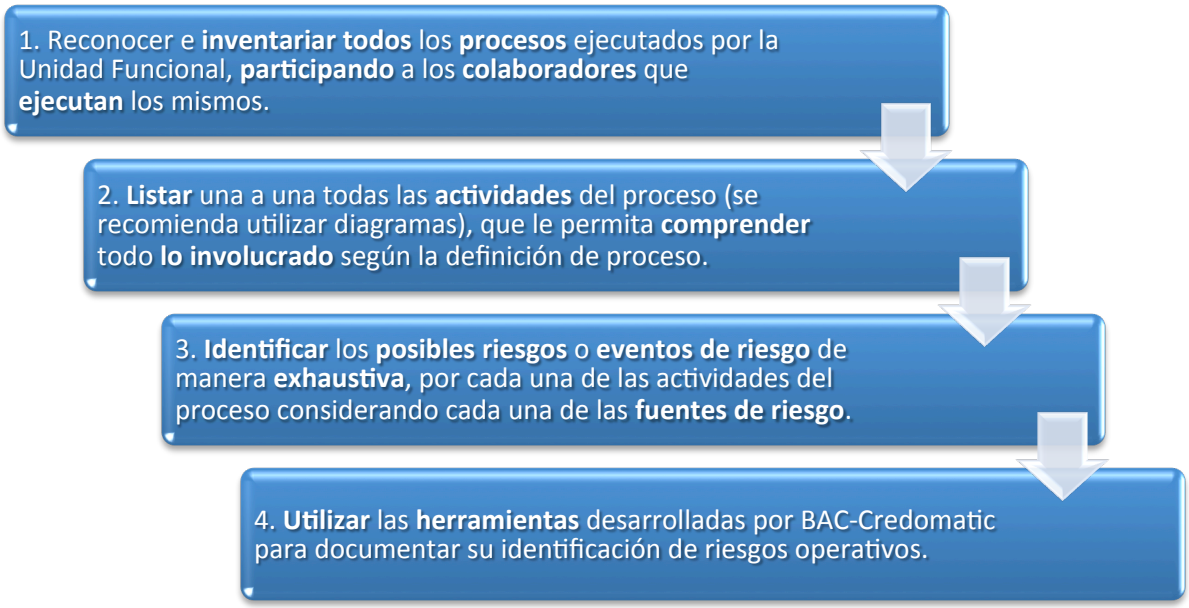


Figura 18 Identificación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

Para cumplir con la evaluación de riesgos, el ciclo propone las siguientes actividades:

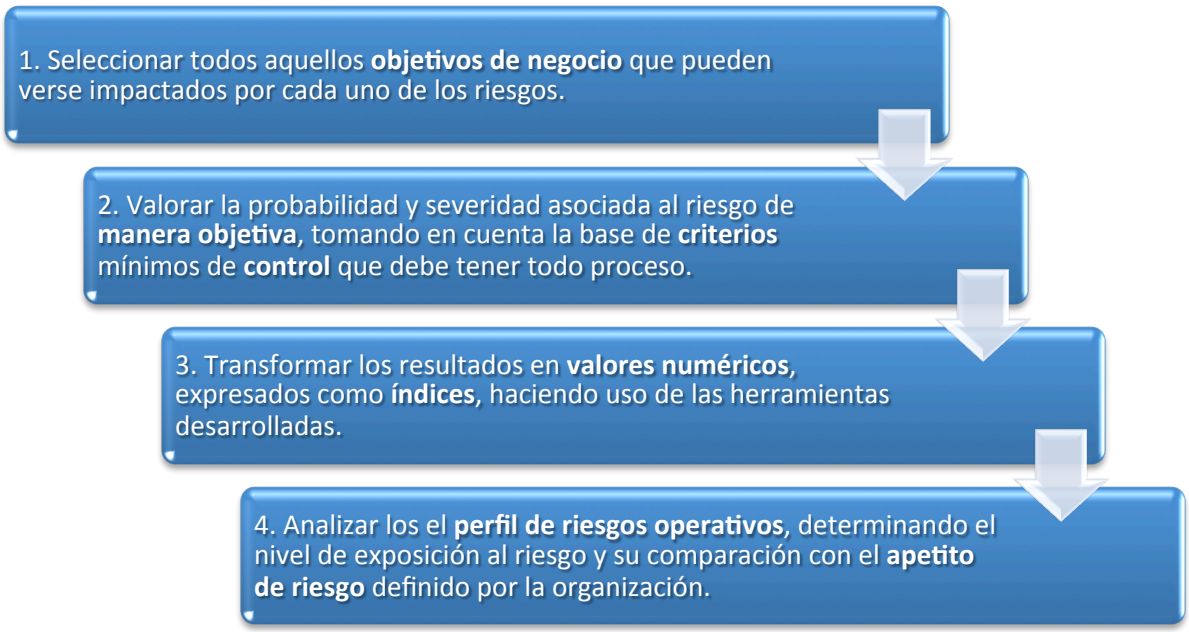


Figura 19 Evaluación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

Estos pasos se deben de ejecutar siempre con **visión de proceso** y se recomienda al usuario "tomar en cuenta criterios de priorización cuando aplique".

10.1.1.1.1. Objetivo:

En este enfoque se deben gestionar los modos de fallos a partir de las actividades ejecutadas en los procesos de TI y Negocio. Incluye riesgos operativos derivados de riesgos tecnológicos. Estos eventos se identifican a partir de: procesos, gente, infraestructura y tecnologías de información.

10.1.1.1.2. Insumos:

- ✓ Expertos del Servicio
- ✓ Mapeo de componentes COBIT
- ✓ Incidencias
- ✓ Formulario de identificación y evaluación

10.1.1.1.3. Ejemplo herramienta a documentar:

Identificación de riesgos:

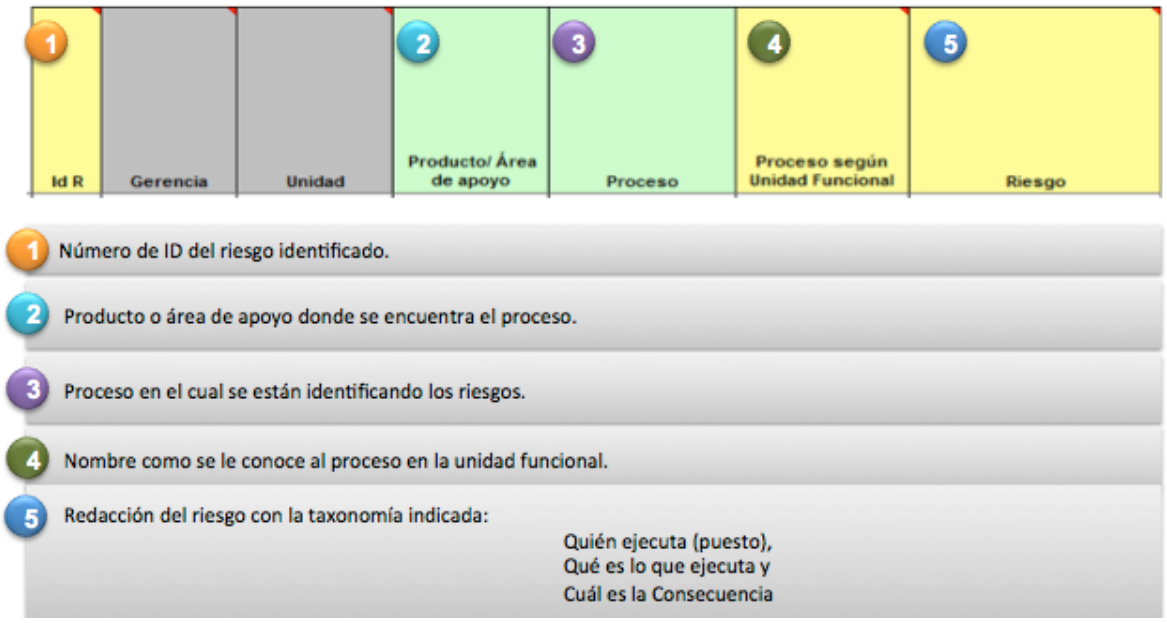


Figura 20 Herramienta identificación de riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

Evaluación de riesgos:

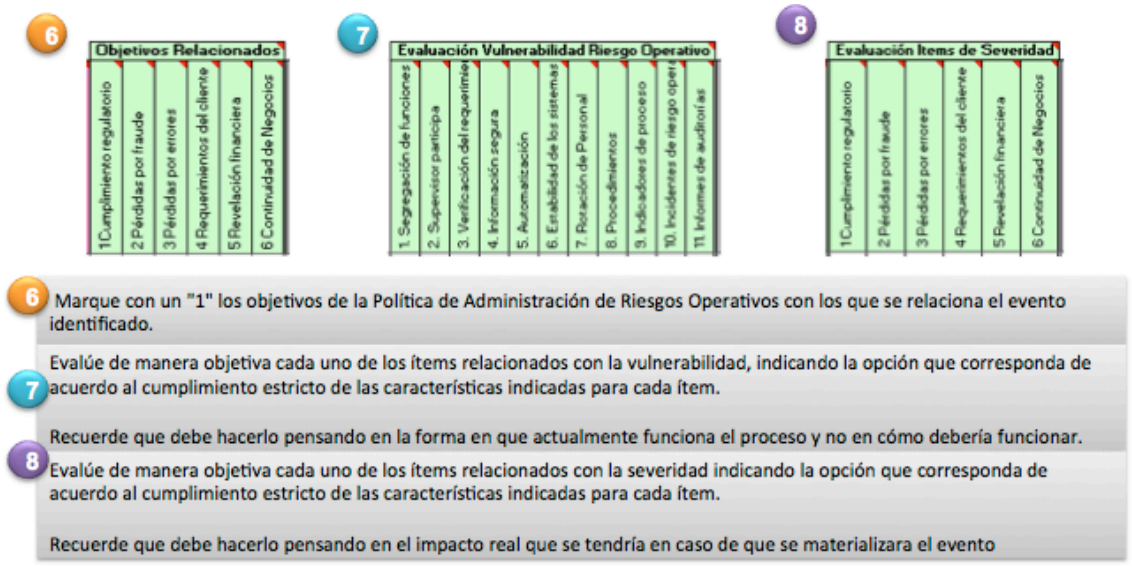


Figura 21 Herramienta evaluación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

10.1.1.2. *Método Mitigación de Riesgos*

Para cumplir con la etapa de Mitigación de riesgos, el ciclo propone las siguientes actividades:

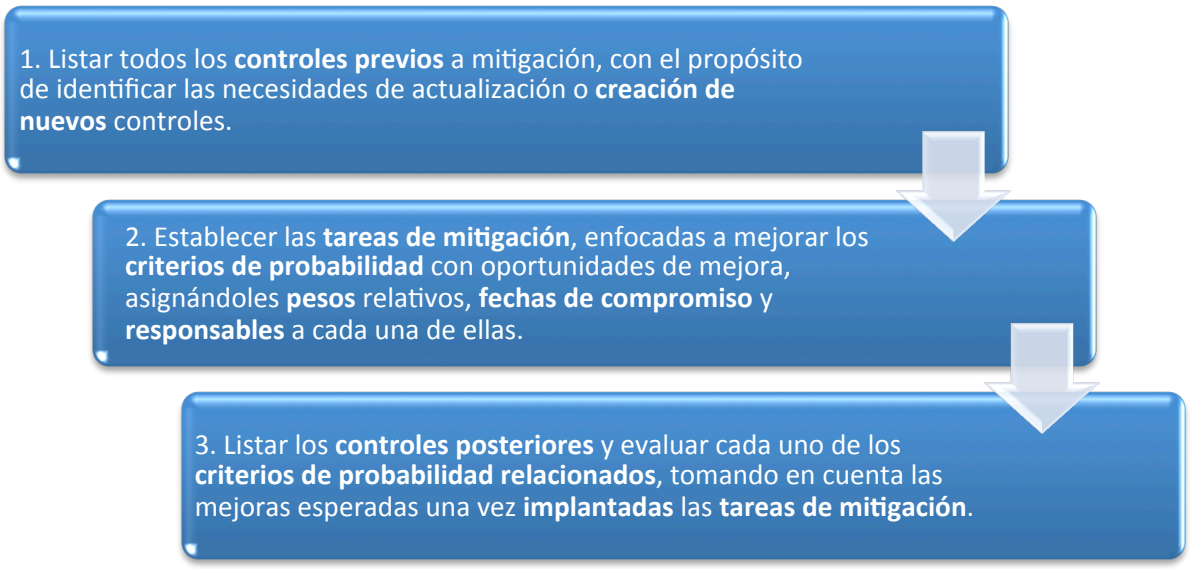


Figura 22 Mitigación de riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

10.1.1.2.1. Objetivo

Establecer las estrategias y responsables de mitigación de los riesgos operativos que superan el apetito definido.

10.1.1.2.2. Insumos

- ✓ Plantilla de identificación y evaluación de riesgos
- ✓ Mapa de Calor
- ✓ Plantilla de mitigación de riesgos

10.1.1.2.3. Ejemplo herramienta a documentar:

Detalle de Eventos y sus Controles Iniciales		EVALUACION INICIAL (Tomando en cuenta los Controles Iniciales)																																
Id Ev	Evento	1. Cumplimiento regulatorio	2. Pérdidas fraude	3. Pérdidas errores	4. Reproceso	5. Revelación financiera	6. Metas financieras	Pr (1)	S (1)	IP(1)	Requiere plan	Segregación	Supervisor participa	Revisión formal	Información segura	Automatización	Estabilidad sistemas	Rotación personal	Procedimientos	Control cruzado	Indicadores	Eventos de 'pérdida'	Informes de auditoria	Probabilidad	1. Cumplimiento regulatorio	2. Pérdida por fraude	3. Pérdida por errores	4. Reproceso	5. Revelación financiera	6. Metas financieras	Severidad			
1	XXXX	1		1	1			4,0	3,5	3,7	1													4,0	3,0		3,5	2,0			3,5			
2	XXXX	1		1	1			4,0	3,5	3,7	1													4,0	3,0		3,5	2,0			3,5			
3	XXXX	1		1	1			4,0	3,5	3,7	1													4,0	3,0		3,5	2,0			3,5			

Figura 23 Herramienta Identificación y evaluación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

1 Id Ev	Eventos de riesgo principales	2 N° medida o tarea	3 ID Ctrol Ref	4 Descripción de la tarea	5 Reduce Pr? S/N	6 Reduce S? S/N	7 Peso
1	XXXX	1	A2	Revisión y actualización de los formularios FGSJ 7.2.42.0.2 CRI Check List para Crédito Hipotecario y FGSJ 7.2.42.0.5 CRI Formulario Detalle de Documentos Pendientes, lo cuales deben contemplar el 100% de la información del expediente según regulación local y requisitos BAC.	S	N	15%
2	XXXX	1.1	A2	Oficializar la utilización por parte de los asistentes operativos de los formularios actualizados FGSJ 7.2.42.0.2 CRI Check List para Crédito Hipotecario para la documentadora y del FGSJ 7.2.42.0.5 CRI Formulario Detalle de Documentos Pendientes. Estos check list deben revisarse formalmente dejando evidencia con nombre o sello, firma y fecha de revisión.	S	N	20%
3	XXXX	2	A2	Segregación de las funciones actuales de las asistentes de ejecutivos. Haciendo la división en asistentes ejecutivos (a) los cuales darán apoyo al ejecutivo y mantendrán la relación con el cliente. Asistentes operativos, encargados de toda las labores operativas para formalizar el crédito, estas funciones serán divididas según las etapas del proceso y serán las encargadas de la validación de la documentación de cada expediente.	S	N	40%
		3	A2	El asistente operativo (a) deberá realizar una verificación en la etapa OPF para asegurar que el caso cuente con todas las aprobaciones y documentos requeridos.	S	N	15%
		4	B2	Automatización del proceso Hipotecario en un 60% de las formalizaciones correspondientes a compra de casa por medio del Workflow Ultimus	S	N	10%
Proyectos a Largo Plazo							
					Peso Total		100 %

Figura 24 Herramienta Mitigación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

1 Responsable	2 Fecha de Inicio	3 Fecha de Finalización	Fecha de Evaluación	4 % Avance Real (Base 100%)
Recurso 1	01-Abr-07	31-Dic-07	30-Sep-08	100,0%
Recurso 2	02-Ene-07	31-Dic-07	30-Sep-08	100,0%
Recurso 1 y Recurso 2	01-Abr-07	31-Jul-07	30-Sep-08	100,0%
Recurso 3	02-Ene-07	31-Dic-07	30-Sep-08	100,0%
Recurso 1 y Recurso 3	02-Ene-06	31-Dic-07	30-Sep-08	50,0%

Figura 25 Herramienta Mitigación de Riesgos. Fuente: Metodología Riesgos Operativos Organizacional BAC

10.2. Lineamientos y Procesos

Dado que la organización se encuentra certificada en norma ISO 9000, la misma se apalancó en su sistema de calidad para definir un Lineamiento de Gestión de Riesgos Operativos. El propósito de dicho lineamiento se resume poder llegar a calcular la reserva que debe hacer la organización para afrontar cualquier riesgo materializado. Esta definición es congruente con las normativas establecidas por Basilea II y que son reforzadas por las entidades de supervisión de entidades financieras a nivel de cada país (pe SUGEF para Costa Rica). La existencia de dicha política o lineamiento favorece a la organización de manera que no tenga que sobreestimar el monto que debe reservar para efectos de cubrir impactos de riesgos materializados. Esto se traduce en mayor eficiencia de la organización en todo lo relacionado al uso de sus fondos.

Adicionalmente se identifican dos procesos relacionados con la gestión de riesgos relacionados con tecnología de información:

1. Proceso “Evaluar y administrar los Riesgos (PO9)
2. Proceso “Evaluación y gestión de Riesgos Tecnológicos (PO9)”

El proceso 1 está orientado a la revisión de los riesgos operativos inherentes a los procesos de gestión de tecnología, su evaluación y respectivos planes de mitigación.

El proceso 2 tiene como objetivo la identificación de riesgos asociados a la tecnología de información y sus respectivos componentes que puedan impactar en alguna medida los servicios brindados a los diferentes clientes.

Ambos procesos fueron definidos tomando como referencia el proceso PO9 (Evaluar y Administrar los Riesgos de TI) que forma parte del dominio Organización y Planificación de COBIT.

Los procesos se han desarrollado de manera tal que puedan cumplir con el nivel de madurez 3 que COBIT propone. Esto significa que la administración del

proceso de Evaluar y administrar los riesgos de TI que satisfaga el requerimiento de negocio de TI de analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y las metas de negocio se encuentre en estatus Definido (nivel 3 de madurez).

Esto se cumple cuando:

1. Existe una política de administración de riesgos para toda la organización que define cuándo y cómo realizar las evaluaciones de riesgos.
2. La administración de riesgos sigue un proceso definido, el cual está documentado.
3. El entrenamiento sobre administración de riesgos está disponible para todo el personal.
4. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo.
5. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados.
6. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican.
7. Las descripciones de puestos consideran las responsabilidades de administración de riesgos.

Los procesos indicados anteriormente se han sometido a diferentes auditorías internas y externas, logrando certificar el cumplimiento mínimo necesario para satisfacer los requerimientos regulatorios. Sin embargo, no se ha cuestionado la eficiencia y efectividad del proceso en sí, razón por la cual entrevistamos y encuestamos a los participantes para obtener retroalimentación acerca de algunas de las variables de interés para esta investigación.

10.3. Resultado de entrevistas a Mandos Medios del Proceso

Aplicando el formato de entrevistas indicada en el marco metodológico, se logró sintetizar la siguiente información aportada por el Gerente Regional de Seguridad y Riesgos, principal interesado del resultado de esta investigación:

1. Metodología actual de identificación de riesgos es empírica (no es un ejercicio guiado paso a paso sino resultado de un proceso de lluvia de ideas donde cada quien documenta según su imaginación y experiencia).
2. No hay énfasis en la identificación de riesgos de la dimensión personas que se pueden materializar por “actos de Dios” (agentes externos como terremotos, huracanes, inundaciones, etc.).
3. Evaluación de los riesgos no es consistente si lo hacen dos personas diferentes, altamente sujeto a interpretación (poca predictibilidad).
4. Considerar dentro del análisis y propuesta, una práctica que ha resultado exitosa en el pasado y es la identificación de riesgos de manera conjunta y no individual.
5. Considerar dentro del análisis y propuesta la eliminación de ambigüedades (por ejemplo, hoy en día la metodología propone una revisión exhaustiva una vez al año. No se especifica ni aclara que significa exhaustivo)
6. Cuestionar dentro del análisis si realmente el proceso de gestión de riesgos es costo efectivo dado que actualmente es muy complejo.
7. Revisar si existe un desenfoque en la identificación y clasificación de riesgos. Por ejemplo:
    a. Se han detectado como riesgos principales situaciones que no corresponden a tal criticidad (por ejemplo, Riesgos asociados al manejo de Caja Chica).
    b. Incidentes mayores que se han materializado no estaban identificados previamente como riesgos y eso ha generado cuestionamientos sobre la efectividad de este proceso.
    c. El volumen de riesgos detectados por un área es alto (más de 4,000 riesgos identificados solo en una gerencia).

Mediante la entrevista realizada al Supervisor de Riesgos, se logró recolectar la siguiente retroalimentación:

1. Necesidad de eliminar la subjetividad en el uso de las herramientas de gestión de riesgos.
2. Considerar mejorar los instrumentos utilizados para la gestión de riesgos puesto que lo que se tiene en este momento es el vehículo o marco de trabajo general, pero no es específico, prescriptivo ni detalla el orden a seguir para recolectar ordenada y sistemáticamente la información. Actualmente el área encargada está planteando un borrador de una lista de chequeo ("checklist") que puede utilizarse para hacer más objetiva y clara la gestión.
3. Analizar cómo hacer un uso eficiente del tiempo de las personas invertido en la gestión de riesgos ("lo que está escrito no promueve esta efectividad").
4. Considerar la eliminación de incentivos perversos (por ejemplo, se bajan puntos en la evaluación de rendimiento de las personas si no logran identificar una cantidad mínima de riesgos cada período).
5. Revisar las siguientes debilidades dentro del análisis:
    a. No están documentados los argumentos para asignar o transferir la propiedad de un riesgo una vez identificado
    b. Las áreas de negocio no son propietarias de riesgos tecnológicos en la actualidad
    c. Debe mejorarse el seguimiento al estado de los planes definidos para atender los riesgos.

10.4. Hallazgos relevantes de la encuesta

Al aplicar la encuesta a los dos grupos identificados como muestras se encuentran los siguientes resultados.

10.4.1. Marcos de trabajo de gestión de riesgos

Al evaluar el conocimiento de los marcos de trabajo para gestión de riesgos existentes y utilizados dentro de la organización para implementar los procesos

actuales, se consultó a los miembros de ambas muestras con el fin de identificar el nivel de consistencia entre el conocimiento ambos grupos manejan sobre el tema.

A continuación se incluye un gráfico con el resumen de ambas evaluaciones:

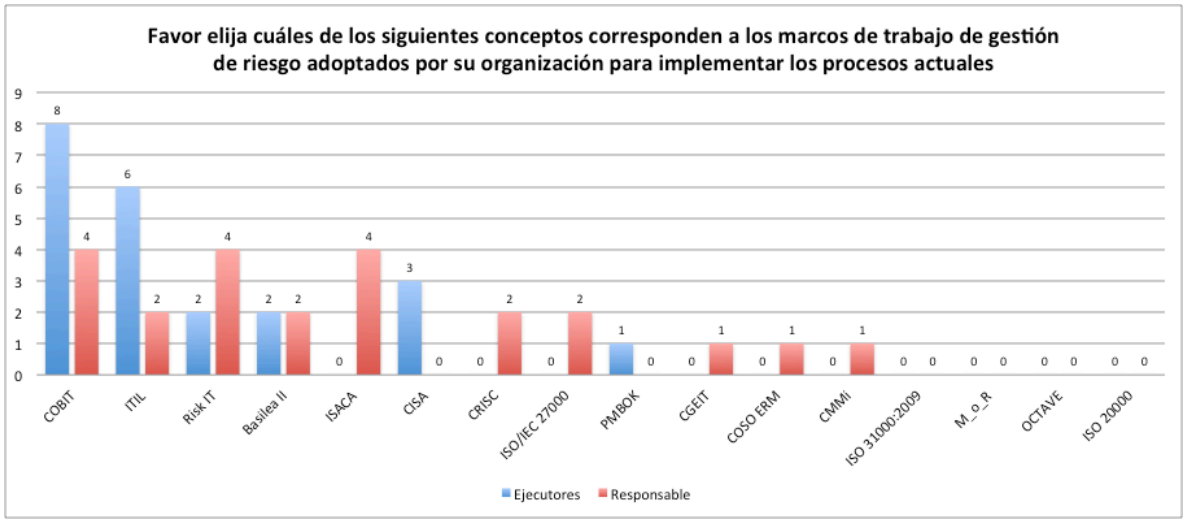


Figura 26 Respuestas Pregunta 1 – Encuesta personal ejecutor y responsable de la metodología de gestión de riesgos

De la comparación de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. Se identifica por ambos grupos con 100% de consistencia que COBIT es uno de los marcos de trabajo utilizados por la organización como referencia para la gestión de riesgos. Sin embargo, a pesar de la coincidencia en ambos grupos es importante aclarar que como se mencionó en el marco teórico, COBIT es una guía de mejores prácticas presentado como un marco de trabajo, dirigido al control y supervisión de la tecnología de información en general pero no se puede considerar un marco de trabajo de gestión de riesgos.
2. El personal responsable de la metodología de gestión de riesgos (en adelante responsables) identifica, con 100% de consistencia, como metodología primaria a ISACA. Sin embargo, es importante aclarar que ISACA es una asociación internacional que apoya metodologías y certificaciones más no representa por sí misma un marco de trabajo de gestión de riesgos. Del grupo de ejecutores de la metodología de gestión

(en adelante ejecutores) riesgos ninguno de los 8 evaluadores consideró a ISACA como un marco de referencia.

3. Los responsables identifican, con un 100% de consistencia, como metodología primaria a Risk IT, lo cual es congruente con las definiciones brindadas en el marco teórico. No obstante, solo un 25% de los ejecutores identificaron a Risk IT como marco de trabajo utilizado por la organización.
4. Ambos grupos seleccionaron a CRISC, CISA y CGEIT como marcos de trabajo referentes. Sin embargo, es importante aclarar que estos conceptos corresponden más bien a certificaciones patrocinadas por ISACA y no marcos de trabajo de gestión de riesgos.
5. Se presentó mayor dispersión en las respuestas del grupo de evaluadores a cargo de la gestión de riesgos (10 opciones diferentes seleccionadas en la encuesta) comparado contra los ejecutores de la metodología (6 opciones seleccionadas).

10.4.2. Fortalezas de la metodología implementada

Al consultar sobre las fortalezas que identifican ambos grupos sobre la metodología utilizada actualmente se logró resumir las respuestas en el siguiente gráfico:

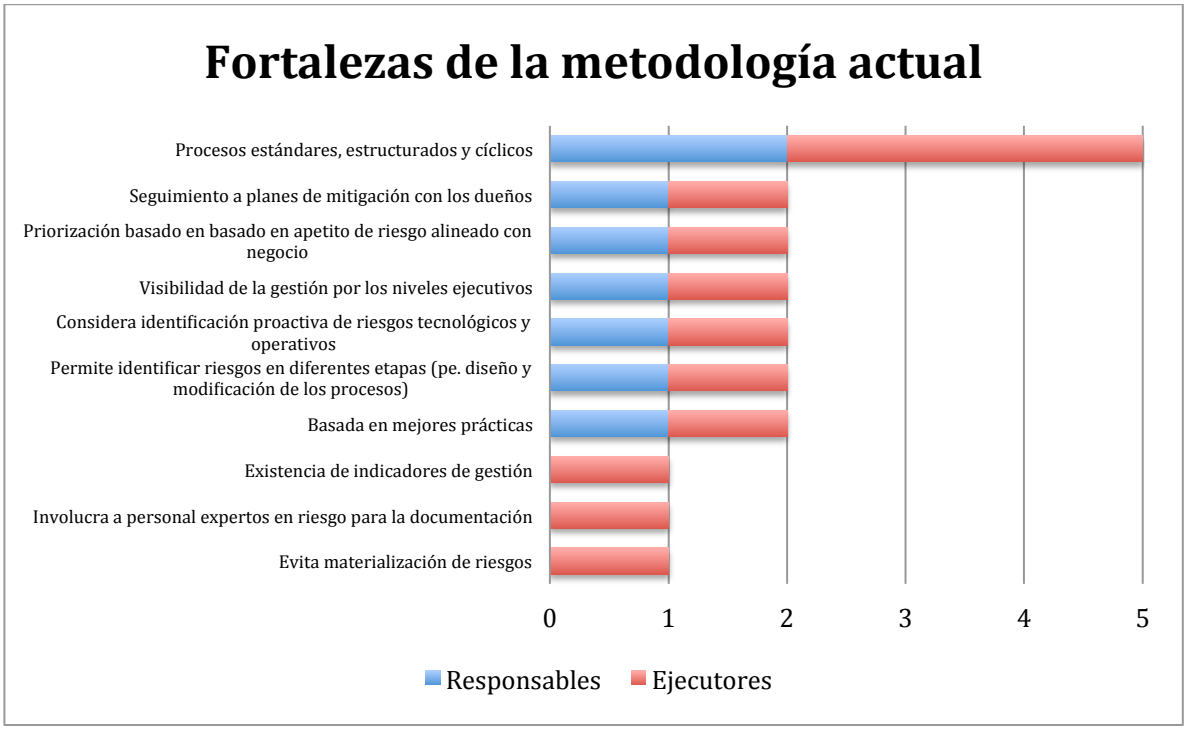


Figura 27 Respuestas Pregunta 2 – Encuesta a personal responsable y ejecutor sobre las fortalezas de la gestión de riesgos

De este resumen de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. La principal fortaleza que ambos grupos reconocen es la existencia de procesos formales, documentados, estándares y versionados dentro del sistema de calidad lo cual permite hacer repetible y estructurada la ejecución de la metodología.
2. Se mencionan 6 fortalezas adicionales con una misma cantidad de respuestas. Dentro de estas, son relevantes para la presente investigación la Visibilidad de la gestión por los niveles ejecutivos, que existe un esquema de priorización alineado con negocio y el seguimiento a los planes de mitigación.
3. Se mencionan otras tres fortalezas con una única mención cada una, las cuales no obtuvieron el mayor consenso pero son relevantes.

10.4.3. Oportunidades de mejora de la metodología implementada

Al consultar sobre las oportunidades de mejora que identifican ambos grupos sobre la metodología utilizada actualmente se logró resumir las respuestas en el siguiente gráfico:

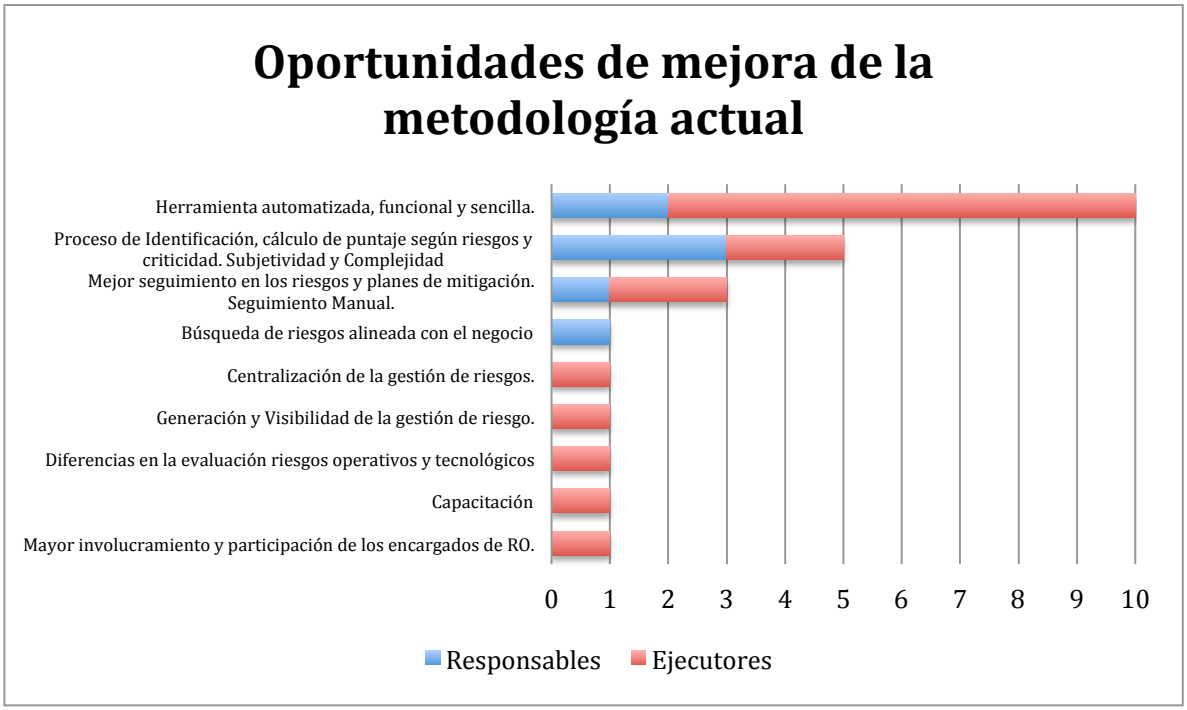


Figura 28 Respuestas Pregunta 3 – Encuesta a personal responsable y ejecutor sobre las oportunidades de la gestión de riesgos

De la comparación de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. La principal oportunidad que se identifica es la necesidad de contar con una herramienta tecnológica que automatice, centralice y facilite la gestión de riesgos. Actualmente se utilizan plantillas en Excel.
2. Si bien es cierto se identificó como una fortaleza la existencia de procesos formales, documentados, estándares y versionados. Los responsables señalan oportunidades de mejora en los procesos existentes, señalando entre las principales el cálculo para la puntuación de riesgos, complejidad del proceso en general y subjetividad de los ejecutores.

3. Tres encuestados mencionaron oportunidades en el seguimiento de los riesgos identificados y planes de mitigación. El seguimiento se hace en forma manual. En esto coinciden ambos grupos.
4. Se identificaron 6 oportunidades adicionales, relevantes para quienes ejecutan, no así para los responsables. Estas oportunidades no tuvieron coincidencias entre sí. Dentro de las más destacadas para la presente investigación se pueden mencionar: la falta de capacitación, involucramiento de los responsables de la gestión de riesgos, diferencias en la evaluación de riesgos operativos y tecnológicos, visibilidad de la gestión de riesgos, centralización y alineamiento con negocio.

10.4.4. Uso de características para la identificación de riesgos.

Al evaluar el proceso de identificación de riesgos asociados a los servicios de TI en la organización, se consultó a los encuestados la frecuencia con que se capturan las principales características con el fin de determinar el uso que se le da a cada una.

A continuación se incluyen los gráficos con el resumen de ambas evaluaciones:

Resultados de personal responsable de la metodología de gestión riesgos.

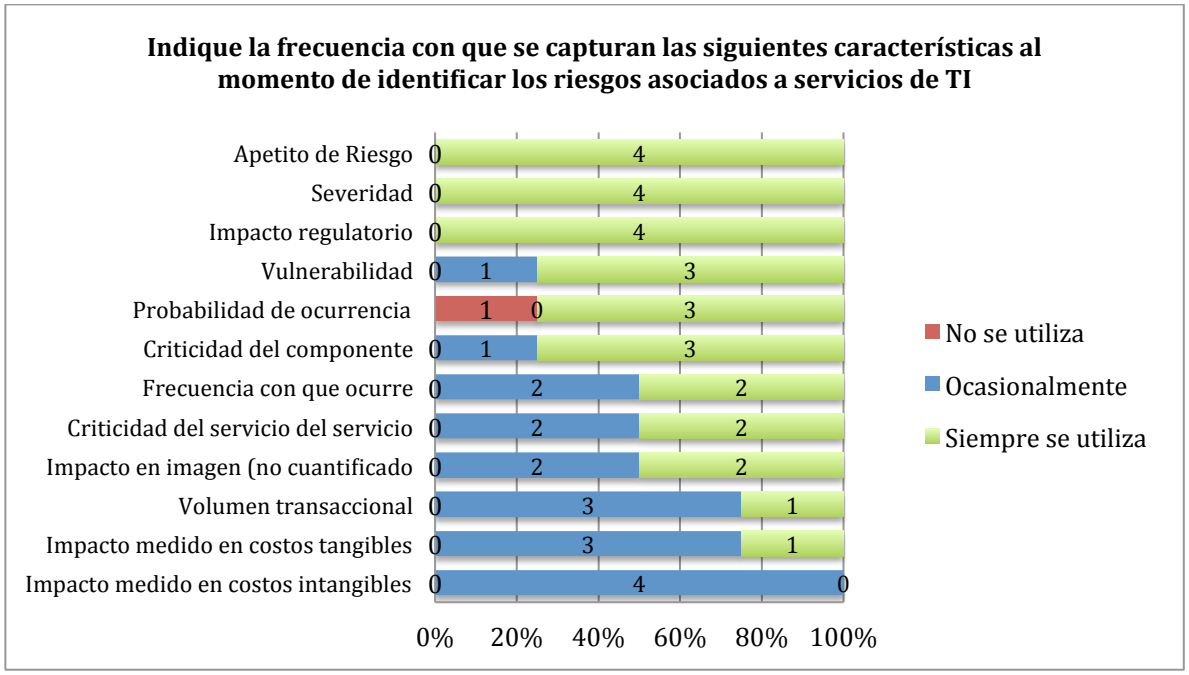


Figura 29 Respuestas Pregunta 4 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre las características utilizadas para la identificación de riesgos.

Resultados de personal ejecutor de la metodología de gestión riesgos.

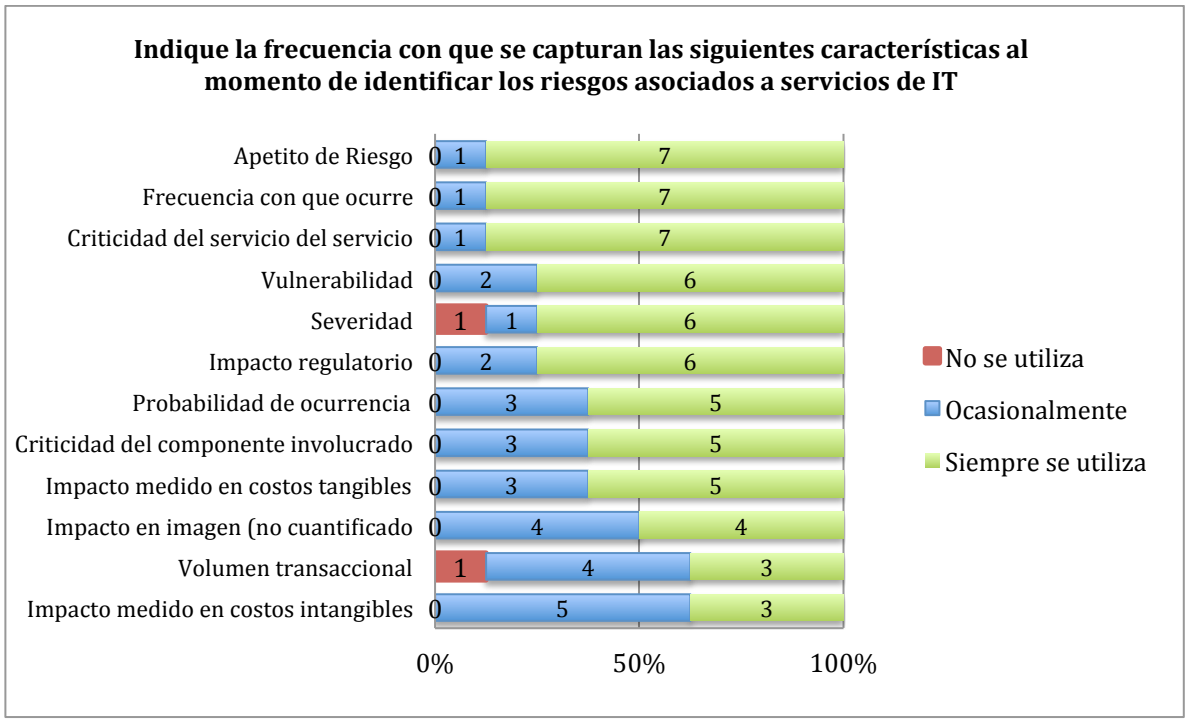


Figura 30 Respuestas Pregunta 4 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre las características utilizadas para la identificación de riesgos.

De la comparación de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. Se identifica por ambos grupos con más de un 91% de consistencia que el apetito de riesgo es la característica más utilizada para la identificación de riesgos.
2. Se identifican características en común para ambos grupos como el impacto medido en costos intangibles, impacto en costos tangibles, volumen transaccional e impacto en imagen como utilizadas ocasionalmente. Lo anterior indica poca cultura en la organización para cuantificar riesgos y el impacto que podrían tener en la organización en términos económicos para los riesgos tecnológicos.
3. La opinión de ambos grupos es que todas las características consideradas en la encuesta se utilizan, aunque no de manera consistente, si ocasionalmente, dejando en evidencia que el criterio empleado para la elección de cada característica es de manera subjetiva.
4. Se muestra diversidad de criterios sobre las características de apetito de riesgo, severidad e impacto regulatorio. Esto ocurre tanto entre ambos grupos como en participantes de un mismo grupo. Por ejemplo, los responsables afirman que las características anteriores siempre son utilizadas para la identificación de riesgos. Sin embargo, un 25% de los ejecutores difieren de esta elección indicando que no se utilizan del todo o que se hace uso ocasionalmente de las mismas características.

10.4.5. Nivel de eficiencia, efectividad y agilidad en la gestión de riesgos.

Al evaluar el proceso de identificación de riesgos asociados a los servicios de TI en la organización de manera integral, se consultó a los encuestados el nivel de eficiencia, efectividad y agilidad de dicho proceso.

A continuación se incluyen los gráficos con el resumen de ambas evaluaciones:

Resultados de personal responsable de la metodología de gestión riesgos.

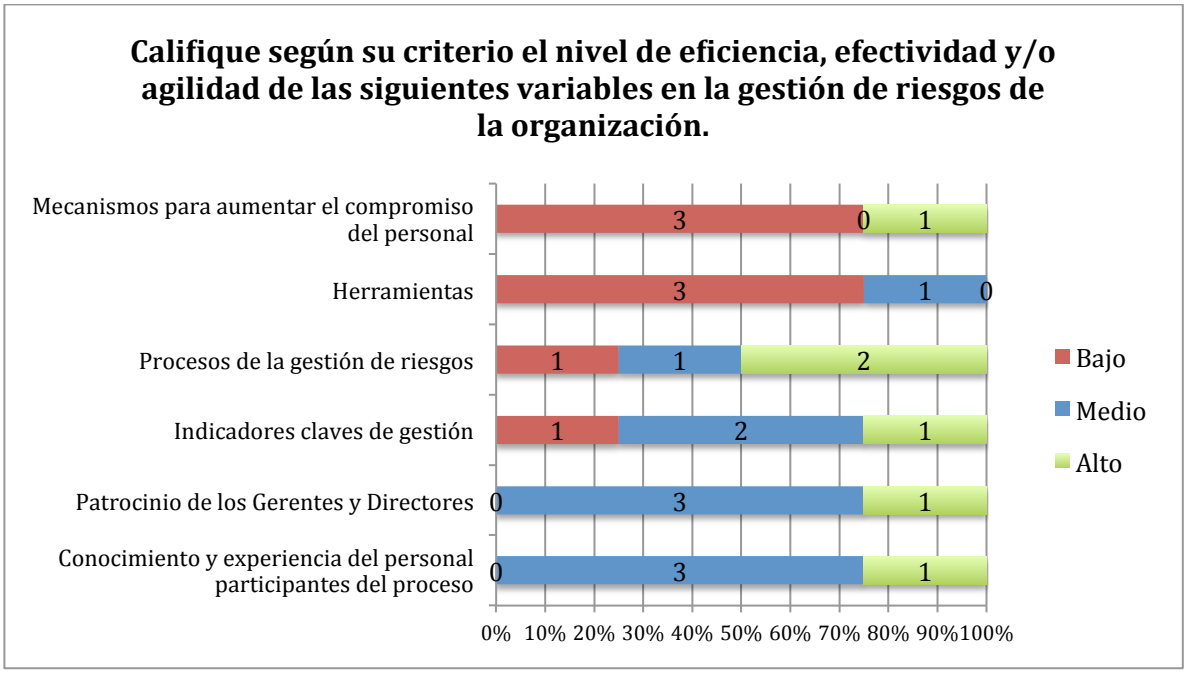


Figura 31 Respuestas Pregunta 5 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre las características sobre nivel de eficiencia, efectividad y agilidad.

Resultados de personal ejecutor de la metodología de gestión riesgos.

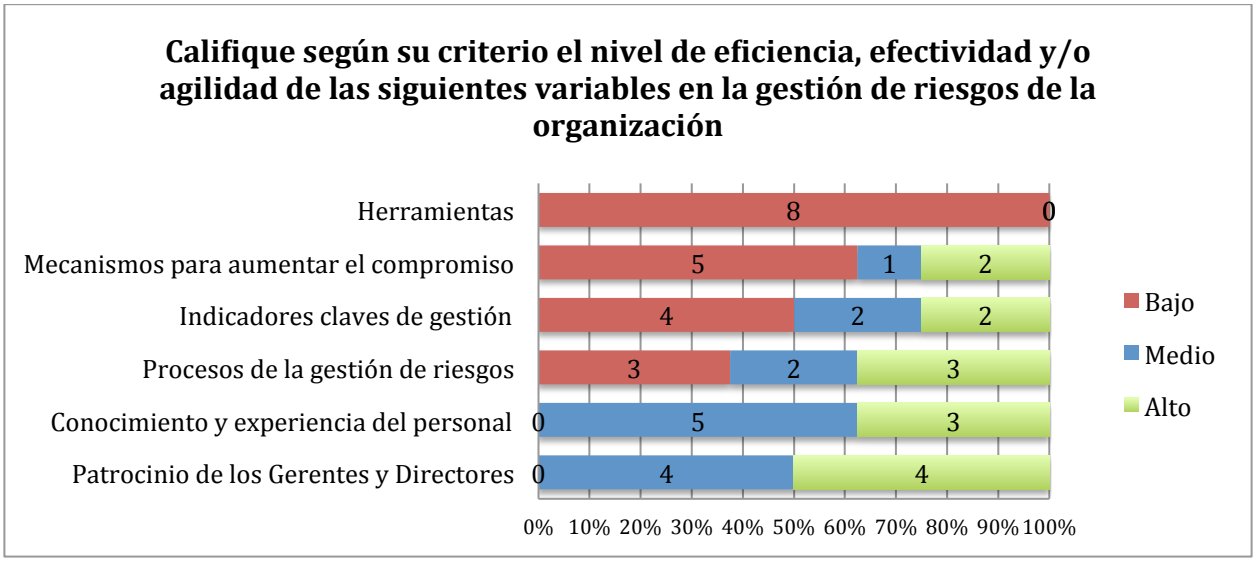


Figura 32 Respuestas Pregunta 5 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre las características sobre nivel de eficiencia, efectividad y agilidad.

De la comparación de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. Se reconoce en ambos grupos que la herramienta que actualmente se utiliza no contribuye con la agilidad y eficiencia que se requiere en la organización para la gestión de riesgos.
2. Se identifica la necesidad de establecer mecanismos más robustos, sistemáticos y atractivos que estimulen al personal involucrado, con el fin de aumentar el nivel de compromiso y conocimiento sobre la gestión de riesgos de manera integral.
3. Lo anterior pone en evidencia las oportunidades definidas en la *Figura 28 Respuestas Pregunta 3 – Encuesta a personal responsable y ejecutor sobre las oportunidades de la gestión de riesgos.*
4. Adicionalmente a las oportunidades ya señaladas, se identifica la mejora en los indicadores claves de gestión como un mecanismo para hacer más eficiente el trabajo que realizan las áreas.

10.4.6. Características utilizadas para priorizar los riesgos.

Al evaluar el proceso de identificación de riesgos asociados a los servicios de TI en la organización de manera integral, se consultó a los encuestados las características más utilizadas para la priorización de riesgos.

A continuación se incluyen los gráficos con el resumen de ambas evaluaciones:

Resultados de personal responsable de la metodología de gestión riesgos.

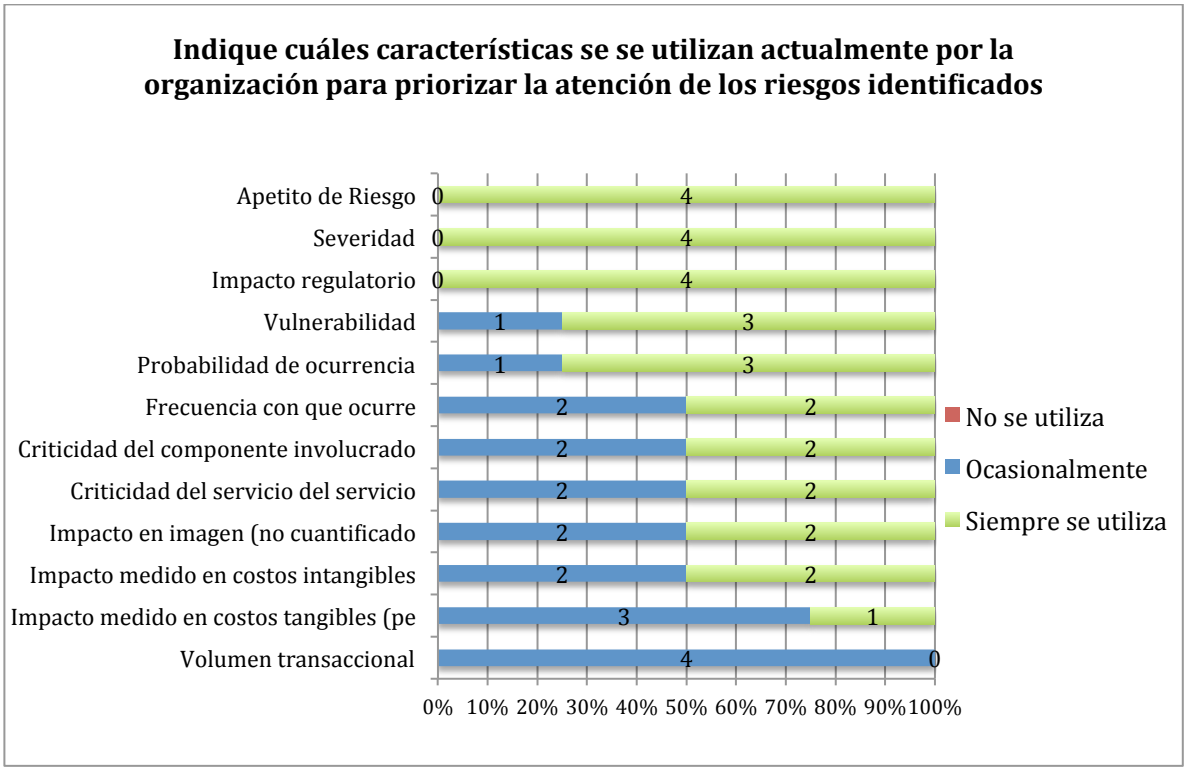


Figura 33 Respuestas Pregunta 6 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre las características utilizadas para la priorización de riesgos.

Resultados de personal ejecutor de la metodología de gestión riesgos.

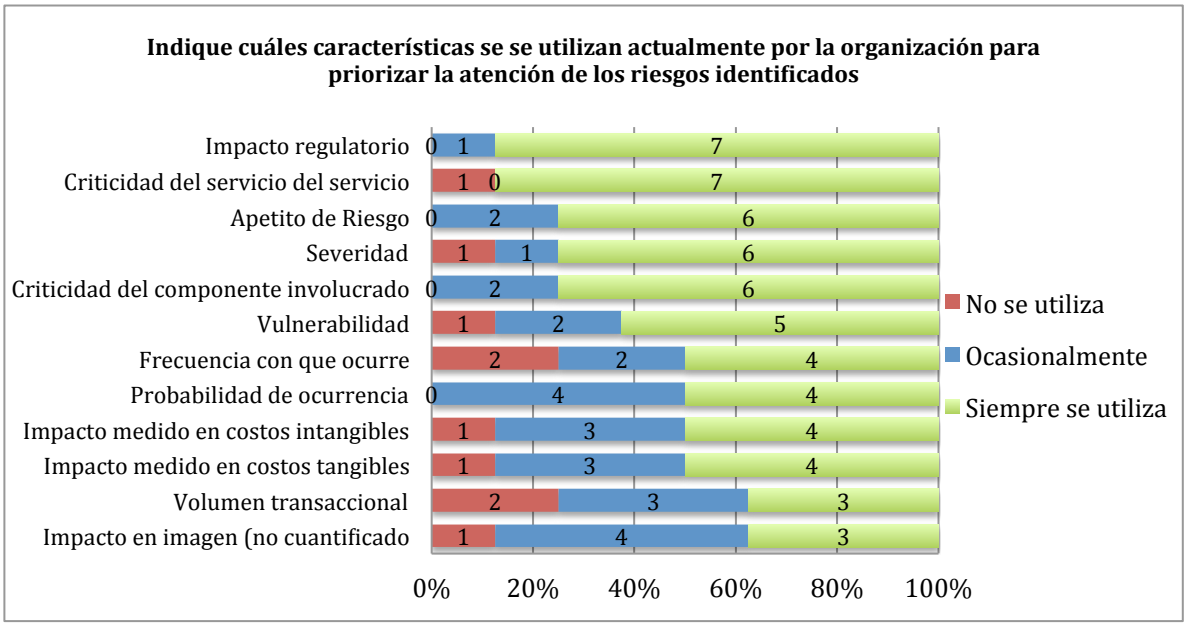


Figura 34 Respuestas Pregunta 6 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre las características utilizadas para la priorización de riesgos.

De la comparación de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. Se identifica por ambos grupos con más de un 91% de consistencia que la característica impacto regulatorio siempre se utiliza para la priorización de riesgos.
2. Se identifican características en común para ambos grupos, como el impacto medido en costos intangibles, impacto en costos tangibles, volumen transaccional e impacto en imagen como utilizadas ocasionalmente. Lo anterior confirma los resultados de la pregunta 4 poca cultura en la organización para cuantificar riesgos y el impacto que podrían tener en la organización en términos económicos para los riesgos tecnológicos.
3. Se muestra diversidad de criterios sobre todas las características. Esto ocurre tanto entre ambos grupos como en participantes de un mismo grupo. Por ejemplo, los responsables afirman que las todas las características al menos son utilizadas ocasionalmente o siempre. Sin embargo, para los ejecutores algunas características no se utilizan del todo.

10.4.7. Variables se cuantifican o traducen a términos económicos según el tiempo de afectación.

Al evaluar el proceso de identificación de riesgos, asociados a los servicios de TI en la organización de manera integral, se consultó a los encuestados cuales variables se cuantifican o traducen a términos económicos tomando en cuenta el tiempo de afectación.

A continuación se incluyen los gráficos con el resumen de ambas evaluaciones:

Resultados de personal responsable de la metodología de gestión riesgos.

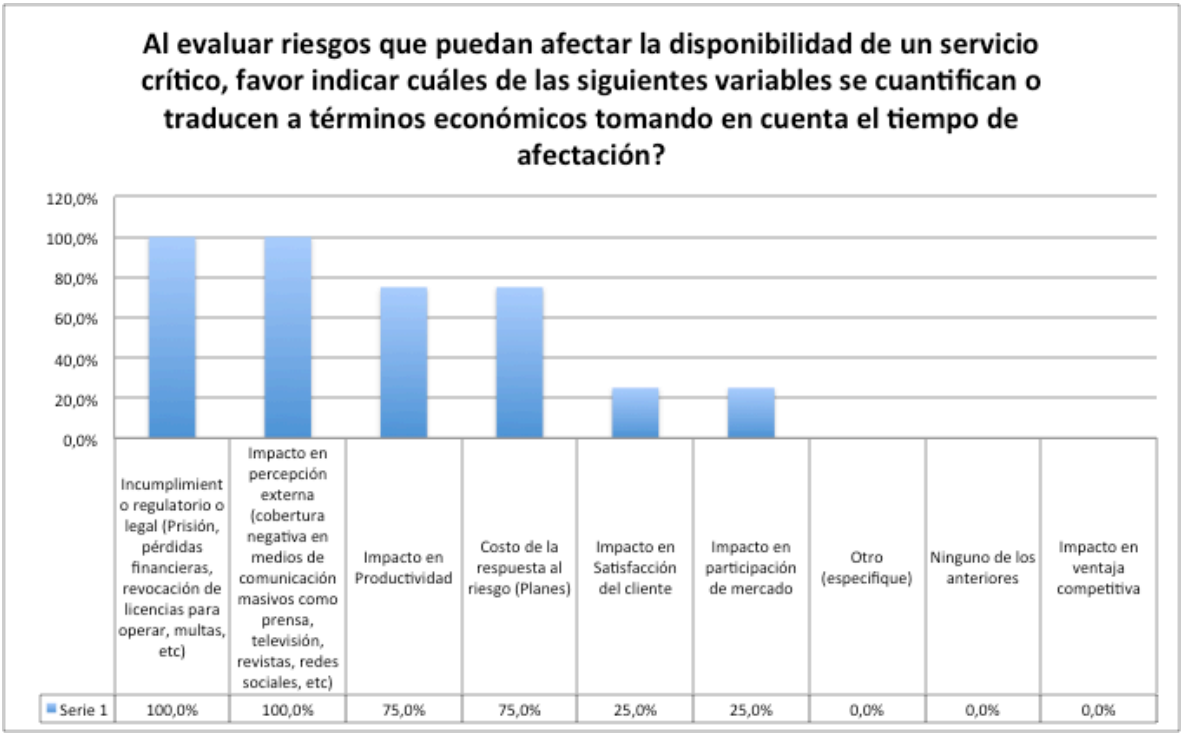


Figura 35 Respuestas Pregunta 7 – Encuesta a personal responsable de la metodología de gestión de riesgos las variables que se cuantifican o traducen a términos económicos.

Resultados de personal ejecutor de la metodología de gestión riesgos.

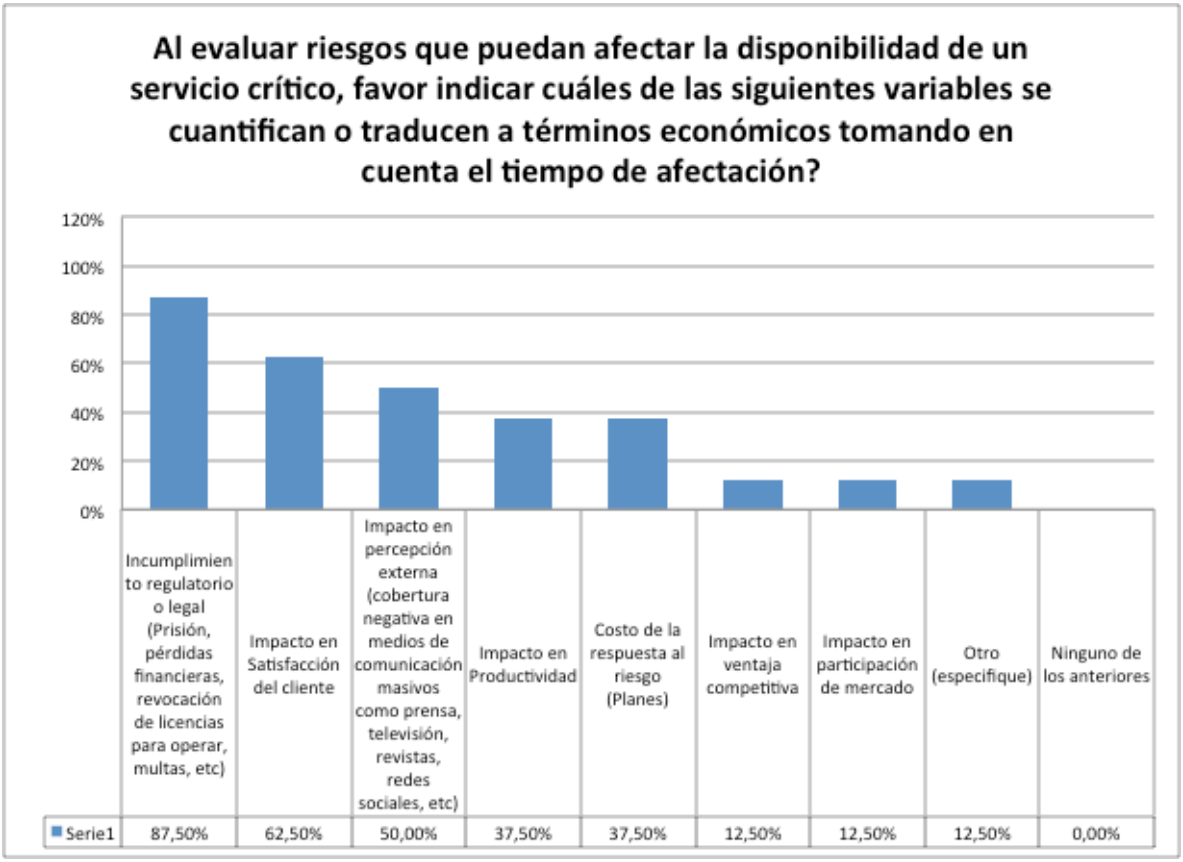


Figura 36 Respuestas Pregunta 7 – Encuesta a personal ejecutor de la metodología de gestión de riesgos las variables que se cuantifican o traducen a términos económicos.

De la comparación de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. Ambos grupos coinciden que el incumplimiento regulatorio o legal, e impacto en percepción externa son variables que se cuantifican o traducen en términos económicos al momento de evaluar los riesgos. Sin embargo, como ya se ha evidenciado en los resultados de preguntas anteriores, no se aprecia que la organización tenga una cultura y herramientas que apoyen la cuantificación de las variables a nivel monetario.
2. Importante notar que el personal ejecutor indica con un 62% que la variable de Impacto de Satisfacción del cliente se cuantifica, pero no así el 75% del personal responsable. Lo anterior sugiere que hay una falta

de alineamiento entre áreas para evaluar los riesgos bajo un mismo criterio o procedimiento.

3. Otras variables como Impacto en productividad, costo de la respuesta al riesgo y participación del mercado se cuantifican en menor escala por los interesados, sin embargo son importantes si se quiere como alcance de este trabajo proponer un modelo de cuantificación de variables, costos tangibles e intangibles.

10.4.8. Elementos que se cuantifican para definir planes de mitigación.

Al evaluar el proceso de identificación de riesgos asociados a los servicios de TI en la organización de manera integral, se consultó a los encuestados cuales son los elementos que se cuantifican y documentan en la definición de planes de mitigación de riesgos.

A continuación se incluyen los gráficos con el resumen de ambas evaluaciones:

Resultados de personal responsable de la metodología de gestión riesgos.

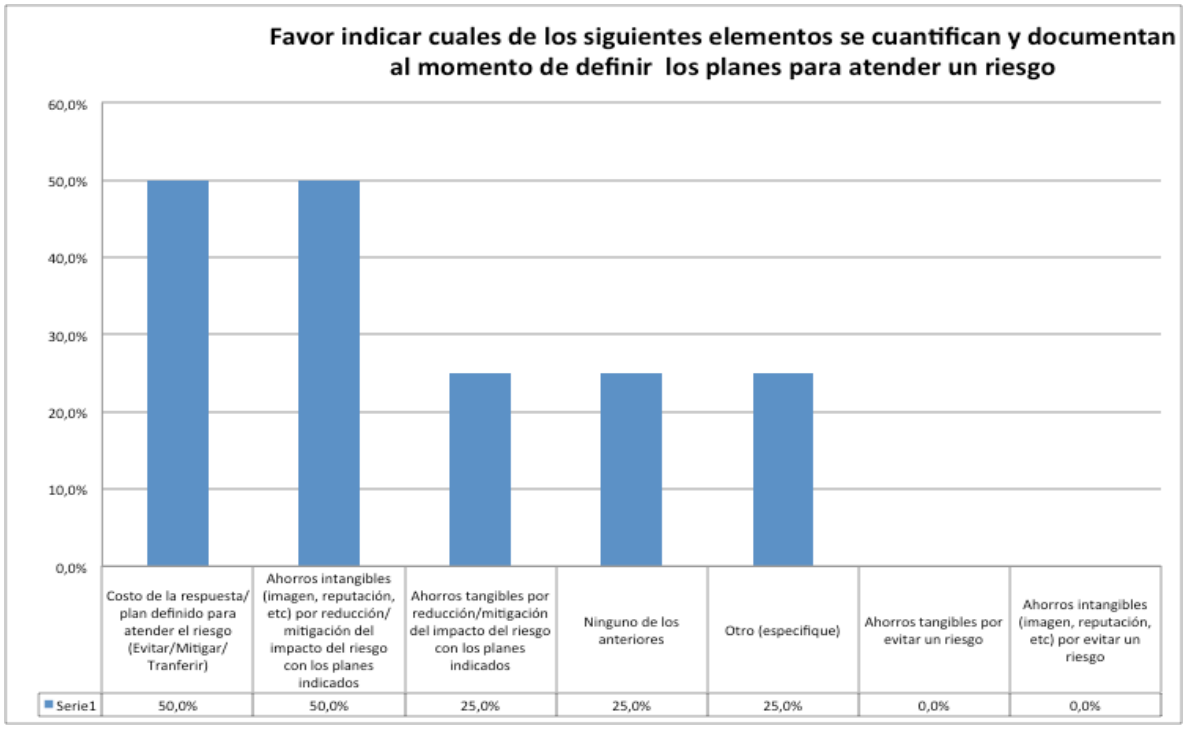


Figura 37 Respuestas Pregunta 8 – Encuesta a personal responsable de la metodología de gestión de riesgos sobre los elementos que se cuantifican y documentan.

Resultados de personal ejecutor de la metodología de gestión riesgos.

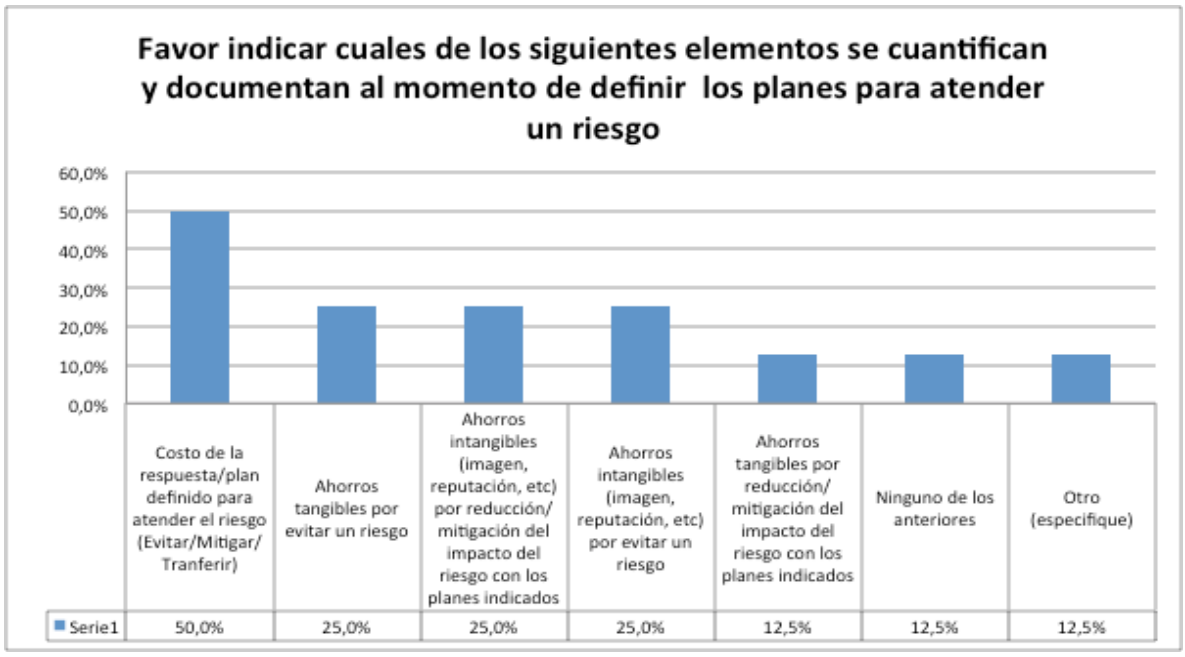


Figura 38 Respuestas Pregunta 8 – Encuesta a personal ejecutor de la metodología de gestión de riesgos sobre los elementos que se cuantifican y documentan.

De la comparación de las respuestas de ambos grupos se pueden realizar las siguientes conclusiones relevantes:

1. Hay diversidad de criterios en ambos grupos, lo que evidencia aún más los resultados de la pregunta 7. Se deberá tomar en cuenta estos elementos para la propuesta de modelo de cuantificación de variables, costos tangibles e intangibles.

10.5. Análisis final

A partir de la información analizada en las secciones anteriores se resume a continuación los principales hallazgos que realiza el investigador a través de los diferentes instrumentos que se aplicaron:

1. Desconocimiento de conceptos como marcos de trabajo de gestión de riesgos, certificaciones y organizaciones que representan dichos estándares o certificaciones.
2. Se detectaron contradicciones entre las respuestas de los ejecutores comparados con las respuestas de los responsables en relación a las distintas variables consultadas.
3. Se detectó desconocimiento del personal cuando se consultó sobre las variables monetarias que actualmente se consideran en la gestión de riesgos. Esta afirmación se realiza por cuanto los encuestados no pudieron responder con claridad que la única variable monetaria que se está capturando actualmente en el análisis de riesgo tecnológico tiene que ver con el costo de la solución a implementar.
4. Se identifica que existe complejidad e ineficiencia en la ejecución de la metodología actual de riesgos (tiempo requerido por parte del personal).
5. Se identifica que la herramienta que se utiliza actualmente para dar soporte a la gestión de riesgos es manual y compleja (plantillas de Excel).
6. La identificación de los riesgos actualmente no es estructurada por lo que no se orienta al personal respecto a un orden específico a seguir para generar información de valor.

7. Se presentan diferentes interpretaciones cuando se evalúan los riesgos (subjetividad en uso de herramientas).
8. Existen ambigüedades en las instrucciones del proceso.
9. Se presenta una inadecuada valoración de riesgos (desenfoque en identificación/clasificación) por la multiplicidad de riesgos identificados y algunos evaluados muy altos (cuando la criticidad es baja).
10. Se detecta la necesidad de mejorarlos métodos para mejorar la contribución del personal al uso y fortalecimiento de la metodología de gestión de riesgos.

CAPITULO V – Solución del Problema

11.1. Propuesta de solución

En este capítulo realizaremos una propuesta de solución, a partir de los hallazgos de la situación actual y la investigación considerada en el marco teórico.

Dada la necesidad de apegarse a un marco de trabajo de gestión de riesgos que sea integral, estándar, alineado al negocio y enfocado a la gestión de riesgos de la tecnología de información, donde los riesgos asociados al nivel operacional sean considerados, se propone al Risk IT como base para dicha metodología. Adicionalmente esta decisión es congruente y refuerza las respuestas brindadas por el personal que controla y dirige la metodología de gestión de riesgos, quienes identificaron Risk IT como el marco de trabajo sobre el cual están basados sus procesos.

El marco de gestión de riesgos propuesto por el Risk IT se resume en la siguiente figura:

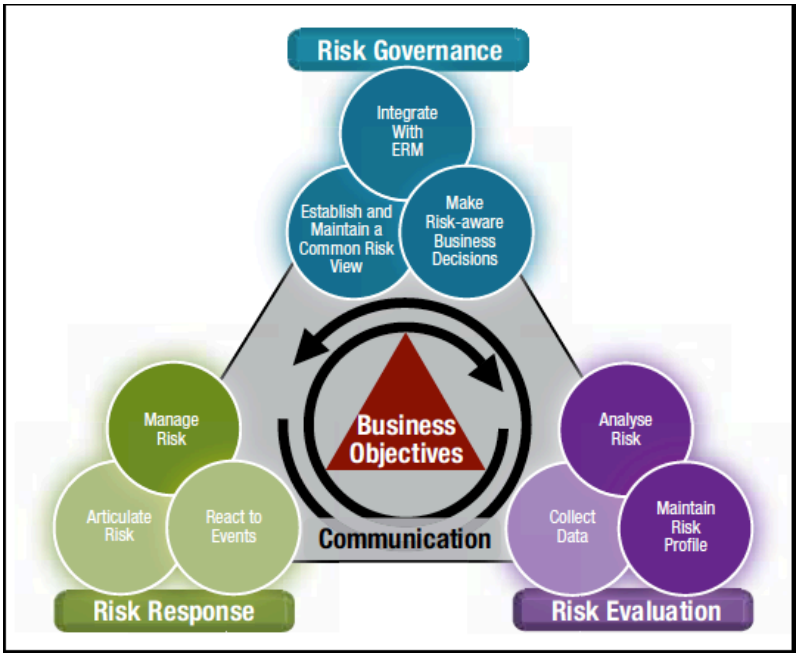


Figura 39 Fuente: ISACA, Risk IT Framework, USA, 2009

Para efectos de cerrar las brechas identificadas durante el diagnóstico de situación actual y adicionalmente generar un valor agregado, aporte del investigador, se propone el siguiente ciclo de gestión de riesgos:

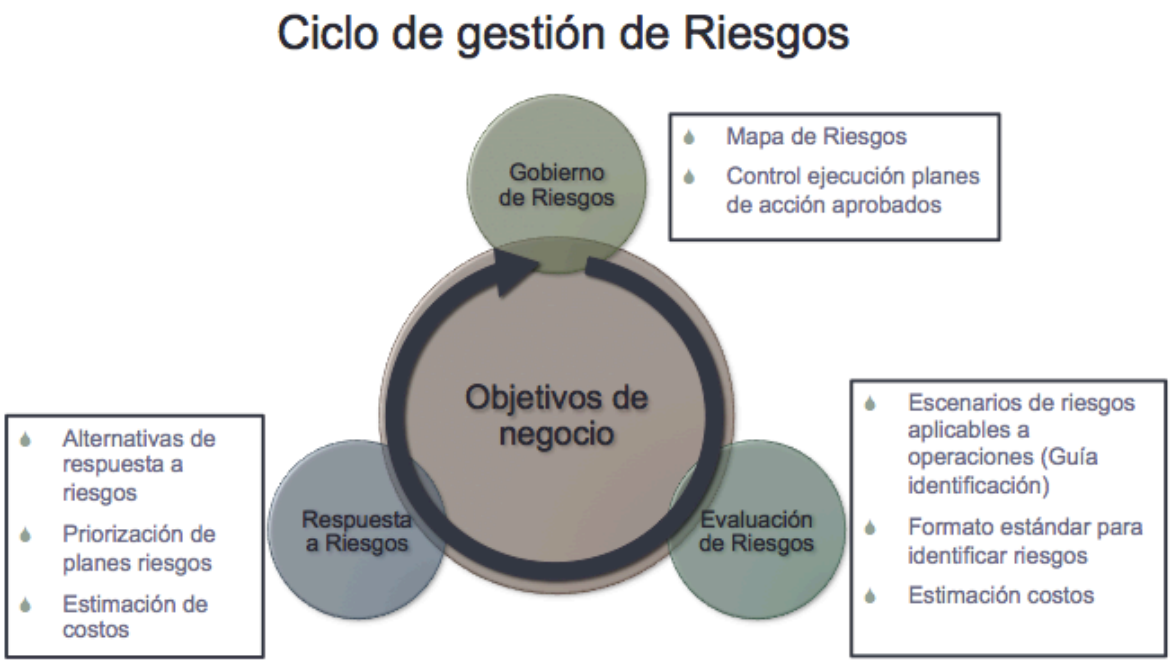


Figura 40 Fuente: Propia, Basado en Risk IT Framework, USA, 2009

Aunque si bien este ciclo es la propuesta base que realiza el marco de trabajo de gestión de riesgos del Risk IT, el investigador considera necesario complementar algunos de sus componentes con el fin de poder atender las necesidades identificadas en el análisis de situación actual y parte de los objetivos de esta investigación.

Los principales elementos que esta metodología debe considerar comprenden:

1. Escenarios de riesgos aplicables a las operaciones
2. Guía de identificación de riesgos
3. Formato para identifica, describir y evaluar los riesgos a nivel cualitativo pero también con variables cuantitativas (monetarias)
4. Esquema para respuesta y priorización de los riesgos con base a su efectividad y costo

Como se mencionó en el marco teórico, Risk IT se compone de tres dominios:

1. Gobierno de Riesgos, cuyo objetivo es asegurarse que las prácticas de gestión de riesgo estén implementadas en la organización, permitiendo asegurar un retorno óptimo ajustado a los riesgos.
2. Evaluación de Riesgos cuyo objetivo es asegurarse que las oportunidades y riesgos asociados a la TI sean identificados, analizados y presentados en términos de negocio. Este dominio está compuesto de tres procesos: Análisis de riesgos, recolección de datos y mantenimiento del perfil de riesgos.
3. Respuesta a Riesgos, cuyo objetivo es asegurarse que los problemas, oportunidades y eventos relacionados con riesgos de TI sean tratados de manera costo/efectiva y alineados con las prioridades del negocio. Este dominio está compuesto de tres procesos: gestión de riesgos, articulación de riesgos y reacción a riesgos.

Considerando que en las encuestas el personal identificó como principales fortalezas la formalidad de los procesos de la metodología de gestión de riesgos, los cuales son estándares, estructurados y sistematizados. Además, que se cuenta con visibilidad de la gestión en los niveles ejecutivos y una priorización basada en el apetito de riesgo alineado con negocio, consideramos que el dominio Gobierno de Riesgos, se encuentra en un nivel de madurez aceptable. Por esta razón, la concentración de esta propuesta estará enfocada en la mejora de los procesos y herramientas correspondientes a los dominios 2 (Evaluación de Riesgos) y 3 (Respuestas a Riesgos) mencionados anteriormente.

Adicionalmente, las principales oportunidades de mejora que identificó el personal en el diagnóstico de situación actual corresponden a estos dos dominios.

Para efectos de realizar una propuesta que solvente las necesidades y oportunidades de mejora identificadas se debe:

1. Definir una guía para facilitar la identificación de riesgos de operación tomando como base el catálogo de escenarios de riesgos, planteada por el Risk IT, como se ejemplifica en la Figura 41.

2. Proponer una plantilla para el registro de nuevos riesgos de operación que considere dentro del análisis del riesgo diferentes variables (como por ejemplo: frecuencia, impacto en confidencialidad de la información, impacto en la disponibilidad, impacto en imagen, impacto legal, etc.) con el objetivo de estandarizar, simplificar y hacer más predecible la evaluación de los riesgos cuando se incluyen nuevos riesgos, reduciendo la subjetividad en la calificación.
3. Incorporar la cuantificación de los costos tangibles e intangibles y posibles ahorros al aplicar los planes de respuesta, calculando el retorno de inversión que se tendría por cada dólar invertido en prevención y/o evaluación. Lo anterior se propone con el fin de reforzar la efectividad del modelo al contar con insumos adicionales que facilitarán la priorización de los riesgos utilizando variables monetarias.
4. Unificar en un único repositorio toda la información relacionada con los riesgos de manera que se simplifique el uso de la información y se reduzca la dispersión de los datos en múltiples hojas de cálculo (Excel).
5. Automatizar, a corto plazo, los instrumentos actuales de identificación de riesgos y planes utilizando la herramienta Sharepoint con el fin de hacer más eficiente y confiable el proceso de gestión de riesgos. A largo plazo, se considera necesario ampliar la propuesta hecha en el piloto o buscar una solución automatizada de gestión integral de riesgos para hacer más eficiente la gestión y seguimiento de planes.
6. Mejorar el enfoque de los esfuerzos del personal y los recursos de la organización brindando respuestas a los riesgos de mayor peso, considerando los parámetros para seleccionar la respuesta a los riesgos, como se ejemplifica en la Figura 42 y 43.

Figura 41 Fuente: The Risk IT Practitioner Guide. Componentes de un escenario de Riesgo de TI

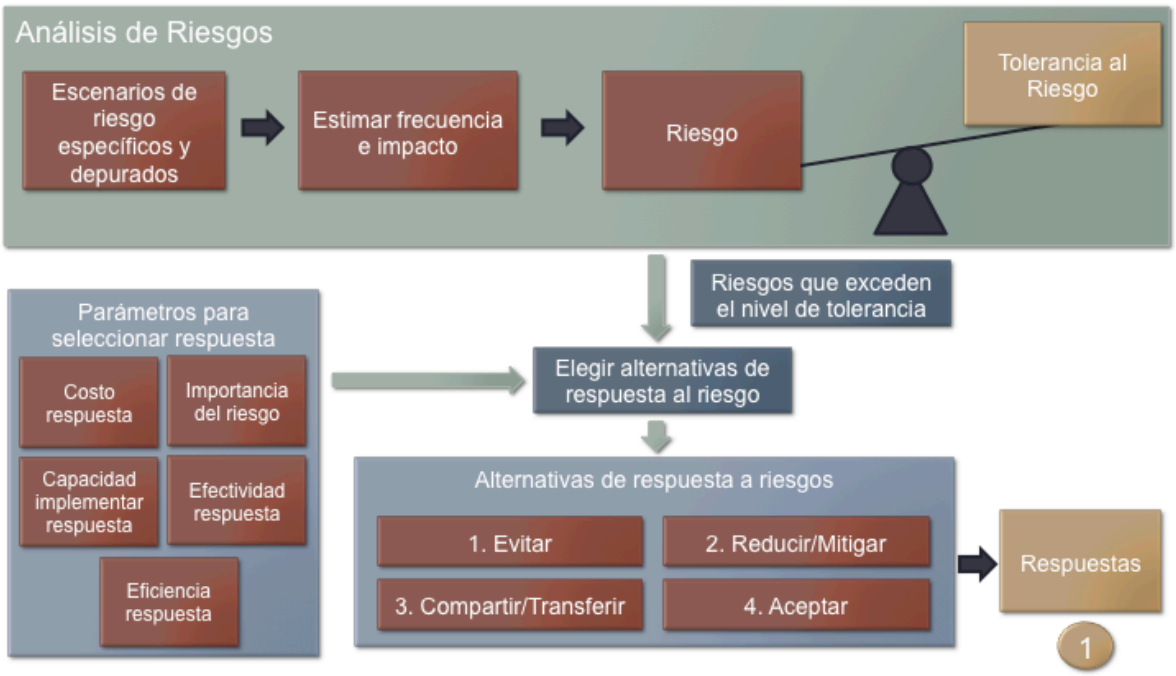


Figura 42 Fuente: The Risk IT Practitioner Guide. Flujo de Respuesta y Priorización para Riesgos

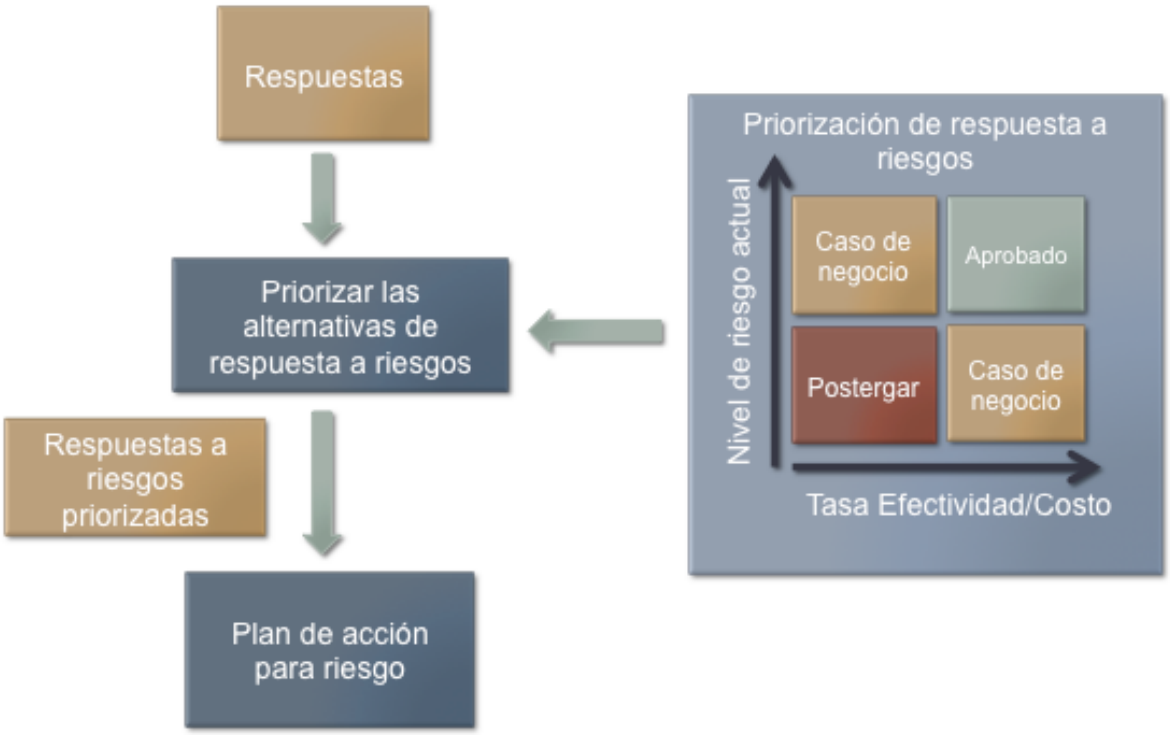


Figura 43 Fuente: The Risk IT Practitioner Guide. Flujo de Respuesta y Priorización para Riesgos

Adicionalmente, a partir de la aplicación de los instrumentos a los dos grupos seleccionados como muestra, en esta investigación logramos identificar otras oportunidades de mejora relacionadas mayoritariamente con capacitación y conocimiento sobre diferentes conceptos, lo cual generó que se encontraran respuestas contradictorias entre ambos grupos encuestados.

Para la atención de los anteriores hallazgos se propone que la Gerencia Regional de Riesgos y Seguridad capacite a la población involucrada en la metodología de gestión de riesgos (ejecutores y responsables) con el fin de esclarecer la terminología y aclarar cuál es la metodología base para implementar la gestión de riesgos organizacional y su relación con el resto de conceptos.

Por otro lado, es necesario aclarar la diferencia entre costos tangibles y costos intangibles, además de indicar las variables monetarias que se están contemplando actualmente dentro de la metodología y las que podemos llegar a manejar como parte del resultado de la presente investigación.

Retomando la metodología de gestión de riesgos utilizada actualmente por la organización, a continuación se presenta el ciclo de gestión propuesto:

Figura 44 Ciclo de Gestión de Riesgos Operativos. Fuente: Metodología Riesgos Operativos BAC

Realizando una comparación de la metodología actual con la metodología propuesta, podemos encontrar las siguientes diferencias:

Característica	Metodología actual	Metodología Propuesta
Enfoque	Orientada a la detección de riesgos en procesos. Los riesgos tecnológicos se consideran como un apéndice de esta metodología macro organizacional. La metodología es la misma para toda la organización y es particular para TI.	Es una metodología para la gestión integral (tecnológicos y de procesos) de riesgos en TI la cual se integra a la gestión de riesgos corporativa.

Evaluación de riesgos	Evalúa los riesgos únicamente a nivel cualitativo, no incorpora variables monetarias en la calificación del riesgo.	Incorpora una evaluación cuantitativa (pérdidas económicas) adicional a la valoración cualitativa.
Respuesta a riesgos	Únicamente considera la Mitigación como posible estrategia de respuesta cuando la evaluación del riesgo supera el apetito de riesgo.	Permite seleccionar otras estrategias de respuesta como Evitar, Transferir o Aceptar cuando el riesgo supera el apetito de riesgo de la organización.
Efectividad de los planes	No cuestiona la efectividad y costo de las acciones de respuesta antes de confirmarlos como planes de acción.	Permite analizar el costo y efectividad de cada acción de respuesta para que el evaluador defina si la acción debe formar parte del plan de acción.
Control de planes	Documenta fechas de inicio y fin dentro de cada plan dentro de la misma metodología, duplicando un esfuerzo o actividad que debe corresponder a la gestión de proyectos.	Únicamente documenta el responsable de cada plan y se apalanca sobre la gestión de proyectos para priorizar y dar seguimiento a la ejecución de los planes.
Cantidad de fases (dominios)	Incorpora fases que se consideran muy operativas (poco estratégicas) como por ejemplo la Generación de reportes.	Establece únicamente tres fases (dominios) de alto nivel centradas en los aspectos estratégicos de la gestión de riesgos y los aspectos operativos se ven dentro de cada fase.

Tabla 8 Comparación Metodología actual vs Propuesta. Fuente Propia

11.2. Desarrollo de la solución

El propósito de este capítulo consiste en explicar en detalle cómo se logró la implementación de cada uno de los componentes mencionados dentro de la propuesta de solución.

11.2.1. Catálogo de escenarios de Riesgos

Para desarrollar la propuesta, uno de los elementos claves de la misma es el catálogo de escenarios de riesgo. Este es un documento con una estructura estándar que permite documentar, mantener y extender un inventario de todos los diferentes escenarios de riesgos posibles que puedan impactar negativa o positivamente las operaciones. Esta herramienta permitirá que el ejercicio de identificación de riesgos sea mucho más ordenado y guiado facilitándoles a los usuarios canalizar su creatividad y conocimiento de los sistemas, permitiéndoles documentar los nuevos riesgos de manera estructurada y ordenada.

El catálogo de escenarios de riesgos propuesto para el desarrollo de la solución y utilización durante el piloto se encuentra en el Anexo 5. Dicho documento se documentó con 32 escenarios de riesgos genéricos que aplican en forma directa a las operaciones de tecnología o su capacidad para prestar servicios tecnológicos. Estos escenarios genéricos forman parte de las recomendaciones de las mejores prácticas de gestión de riesgos de ISACA. No obstante, el inventario no está limitado exclusivamente a los escenarios actualmente documentados, por lo que es posible extender el contenido incluyendo nuevos escenarios que los usuarios de la metodología propongan y que puedan ser utilizados a futuro.

El catálogo de escenarios de riesgos fue incorporado como parte de la aplicación desarrollada en Sharepoint con el fin de que pueda ser consultado en línea por parte de los usuarios y de esta manera evitar manejar múltiples versiones en archivos Excel.

La taxonomía del catálogo de escenarios de riesgos es la siguiente:

Jerarquía	Campo	Descripción
1	Número	Código identificador único del escenario de riesgo
2	Escenario de riesgo de Alto Nivel	Nombre único del escenario de riesgo de alto nivel
2.1	Componentes del escenario de riesgo	Título para agrupar los diferentes componentes del escenario de riesgo
2.2	Actor	Figura que genera la amenaza, puede ser interno o externo, puede ser humano o una persona jurídica o intangible: Alternativas: 1. Interno: Se encuentran dentro de la organización. Pueden ser colaboradores o contratistas) 2. Externo: Son foráneos a la organización como competidores, socios de negocio, reguladores y el mercado) No todo tipo de amenaza requiere un actor como por ejemplo, las fallas o las causas naturales
2.3	Tipo de Amenaza	Tipo de amenaza se refiere a la naturaleza del evento. Alternativas: 1. Malicioso 2. Accidental/error

		3. Falla 4. Natural 5. Requerimiento externo
2.4	Evento	Es una revelación (de información confidencial), interrupción (de un sistema/proyecto), Robo o destrucción. La acción también puede incluir diseño inefectivo (de sistemas, procesos, etc.) o ejecución inefectiva de procesos (pe, procedimientos de gestión de cambios, procedimientos de adquisición, procesos de priorización de proyectos, etc.) Alternativas: 1. Revelación 2. Interrupción 3. Modificación 4. Robo 5. Destrucción 5. Diseño inefectivo 6. Ejecución inefectiva 7. Leyes y regulaciones 8. Uso inapropiado
2.5	Activo/Recurso	Activo o recurso (que se ve involucrado en el escenario del riesgo). Un activo es cualquier objeto de valor para la organización que puede ser afectado por el evento y llevar a provocar un impacto al negocio. Un recurso es cualquier cosa que contribuye a

		alcanzar los objetivos de TI. Los activos y los recursos pueden ser idénticos, por ejemplo., el hardware de TI es un recurso importante porque todas las aplicaciones de TI lo utilizan, y al mismo tiempo, es un activo porque tiene cierto valor para la organización. Activos/recursos pueden incluir: 1. Personal y organización 2. Procesos de TI (COBIT) o de negocio 3. Infraestructura (instalaciones, equipos) 4. Infraestructura de TI 5. Información 6. Aplicaciones
2.6	Criticidad del recurso	Identifica si el recurso afectado por el escenario de riesgo es crítico o no. Los activos pueden ser críticos o no críticos. Los recursos críticos normalmente van a atraer un mayor número de ataques o mayor atención en caso de una falla, por esta razón la frecuencia de los escenarios relacionados a dichos activos probablemente sean más altas vs otros recursos no críticos. Se requiere mucha habilidad, experiencia y amplio entendimiento de las dependencias para comprender las diferencias entre un activo crítico y uno que no lo es.
2.7	Dimensión de	Esta variable puede utilizarse para describir si es

	Tiempo	relevante para el escenario: 1. La duración del evento (una caída prolongada de un servicio o centro de datos) 2. La estacionalidad (analiza si el evento ocurrió en un momento crítico) 3. Oportunidad de consecuencias: Tiempo transcurrido entre el evento y sus consecuencias (Inmediato: caída inmediata de un sistema, falla en la red o una consecuencia retrasada generada por una arquitectura de TI inadecuada que genera altos costos con el transcurrir del tiempo en muchos años. 4. Oportunidad para detección: Oportunidad con que se detecta el evento. Alternativas: 1. Estacionalidad (crítico/no crítico) 2. Duración 3. Detección 4. Oportunidad de consecuencias
3	Impacto de Riesgo	Alternativas: 1. Directo: El riesgo impacta directamente las operaciones de tecnología o la capacidad para prestar servicios tecnológicos. 2. Indirecto: El riesgo impacta de forma directa la capacidad de la tecnología para agregar valor o dar

		beneficio al negocio o bien la capacidad de entregar programas y proyectos de tecnología al negocio pero las operaciones sufren indirectamente las consecuencias.
4	Riesgo	Título para agrupar la descripción de escenarios negativos y positivos de los riesgos
4.1	Ejemplos de escenarios negativos	Descripción general de la situación negativa asociada al escenario de riesgo
4.2	Consecuencias negativas riesgo	Título para agrupar las pérdidas asociadas a los ejemplos de escenarios de riesgos negativos.
4.2.1	Pérdida de Oportunidad	Se relaciona a la pérdida de oportunidades de utilizar la tecnología para mejorar la eficiencia o efectividad de los procesos del negocio, o utilizar la tecnología como un habilitador para nuevas iniciativas del negocio. Cuando se marca esta columna significa que esta consecuencia implica pérdida de ganancias o beneficios para el negocio.
4.2.2	Pérdida de Valor	Se relaciona a la pérdida de oportunidades de utilizar la tecnología para mejorar la eficiencia o efectividad de los procesos del negocio, o utilizar la tecnología como un habilitador para nuevas iniciativas del negocio. Cuando se marca esta columna significa que esta consecuencia implica destrucción de valor.
4.3	Ejemplos de	Descripción general de la situación positiva

	escenarios positivos	asociada al escenario de riesgo
4.4	Consecuencias positivas riesgo	Título para agrupar las ganancias asociadas a los ejemplos de escenarios de riesgos positivos.
4.4.1	Ganancia de valor	Se relaciona a la generación de oportunidades de utilizar la tecnología para mejorar la eficiencia o efectividad de los procesos del negocio, o utilizar la tecnología como un habilitador para nuevas iniciativas del negocio. Cuando se marca esta columna las consecuencias del riesgo implican la obtención de ganancias o beneficios para el negocio a partir del aprovechamiento de oportunidades.
4.4.2	Preservar valor	Se relaciona a la generación de oportunidades de utilizar la tecnología para mejorar la eficiencia o efectividad de los procesos del negocio, o utilizar la tecnología como un habilitador para nuevas iniciativas del negocio. Cuando se marca esta columna las consecuencias del riesgo implican la preservación de valor para el negocio a partir del aprovechamiento de oportunidades.

Tabla 9 Taxonomía del catálogo de Riesgos. Fuente: Risk

11.2.2. Herramienta de evaluación de Riesgos

El segundo componente clave asociado a la propuesta de solución corresponde a la herramienta de evaluación de riesgos. Esta herramienta comprende el formulario utilizado para la identificación de nuevos riesgos y la guía para la identificación de riesgos utilizando el catálogo propuesto en el apartado anterior de este documento.

11.2.2.1. *Formulario para identificación de riesgos*

Para efectos de estandarizar, simplificar y reducir la cantidad de herramientas utilizadas en la gestión de riesgos (mayoritariamente hojas de Excel), se desarrolló en Sharepoint un formulario automatizado, accesible únicamente para los usuarios autorizados para uso de la herramienta. Dicho formulario fue construido con base a un prototipo de la plantilla para la identificación de riesgos que se incluye en el Anexo 6.

El formulario consta de las siguientes secciones:

Sección	Descripción	Propósito
I	Resumen del Riesgo	Brindar al usuario una vista global del riesgo identificando las características más relevantes del riesgo.
II	Descripción del Riesgo	Detallar el riesgo y su alcance, a que escenario de riesgo de alto nivel está relacionado (proveniente del catálogo de escenarios de riesgos)
III	Resultados del Análisis del Riesgo	Documenta las variables cualitativas que permiten calcular una calificación general del riesgo y los parámetros cuantitativos adicionales que facilitarán posteriormente la priorización de los riesgos dentro de una misma categoría.

IV	Respuesta al Riesgo	Permite seleccionar la(s) estrategia(s) general de respuesta al riesgo y las acciones específicas con sus respectivos costos y contribución a la atención del riesgo.

Tabla 10 Secciones del formulario para identificación de riesgos. Fuente propia.

Las primeras tres secciones tienen relación directa con la herramienta de evaluación de riesgos y serán detalladas a continuación. La sección IV se explicará en la siguiente sección 4.3 “Herramienta de Respuesta a Riesgos” de este documento.

11.2.2.1.1. Sección I - Resumen del riesgo

Esta sección contiene los elementos más importantes que describen el riesgo documentado en dicho formulario. La intención es que pueda brindar de una sola vista toda la información relevante para un revisor o tomador de decisiones. En caso de que surja alguna duda, puede profundizar en el detalle incorporado en las siguientes secciones.

El detalle y significado de los campos que se incorporaron en esta sección se encuentran en el Anexo 10.

En la aplicación desarrollada en Sharepoint todos los campos de esta sección son únicamente de lectura puesto que se documentan o calculan en las secciones subsiguientes.

11.2.2.1.2. Sección II – Descripción del Riesgo

El propósito de esta sección es realizar una descripción detallada del riesgo y su alcance. Adicionalmente se clasifica el riesgo relacionándolo a uno de los de escenarios riesgo de alto nivel (proveniente del catálogo de escenarios de riesgos) con el objetivo de poder hacer agrupaciones para análisis posterior.

Los campos que se incorporaron en esta sección son: Enunciado del Riesgo, Dueño del Riesgo, Canal Afectado, Servicio Afectado, Escenario de riesgo de alto nivel, Descripción detallada del escenario e Información adicional del escenario.

Un mayor detalle del significado de cada campo se puede encontrar en el Anexo 11.

11.2.2.1.3. Sección III - Resultados del Análisis del Riesgo

El propósito de esta sección consiste en asignar al riesgo documentado una calificación general a partir de las características de frecuencia e impacto cualitativo. Adicionalmente se documentan por parte del evaluador algunas variables críticas que se utilizarán para determinar el impacto cuantitativo. Los datos de impacto cuantitativo no tendrán incidencia en la calificación general del riesgo pero se pueden utilizar como un criterio de priorización adicional a la calificación general del riesgo o bien como un insumo para calcular el retorno de inversión sobre los planes definidos para cada riesgo.

La información que se captura en esta sección está clasificada en las siguientes agrupaciones que se detallaran posteriormente:

Agrupación	Descripción
Frecuencia del riesgo	Determina la frecuencia con que se presenta el riesgo al año, es un dato ingresado por el evaluador del riesgo en un rango que va de 1 a 5.
Impacto Cualitativo	Captura en un rango de 1 a 5, el impacto que el riesgo puede generar al negocio según cada una de las siguientes dimensiones: Confidencialidad, Integridad, Disponibilidad, Imagen y Legal

	(Cumplimiento Regulatorio)
Impacto Cuantitativo	A partir de variables críticas, se realiza una estimación del costo que puede generar cada riesgo según la dimensión a la que pertenece.
Calificación general del riesgo	Determina la calificación asignada al riesgo según el mapa de calor de riesgos definido por la organización.

Tabla 11 Agrupaciones Información Análisis de Riesgo. Fuente Propia.

11.2.2.1.3.1. Frecuencia del Riesgo

La frecuencia del riesgo se identifica dentro de una escala logarítmica que clasifica las veces que el evento puede ocurrir en un período de un año.

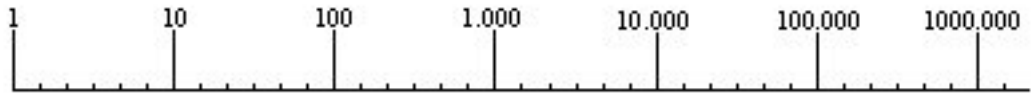


Figura 45 Escala logarítmica. Fuente: http://www.scribd.com/doc/145713459/Escala-logaritmica#scribd

Existen otras variables que pueden afectar la frecuencia con la que ocurre un evento como son la explotabilidad y la exposición de la vulnerabilidad asociada al riesgo, en caso que estos criterios apliquen. Por otro lado, la frecuencia con la que han ocurrido en el pasado incidentes similares al riesgo que se está documentando es un insumo importante a considerar para seleccionar la frecuencia del riesgo.

Cada riesgo se debe clasificar dentro de cualquiera de las siguientes categorías:

Calificación de frecuencia	Veces que ocurre al año	Exposición	Explotabilidad
1	0.01	Vulnerabilidad poco conocida, presente en pocas ubicaciones	Se requiere alto grado de conocimiento y/o esfuerzo de la amenaza para poder explotar la vulnerabilidad
2	0.1		
3	1	Vulnerabilidad es accesible por las amenazas de forma limitada, está presente en varias localizaciones pero no es muy conocida.	La amenaza requiere un grado intermedio de conocimiento y/o un esfuerzo significativo para poder explotar la vulnerabilidad.
4	10		
5	100	Vulnerabilidad fácilmente accesible por las amenazas, presente en muchas ubicaciones o es muy conocida	La amenaza no requiere de conocimiento especializado para explotar la vulnerabilidad y/o no necesita de un esfuerzo considerable para explotarla.

Tabla 12 Calificación de frecuencia de riesgos. Fuente Propia

11.2.2.1.3.2. Impacto Cualitativo

El impacto cualitativo del riesgo se determina estimando el grado de afectación que tiene el riesgo para el negocio analizando cada una de las siguientes dimensiones:

1. Confidencialidad
2. Integridad
3. Disponibilidad
4. Imagen
5. Cumplimiento Regulatorio

Esta evaluación cualitativa es la misma que utiliza la metodología de riesgos actual y no se consideró necesario en este momento hacer algún tipo de ajuste o variación a la forma en que se calcula.

La asignación del grado de severidad de impacto para cada dimensión, depende del juicio experto y el conocimiento del evaluador sobre el servicio de TI analizado. El evaluador del riesgo debe definir el nivel de afectación correspondiente para cada una de las dimensiones anteriores. En caso que la dimensión no aplique para el riesgo en cuestión, se debe seleccionar la opción de No Aplica (NA). Esta última alternativa excluye del cálculo de riesgo la dimensión seleccionada.

Cada dimensión se puede definir entre 5 diferentes niveles de afectación, según se describe en la tabla incluida en el Anexo 12.

Una vez que se definió por parte del evaluador de riesgo, el nivel de afectación correspondiente para cada una de las dimensiones anteriores, se calcula el **Impacto Final del riesgo** que corresponde al promedio del nivel de afectación de cada una de las dimensiones que apliquen y tengan un valor asignado. En caso que el promedio contenga decimales, se realiza un redondeo hacia el siguiente número entero. Como datos informativos también se identifica el valor máximo de nivel de afectación asignado las diferentes dimensiones y también el impacto porcentual que corresponde al promedio de nivel de afectación expresado en una escala porcentual tomando como máximo el valor de 5.

Con el Impacto Final del riesgo más la calificación de la Frecuencia, es posible determinar la calificación general del riesgo. Esto se realiza ubicando dentro del mapa de calor incluido en el Anexo 13, la frecuencia y el Impacto. El valor que se encuentre en la celda de la matriz corresponde a la calificación general del riesgo.

Para explicar de una manera más clara, el método de cálculo a continuación se presenta un ejemplo de una calificación de riesgo.

Sección III - Resultados del Análisis del Riesgo							
Frecuencia del riesgo (número de veces al año)	1	2	3	4	5		
	N<=0.1	0.1<=N<=1	1<=N<=10	10<=N<=100	100<N		
	☐	☐	☒	☐	☐		
Comentarios adicionales sobre frecuencia							
	Impacto Cualitativo						
Impacto del riesgo en el negocio	1	2	3	4	5	NA	Impacto final
Confidencialidad			1				3
Integridad					1		5
Disponibilidad				1			4
Imagen		1					2
Cumplimiento Regulatorio						1	
Impacto general (promedio de los cinco rangos de impacto)						Promedio	3.5
						Máximo	5
						Impacto Porcentual	70

Figura 46 Evaluación de Riesgos Cualitativos. Fuente Propia.

La frecuencia se calificó en nivel 3. El Impacto Final del riesgo se calculó en 3.5, el cual corresponde al promedio considerando únicamente las dimensiones que tienen calificación asignada. Como se mencionó anteriormente el Impacto Final se redondea al siguiente número entero por esta razón se asigna la calificación de 4.

Posteriormente identificamos dentro del mapa de calor la frecuencia y el impacto, encontrando que el nivel de riesgo que corresponde es Alto (3).

11.2.2.1.3.3. Impacto Cuantitativo

El impacto cuantitativo aplica cuando en la determinación del impacto cualitativo, se seleccionan para cada dimensión los niveles de afectación que conllevan una afectación económica a la organización, la cual puede ser estimada mediante algunas variables críticas asociadas a cada criterio o dimensión.

En el siguiente mapa de calor, se identifican en color naranja o rojo, los rangos definidos para las dimensiones o criterios usados en el impacto cualitativo, en los cuales se asocia que puede existir una afectación económica.

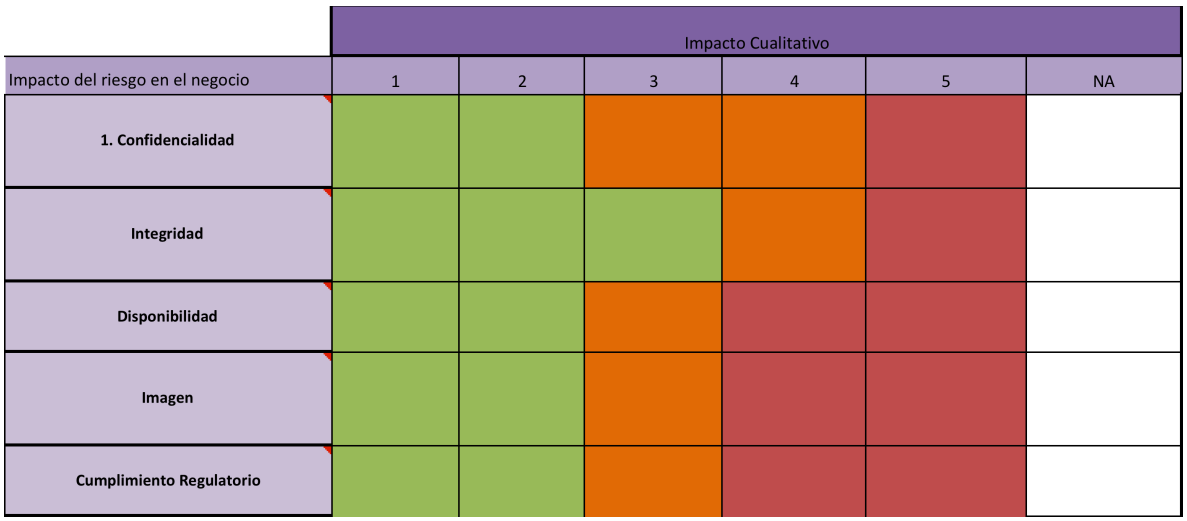


Figura 47 Mapa de calor para asignar impacto económico. Fuente propia.

En caso de que se seleccione alguno de los valores en color naranja o rojo, a continuación se listan las variables críticas que pueden documentar dentro de la herramienta con el fin de que se pueda realizar una cuantificación económica del riesgo a partir del valor que se indique. En esta sección se propone un modelo para estimar la pérdida a la que estaría sujeta la organización en caso que el riesgo se materialice a partir de estas variables críticas.

Criterio	Variable crítica	Estimación	Tipo Costo
Confidencialidad	Cantidad de registros con información privada, sensible o confidencial comprometidos	Se realiza una estimación de pérdidas monetarias tomando como unidad de cálculo cada registro de información comprometido.	Intangible
Integridad	Cantidad de registros críticos perdidos / dañados / alterados	Se realiza una estimación de pérdidas monetarias por datos dañados / alterados /perdidos.	Intangible
Disponibilidad	Total de transacciones afectadas durante tiempo fuera de servicio	Se realiza una estimación de pérdidas monetarias por el costo de utilizar canales sustitutos para la cantidad de transacciones afectadas.	Tangible
Imagen	Cantidad de usuarios impactados potencialmente por el riesgo	Esta variable es informativa, no fue posible derivar una estimación económica a partir de la misma.	Intangible
Cumplimiento Regulatorio	¿Riesgo implica la aplicación de multa	Se cuantifica el monto correspondiente a	Tangible

	regulatoria?	multas por incumplimiento regulatorio.	

Tabla 13 Variables críticas para estimación de costos. Fuente Propia

En el caso de las dimensiones de **Confidencialidad** e **Integridad** se realizó una propuesta para cuantificar el impacto económico, tomando como base el estudio global sobre violación de datos realizado por el Instituto Ponemon en el año 2014. En dicho estudio, se concluye que es posible asignarle un costo a cada registro comprometido (en términos de seguridad de información) o dañado. A nivel global, el costo de cada registro afectado es de $145 USD (Ponemon Institute, 2014). Sin embargo, fue posible realizar un cálculo específico para la organización utilizando una calculadora en línea provista por el Instituto Ponemon en conjunto con el proveedor de seguridad global Symantec (Symantec, 2013). Con esta herramienta el costo por registro afectado fue estimado en $133 USD y es el monto que será utilizado en el modelo y la herramienta. En el anexo 8 se incluye el informe personalizado que se generó a partir de dicha calculadora.

Para la dimensión **Disponibilidad**, posterior a realizar reuniones con la Gerencia Regional de Canales, se concluyó que el mayor costo de una afectación por disponibilidad para la organización (además del costo intangible por afectación de imagen), corresponde a la utilización de canales de mayor costo por parte de los clientes durante el tiempo de afectación del servicio. Por ejemplo, si el servicio de transferencia de fondos interbancario fallara por cuatro horas, el costo de que un cliente se vea obligado a utilizar cheques físicos en vez de transferencias a través de SINPE durante ese tiempo, se traduce en un costo operativo superior que la organización tiene que asumir como pérdida. Este costo será igual a la diferencia entre el costo operativo de cada transacción del canal de mayor costo versus el costo de hacer la misma transacción a través de la banca electrónica.

Para poder realizar esta estimación, se identificó el costo de utilizar un canal sustituto, donde fue posible, para cada uno de los servicios que se prestan a través del canal de banca electrónica, el cual se resume en la siguiente tabla:

Servicio	Costo Sustituto
Consulta Consolidada	$0.00
Consulta Banco	$0.10
Consulta Tarjeta	$0.10
Transf. Locales	$2.50
Pago de Tarjeta	$1.50
Consulta Afiliados	$5.00
Transf. otros Bancos	$5.00
Envío PPP	$25.00
Consulta Préstamo	$2.00
Pago de Préstamo	$2.50
Transf. Regionales	$15.00
Transf. Internacionales	$30.00
Consulta OPC	$0.00
Consulta Certificado	$0.00
Consulta SFI	$0.00

Tabla 14 Costo por transacción de utilizar canal sustituto. Fuente propia

De esta forma, cuando se identifica un riesgo que tiene una afectación de un único servicio entonces se cuantifican la cantidad de transacciones que se pueden ver impactadas potencialmente por dicho riesgo y mediante una multiplicación simple se puede estimar el impacto que genera que el servicio no esté accesible para los cliente.

Para el caso de riesgos que puedan impactar de manera general todos los servicios, dado que afectan la disponibilidad completa del canal de banca electrónica, se consideró el porcentaje del volumen transaccional que representa cada uno de los servicios mensualmente. Para calcular el porcentaje se analizaron los últimos 6 meses del 2014, encontrando que existe mucha consistencia entre todos los meses.

A continuación se resume el porcentaje que cada servicio representa.

Servicio	Porcentaje mensual que representa
Consulta Consolidada	48.64%
Consulta Banco	27.77%
Consulta Tarjeta	14.34%
Transf. Locales	3.50%
Pago de Tarjeta	1.84%
Consulta Afiliados	1.40%
Transf. otros Bancos	1.07%
Envío PPP	0.57%
Consulta Préstamo	0.46%
Pago de Préstamo	0.12%
Transf. Regionales	0.11%
Transf. Internacionales	0.07%
Consulta OPC	0.07%
Consulta Certificado	0.05%
Consulta SFI	0.01%

Tabla 15 Distribución porcentual de volumen transaccional por tipo transacción. Fuente propia.

A partir de los datos anteriores, si un riesgo se documenta de forma que afecta un único servicio, entonces se calcula la afectación por Disponibilidad de manera individual multiplicando la cantidad de transacciones afectadas potencialmente por el costo de utilizar un canal sustituto para el servicio en particular. Pero si un riesgo se documenta de forma que afecta todos los servicios del canal, entonces la cantidad de transacciones afectadas se considera como la cantidad general de transacciones que procesan todos los servicios conjuntamente y esta cifra se desglosa según el porcentaje descrito en la tabla anterior. La afectación por Disponibilidad se calcula realizando una sumatoria de la estimación de cada servicio individual prorrateando las transacciones afectadas en general según los porcentajes anteriores.

Para ejemplificar de manera más clara, lo indicado anteriormente a continuación se presenta un cálculo para una afectación individual de un servicio y una afectación general (todos los servicios) de 1,500 transacciones.

Servicio	Costo Sustituto	Porcentaje	Cálculo General	Cálculo Individual
Consulta Consolidada	$0.00	48.64%		
Consulta Banco	$0.10	27.77%	$41.65	$150.00
Consulta Tarjeta	$0.10	14.34%	$21.50	$150.00
Transf. Locales	$2.50	3.50%	$131.37	$3,750.00
Pago de Tarjeta	$1.50	1.84%	$41.36	$2,250.00
Consulta Afiliados	$5.00	1.40%	$104.77	$7,500.00
Transf. otros Bancos	$5.00	1.07%	$80.37	$7,500.00
Envío PPP	$25.00	0.57%	$212.33	$37,500.00
Consulta Préstamo	$2.00	0.46%	$13.74	$3,000.00
Pago de Préstamo	$2.50	0.12%	$4.38	$3,750.00
Transf. Regionales	$15.00	0.11%	$24.09	$22,500.00
Transf. Internacionales	$30.00	0.07%	$33.50	$45,000.00
Consulta OPC	$0.00	0.07%		
Consulta Certificado	$0.00	0.05%		
Consulta SFI	$0.00	0.01%		
		Costo Total No Disponibilidad del canal (todos los servicios)	$709.06	

Tabla 16 Ejemplo cuantificación de costos individual vs general. Fuente Propia

Al tratar de analizar el impacto económico de la dimensión **Imagen**, se propuso la variable “Cantidad de usuarios impactados potencialmente por el riesgo”. A partir de esta variable se realizaron diferentes intentos para lograr cuantificar de una manera aproximada costo monetario que esto puede representar. Una alternativa que se consideró y propuso fue la posibilidad de estimar la afectación en la rentabilidad de algunos clientes actuales o potenciales, posterior a recibir un comentario o retroalimentación negativa por parte de otra persona que tuvo una mala experiencia con los servicios del banco. Otra alternativa consideraba el efecto de una mala reputación en redes sociales y cómo impacta económicamente a la organización pero no aplica directamente para esta propuesta.

El principal inconveniente con los problemas de imagen es la dificultad que existe para anticipar el impacto que puede generar un riesgo. El impacto de imagen de un riesgo va a estar determinado por: a que clientes afecta y por cuánto tiempo. Estimar con cierto nivel de precisión estas variables es muy complejo por la aleatoriedad de los eventos, según el criterio de la gerencia de canales.

Debido a esto, la conclusión es que no es viable ni recomendable realizar una cuantificación económica de la dimensión Imagen. Al menos no dentro de este trabajo de investigación y con el tiempo disponible pues existen muchos elementos aleatorios que pueden variar positiva o negativamente el impacto que puede tener un riesgo y que podrían afectar la credibilidad en el modelo propuesto y la herramienta asignando valores que podrían ser cuestionados.

Por esta razón, se captura la variable “Cantidad de usuarios impactados potencialmente por el riesgo” como un dato informativo que puede ser utilizado como elemento de priorización más no se deriva ninguna estimación monetaria a partir de esta variable.

En el caso de la dimensión **Cumplimiento Regulatorio** (Legal) la estimación económica es mucho más directa comparado con las dimensiones anteriores. Principalmente porque los impactos están directamente relacionados con multas impuestas por la entidades regulatorias por incumplimientos. Para efectos de simplificar el modelo, se agruparon las variables en tres rangos de impacto:

1. $0 a $50,000
2. $50,000 a $500,000
3. $500,000 a $1,000,000

Estos montos aplican únicamente cuando la materialización del riesgo implica la aplicación de una multa por incumplimiento, lo cual queda a criterio del evaluador del riesgo.

Uno de los principales aportes del investigador para la nueva propuesta de evaluación de riesgos se encuentra en esta sección del formulario dado que se incorporan, además de las variables cualitativas, datos nuevos que permiten realizar estimaciones de elementos cuantitativos que anteriormente no se estaban considerando y que permitirán a los tomadores de decisiones contar con información adicional.

11.2.2.2. *Guía para la identificación de riesgos*

La guía para la identificación de riesgos es un documento que sirve de apoyo y orienta a la persona en la aplicación de nueva la metodología propuesta y el uso de la herramienta en Sharepoint para que pueda registrar nuevos riesgos dentro de la aplicación.

La guía para la identificación de riesgos propuesta se encuentra en el anexo 7.

11.2.3. Herramienta de respuesta a Riesgos

El último componente de la propuesta de solución corresponde a una herramienta para dar respuesta a los riesgos. La herramienta para definir la respuesta a los riesgos fue incorporada dentro del mismo formulario para identificación de riesgos dentro de la Sección IV - Respuesta al Riesgo. Esto con el fin de reducir la dispersión de la información y así facilitar la revisión futura del estado del riesgo, encontrando toda la información relevante en un único punto.

Los campos que se incorporaron en esta sección son:

Campo	Descripción
Respuesta seleccionada para este riesgo	Identifica la(s) estrategia(s) a utilizar para dar respuesta al riesgo documentado. Las opciones posibles son: Aceptar, Transferir, Mitigar o Evitar.

Justificación	Permite ingresar un comentario para justificar la razón del por qué se eligieron las estrategias de respuesta.
Descripción detallada de la respuesta (no aplica si la respuesta es Aceptar)	Es una subsección que permite documentar hasta 9 acciones de respuesta diferentes considerando para cada una: el costo, la tasa de efectividad/costo para resolver el riesgo, si forma parte del plan de acción y si fue completado o no.
Estatus general del plan de acción	Se utiliza para documentar cual es el estado de avance del plan a una fecha determinada.
Principales problemas con el plan de acción	Se utiliza para documentar y ampliar sobre posibles obstáculos con la ejecución del plan de acción definido.
Estatus general de las respuestas completadas	Permite ingresar un comentario con el detalle de la contribución de las acciones de respuesta que han sido finalizadas.
Principales inconvenientes con las respuestas completadas	Se utiliza para resumir los posibles problemas experimentados con las acciones de respuesta completadas.
Fecha de la última evaluación del riesgo:	Se utiliza para documentar cuando fue la última vez que se evaluó el riesgo.
Fecha de la próxima evaluación de riesgo:	Se utiliza para documentar cuando corresponde revaluar nuevamente el riesgo puesto que su calificación se considera que caducó. Es una buena práctica revalidar la calificación de los

	riesgos cada cierto tiempo.

Tabla 17 Campos Sección Respuesta a Riesgos. Fuente Propia.

El propósito de esta sección del formulario es determinar cuáles acciones son las que aplican para darle una respuesta a cada riesgo, de forma tal que dicha decisión sea conveniente para los intereses de la organización.

A nivel general, un riesgo puede recibir como respuesta cualquiera de las siguientes estrategias (Valdez, 2012):

Estrategia	Significado
Aceptar	Esta estrategia se adopta debido a que rara vez es posible eliminar todas las amenazas de una organización debido a que los costos pueden resultar prohibitivos. Se puede seleccionar esta alternativa cuando no se ha podido encontrar ninguna otra estrategia de respuesta adecuada (costo/efectiva o viable). La aceptación puede ser pasiva lo cual requerirá documentar la decisión únicamente y la aceptación activa que podría considerar el establecimiento de una reserva para contingencias.
Compartir/Transferir	Implica transferir a un tercero los efectos negativos de una amenaza y la potestad de asignar una respuesta. La transferencia de un riesgo simplemente confiere a una tercera persona la responsabilidad de su gestión; no elimina el riesgo. Esta alternativa se utiliza mucho en la exposición a riesgos financieros. Normalmente implica el pago de una prima a la parte que asume el riesgo. Las herramientas de transferencia incluyen contratos, seguros, garantías de cumplimiento, fianzas,

	certificados de garantía, etc. Ejemplo seguros: 1. Contra daños directos a la propiedad (Colisión de automóviles, Cobertura de equipos/materiales del proyecto, Seguro contra incendios y desastres naturales, Seguro contra robo) 2. Contra pérdidas por consecuencia indirecta (Seguro contra daños a terceros, reemplazo de equipo) 3. Protección por responsabilidad legal, penal, civil (daños a la entidad del proyecto producto de: Errores de diseño, errores durante la ejecución, Fallas en el desempeño del proyecto) 4. Seguros relacionados con el personal (Seguro contra lesiones físicas de los empleados, Costos de reemplazo de trabajadores)
Mitigar/Reducir	Mitigar el riesgo implica reducir a un umbral aceptable la probabilidad y/o el impacto de un evento adverso de manera que se encuentre dentro los límites de tolerancia de la organización (apetito de riesgo). El nivel de riesgo resultante posterior a aplicar los planes se le conoce como riesgo residual.
Evitar	Implica cambiar el objetivo, plan o tecnología a fin de eliminar por completo la amenaza que representa el

	riesgo adverso. Usualmente el riesgo se anula eliminando la causa o reduciendo la probabilidad de ocurrencia a cero.

Tabla 18 Estrategias para respuesta a Riesgos (Valdez, 2012)

Para cada riesgo, se debe utilizar la estrategia o combinación de estrategias adecuadas (y además efectivas) y luego desarrollar acciones específicas para implementar dicha estrategia.

Se considera una buena práctica, seleccionar estrategias de apoyo o refuerzo a la estrategia primaria, y/o un plan de reserva que será activado en caso que la estrategia seleccionada no resulte ser totalmente efectiva.

Lo que va a determinar qué tipo de respuesta debe darse a un plan es en primer lugar, la tolerancia al riesgo definida por la organización. Esto significa, cuales son los niveles de riesgo que la organización está dispuesta a tolerar.

Para el caso de la institución en la cual se realiza este trabajo de investigación, el apetito de riesgo está definido hasta los colores verde y amarillo del mapa de calor de riesgos incluido en el Anexo 13. Es decir, los niveles de riesgo bajo y medio no requieren de definir un plan de respuesta sino que se Aceptan por definición.

En cambio, los niveles de riesgo Alto y Crítico (colores naranja y rojo) si requieren ser analizados y elegir la estrategia y plan de respuesta a considerar.

Como se indicó en la propuesta de solución, una vez que conoce la calificación general de un riesgo (obtenida de combinar la frecuencia e impacto en el mapa de riesgos), si el nivel de riesgo supera el nivel de tolerancia establecido por la organización corresponde elegir una alternativa de respuesta al riesgo.

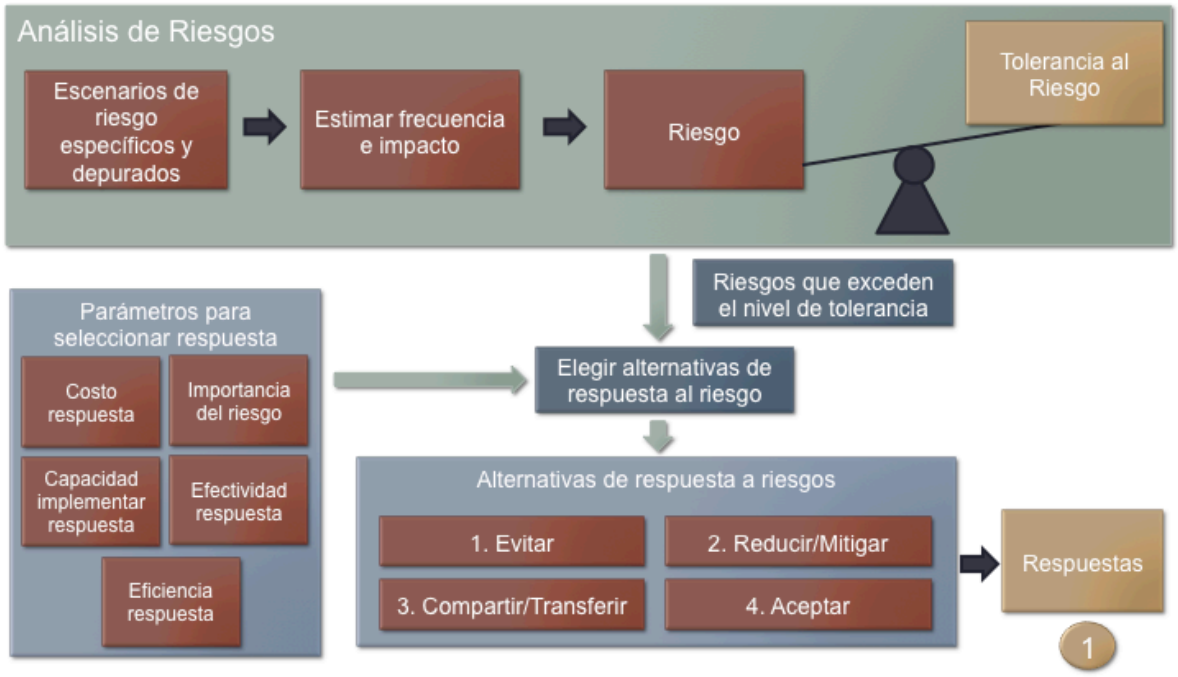


Figura 48 Flujo de Respuesta y Priorización para Riesgos Fuente: The Risk IT Practitioner Guide.

Al momento de seleccionar la alternativa de respuesta, se debe tomar en cuenta los parámetros que se describen a continuación (ISACA, 2009, p. 76):

Parámetros	Descripción
Costo de la respuesta para reducir la calificación del riesgo a niveles de tolerancia permitidos por la organización	En el caso de elegir como estrategia la trasferencia de un riesgo, este costo puede ser el valor de la prima de un seguro. En el caso de seleccionar mitigación como estrategia, correspondería al costo total de implementar las medidas de control (salarios, gastos de capital, consultorías, etc.)
Importancia del riesgo	Se refiere a la posición que ocupe la calificación del riesgo dentro del mapa de calor (la cual refleja la combinación

	de los niveles de frecuencia e impacto). A mayor frecuencia y/o impacto, mayor relevancia tendrá la respuesta que se elija.
Capacidad de la organización para implementar la respuesta	Está relacionado directamente a las habilidades de la organización para desarrollar el plan y el nivel de madurez que la organización tenga para afrontar dicha respuesta. Cuando la empresa es inmadura en sus procesos de gestión de riesgos, varias respuestas básicas podrían ser mejores que unas pocas sofisticadas.
Efectividad de la respuesta planteada	La magnitud en que la respuesta reducirá ya sea la frecuencia o el impacto del riesgo
Eficiencia de la respuesta planteada	Los beneficios relativos de una respuesta en comparación con: otras inversiones requeridas en TI y otras respuestas a riesgos (una respuesta podría resolver varios riesgos, otras solamente uno)

Tabla 19 Parámetros para seleccionar la alternativa de respuesta a un riesgo. Fuente: Risk IT

Una vez elegida(s) la(s) estrategia(s) a utilizar como alternativa de respuesta, se seleccionan dentro de la herramienta en la “Sección IV - Respuesta al riesgo” en el campo “Respuesta seleccionada para este riesgo”. Opcionalmente se puede detallar la justificación del porqué se eligen estas estrategias dentro del campo “Justificación”.

Con las estrategias de respuesta definidas, corresponde ahora definir las respuestas al riesgo que son planteamientos de acciones que se pueden ejecutar y que típicamente tendrán asociado un costo.

Las respuestas a los riesgos requieren muchas creatividad y análisis. A continuación se enumeran las características con las que debe cumplir una respuesta a un riesgo (Martinez):

Característica	Descripción
Apropiadas:	Las respuestas deben ser congruentes con la importancia del riesgo. Deben ser costo/efectivas en relación al desafío.
Ejecutables:	Ser realistas dentro del contexto de la organización e industria. Factibles técnica y legalmente.
Financiadas:	Cada respuesta debe tener un presupuesto acordado. La cantidad de tiempo, esfuerzo y dinero que se dedique al riesgo no debe exceder su presupuesto disponible.
A tiempo:	Algunos riesgos requieren acción inmediata, mientras que otros planes pueden quedar a la espera de priorización para su ejecución posterior.
Acordadas:	Estar acordadas por todas las partes implicadas y estar a cargo de una persona (“dueño”) que acepta su responsabilidad respecto a la implementación.
Evaluables:	Poder analizar la efectividad posterior a su implementación, durante el seguimiento a los riesgos.

Tabla 20 Características que una respuesta a un riesgo debe cumplir. Fuente: Martínez

Es muy común que el esfuerzo requerido para implementar las diferentes respuestas de mitigación excedan los recursos disponibles. En este caso, será necesario realizar un ejercicio de priorización para el cual se implementó una

matriz de decisión. Se debe ubicar cada propuesta de respuesta dentro de la matriz de cuatro cuadrantes ilustrada en la siguiente figura.

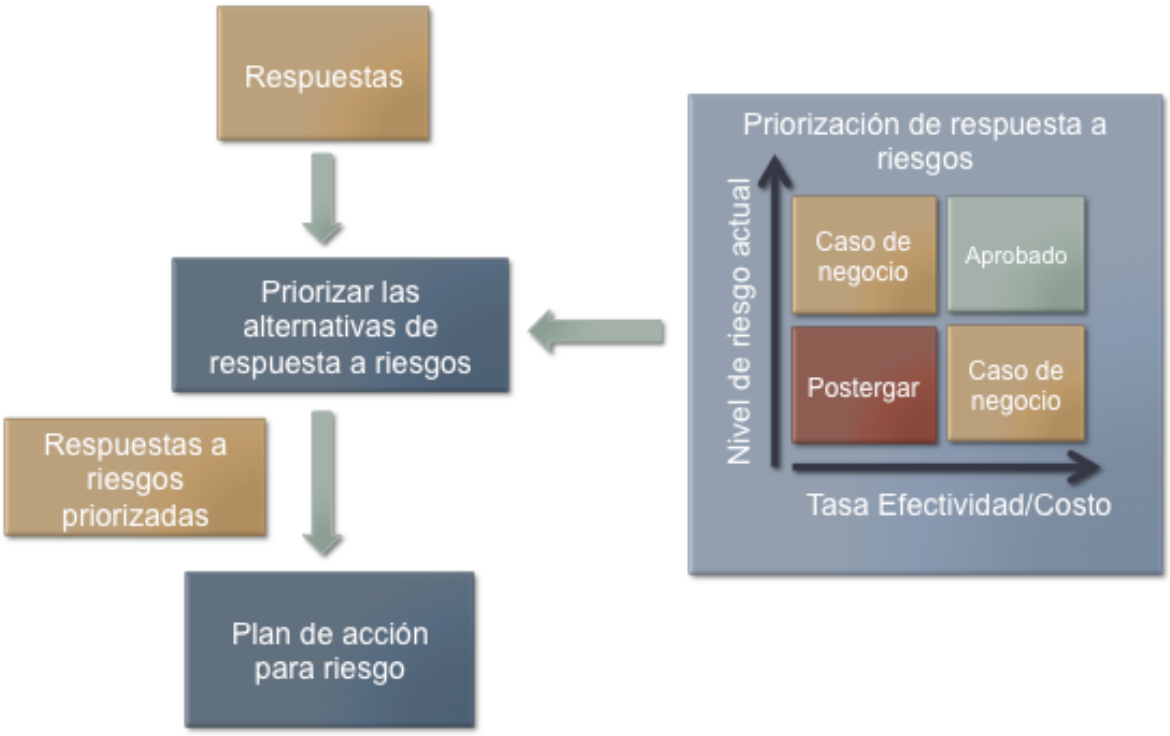


Figura 49 Fuente: The Risk IT Practitioner Guide. Flujo de Respuesta y Priorización para Riesgos

La matriz posee tres decisiones posibles descritas dentro de la siguiente tabla.

Decisión	Nivel Riesgo	Tasa Efectividad/ Costo	Descripción
Aprobado	Alto	Alto	Este tipo de planes son victorias rápidas dado que son respuestas muy eficientes y efectivas en la atención de riesgos con una calificación alta.
Caso de Negocio	Alto	Baja	Respuestas complejas o de alto costo para atacar riesgos con

			calificación alta, se requiere un análisis cuidadoso y una decisión de la administración acerca de las inversiones.
Caso de Negocio	Bajo	Alta	Respuestas eficientes y efectivas para riesgos con una calificación baja, se requiere un análisis cuidadoso y una decisión de la administración acerca de las inversiones.
Postergar	Bajo	Baja	Respuestas costosas a riesgos con una calificación baja.

Tabla 21 Matriz de decisión para respuesta a riesgos. Fuente Risk IT.

El nivel de riesgo que se indica en la tabla anterior, es un cálculo automático que realiza la herramienta agrupando la calificación general del riesgo Bajo (1) y Medio (2) como Nivel de Riesgo Bajo para efectos de la matriz de decisión y la calificación general del riesgo Alto (3) y Crítico (4) se considera Nivel de Riesgo Alto para efectos de la matriz de decisión.

La tasa de efectividad/costo es Alta cuando son respuestas eficientes y efectivas y se consideran Bajas cuando son complejas o costosas de implementar o bien no reducen significativamente el impacto o la frecuencia del riesgo.

A partir de la explicación anterior, se debe documentar dentro de la “Sección IV – Respuesta al Riesgo” cada una de las acciones de respuestas, el responsable, el costo que implica desarrollar dicha acción y su tasa de efectividad/costo. Con esta información, la herramienta calculará en forma automática el ahorro estimado en costos intangibles y la acción/decisión que se recomienda para el plan.

Este insumo de priorización, le permitirá a quien documenta el riesgo elegir cuáles de las diferentes acciones de respuesta serán las que queden formalizadas como parte del plan de acción de este riesgo, que se presentarán a la administración para luego integrarlos al Control de Ejecución de Planes aprobados, actividad que forma parte del Gobierno de Riesgos.

Teniendo claro lo anterior, es posible identificar dentro de la herramienta las acciones de respuesta que se definan como parte de plan de acción. Una vez finalizado este punto, será posible cuantificar el costo del plan de acción.

Con este último punto, se finaliza con la documentación del plan de acción en la herramienta de respuesta a los riesgos. Los siguientes pasos implican el análisis, priorización y aprobación de los riesgos y sus respectivos planes. Sin embargo, estas actividades corresponden al dominio de Gobierno de Riesgos el cual está fuera del alcance de esta investigación.

En el Anexo 9 se incorporan algunas copias de pantallas ejemplo de la herramienta diseñada en Sharepoint considerando todo lo descrito hasta ahora en este capítulo. Adicionalmente la herramienta junto con los datos capturados fue mostrada al profesor durante una reunión de seguimiento utilizando una conexión remota al servidor ubicado en la institución.

11.2.4. Indicadores de medición propuestos

Para efectos de evaluar y comparar la efectividad de la metodología propuesta versus la metodología actual se consideraron los siguientes indicadores:

1. Correlación de Riesgos vs Incidentes materializados
2. Nivel de satisfacción de clientes con la metodología (usuarios)
3. Identificación de costos (tangibles / intangibles) asociados a los riesgos

Para un mayor detalle sobre los indicadores, favor refiérase al Anexo 14 de este documento.

Analizando los indicadores anteriores aplicados a la metodología de gestión de riesgos utilizada actualmente por la organización se encuentran los siguientes resultados:

11.2.4.1.1. Correlación de Riesgos vs Incidentes materializados

Para efectos de poder medir la efectividad de la metodología actual se propone una comparación entre la cantidad de riesgos identificados según su criticidad comparados contra los incidentes según impacto que se han materializado para el servicio de banca electrónica.

Considerando lo anterior, se obtuvieron los siguientes datos correspondientes a los riesgos tecnológicos e incidentes identificados para el servicio de Banca Electrónica utilizando la metodología actual.

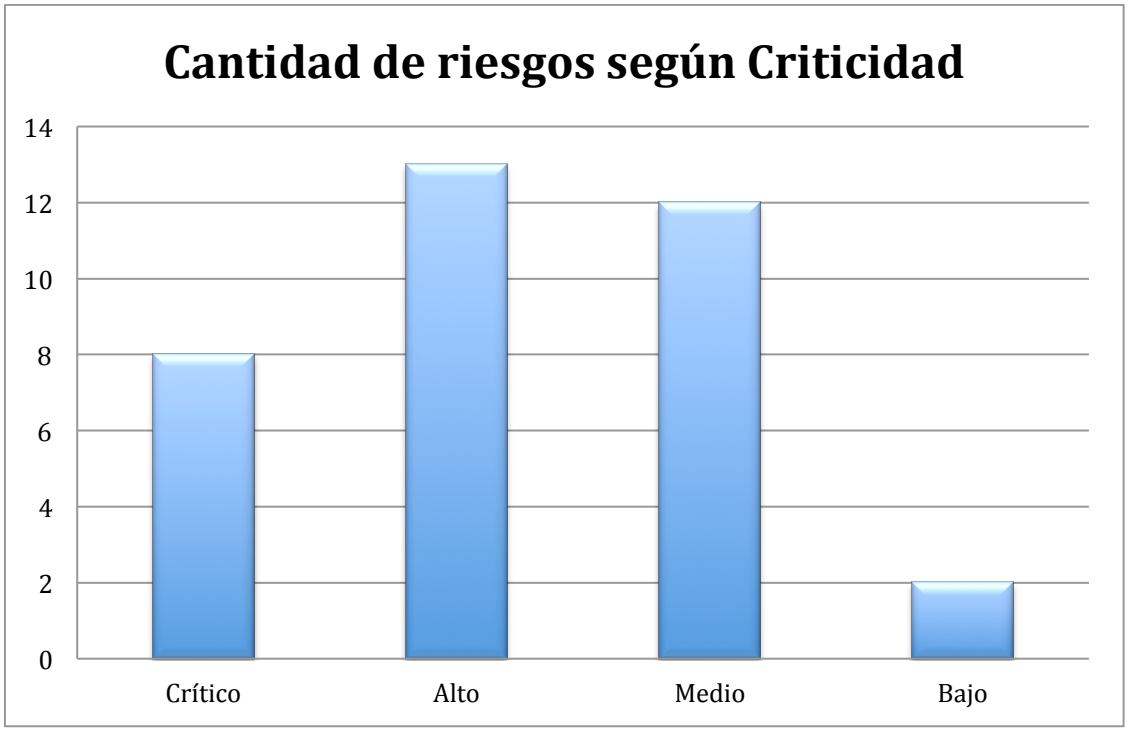


Figura 50 Cantidad de riesgos identificados por metodología actual según criticidad. Fuente propia.

Al analizar la composición de los mismos riesgos según criticidad se obtiene el siguiente gráfico de pastel:

Figura 51 Composición de riesgos identificados por metodología actual según criticidad. Fuente propia.

De la misma forma, se cuantificaron los incidentes clasificándolos según su criticidad y se obtuvo el siguiente resultado:

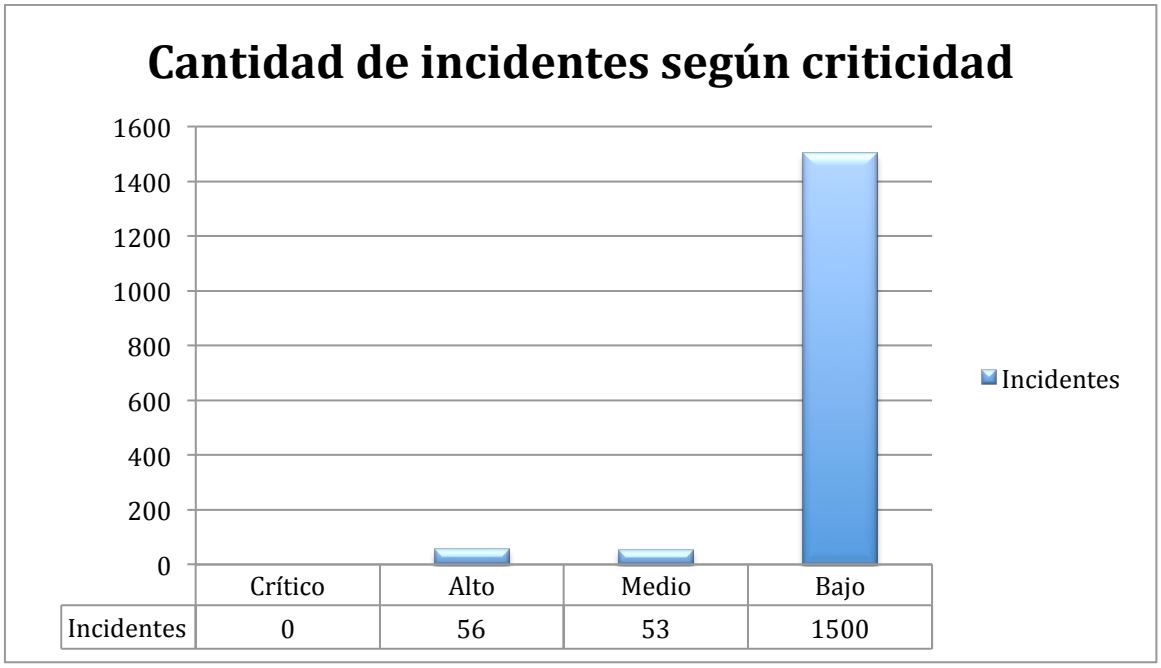


Figura 52 Cantidad de incidentes según criticidad 2014. Fuente propia.

Considerando que la cantidad de incidentes de criticidad baja se encuentra muy por encima de los valores de las demás categorías, se excluirán del análisis para no distorsionar el cálculo de la correlación y además mantener la concentración del análisis en los riesgos e incidentes más relevantes. Analizando únicamente en los riesgos e incidentes de criticidad Medio, Alto y Crítico se tabuló la información de incidentes y riesgos en una misma tabla y se calculó el coeficiente de correlación de Pearson encontrando como resultado que *para la metodología actual el coeficiente de correlación de Pearson entre incidentes y riesgos es de 0.99.*

Clasificación	Riesgos	Incidentes
Crítico	8	0
Alto	13	56
Medio	12	53

Tabla 22 Comparación de Riesgos e incidentes según criticidad. Fuente propia.

Esto significa que ambas variables tienen correlación muy alta como se puede comprobar el siguiente gráfico donde se incluyeron las líneas de regresión lineal de ambas curvas.

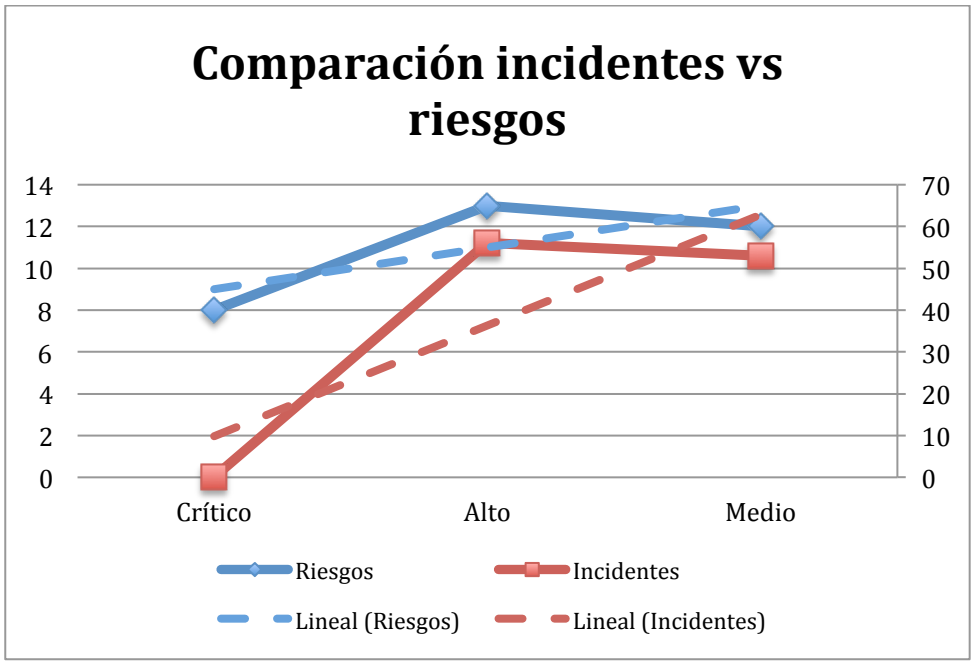


Figura 53 Comparación de incidentes 2014 vs riesgos identificados. Fuente propia.

11.2.4.1.2. Nivel de satisfacción

El nivel de satisfacción de gerentes y usuarios con la metodología actual fue cuantificado a través de la encuesta propuesta con el instrumento incluido en el Anexo 4.

El instrumento consideró la evaluación de los siguientes criterios:

1. Herramienta
2. Proceso guiado y predecible
3. Elementos cuantitativos para toma decisiones
4. Considera costos asociados para elegir respuesta
5. Nivel de satisfacción

Cada encuestado debió identificar para cada criterio, su nivel de satisfacción en siete posibles niveles.

11.2.4.1.2.1. Gerentes

De un total de 8 gerentes a quienes se les remitió la encuesta, respondieron 6 personas.

Los resultados generales de dicha encuesta se muestran a continuación en formato de mapa de calor.

Variable	Totalmente en desacuerdo	En desacuerdo	Ligeramente en desacuerdo	Neutral	Ligeramente de acuerdo	De acuerdo	Totalmente de acuerdo
Herramienta	1	3	0	0	2	0	0
Proceso guiado y predecible	0	3	0	0	3	0	0
Elementos cuantitativos para toma decisiones	2	1	1	0	2	0	0
Considera costos asociados para elegir respuesta	1	2	0	0	1	2	0
Nivel de satisfacción	0	2	1	0	3	0	0

Figura 54 Resultados encuesta de satisfacción con metodología de gestión de riesgos actual realizada a gerentes. Fuente propia.

De la anterior tabla se puede apreciar que existe una concentración en las respuestas en los niveles “En desacuerdo” y “Ligeramente de acuerdo” para muchas variables.

Adicionalmente no se encontró ninguna respuesta que mostrara un nivel de satisfacción total con la metodología. No obstante, si existen 4 respuestas que señalan insatisfacción total con algunos de los criterios evaluados. Finalmente solo en dos variables fue posible observar un nivel de satisfacción apropiado (De acuerdo).

Para lograr generar una calificación general de cada variable se utilizará el siguiente indicador de satisfacción:

$$Nivel\ de\ satisfacción = \frac{Total\ de\ usuarios\ que\ respondieron\ De\ acuerdo\ o\ Totalmente\ de\ acuerdo}{Total\ de\ personas\ que\ respondieron\ la\ encuesta}$$

Al aplicar dicho indicador a las respuestas de los encuestados se obtiene el siguiente resultado:

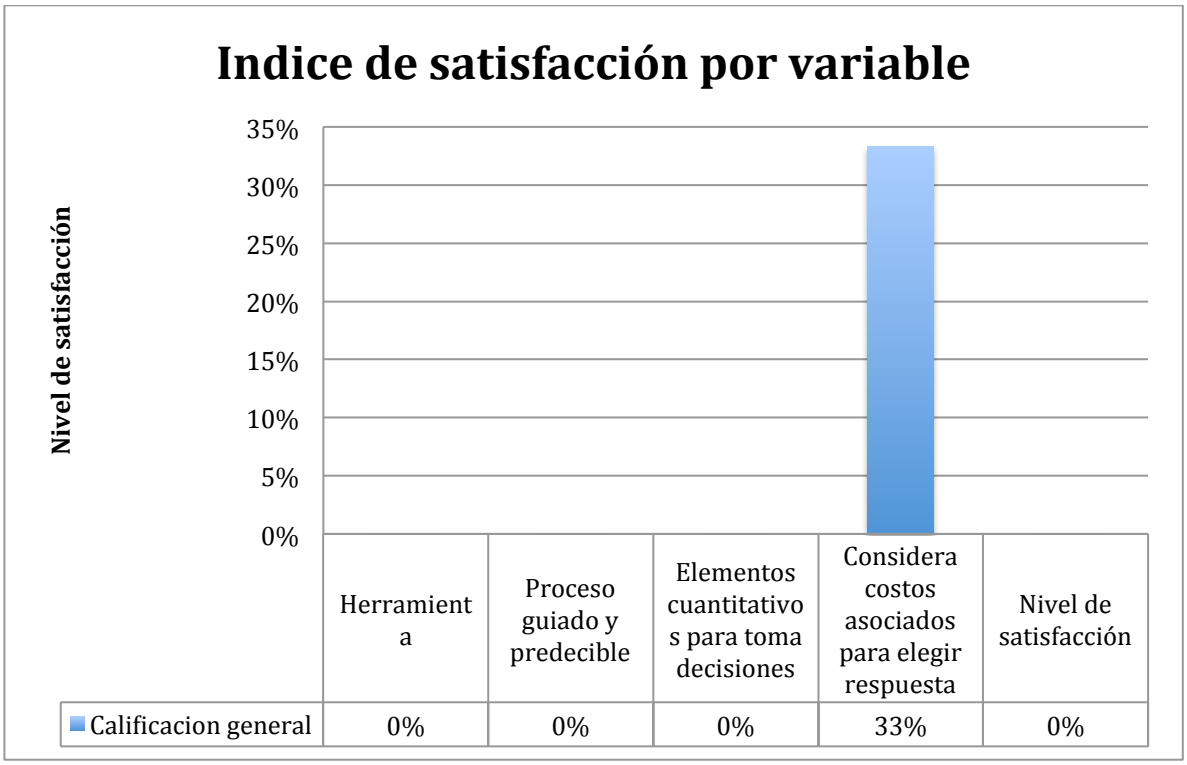


Figura 55 Índice de satisfacción Gerentes con metodología actual por variable. Fuente propia.

De esta información se puede concluir que la mayor calificación obtenida corresponde a la variable de que se consideran costos para elegir la respuesta a un riesgo con una nota de 33%. El resto de variables obtuvo nota cero.

De los resultados anteriores, se puede concluir que *la nota promedio de evaluación de todos los criterios es de un 7%* y que existe mucho margen de mejora, lo cual será posible medir posterior a la ejecución del piloto.

11.2.4.1.2.2. Usuarios de la metodología seleccionados para el piloto

De un total de 14 usuarios a quienes se les remitió la encuesta, respondieron 10 personas.

Los resultados generales de dicha encuesta se muestran a continuación en formato de mapa de calor.

	Totalmente en desacuerdo	En desacuerdo	Ligeramente en desacuerdo	Neutral	Ligeramente de acuerdo	De acuerdo	Totalmente de acuerdo
Herramienta	2	2	2	0	3	1	0
Proceso guiado y predecible	0	1	3	0	3	3	0
Elementos cuantitativos para toma decisiones	0	2	0	2	2	3	1
Considera costos asociados para elegir respuesta	1	2	3	1	1	1	1
Nivel de satisfacción	0	2	3	1	4	0	0
Total	5	10	13	6	14	10	2

Figura 56 Resultados encuesta de satisfacción con metodología de gestión de riesgos actual realizada a usuarios del piloto. Fuente propia.

De la anterior tabla se puede apreciar que existe una concentración en las respuestas en los niveles “Ligeramente en desacuerdo” y “Ligeramente de acuerdo” obteniendo la mayor cantidad de respuestas.

Adicionalmente la menor concentración de respuestas se encuentra en el nivel de satisfacción total con los diferentes variables. En esta evaluación existe una mayor dispersión en las respuestas de los evaluados y prácticamente las respuestas favorables y desfavorables son muy similares con una ligera inclinación a la opinión negativa.

Para lograr generar una calificación general de cada variable se utilizará el siguiente indicador de satisfacción:

$$Nivel\ de\ satisfacción = \frac{Total\ de\ usuarios\ que\ respondieron\ De\ acuerdo\ o\ Totalmente\ de\ acuerdo}{Total\ de\ personas\ que\ respondieron\ la\ encuesta}$$

Al aplicar dicho indicador a las respuestas de los encuestados se obtiene el siguiente resultado:

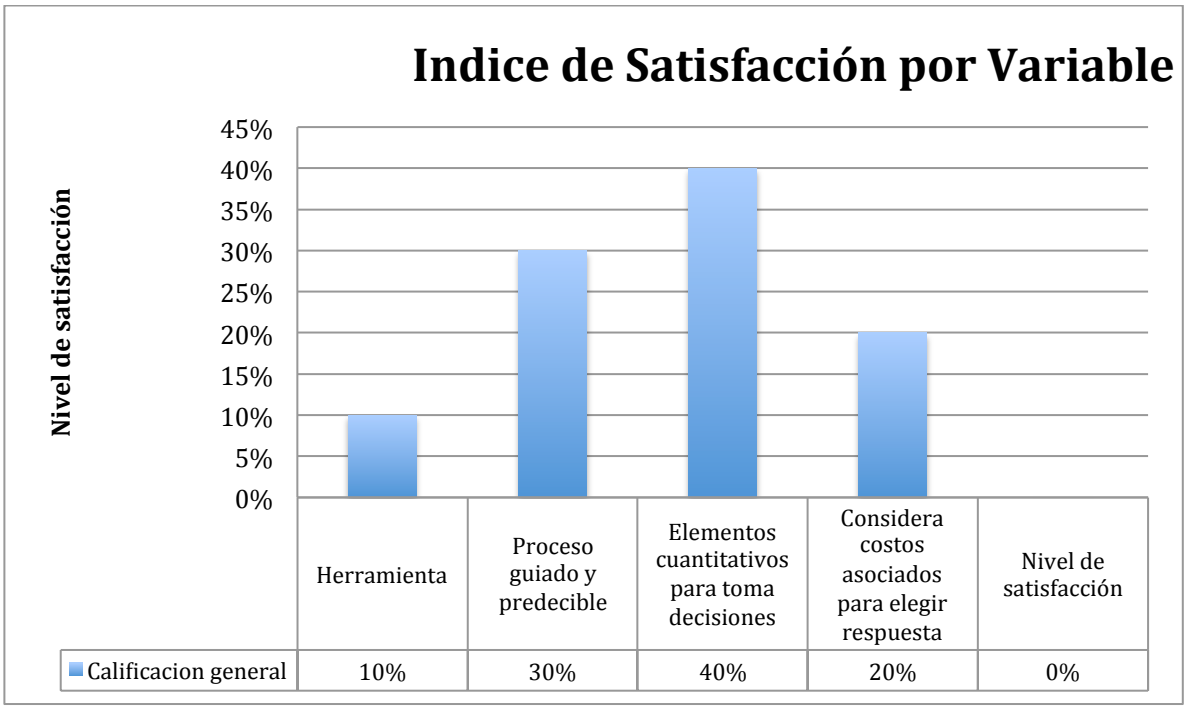


Figura 57 Índice de satisfacción usuarios del piloto con metodología actual por variable. Fuente propia.

De esta información se puede concluir que la mayor calificación obtenida corresponde a la variable de que se consideran elementos cuantitativos para la toma de decisiones con una nota de 40%. La herramienta y el nivel de satisfacción en general con la metodología obtuvieron las notas más bajas.

De los resultados anteriores, se puede concluir que *la nota promedio de evaluación de todos los criterios es de un 20%* que el nivel de satisfacción es superior al de los gerentes pero existe todavía un margen de mejora lo cual será posible medir posterior a la ejecución del piloto.

11.2.4.1.3. Identificación de costos (tangibles / intangibles) asociados a los riesgos

Al analizar los riesgos tecnológicos identificados por la metodología actual se encuentra que ninguno de los riesgos posee en este momento variables económicas o cuantitativas dentro de la estimación de impacto. Únicamente se toman en cuenta las variables cualitativas expresadas en el formato (Posibilidad x Impacto). A nivel de planes de respuesta a riesgos si se han documentado los costos pero en el portafolio de proyectos y no directamente dentro de la herramientas de gestión de riesgos lo cual hace complejo la identificación de costo/beneficio al momento de seleccionar la respuesta.

Debido a lo anterior, *la nota del indicador de Identificación de costos (tangibles / intangibles) asociados a los riesgos tecnológicos en este momento es de cero*.

11.2.4.1.4. Resumen indicadores actuales

A continuación se presenta una tabla resumen de los indicadores explicados en el apartado anterior calculados con los resultados de la metodología de gestión de riesgos actual.

Indicador	Meta	Resultado	Semáforo
Correlación de Riesgos vs Incidentes materializados	x > 0.8	0.99	
Nivel de satisfacción de clientes con la metodología (usuarios)	x > 60%	20%	
Identificación de costos (tangibles / intangibles) asociados a los riesgos	x > 60%	0%	

Tabla 23 Resumen Indicadores metodología actual. Fuente propia.

11.3. Procedimiento de implementación

El propósito de este capítulo consiste en detallar como fue puesta a prueba la propuesta de solución y los resultados obtenidos durante su ejecución como plan piloto.

11.3.1. Alcance del plan piloto

El alcance del plan piloto fue determinado en conjunto con el sponsor estableciendo como objetivos:

1. Selección del personal participante
2. Capacitación del personal involucrado en la metodología y la herramienta
3. Ejecución de un simulacro de identificación de riesgos y acciones de respuesta para el servicio de banca electrónica
4. Evaluación de resultados

11.3.2. Personal participante

Una parte del personal participante del piloto fue seleccionado del grupo de ejecutores de la metodología de gestión de riesgos actual más una persona perteneciente al grupo de responsables de los procesos de gestión de riesgos.

El criterio para seleccionar a estos candidatos fue que tuvieran algún conocimiento de la metodología de gestión de riesgos actual y adicionalmente que tuvieran conocimiento del servicio de banca en línea de manera que pudieran contribuir en ejercicio de identificación de nuevos riesgos asociados a este servicio.

Adicionalmente se invitó al personal involucrado en la gestión y operación del servicio de banca electrónica, que aunque si bien no habían tenido participación previa en la gestión de riesgos, si tienen mucho conocimiento de la aplicación y su ambiente y por ende manejan mucha información sobre posibles vulnerabilidades que el servicio puede tener y que es relevante documentar dentro de la herramienta de gestión de riesgos. A estas personas se les brindó una nivelación

dentro de la capacitación con el fin de que pudieran tener elementos de comparación de la metodología anterior versus la propuesta.

A continuación se lista el personal participante del piloto según puesto desempeñado:

Puesto	Colaboradores	Conocimiento previo gestión riesgos
Administradores de Aplicación	6	NO
Jefes de departamento	4	SI
Gestor administrativo	2	SI
Ingenieros de Procesos	1	SI
Oficial de Seguridad de Sistemas	1	SI

Tabla 24 Personal participante del piloto según puesto. Fuente propia.

En total de personas participantes del piloto fue de 14 colaboradores. Aunque si bien la lista de convocados fue de 16 personas, dos no pudieron asistir a última hora por imprevistos que se les presentaron en el horario en el que se llevó a cabo la ejecución del piloto.

11.3.3. Capacitación

Para capacitar al personal en la metodología propuesta y el uso de la herramienta, se realizaron dos convocatorias el 17 y 18 de Marzo del 2015 separando a los participantes en dos grupos de ocho personas cada uno.

Previo al entrenamiento se envió un correo con una motivación explicando el propósito del ejercicio que se iba realizar y que el mismo contaba con el patrocinio de la Gerencia Regional de Riesgos y Seguridad y el CIO. Adicionalmente se

anexó la guía para la identificación de riesgos (incluida en el Anexo 7), con el fin de que los participantes pudieran estudiar el documento de previo y plantear cualquier duda durante la capacitación.

Durante la capacitación se utilizó una presentación donde se resumió de manera ejecutiva los objetivos de esta investigación, los resultados del análisis de situación actual y las recomendaciones del investigador generadas en la primera parte de este proyecto. Luego se presentó la herramienta utilizada actualmente por la organización con sus diferentes debilidades para luego explicar la metodología propuesta y finalmente presentar la herramienta propuesta brindando un ejemplo de cómo ingresar un nuevo riesgo y sus respectivos planes.

El tiempo asignado la capacitación de cada grupo fue de dos horas.

11.3.4. Ejecución de un simulacro de identificación de riesgos y acciones de respuesta para el servicio de banca electrónica

Para la ejecución del piloto de identificación de riesgos y acciones de respuesta, se convocó a los mismos grupos que se definieron para la capacitación el 17 y 18 de Marzo posterior a la capacitación. Luego se organizaron equipos de dos personas cada uno. A cada equipo se le asignó la responsabilidad de ingresar la mayor cantidad de riesgos que pudiera identificar guiados por el catálogo de escenarios de riesgo, el cual forma parte de la metodología. Como incentivo se mencionó a los participantes que el equipo que ingresara más riesgos recibiría un reconocimiento posterior, una vez que finalizara el ejercicio y se analizaran los datos.

Durante la ejecución del piloto, el investigador estuvo accesible para evacuar cualquier duda que surgiera con la herramienta, la guía o bien el entendimiento de las instrucciones. Asimismo, se coordinó con el desarrollador de la herramienta con el fin de que estuviera disponible para atender cualquier inconveniente que se pudiera llegar a presentar durante la ejecución del piloto.

Durante el primer día se presentaron algunos inconvenientes con la herramienta que impidieron el adecuado registro de algunas variables monetarias. Estos problemas no fueron detectados durante las pruebas de calidad realizadas a la herramienta por parte del investigador previo al piloto. Por esta razón, se acordó con los participantes que dejaran esta información pendiente de completar mientras se lograba corregir el problema. El error fue analizado en sitio por parte del desarrollador, quien detectó el origen de la falla y procedió con su corrección inmediata la cual quedó implementada la misma noche.

Dado que este inconveniente se pudo resolver el mismo día, se habilitó por espacio de 4 días (hasta el último día hábil de la semana) el acceso a la herramienta Web con el fin de que cada equipo pudiera ingresar a registrar la información que quedó pendiente como parte del análisis de riesgo. El segundo grupo no tuvo estos inconvenientes pues ya se habían realizado las correcciones.

Durante la ejecución del piloto los participantes retroalimentaron al investigador sobre algunas dudas, mejoras u oportunidades que identificaron para la herramienta. A continuación se detallan agrupadas por categoría:

Dudas sobre la metodología

1. Se solicitó aclarar si la pérdida de registros corresponde a un problema de la dimensión de disponibilidad o la dimensión de integridad. La aclaración para esta inquietud fue que para este escenario de fallo, la dimensión correcta a utilizar es la dimensión de integridad. La interpretación semántica que se otorga a la dimensión disponibilidad se asocia a la disponibilidad de los sistemas y la capacidad de los clientes para poder realizar transacciones adecuadamente a través del servicio de banca en línea.

Solicitud de mejoras de usabilidad sobre la herramienta

1. Se solicitó limpiar el formulario cada vez que se ingrese un nuevo riesgo o se actualice la información de uno existente. Esto por cuanto la información del riesgo permanecía en los campos cada vez que se presionaba el botón para almacenar la información de un nuevo riesgo o la actualización de un campo. Esto provocaba confusión en los usuarios y podría generar duplicación de información al reingresar nuevamente un riesgo previamente almacenado en la herramienta.
2. Se solicitó que cuando se realiza la búsqueda de un riesgo ingresado con anterioridad, que la herramienta permita mostrar la descripción resumida del riesgo además del código identificador único del riesgo. A raíz de esta situación cuando el segundo grupo arrancó el ejercicio de identificación de riesgos, fue necesario indicarles el último número de consecutivo de riesgo ingresado en la herramienta por el grupo anterior. Esto con el fin de que pudieran navegar e identificar de manera más fácil los riesgos ingresados por este grupo sin confundirse con los riesgos ingresados por el grupo anterior.
3. Se solicitó permitir la búsqueda de riesgos por escenario de falla y no únicamente por el código identificador con el fin de valorar si un riesgo ya se encuentra documentado en la herramienta antes ingresar uno nuevo idéntico.
4. Se solicitó la habilitar la opción de seleccionar varios servicios afectados por un riesgo dado que únicamente puede seleccionar un servicio o la opción de Todos los servicios dentro de la herramienta.
5. Se solicitó incorporar otros servicios a la lista considerada dentro de la aplicación. Servicios como Pago de Servicios Públicos o Pago de Impuestos no fueron considerados dentro de la herramienta. La lista que se cargó en la herramienta fue tomada de los indicadores de volumen transaccional que proporcionó el área de Canales y dentro de esa lista no aparecían estos servicios que mencionó el personal.

11.4. Pruebas y resultados

Posterior a la ejecución del piloto se encontraron los siguientes resultados:

11.4.1. Cantidad de riesgos documentados

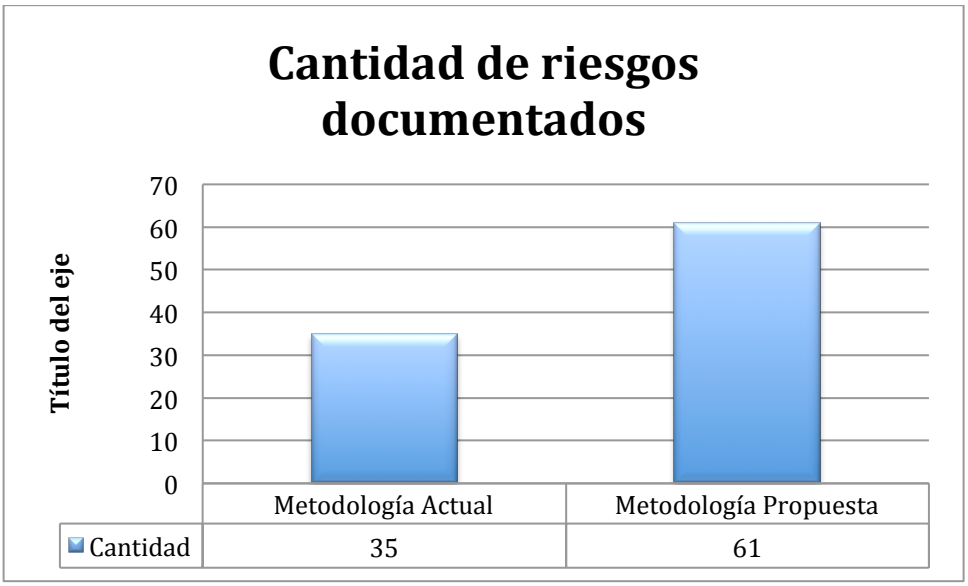


Figura 58 Comparación cantidad de riesgos documentados Metodología actual vs Metodología propuesta. Fuente propia

Con la herramienta propuesta fue posible identificar durante la ejecución del piloto, un total de 61 riesgos. Esto corresponde a un 74% más de los riesgos identificados con la metodología actual.

Es importante reconocer que este resultado es bastante favorable para la organización considerando que en un ejercicio de cuatro horas con 14 participantes fue posible casi duplicar la cantidad total de riesgos formalmente documentados y activos utilizando la herramienta actual. Estos riesgos adicionalmente se documentaron en un período de tiempo considerablemente mayor (alrededor de un año) comparado con el tiempo asignado al piloto de la herramienta propuesta.

Un aspecto relevante a mencionar es que la herramienta en Sharepoint permitió a cada equipo participante, ingresar los riesgos de manera autónoma e

independiente. Con la herramienta actual esto no sería viable por cuanto la identificación de riesgos se realiza en reuniones con cada gerencia, involucrando a los líderes de riesgos y únicamente una persona es quien documenta dentro de la herramienta en Excel por lo cual el resto de participantes se limita exclusivamente a observar o en el mejor de los casos opinar sobre la calificación que se asigna a cada riesgo.

Esta facilidad permite a la organización incrementar de manera considerable la productividad en la gestión de riesgos, brindando eficiencia y haciendo un uso racional del tiempo de los participantes.

Otro hallazgo importante, no ligado directamente a la herramienta, sino más bien a un aspecto cultural de la gestión de riesgos en la organización es que la identificación de riesgos durante el piloto se hizo bajo un ambiente controlado y no vinculante. Esto permitió que las personas participantes identificaran riesgos con toda libertad y sin ningún tipo de censura lo cual aumentó su productividad. Contrario a esta situación, con la metodología actual de la organización, cualquier persona que identifica un riesgo automáticamente se le asigna la responsabilidad no únicamente de calificarlo sino también del seguimiento de planes de acción asociados a la respuesta del riesgo y la rendición de cuentas sobre el estatus del riesgo y sus planes de acción. Esta situación desincentiva que las personas realicen aportes a la gestión de riesgos porque implícitamente les generará una carga de trabajo adicional, lo cual no sería problema si la ejecución de los planes de acción dependieran enteramente de su responsabilidad. El principal inconveniente se presenta cuando la ejecución o priorización de los planes de acción no depende directamente de la persona o unidad que lo identifica sino de otras áreas. Esta situación, aunque no está relacionada con aspectos tecnológicos, es indispensable resolverla con el fin de que no siga impactando negativamente el adecuado funcionamiento y eficiencia de la gestión de riesgos organizacional.

11.4.2. Criticidad de los Riesgos

Posterior a que el personal participante del piloto realizara la evaluación de los 61 riesgos ingresados en la herramienta, la calificación general (criticidad) quedó distribuida de la siguiente manera:

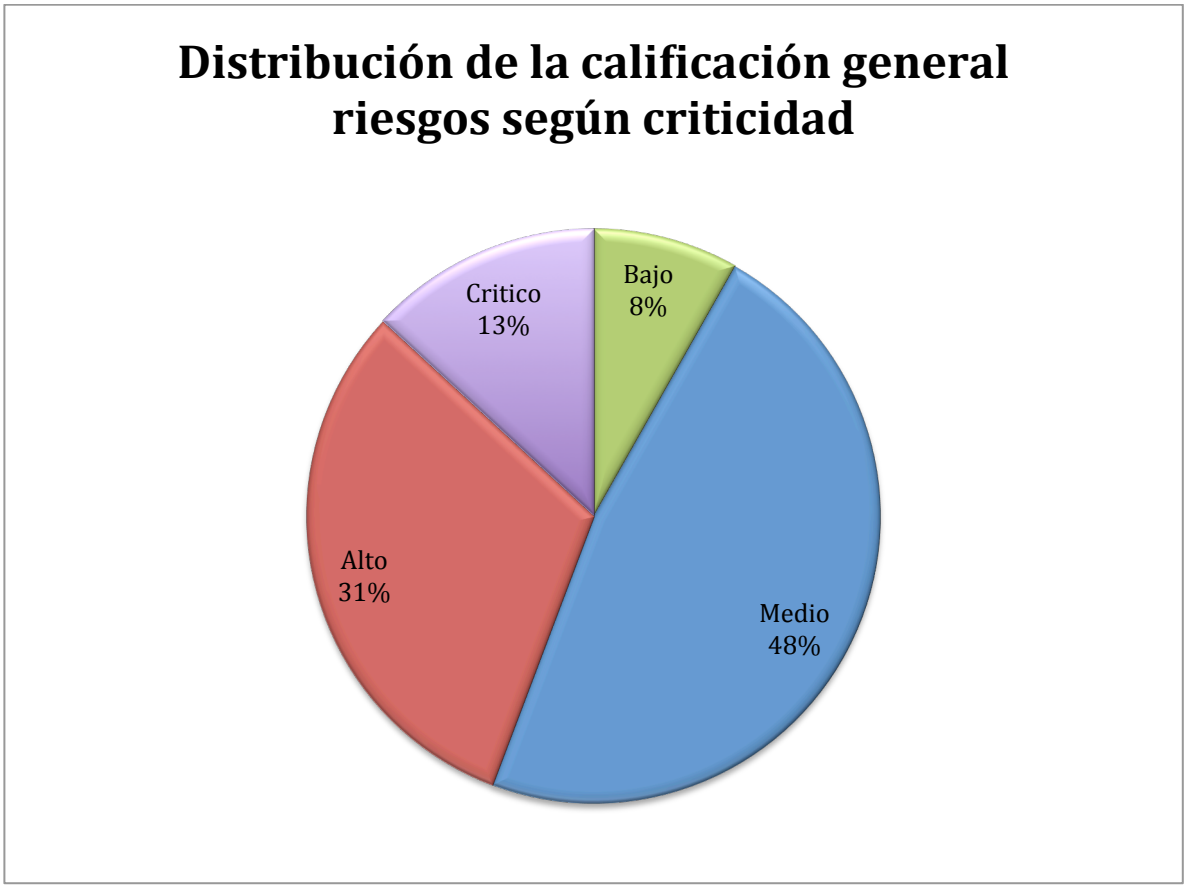


Figura 59 Distribución calificación general riesgos por criticidad. Fuente propia.

Considerando esta distribución se concluye que, según el principio de Pareto, el 80% de los riesgos quedaron asignados a la criticidad media y alta, en ese orden. Por el contrario, los riesgos de criticidad baja y crítica representaron únicamente un 20% del total identificado durante el piloto.

Adicionalmente, menos de un 10% de los riesgos fueron clasificados como de Baja criticidad. Al revisar estos resultados con el patrocinador del proyecto, se encontró como posible justificación a este comportamiento el hecho de que la concentración del personal típicamente se centra en las vulnerabilidades que

puedan afectar considerablemente el servicio y no así eventos de poca relevancia. A pesar de lo anterior, posterior a evaluar los riesgos identificados por el personal participante del piloto, predominan los riesgos de criticidad media sobre los altos y críticos. Esto significa que la metodología ayuda a sensibilizar el impacto de los riesgos apoyados en los criterios de evaluación utilizados por la metodología.

11.4.3. Estimación de impacto cuantitativo

Uno de los aportes más importantes a la metodología propuesta es la posibilidad de que los participantes puedan identificar el impacto cuantitativo de los riesgos traducido a costos por pérdidas en caso de materialización del riesgo. Del total de riesgos ingresados esta fue la composición según estimación de impacto cuantitativo:

Figura 60 Porcentaje riesgos con estimación de impacto cuantitativo. Fuente Propia.

Es relevante notar que más de 50% de los riesgos identificados durante el piloto lograron contar con al menos una dimensión con un impacto económico asociado. Como se mencionó anteriormente, ninguno de los riesgos documentados con la metodología actual de la organización tienen impacto económico asociado al mismo.

11.4.4. Impacto cuantitativo por tipo de costo

Del 64% de los riesgos que contaron con impacto económico asociado, a continuación se detalla la distribución según el tipo de costo identificado

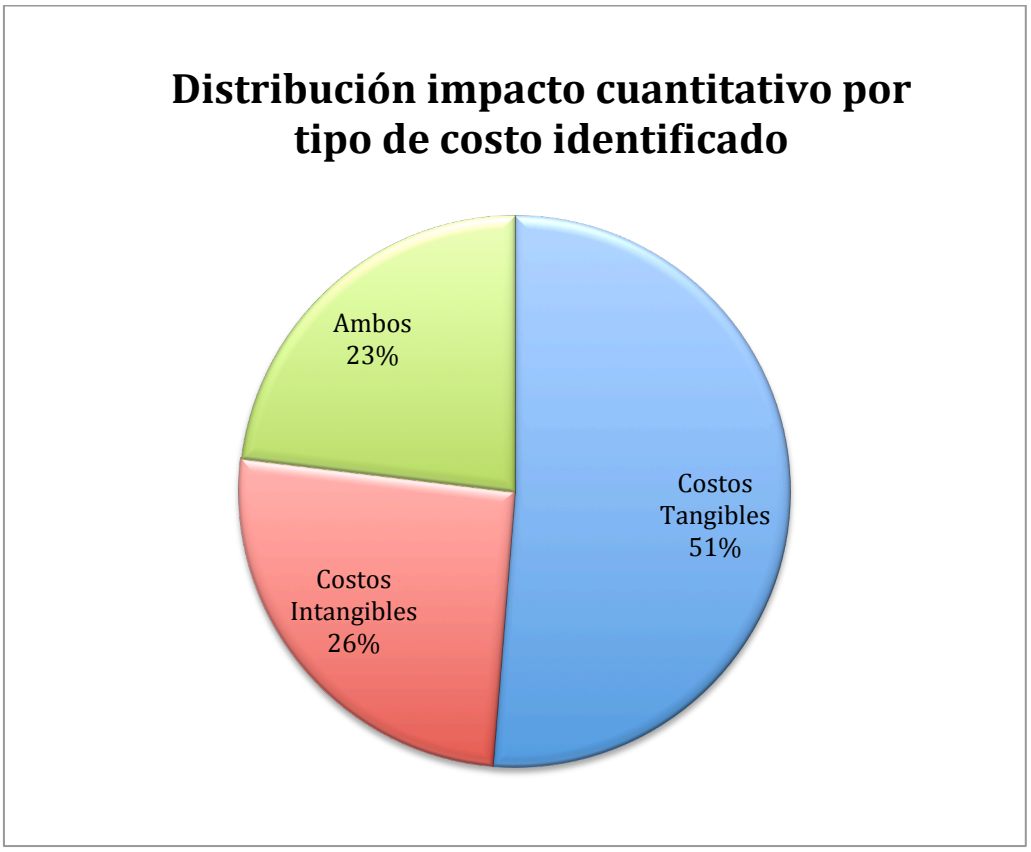


Figura 61 Distribución de riesgos con impacto cuantitativo asignado por tipo de costo. Fuente propia.

El 50% de los riesgos que tienen impacto económico identificado, los montos corresponden a costos tangibles únicamente, esto significa que el valor económico asignado tiene una certeza muy alta de cumplirse en caso de materializarse el riesgo. Estos costos tangibles corresponden a las dimensiones de Disponibilidad y Cumplimiento Regulatorio.

El 26% de los riesgos que tienen impacto económico identificado, los montos corresponden a costos intangibles únicamente. Se analizó si la mayoría de estos riesgos corresponden a riesgos de seguridad de información por cuanto las dimensiones involucradas son Integridad y Confidencialidad, criterios muy afines a

riesgos de seguridad. Sin embargo, no se detectó un predominio de riesgos de tipo seguridad entre esta agrupación de riesgos, únicamente 2 riesgos de 10 en total corresponden a eventos de seguridad.

Un 23% de los riesgos que tienen impacto económico identificado, los montos corresponden a costos intangibles como también costos tangibles. Se analizó si estos riesgos corresponden a los que se evaluaron como críticos o altos. Sin embargo, únicamente 4 riesgos de los 9 que corresponden a esta categoría están clasificados como un impacto alto o crítico.

11.4.5. Costo de los Planes

De la totalidad de los riesgos identificados, a 29 se les logró documentar al menos una acción de respuesta con un costo de ejecución asociado. Esto representa un 48% de la totalidad de los riesgos identificados durante la ejecución del piloto.

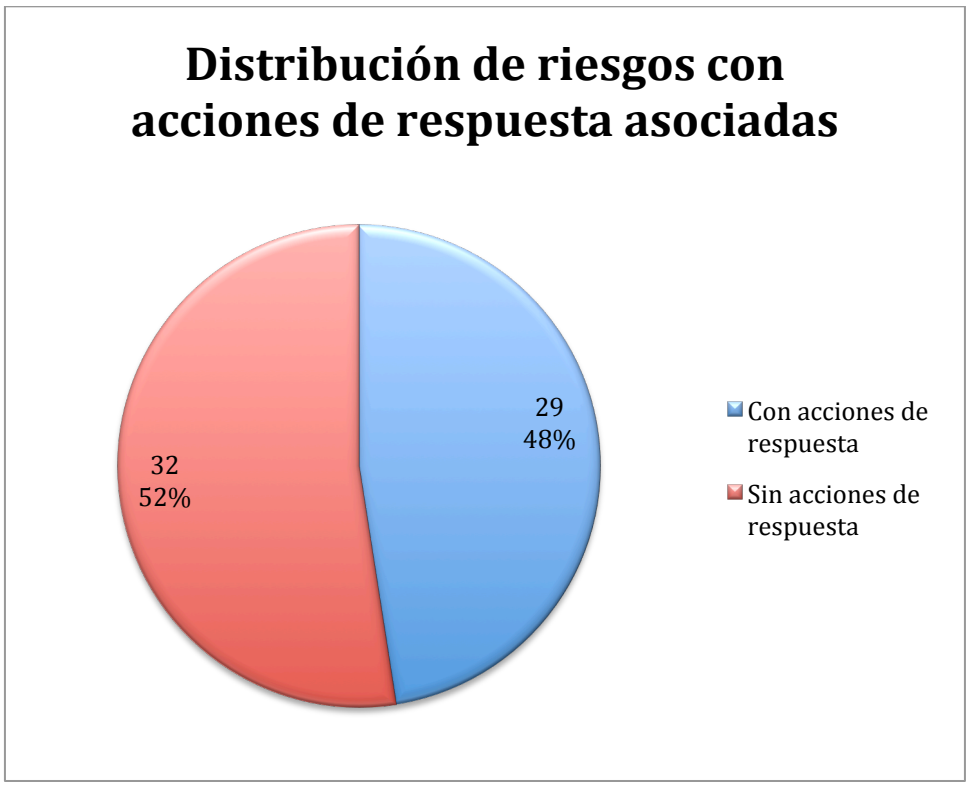


Figura 62 Distribución de riesgos con acciones de repuestas asociadas. Fuente propia.

De estos 29 riesgos, solo a 19 se les designó al menos un plan de acción, seleccionado de las acciones de respuesta identificadas.

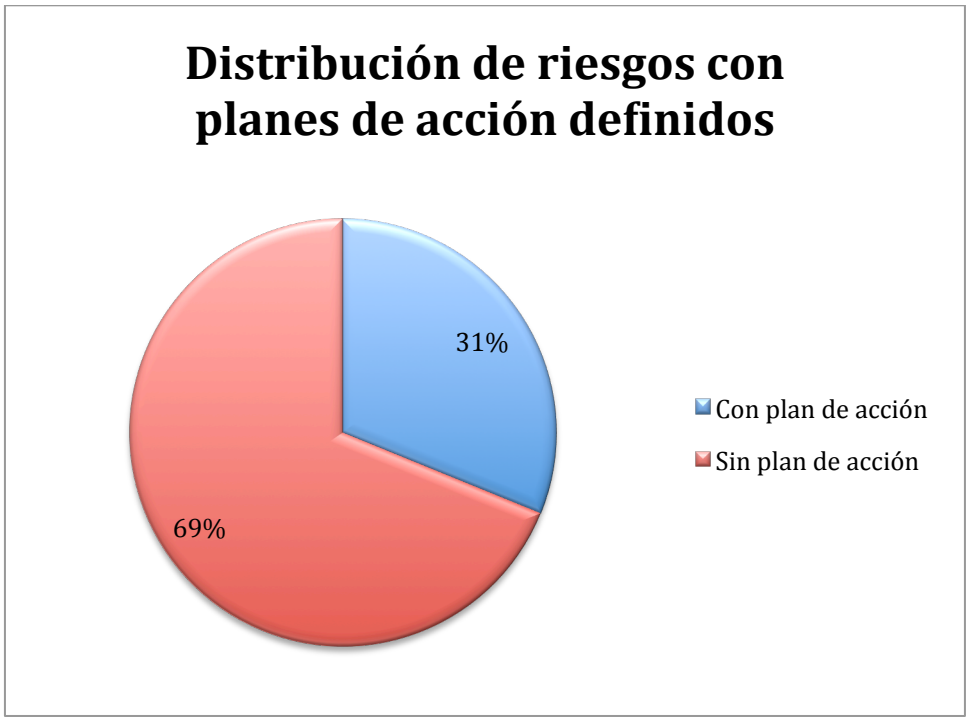


Figura 63 Distribución de riesgos con planes de acción definidos. Fuente propia.

Esto representa un 31% del total de riesgos identificados por el personal participante del piloto.

La razón por la cual no se logró alcanzar un porcentaje superior se debió a que en el primer día los inconvenientes con la herramienta limitaron la concentración del personal hacia la identificación y calificación de riesgos, no así la identificación de acciones de respuesta, planes y sus respectivos costos.

Esto se puede afirmar puesto que del primer grupo únicamente se definieron 4 riesgos con al menos un plan de acción. En cambio, el segundo grupo logró documentar 15 riesgos con al menos un plan de acción. Este último valor representa un 79% del total de 19 planes con al menos un plan de acción establecido.

11.4.6. Estrategia de respuesta asignada a los riesgos

Con la metodología actual de la organización, el 100% de las estrategias de respuesta definidas corresponden a la mitigación de los riesgos identificados. Posterior a la ejecución del piloto se analizó la composición de la estrategia de respuesta asignada a los riesgos identificados por el personal participante. A continuación se presentan los resultados:

Figura 64 Distribución de riesgos según estrategia de respuesta asignada. Fuente propia.

Un hallazgo relevante corresponde a que para un 33% de los riesgos se eligió la estrategia de Aceptar el riesgo por parte de los participantes del piloto. Esto significa que para la organización representa un ahorro el hecho de no tener que invertir tiempo del personal en la definición de planes y también el costo de cada plan.

Un 6% seleccionó la estrategia de respuesta de Evitar y un 2% eligió la alternativa de Transferir el riesgo lo cual es una modalidad nueva de tratamiento para los riesgos identificados.

Lamentablemente un 18% de los riesgos no definió estrategia de respuesta. Analizando la información se detectó que 7 de los 11 riesgos sin respuesta son riesgos que en su calificación general no superaron el apetito de riesgo, por esta razón la estrategia de respuesta por defecto a asignar es la de Aceptar el riesgo. Esto reduce a 4 riesgos de criticidad Alto, la cantidad de riesgos que quedaron sin estrategia de respuesta definida.

Finalmente a un 41% de los riesgos, se les asignó Mitigar como estrategia de respuesta que es el enfoque tradicional de respuesta de la metodología anterior. Con esto se concluye que se redujo a más de la mitad la cantidad de riesgos a Mitigar.

11.4.7. Indicadores de medición

Como se mencionó anteriormente, para efectos de evaluar y comparar la efectividad de la metodología propuesta versus la metodología actual se propusieron los indicadores descritos en el anexo 14.

Analizando los indicadores anteriores con base a los resultados del piloto se encuentran los siguientes resultados:

11.4.7.1. *Correlación de Riesgos vs Incidentes materializados*

Para efectos de poder medir la efectividad del piloto se realiza una comparación entre la cantidad de riesgos identificados según su criticidad, comparados contra los incidentes que se han materializado para el servicio de banca electrónica en el último año según el impacto que generaron.

Analizando únicamente en los riesgos e incidentes de criticidad Medio, Alto y Crítico se tabuló la información de incidentes y riesgos en una misma tabla y se calculó el coeficiente de correlación de Pearson teniendo como resultado que *el coeficiente de correlación de Pearson entre incidentes y riesgos identificados por la metodología propuesta es de 0.86.*

Clasificación	Riesgos	Incidentes
Crítico	8	0
Alto	19	56
Medio	29	53

Tabla 25 Comparación Riesgos vs Incidentes según criticidad. Fuente Propia

Esto significa que ambas variables tienen una correlación alta como se puede comprobar el siguiente gráfico donde se incluyeron las líneas de regresión lineal de ambas curvas.

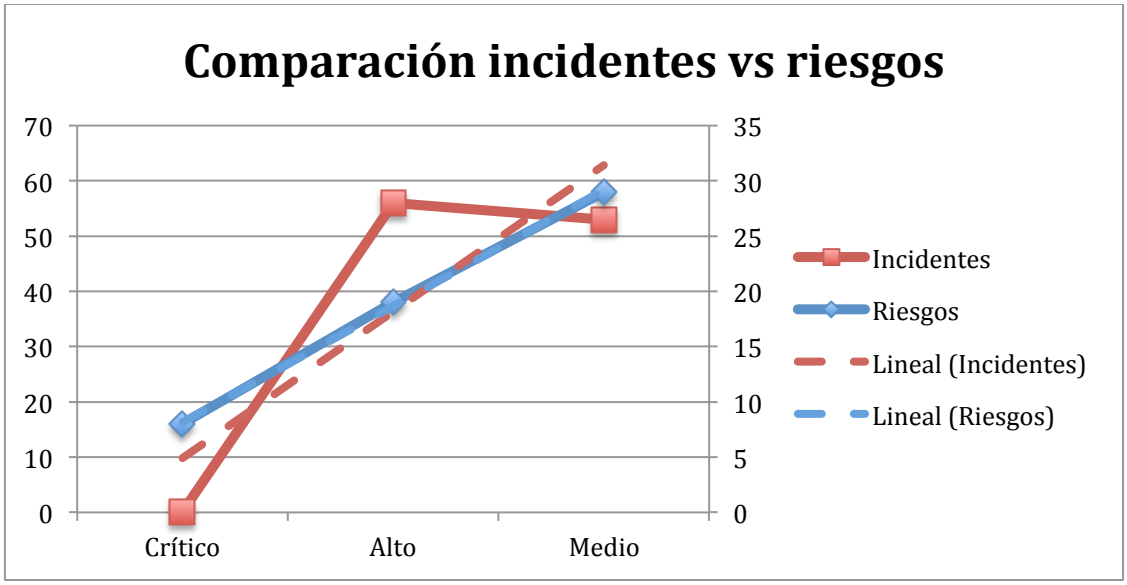


Figura 65 Comparación de incidentes vs riesgos identificados en el piloto. Fuente propia

Aunque si bien la correlación es alta y se cumplió el indicador propuesto, no superó el nivel de correlación que se calculó para los riesgos identificados por la metodología actual.

La diferencia, aunque no sea significativa, puede estar fundamentada en el corto tiempo que se pudo destinar al uso de la herramienta dentro del piloto. En caso que la organización decida implementar la metodología es importante que pueda seguir generando este indicador para medir la congruencia entre la realidad de los incidentes y los riesgos identificados.

11.4.7.2. *Nivel de satisfacción*

El nivel de satisfacción de los usuarios participantes del piloto fue analizado a través de la encuesta propuesta con el instrumento incluido en el Anexo 2.

El instrumento consideró la evaluación de los siguientes criterios:

1. Herramienta
2. Proceso guiado y predecible
3. Elementos cuantitativos para toma decisiones
4. Considera costos asociados para elegir respuesta
5. Nivel de satisfacción

Cada encuestado debió identificar para cada criterio, su nivel de satisfacción en siete posibles niveles. De un total de 14 usuarios a quienes se les remitió la encuesta, respondieron 9 personas.

Los resultados generales de dicha encuesta se muestran a continuación en formato de mapa de calor.

	Totalmente en desacuerdo	En desacuerdo	Ligeramente en desacuerdo	Neutral	Ligeramente de acuerdo	De acuerdo	Totalmente de acuerdo
Herramienta	0	0	0	0	2	5	2
Proceso guiado y predecible	0	0	1	0	4	3	1
Elementos cuantitativos para toma decisiones	0	0	0	0	3	5	1
Considera costos asociados para elegir respuesta	0	0	0	0	3	4	2

Nivel de satisfacción	0	0	0	0	2	4	3
Total	0	0	1	0	14	21	9

Figura 66 Resultados encuesta de satisfacción con piloto realizada a usuarios. Fuente propia.

De la anterior tabla se puede apreciar que existe una alta concentración en las respuestas en los niveles “Ligeramente de acuerdo” y “De acuerdo” obteniendo la mayor cantidad de respuestas. Adicionalmente solo existe una respuesta en el nivel “Ligeramente en desacuerdo” y no existe ninguna otra calificación negativa.

Esto muestra una mejoría bastante significativa en el nivel de satisfacción de los usuarios con la gestión de riesgos propuesta comparado con la metodología actual.

Para lograr generar una calificación general de cada variable se utilizará el siguiente indicador de satisfacción:

$$Nivel\ de\ satisfacción = \frac{Total\ de\ usuarios\ que\ respondieron\ De\ acuerdo\ o\ Totalmente\ de\ acuerdo}{Total\ de\ personas\ que\ respondieron\ la\ encuesta}$$

Al aplicar dicho indicador a las respuestas de los encuestados y comparar el resultado con la metodología actual se obtiene el siguiente resultado:

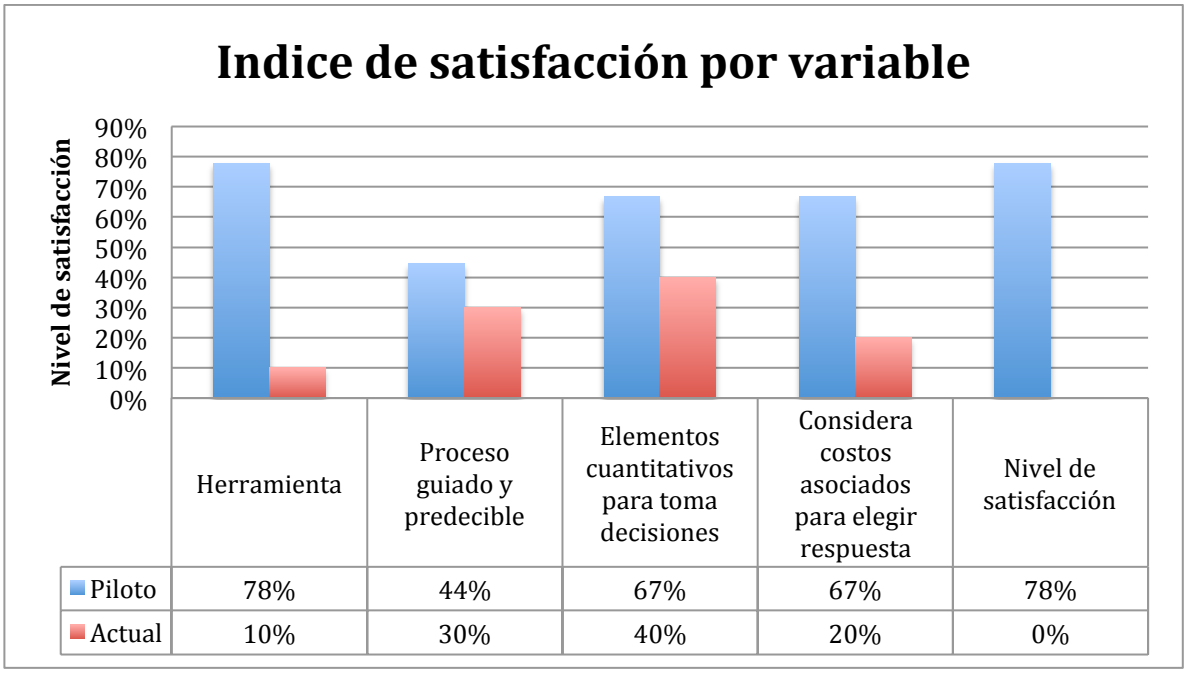


Figura 67 Comparativo índice de satisfacción usuarios con metodología actual vs piloto. Fuente propia.

De esta información se puede concluir que la mayor calificación obtenida corresponde a la variable que mide el Nivel de satisfacción en general que aumento de 0% a 78% y la variable que mide la satisfacción con la herramienta que aumentó de 10% en la metodología actual a 78% con la herramienta utilizada en el piloto.

La variable Proceso guiado y predecible fue la que obtuvo la nota más baja aunque sí tuvo mejoría respecto a la calificación de la metodología actual.

De los resultados anteriores, se puede concluir que *la nota promedio de evaluación de todos los criterios es de un 67%* y este porcentaje es superior al 20% que obtuvo como calificación la metodología actual.

11.4.7.3. *Identificación de costos (tangibles / intangibles) asociados a los riesgos*

Tal como se mencionó en el apartado 5.4.3 de este documento, al analizar los riesgos tecnológicos identificados durante el piloto en confirmó que del total de riesgos ingresados, un 64% contaba con una estimación de impacto cuantitativo traducido a costos por pérdidas en caso de materialización del riesgo.

Figura 68 Porcentaje de riesgos identificados en el piloto con estimación de impacto cuantitativo. Fuente propia.

Debido a lo anterior, *la nota del indicador de Identificación de costos (tangibles / intangibles) asociados a los riesgos tecnológicos para los riesgos identificados durante el piloto fue de 64%*.

11.4.7.4. *Comparativo de indicadores metodología actual vs metodología propuesta*

A continuación se presenta una tabla resumen de los indicadores explicados en el apartado anterior, que fueron el resultado de la aplicación del piloto, comparados contra los resultados de la metodología de gestión de riesgos actual.

Indicador	Meta	Metodología Actual	Resultado Piloto	Tendencia
Correlación de Riesgos vs Incidentes materializados	x > 0.8	0.99	0.8	↓
Nivel de satisfacción de clientes con la metodología (usuarios)	x > 60%	20%	67%	↑
Identificación de costos (tangibles / intangibles) asociados a los riesgos	x > 60%	0%	64%	↑

Tabla 26 Comparativo de indicadores metodología actual vs metodología propuesta. Fuente propia.

CAPITULO VI – Análisis financiero

En este capítulo se presenta un análisis de factibilidad con el fin de confirmar si la implementación de la propuesta realizada en esta investigación resulta rentable. El análisis se presenta en dólares, dado que todas las inversiones y análisis de presupuestos en la organización se gestionan en ésta moneda.

12.1. Egresos

Los egresos corresponden a todos los gastos y desembolsos que la organización debe realizar con el fin de poder implementar la metodología propuesta a través de una herramienta.

Algunos de los gastos se ejecutarán únicamente durante el año 0, que corresponde al año donde se desarrolla la metodología y otros son gastos recurrentes principalmente relacionados con el mantenimiento y soporte del producto.

Para efectos del cálculo de los costos se tomará en cuenta el costo por hora de un desarrollador externo a la organización, especialista en Sharepoint, a una tarifa de $45 dólares por hora. Este costo es preciso por cuanto ya actualmente se cuenta con una organización que presta estos servicios a la institución. Por otro lado, se considera el costo por hora del recurso humano interno a una tarifa de $35 dólares la hora que representa el costo de oportunidad utilizado por el área de informática para generar presupuestos.

Los egresos del proyecto se estimaron a partir de las siguientes inversiones y gastos que la organización debe incurrir con el fin de desarrollar e implementar la herramienta propuesta.

Ítem	Comentarios	Año 0	Año 1	Año 2	Año 3
Hardware	Actualización de los equipos para soportar el aumento en información almacenada más el incremento en volumen transaccional y de	$10,000	$0	$0	$0

	usuarios por la implementación de la nueva aplicación de riesgos.				
Licencias	Tanto el licenciamiento de servidor como las licencias de acceso de los usuarios representan un costo hundido para este proyecto pues la organización actualmente ya sufragó este costo.	$0	$0	$0	$0
Mantenimiento licencias	Dado que es un costo compartido, se considera una fracción del monto total anual.	$1,000	$1,000	$1,000	$1,000
Desarrollo de Software	Costo de outsourcing para el desarrollo del software, se estiman 6 meses (120 días) a $45 la hora. Este costo se justifica puesto que la herramienta desarrollada durante el piloto debe ajustarse para que trabaje bajo los estándares de seguridad, mantenimiento y desarrollo de software que requiere la organización para ser implementada a nivel corporativo.	$43,200	$0	$0	$0
Recurso Humano Interno	Costo del tiempo del personal interno participante en el implementación de la herramienta para levantar requerimientos, hacer pruebas, documentar, etc. Se estima un total de 10 personas involucradas,	$33,600	$0	$0	$0

	durante seis meses, con 4 horas de participación semanal en el proyecto a un costo por hora aproximado del recurso interno de $35 la hora por recurso.				
Capacitación personal	Entrenamiento del personal en la metodología y herramienta. Se consideran 200 personas distribuidos en grupos de 20 personas, en sesiones de ocho horas a un costo de $35 la hora.	$2,800	$0	$0	$0
Contrato soporte	Pago anual a la empresa de desarrollo por el soporte y mantenimiento de la herramienta desarrollada. Se estima un 20% del costo del desarrollo.		$8,640	$8,640	$8,640
	Total	$89,200	$9,640	$9,640	$9,640

Tabla 27 Resumen de egresos por período. Fuente propia.

12.2. Ingresos

Para calcular los ingresos, se consideraron los ahorros que representa para la organización la aplicación de la metodología para reducir o mitigar el impacto de los riesgos identificados. Los ahorros se estimaron tomando como muestra los 19 riesgos identificados durante la ejecución del piloto, los cuales que tienen al menos un plan de acción definido. Se realiza esta selección considerando que para estos riesgos se registró cómo mínimo el costo de los planes de acción y en la mayoría de los casos la cuantificación del impacto.

Para calcular el ahorro se utilizará únicamente la estimación de costos tangibles considerando que tienen una certeza muy alta de cumplirse en caso de materializarse el riesgo. Adicionalmente, el dejar por fuera la estimación de costos

intangibles implica tomar un escenario pesimista de ahorro, esto por cuanto el ahorro podría ser aún mayor del que se va calcular en este análisis.

El ahorro para la organización se calcula restando el costo de los planes al monto impacto económico del riesgo estimado. A continuación se presenta una tabla resumen con los costos calculados para cada uno de los riesgos y el total:

Numero Riesgo	ID Riesgo	Estimación impacto costos tangibles	Costo Planes de Acción	Diferencia
1	FR0011	$-	$1,100,000	$-1,100,000
2	FR0020	$-	$300,000	$-300,000
3	FR0021	$-	$300,000	$-300,000
4	FR0037	$-	$15,000	$-15,000
5	FR0051	$52,489	$10,000	$42,489
6	FR0052	$50,000	$300,000	$-250,000
7	FR0054	$102,489	$4,000	$98,489
8	FR0058	$522,403	$45,000	$477,403
9	FR0060	$516,665	$3,000	$513,665
10	FR0062	$53,679	$300,000	$-246,321
11	FR0065	$1,472,403	$600,000	$872,403
12	FR0066	$16,550	$50,000	$-33,450
13	FR0067	$-	$450,000	$-450,000
14	FR0069	$1,000,000	$1,000	$999,000
15	FR0070	$472,403	$15,000	$457,403
16	FR0073	$522,403	$3,000	$519,403
17	FR0075	$104,978	$1,000	$103,978
18	FR0076	$-	$100,000	$-100,000
19	FR0077	$63,060	$101,000	$-37,940
	Total	**$4,949,523**	**$3,698,000**	**$1,251,523**

Tabla 28 Ahorros estimados por implementar respuesta a riesgos. Fuente propia.

De la información anterior se puede concluir que existe un ahorro estimado de $1,251,523 para la organización por implementar las acciones de respuesta identificadas como parte del plan de acción para reducir el impacto de los riesgos identificados. Este monto representa la cifra mínima de ahorro que se puede lograr con la utilización de la metodología.

Existen otros ahorros intangibles que se pueden mencionar como por ejemplo, la ganancia en productividad que se puede lograr al implementar la metodología al hacer un uso más racional del tiempo del personal involucrado. Asimismo la satisfacción con el proceso de gestión de riesgos, pero esto no se utilizarán dentro del modelo y se considerará como una ganancia indirecta.

12.3. Flujo de caja

Los egresos del proyecto se consideraron dentro del modelo con una proyección a tres años.

Sin embargo, para efectos realizar el análisis financiero es necesario elaborar algunos supuestos sobre los ahorros que servirán como base para el análisis. Considerando que el monto de ahorro es posible lograrlo una vez que se finalicen los planes de acción y que no todos los planes de acción son de corto plazo (3 meses) o mediano plazo (1 año), entonces se distribuirá este monto del ahorro asumiendo que es posible alcanzar un 20% el primer año, un 60% el segundo año y el último 20% en el tercer año.

A continuación se presenta un flujo de caja considerando lo anterior:

	Año 0	Año 1	Año 2	Año 3
Egresos	$90,600	$9,640	$9,640	$9,640
Ingresos		$250,305	$750,914	$250,305
Flujo	$-90,600	$240,665	$741,274	$240,665
Flujo acumulado	$-90,600	$150,065	$891,338	$1,132,003

Tabla 29 Flujo de caja del proyecto. Fuente propia.

12.4. Indicadores de rentabilidad del proyecto

Para medir la rentabilidad del proyecto se utilizarán el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR). Para definir la tasa de descuento, variable necesaria para calcular ambos indicadores, se toma como referencia la tasa de interés de certificados de depósito anuales en dólares en el BAC San José, la cual se ubica en 2.53% anual al momento de realizar el análisis.

A partir de la definición anterior, el resultado para ambos indicadores es el siguiente:

Indicador	Resultado
VAN	$1,046,086.76
TIR	357%

Tabla 30 Indicadores financieros del proyecto. Fuente propia.

Considerando el resultado del Valor Actual Neto (VAN) es positivo se concluye que la inversión en el proyecto generaría resultados ganancias por encima de la rentabilidad mínima.

Por otro lado, el resultado de la Tasa Interna de Retorno (TIR) es de un 357%, el cual es un valor muy superior al 2.53% estimado.

Debido al resultado de los dos indicadores anteriores podemos afirmar que el proyecto sería muy rentable para la organización, aun considerando un escenario bastante pesimista dado que no se tomaron en cuenta los costos intangibles.

Adicionalmente la recuperación de la inversión tendría el siguiente comportamiento por año.

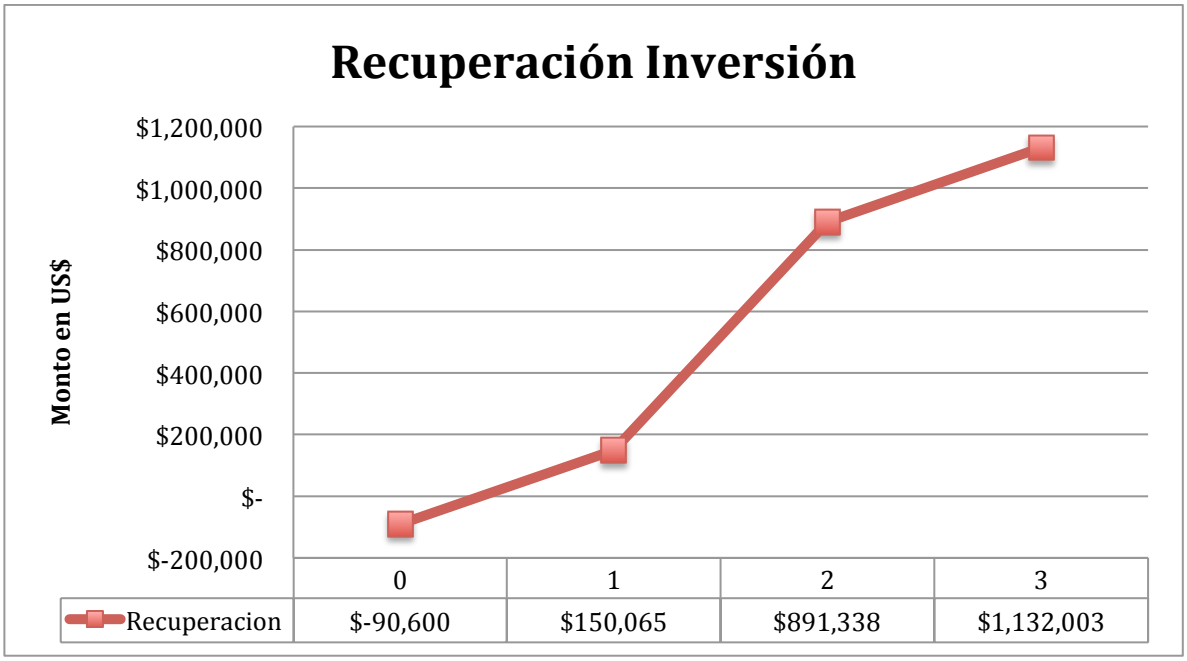


Figura 69 Recuperación de la inversión por período. Fuente propia.

12.5. Conclusiones financieras

A partir de los resultados anteriores, se evidencia que el proyecto es viable financieramente y podemos concluir que:

1. La inversión realizada por la organización en el proyecto, la cual puede tomar alrededor de 6 meses para que pueda ser aprovechada, podrá ser recuperada casi en su totalidad el siguiente año con la finalización los primeros planes identificados dentro del análisis de riesgo.
2. El valor presente neto (VAN) el cual permite estimar los flujos de caja futuros descontados empleando la tasa de descuento, produjo un número positivo cercano a 1 millón de USD lo cual hace que sea un proyecto altamente rentable.
3. La tasa interna de retorno estimada en 357% se encuentra a un factor de rentabilidad superior por más de 100 veces que la tasa de descuento estimada, la cual es la tasa de rendimiento que se podría ganar en una

inversión en los mercados financieros con un riesgo similar. Esto confirma que el proyecto es altamente rentable y por ende valioso para implementar.

CAPITULO VII – Conclusiones y recomendaciones

13.1. Conclusiones

En este apartado se resumen las principales conclusiones que se generan a partir de la investigación realizada:

1. Desconocimiento de conceptos como marcos de trabajo de gestión de riesgos, certificaciones y organizaciones que representan dichos estándares o certificaciones entre todos los participantes de la investigación. Tanto de los responsables de la metodología de gestión de riesgos como de quienes la ejecutan.
2. Al ser una de las primeras empresas financieras en obtener el certificado de calidad ISO 9001, se evidenció una cultura de definición, seguimiento y control de procesos que busca la mejora de los servicios que ofrece la organización, esto favorece y apalanca la gestión de riesgos, al existir procesos formales, documentados, estándares, versionados dentro del sistema de calidad que existe en la organización.
3. Existe un consenso general entre todos los encuestados que la herramienta que se utiliza actualmente para apoyar la metodología de gestión de riesgos es manual, compleja de utilizar (plantillas de Excel) lo cual no favorece el aprovechamiento óptimo de los recursos que apoyan la gestión de riesgos organizacional.
4. Tanto los ejecutores como los responsables de la metodología actual de gestión de riesgos reconocen que la misma es compleja y abierta a subjetividad principalmente cuando se identifican y evalúan los riesgos.
5. La identificación de los riesgos con la metodología actual no sigue un proceso estructurado por lo que no orienta al personal a seguir un orden específico con el fin de mejorar la calidad de la información generada y hacerlo un proceso menos caótico (lluvia de ideas).
6. Se intentó buscar que la identificación de riesgos fuera un “Proceso guiado y predecible” a través de la implementación de un catálogo de escenarios de riesgos y una guía para la identificación de riesgos. Sin embargo, no se obtuvo una mejora significativa pues al realizar la evaluación del nivel de

satisfacción de los participantes con el piloto, la nota de calificación asignada a esta variable fue de un 44%. Esto representa un aumento de un 14% sobre el 30% que obtuvo la metodología actual en este mismo criterio.

7. A excepción de los costos de los planes, con la metodología actual no se están cuantificando en términos económicos costos tangibles e intangibles (impacto en confidencialidad, impacto en integridad, impacto en disponibilidad, etc.) cuando se identifican riesgos tecnológicos.
8. Se detectó desconocimiento del personal cuando se consultó sobre las variables monetarias que actualmente se consideran en la gestión de riesgos. Esta afirmación se realiza por cuanto los encuestados no pudieron responder con claridad que la única variable monetaria que se está capturando actualmente en el análisis de riesgo tecnológico tiene que ver con el costo de las acciones de respuesta a implementar.
9. En general, no existe alineamiento entre el personal ejecutor de la metodología de gestión de riesgos y el grupo que es responsable de dicha metodología. Se detectaron contradicciones entre las respuestas de los ejecutores comparados con las respuestas de los responsables en relación a las distintas variables consultadas.
10. El personal ejecutor y responsable de la metodología de gestión de riesgos considera que deben mejorarse los mecanismos para aumentar el compromiso del personal en el uso de la metodología de gestión de riesgos.
11. Durante la ejecución del piloto, se detectaron situaciones culturales como por ejemplo, la asignación de la responsabilidad de la rendición de cuentas sobre el estatus del riesgo y sus planes de acción a quien lo identifica. Esta condición, no relacionadas con aspectos tecnológicos, desincentiva que las personas realicen mayores aportes a la gestión de riesgos por lo cual es indispensable resolverla con el fin de que no siga impactando negativamente el adecuado funcionamiento y eficiencia de la gestión de riesgos organizacional.
12. El análisis de correlación entre los incidentes materializados y los riesgos, según el nivel de criticidad es una métrica innovadora que permite analizar

si el pronóstico del futuro a nivel de riesgos tiene un apego a la realidad histórica de los incidentes a nivel estadístico.

13. Se encuentran disponibles estudios, accesibles a nivel público, realizados por organizaciones como el Instituto Ponemon los cuales permiten cuantificar en términos económicos afectaciones a la confidencialidad o integridad de la información. Esta es una herramienta valiosa para este tipo de investigaciones pues de manera aislada no era sencillo lograr estimar un costo cercano a la realidad.
14. Con la herramienta propuesta fue posible identificar durante la ejecución del piloto, un total de 61 riesgos. Esto corresponde a un 74% más de los riesgos identificados con la metodología actual, lo cual permitió casi duplicar la cantidad total de riesgos formalmente documentados y activos en un ejercicio de cuatro horas con 14 participantes.
15. La herramienta implementada en Sharepoint permitió a cada participante ingresar los riesgos de manera autónoma e independiente, ingresando a la aplicación desde su propio computador. Con la herramienta anterior esto no era viable por cuanto la identificación de riesgos se realizaba en reuniones con cada gerencia, involucrando a los líderes de riesgos y únicamente una persona era quien documentaba dentro de la herramienta en Excel mientras el resto de participantes se limitaba exclusivamente a observar o en el mejor de los casos opinar sobre la calificación que se asignaba a cada riesgo. Esta facilidad le permite a la organización incrementar considerablemente la productividad en la gestión de riesgos, brindando eficiencia y haciendo un uso racional del tiempo de los participantes.
16. Aunque si bien la herramienta utilizada dentro del piloto permitió aumentar la productividad, se detectaron al menos dos riesgos duplicados debido a que dos participantes diferentes ingresaron el mismo riesgo.
17. El 80% de los riesgos identificados durante el piloto quedaron asignados a las clasificaciones de criticidad media (48%) y alta (31%). Por el contrario, los riesgos de criticidad baja y crítica representaron únicamente un 20% del total identificado durante el piloto.

18. Solamente un 8% de los riesgos identificados durante el piloto fueron clasificados como de Baja criticidad. Como posible justificación a este comportamiento se consideró el hecho de que la concentración del personal típicamente se centra en las vulnerabilidades que puedan afectar considerablemente el servicio y no así eventos de poca relevancia.
19. Posterior a evaluar los riesgos identificados por el personal participante del piloto, predominan los riesgos clasificados como criticidad Media (48%) sobre los clasificados como criticidad Alta (31%) y Crítica (13%). Si consideramos la relación que existe con los incidentes según criticidad, esto implica que la metodología contribuyó a sensibilizar la evaluación de los riesgos apoyados en los criterios utilizados por la metodología.
20. Un 64% de los riesgos identificados durante el piloto lograron contar con al menos una dimensión con un impacto económico asociado. Actualmente ninguno de los riesgos documentados con la metodología actual de la organización tienen impacto económico asociado al mismo.
21. De todos los riesgos a los cuales se les identificó impacto económico, a un 74% se les relacionó un costo tangible, esto significa que el valor económico asignado tiene una certeza muy alta de cumplirse en caso de materializarse el riesgo. Estos costos tangibles corresponden a las dimensiones de Disponibilidad y Cumplimiento Regulatorio. Estas dimensiones tuvieron un predominio sobre las de Integridad y Confidencialidad que generan costos intangibles.
22. De la totalidad de los riesgos identificados durante la ejecución del piloto, a un 48% se les logró documentar al menos una acción de respuesta con un costo de ejecución asociado. De estos 29 riesgos, solo a 19 se les designó al menos un plan de acción, seleccionado de las acciones de respuesta identificadas.
23. Un 33% de los riesgos recibió como estrategia de respuesta la aceptación del riesgo por parte de los participantes del piloto. Para la organización representa un ahorro el no tener que invertir tiempo del personal en la definición de planes y también el costo de cada plan.

24. Un 6% de los riesgos recibió como estrategia de respuesta la alternativa de Evitar y a un 2% se les asignó la alternativa de Transferir el riesgo lo cual son modalidades nueva en el tratamiento que pueden recibir los riesgos identificados.
25. Únicamente a un 41% de los riesgos, se les asignó Mitigar como estrategia de respuesta que es el enfoque tradicional de respuesta de la metodología actual. Con esto se concluye que se redujo a más de la mitad la cantidad de riesgos a Mitigar.
26. Con la nueva metodología el coeficiente de correlación de Pearson entre incidentes y riesgos identificados por la metodología propuesta generó un resultado de 0.86 lo cual significa que existe un buen nivel de alineamiento entre ambas variables.
27. Al evaluar diferentes criterios relacionados con el nivel de satisfacción con la metodología propuesta, la mayor calificación obtenida corresponde a la variable que mide el Nivel de satisfacción en general que aumento de 0% a 78% y la variable que mide la satisfacción con la herramienta que aumentó de 10% a 78% comparando Excel con la herramienta utilizada en el piloto.
28. La nota de evaluación del nivel de satisfacción general con la metodología de gestión de riesgos (nota promedio de evaluación de todos los criterios) aumentó de un 20% que obtuvo la metodología actual a un 67% que obtuvo la metodología propuesta.
29. Se cumplieron todos los indicadores de medición propuestos. Sin embargo, el índice de correlación de incidentes vs riesgos tuvo un mejor resultado (0.99) con la metodología actual versus la metodología propuesta (0.86)
30. Si la organización decide realizar la inversión en este proyecto podrá ser recuperada casi en su totalidad el siguiente año con la finalización los primeros planes identificados dentro del análisis de riesgo y los ahorros que esto puede generar.

13.2. Recomendaciones

A continuación se listan las principales recomendaciones identificadas en la investigación:

1. La Gerencia Regional de Riesgo y Seguridad debe capacitar a corto plazo al personal involucrado en la metodología de gestión de riesgo para que reconozcan los marcos de gestión de riesgos y puedan diferenciarlos de otros estándares, certificaciones o las instituciones que los respaldan. Asimismo considerar en las capacitaciones la aclaración sobre cuál es el marco de trabajo sobre el cual está basada la metodología de gestión de riesgo que utiliza la organización dado que se detectaron algunas confusiones de conceptos en las encuestas.
2. La Gerencia Regional de Riesgo y Seguridad debe continuar aprovechando las ventajas que provee el sistema de calidad que posee la organización, documentando las mejoras a los procesos e instrumentos de gestión de riesgos dentro de dicho sistema y divulgándolos para sacar provecho de la amplia cobertura y seguimiento que tiene esta base documental.
3. La Gerencia Regional de Riesgo y Seguridad debe considerar a corto/mediano plazo sustituir la herramienta utilizada para la gestión de riesgos (plantillas en Microsoft Excel) por una solución automatizada que facilite la gestión de riesgos y provea mayor integridad a la información que ahí se documenta cómo fue posible demostrar en la ejecución del piloto con la herramienta desarrollada en Sharepoint. Adicionalmente el implementar esta solución como una aplicación Web permitirá aumentar la productividad y satisfacción del personal a más del doble comparado con la herramienta actual, según los resultados obtenidos en el piloto.
4. La Gerencia Regional de Riesgo y Seguridad debe realizar mejoras a la plantilla para el registro de nuevos riesgos, consolidando todas las variables cualitativas y cuantitativas (frecuencia, impacto en integridad,

impacto en disponibilidad, impacto en imagen, impacto legal, etc.) con el objetivo de estandarizar, simplificar y hacer más predecible la evaluación cuando se incluyen nuevos riesgos. Esto adicionalmente aumenta la productividad del personal al tener toda la información relacionada unificada en un único repositorio y mejora la satisfacción de los usuarios con la herramienta.

5. La Gerencia de Seguridad y Riesgo debe analizar y profundizar con los usuarios de la metodología de gestión de riesgos por qué a pesar de que se utilizó una guía para la identificación de riesgos y un catálogo de escenarios de riesgos genéricos con el fin de estructurar y proveer más orientación en sustitución del método de lluvia de ideas, aún consideran que la identificación de riesgos no es un proceso guiado y predecible. Asimismo debe continuar los esfuerzos para lograr que la identificación y evaluación de riesgos es un proceso más predecible.
6. La Gerencia Regional de Riesgo y Seguridad debe mejorar el enfoque de los esfuerzos del personal y los recursos de la organización brindando respuestas a los riesgos de mayor peso incorporando a los modelos de priorización de riesgos tecnológicos, donde sea factible, la cuantificación de costos tangibles y intangibles (impacto en confidencialidad, impacto en integridad, impacto en disponibilidad, impacto legal etc.) en términos económicos de manera que permitan obtener una visión completa de la exposición en pérdidas a la que estaría sujeta la organización y potenciales ahorros si se evita la materialización del riesgo.
7. La Gerencia Regional de Riesgo y Seguridad puede incorporar dentro de los instrumentos de evaluación de riesgos, la cantidad de transacciones afectadas por servicio al momento de evaluar un riesgo que afecte la disponibilidad de un servicio para considerar esta variable en el cálculo de los costos tangibles según el esquema propuesto por el investigador y la gerencia de Canales.

8. La Gerencia Regional de Riesgo y Seguridad debe incorporar dentro de los instrumentos de evaluación de riesgos, la cantidad de registros comprometidos / afectados al momento de evaluar un riesgo que afecte la integridad o confidencialidad de un servicio con el fin de utilizar esta variable en el cálculo de los costos intangibles, tomando como referencia los estudios realizados por organizaciones como el Instituto Ponemon, los cuáles permiten cuantificar en términos económicos afectaciones a la confidencialidad o integridad de la información.
9. La Gerencia Regional de Riesgo y Seguridad debe capacitar a corto plazo al personal involucrado en la metodología de gestión de riesgo para que puedan diferenciar entre los impactos tangibles e intangibles que un riesgo conlleva y como algunos de estos impactos intangibles pueden llegar a expresarse en términos económicos para lograr un mejor entendimiento de la contribución que darán cuando se involucren estas variables en los instrumentos de gestión de riesgo.
10. La Gerencia Regional de Riesgo y Seguridad debe capacitar al personal en el uso de los instrumentos que forman parte de la metodología de gestión de riesgos, considerar variables requeridas de manera obligatoria y cuáles son opcionales. Esto es importante por cuanto se detectaron inconsistencias entre los encuestados respecto al uso de estas variables.
11. La Dirección de Informática debe mejorar los métodos utilizados por la organización para incentivar la participación y contribución del personal en el enriquecimiento de la metodología de gestión de riesgos cambiando las evaluaciones de desempeño del personal y la asignación de la responsabilidad de los riesgos de manera tal que promuevan la participación y aporte del personal a la efectividad de la metodología de gestión de riesgos. Asimismo establecer metas comunes para todos los participantes en los indicadores clave de los procesos de gestión de riesgo y publicarlos consistentemente para facilitar la mejora continua del proceso.

12. La Dirección Regional de Productividad y Riesgos debe continuar analizando la correlación entre incidentes materializados y riesgos identificados por criticidad. Estas mediciones permitirán justificar la necesidad de realizar revisiones en la forma en que se evalúan los riesgos en caso de encontrar desviaciones importantes.
13. La Gerencia Regional de Riesgo y Seguridad debe incorporar como posibles estrategias de respuesta las opciones de Evitar, Transferir y Aceptar, además de la alternativa de Mitigar que ya se usa de manera discriminada. Esto permitirá reducir los costos de la organización en evaluación de riesgos que no superar el apetito de riesgo de la organización o considerar otras alternativas menos costosas de atención al riesgo.
14. La Dirección de Informática debe impulsar la adopción de la metodología propuesta en esta inversión considerando que la inversión puede recuperarse al término de un año a partir de los ahorros que puede generar en prevención de riesgos, costos que ahora pueden ser cuantificados con las evaluaciones consideradas en la metodología.
15. La Dirección de Informática puede utilizar los resultados de la implementación de la metodología propuesta para establecer un lenguaje común de comunicación y entendimiento con el negocio en términos económicos al momento de tomar decisiones sobre los riesgos en el dominio de gobierno de riesgos.

13.3. Acciones futuras

En este capítulo se consideran los pasos que la organización debería tomar a corto y largo plazo, a partir de la experiencia obtenida en la ejecución del piloto y los resultados de aplicar la metodología.

13.3.1. Acciones de corto plazo (< 6 meses)

A corto plazo (6 meses), la organización debería considerar las siguientes actividades:

1. Es recomendable que dentro de los requerimientos para el desarrollo de la herramienta de gestión de riesgos se consideren controles adicionales a los utilizados en la herramienta que apoyó la ejecución del piloto con el fin de prevenir la duplicación de riesgos cuando se ingresan nuevos riesgos en la herramienta. Durante la ejecución del piloto, los participantes recomendaron como alternativa, habilitar la opción de consulta previa de todos los riesgos existentes, opción disponible para todas las personas que requieran utilizar la herramienta, con el fin de que puedan consultar que riesgos existen actualmente para así eliminar el riesgo de duplicación.
2. Se recomienda ajustar la metodología propuesta y herramientas de apoyo para que la evaluación de los riesgos realizada por los participantes, principalmente las variables utilizadas para la estimación de aspectos cuantitativos, sean revisados por una persona del equipo de riesgos que tenga la experiencia en el dimensionamiento y evaluación de los mismos. Esto por cuanto algunas de las estimaciones económicas realizadas por quienes ingresan los riesgos podrían no ser realistas. Una alternativa viable, comprendería incorporar a la herramienta facilidades de flujos de trabajo (workflow) para efectos de que los riesgos propuestos por los participantes cumplan con etapas de aprobación y revisión, previa a su oficialización con el fin de reducir la posibilidad de duplicación de riesgos y una inadecuada estimación.
3. En general, es necesario considerar en el desarrollo de la herramienta aspectos de usabilidad que fueron identificados por los usuarios durante la ejecución del piloto con el fin de poder lograr un mayor nivel de satisfacción en el uso de la nueva herramienta que se proponga para implementar la gestión de riesgos.
4. Es recomendable incluir dentro de la lista de servicios considerados actualmente en la herramienta, otros servicios que no forman parte de las métricas que calcula el área de Canales Regionales. Actualmente la lista de servicios que se cargó en la herramienta fue tomada de los indicadores que genera el área de Canales. Sin embargo, se detectó durante el piloto que

existen otros servicios pertenecientes al canal de banca electrónica que no forman parte de esos indicadores y que deben aparecer para poder asignarles riesgos.

5. Se considera importante estandarizar el modelo de priorización de riesgos para que se aplique de la misma forma en todos los contextos y diferentes herramientas de la organización. Esto implica que el modelo y herramienta debe ser exportado a las diferentes áreas de tecnología que se encuentran en los países de forma tal que exista uniformidad y consistencia cuando se analicen los riesgos asociados a tecnología. Para lograr esto es indispensable que se considere a los países en el levantamiento de requerimientos y desarrollo de la herramienta para conocer sus expectativas de antemano.

13.3.2. Acciones a mediano plazo (6 a 24 meses)

1. Someter a evaluación de los Comités de Gobierno Corporativo de cada país los modelos propuestos para estimar los costos intangibles de Confidencialidad e Integridad con el fin de afinar el costo asignado a cada registro y de ser necesario sensibilizarlo a la realidad de cada mercado.
2. Se recomienda que en una segunda etapa se amplíen las funcionalidades de la nueva herramienta que se desarrolle para apoyar la metodología de gestión de riesgos con el fin de que pueda incorporar actividades de la dimensión de Gobierno de Riesgos como por ejemplo, la alternativa de presentar los riesgos de manera resumida dentro de un mapa de riesgos o un informe del estado de los planes de acción para facilitar el seguimiento y la toma de decisiones.
3. Se identifica la oportunidad de incorporar opciones de reportes analíticos a la herramienta de gestión de riesgos que faciliten el análisis de los riesgos y el seguimiento a los planes de acción.
4. Se recomienda que en una segunda etapa se analice la oportunidad de realizar una integración de la herramienta de gestión de riesgos con el repositorio de información que genera el proceso de gestión de incidentes con el fin de

aprovechar la información generada (impactos y pronósticos) al momento de realizar evaluaciones de riesgos.

5. Considerando que uno de los aprendizajes de este trabajo de investigación fue que los riesgos pueden tener impactos positivos (oportunidades) y no únicamente negativos (pérdidas) se recomienda que se analice la posibilidad de incorporar dentro del análisis cuantitativo no únicamente el impacto negativo (pérdidas) sino posibles oportunidades que puedan repercutir positivamente en los resultados de la organización.
6. Se debe considerar la actualización periódica de la distribución transaccional que se procesa a partir del canal de banca electrónica con el fin de mantener actualizado los parámetros en la herramienta automatizada que permiten calcular el impacto generado por una afectación en la disponibilidad de un servicio.
7. Se debe considerar la actualización periódica de los rangos de multas a las que se encuentra expuesta la organización por incumplimiento regulatorio o legal en la banca electrónica con el fin de mantener actualizado los parámetros en la herramienta automatizada que permiten calcular el impacto generado por incumplimientos legales.

13.3.3. Acciones a largo plazo (> 24 meses)

1. Con la experiencia generada en la herramienta se considera que agregaría valor entender el uso de la metodología y herramienta desarrollada a otros servicios diferentes a la Banca Electrónica. Esta ampliación podría priorizarse basado en un criterio de criticidad del servicio para la organización.
2. La organización puede generar perfiles por cada servicio implementado en la metodología de gestión de riesgos que contenga información clave para uso de los evaluadores tales como: transacciones realizadas por unidad de tiempo, clientes afiliados, montos transados por unidad de tiempo, clasificación de la información que maneja dicho servicio, posibles impactos por incumplimientos legales, entre otros. Esta información debería revisarse con una periodicidad de cada seis meses y actualizar los valores que correspondan dentro de la

herramienta de gestión de riesgos y divulgar el resto a todas las personas que contribuyen a la gestión de riesgos.

3. Dentro de esta investigación no fue factible lograr encontrar un modelo apropiado para cuantificar el impacto en imagen que un riesgo puede generar por lo que se puede retomar la investigación de algún método que permita implementar un modelo de estimación de costos intangibles para la dimensión Imagen a partir de la variable “Cantidad de usuarios impactados potencialmente por el riesgo” que el modelo va a seguir capturando aunque no realice ninguna estimación monetaria.

CAPITULO VIII – Análisis retrospectivo

En el presente capítulo se enumeran las diferentes lecciones aprendidas que el desarrollo de este trabajo generó en los autores.

A partir de la realización de este trabajo, se lograron capitalizar varios aprendizajes que fueron generándose en el transcurso de la elaboración del mismo. Tan solo al arranque de la investigación, fue necesario cambiar el nombre y alcance de manera que se enfocara en analizar la metodología de gestión de riesgos comparado contra las mejores prácticas y no la exposición abierta de los riesgos de la organización. Esto fue necesario debido a retos que se presentaron, relacionados con la confidencialidad de la información de la organización. Con el nuevo alcance fue posible reducir considerablemente el nivel de exposición que tenía el anterior alcance y hacer factible la continuidad de la investigación.

Posteriormente, al desarrollar el Marco Teórico se aclararon varios conceptos, lo cual nos condujo a redefinir la propuesta de investigación, de forma tal que se replanteó la propuesta inicial de analizar CRISC, CGEIT y COBIT como marcos de gestión de riesgo y sustituirlos por otros estándares como Risk IT (base de las certificaciones CRISC y CGEIT de ISACA) e ITIL y PMBOK.

En cuanto a la planificación del cronograma de actividades, se cometió un error por parte del investigador por cuanto se construyó el cronograma sin percatarse que no estaba alineado a las entregas programadas a nivel de la maestría en cada semana. Esto generó un conflicto dado que mientras se dedicaba tiempo al diagnóstico de situación actual, a nivel de entregas de la maestría se esperaban resultados de marco teórico y marco metodológico. A pesar de que se pudo adelantar trabajo de las fases posteriores, consideramos que lo mejor debería haber sido arrancar con el marco teórico y metodológico antes realizar el análisis de situación actual.

Definitivamente esta investigación permitió adquirir mucho conocimiento de cómo conducir y documentar una investigación de carácter científico/académico con sus

diferentes partes (marco teórico, marco metodológico, análisis de situación actual, etc.). Sin embargo, el contenido de cada uno de estos apartados no estuvo claro desde el inicio sino hasta que el proyecto ya iba en marcha se iban aclarando los aspectos. Por esta razón, es importante que la maestría considere mejorar la orientación al estudiante en este punto y provea un mejor detalle de lo que se espera en cada apartado del documento final como parte de las guías que se entregan a los estudiantes al inicio del curso y brinde sugerencias de bibliografía que pueden servir de base al estudiante para facilitar su investigación. Esto se torna aún más relevante si consideramos el poco tiempo (3 meses) que se tiene para producir un resultado.

El punto anterior se torna crítico en casos de estudiantes que retoman su proyecto después de haber estado separados como estudiantes regulares por varios años y desligados de actividades académicas con la maestría. Para estos casos particulares, de estudiantes que están retomando su proyecto después de varios años de ausencia, se le hizo la sugerencia a la maestría para considerar una nivelación como parte de los requisitos para desarrollar el proyecto. Es muy satisfactorio confirmar que esta observación fue considerada pues cercano a la finalización de este proyecto se recibió por parte de la maestría una invitación para participar en un Taller de Técnicas de Investigación de manera gratuita. Por esta razón, se reconocen y aprecian los esfuerzos de mejora continua realizados por la Maestría. Esto proyecta una excelente imagen del personal a cargo y este tipo de cultura genera un sentido de orgullo y pertenencia a todos los aspiramos a ser egresados de la misma.

Al finalizar la investigación se reconoce y valora la adquisición de conocimientos sobre marcos de trabajo de gestión de riesgos para tecnología de información y los beneficios que la incorporación de un marco de este tipo provee a las organizaciones. Asimismo obtener conciencia acerca de las brechas que existen sobre un esquema de trabajo actual y lo que las mejores prácticas a nivel de gestión de riesgos de TI pueden aportar para efectos de cerrar dichas brechas.

En cuanto al objetivo que se propuso al inicio del trabajo de investigación, es muy satisfactorio el haber logrado implementar un esquema de cuantificación de costos asociados a riesgos, apoyados en investigaciones realizadas por organizaciones reconocidas a nivel mundial. Esta fuente de información le aporta robustez y sustento a la propuesta realizada por el investigador y permite refinar paulatinamente el modelos de gestión de riesgos utilizado por esta o cualquier otra organización de manera tal que se puedan tomar mejores decisiones considerando no únicamente los aspectos cualitativos sino variables cuantitativas que ninguna de las metodologías de gestión de riesgos analizadas consideran como parte de su estructura base de evaluación de riesgos.

Por otro lado, un aprendizaje menor, pero no menos importante, de la ejecución del proyecto tiene que ver con:

1. Un aumento del conocimiento de herramientas de ofimática (Word, Excel y Powerpoint) por parte del investigador para producir informes y análisis ejecutivos que sustentan mucha de la información generada en esta investigación. El manejo de operadores lógicos (OR, AND) y funciones financieras en Excel, el manejo de estilos y referencias bibliográficas en Word y el manejo de patrones de diapositivas en Powerpoint son algunos ejemplos de los conocimientos adicionales adquiridos.
2. Un conocimiento en el uso de herramientas automatizadas para recolección y análisis de datos de encuestas. Para este trabajo de investigación, se utilizó el servicio de SurveyMonkey.com (https://es.surveymonkey.com/) el cual facilitó la recolección de la retroalimentación de la opinión de los usuarios de la metodología de gestión de riesgos, los gerentes y los participantes del piloto permitiendo realizar estas actividades en un tiempo récord.
3. El uso de la herramienta Dropbox (http://www.dropbox.com) la cual facilitó el desarrollo de la investigación desde diferentes dispositivos pero

manteniendo sincronía entre todo el contenido generado, indistintamente del dispositivo utilizado pues la información se almacena en la nube. Adicionalmente la facilidad de uso se incrementa al contar con aplicaciones para dispositivos móviles que permiten la visualización en cualquier lugar, a cualquier hora y desde cualquier dispositivo más la posibilidad de compartir los documentos con el profesor.

4. El análisis de información no normalizada, principalmente información asociada a la evaluación de riesgos y sus acciones de respuesta, la cual fue capturada por la aplicación implementada para el desarrollo del piloto dentro de la base de datos en un formato relacional no normalizado. Esta situación se origina debido a restricciones con la versión de la herramienta de Sharepoint utilizada la cual impidió separar la información en tablas diferentes. No obstante, con el uso de Excel y el apoyo del desarrollador del piloto fue posible segmentar la información para un análisis posterior de los planes.

Es interesante que culturalmente la palabra riesgo siempre la asociamos con un contexto negativo. Sin embargo, dentro de la literatura consultada se habla de efectos negativos pero también positivos que pueden beneficiar el resultado deseado. Los riesgos, al igual que ocurre en nuestra vida, pueden representar oportunidades que se presentan y está en cada individuo u organización el tomar las decisiones necesarias para tomar ventaja y aprovechar las mismas. La finalización de este proyecto representa precisamente eso, el aprovechamiento de una oportunidad que se presentó en la vida del investigador para efectos de cerrar un pendiente abierto desde inicios del año 2000 y que con el apoyo muchas personas cercanas fue posible capitalizar con éxito.

Referencias Bibliográficas

Basel Committee on Banking Supervision. (01 de 2001). *Operational Risk in the Basil II framework.* Obtenido de http://www.bis.org: http://www.bis.org/publ/bcbsca07.pdf

Fondo Monetario Internacional. (09 de 2011). *Gestión del riesgo operacional y planificación de la continuidad de las operaciones para tesorerías estatales modernas*. Recuperado el 18 de 03 de 2015, de Sitio Web del FMI: https://www.imf.org/external/spanish/pubs/ft/tnm/2011/tnm1105s.pdf

Gaughan, T. (2010). *Comparing ISO/IEC 20000 Part 1 Requirements to ITIL V3 Processes and Functions.* Recuperado el 03 de 2014, de PA&E Global: http://www.paeglobal.com/library/Comparison_of_ISO_20K_to_ITIL_V3.pdf

González, P. A. (15 de 03 de 2008). *Tratado de Basillea II*. Recuperado el 18 de 03 de 2015, de Sitio Web www.monografias.com: http://www.monografias.com/trabajos57/tratado-basilea/tratado-basilea2.shtml

Hernández, S. R. (2006). *Metodología de la investigación.* México: McGraw - Hill.

ISACA. (s.f.). *Certified in Risk and Information Systems Control (CRISC) Fact Sheet*. Recuperado el 03 de 2014, de Sitio Web de ISACA.ORG: http://www.isaca.org/About-ISACA/Press-room/Pages/CRISC-Fact-Sheet.aspx

ISACA. (s.f.). *Certified in the Governance of Enterprise IT (CGEIT) Fact Sheet*. Recuperado el 03 de 2014, de Sitio de ISACA.ORG: http://www.isaca.org/About-ISACA/Press-room/Pages/CGEIT-Fact-Sheet.aspx

ISACA. (2013). *CGEIT Review Manual 2013 (Certified in the Governance of Enterprise IT).*

ISACA. (s.f.). *COBIT 5 Introducción.* Recuperado el 02 de 2015, de http://www.isaca.org: http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

ISACA. (s.f.). *COBIT 5 Introducción.* Recuperado el 03 de 2014, de http://www.isaca.org: http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

ISACA. (03 de 2014). *History of ISACA*. Recuperado el 03 de 2014, de http://www.isaca.org: http://www.isaca.org/about-isaca/history/pages/default.aspx

ISACA. (2009). *The Risk IT Practitioner Guide.* Rolling Meadows, Illinois, EEUU.

ISACA. (2009). *The Risk IT Practitioner Guide.* Rolling Meadows, Illinois, EEUU.

IT Process Maps. (s.f.). *ITIL Gestion del Riesgo.* Recuperado el 03 de 2014, de IT Process Maps: http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_del_Riesgo

ITIL ORG. (s.f.). *What is COBIT - Overview*. Recuperado el 02 de 2015, de Sitio Web de itil.org: http://os.itil.org/en/vomkennen/cobit/ueberblick/index.php

ITIL ORG. (s.f.). *What is COBIT - Overview*. Recuperado el 03 de 2014, de Sitio Web de itil.org: http://www.itil.org/en/vomkennen/cobit/ueberblick/index.php

Martinez, F. F. (s.f.). *Gestión de la Planificación de los Riesgos del Proyecto*. Recuperado el 18 de 03 de 2015, de UCI: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CD8QFjAE&url=http%3A%2F%2Fwww.ucipfg.com%2FRepositorio%2FMAP%2FMAPD-10%2Fpresentaciones%2FGesti%25C3%25B3n%2520de%2520la%2520Planificaci%25C3%25B3n%2520de%2520los%2520Riesgos%2520del%2520Proyecto%2520-%2520Tema%252006.pptx&ei=TKglVeyXIYP3oATM9oEY&usg=AFQjCNEwjI-24vYOXc9FnPg2hHG5Cyljdg&sig2=VFt1I-Ew4kRAO1V0yaGQ2g&bvm=bv.90491159,d.cGU

Monografías. (s.f.). *Monografias*. Recuperado el 15 de 03 de 2015, de http://www.monografias.com: http://www.monografias.com/trabajos85/coeficiente-correlacion-karl-pearson/coeficiente-correlacion-karl-pearson.shtml

Odin. (12 de 12 de 2009). *Which ITIL processes include risk analysis and management activities?* . Recuperado el 03 de 2014, de IT Service Management Oasis: http://askme4itsm.blogspot.com/2009/10/which-itil-processes-include-risk.html

Oficina de Calidad de los Servicios Secretaria General de la Gobernación de Salta. (s.f.). *Algunas nociones sobre los costos de la No Calidad.* Recuperado el 03 de 2014, de Gobierno de la Provincia de Salta:

http://www.salta.gov.ar/descargas/archivos/ocspdfs/ocs_algunas_nociones_sobre_los_costos_de_la_no_calidad.pdf

OGC. (2007). *Libro ITIL V3 Service Design.* Londres, Reino Unido: TSO.

OGC. (2007). *Libro ITIL V3 Service Transition.* Londres, Reino Unido: TSO.

OGC. (2007). *Libro ITIL V3 Service Transition.* Londres, Reino Unido: TSO.

PMI. (2013). *A Guide to the Project Management Body of Knowledge (PMBOK Guide 5th edition).* Pennsylvania, EEUU: PMI Publications.

Ponemon Institute. (2014). *http://www.ibm.com/services/costofbreach*. Recuperado el 18 de 3 de 2015, de http://www.ibm.com/services/costofbreach: http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Purdy, G. (2010). *ISO 31000:2009—Setting a New Standard for Risk Management.* Recuperado el 03 de 2014, de http://broadleaf.com.au/: http://broadleaf.com.au/wp-content/uploads/2010/06/Art_RiskAnalysis_ISO31000.pdf

Purdy, G. (2010). *ISO 31000:2009—Setting a New Standard for Risk Management.* Recuperado el 03 de 2014, de http://www.broadleaf.com.au/: http://www.broadleaf.com.au/pdfs/articles/art_riskanalysis_iso31000.pdf

Sampieri, R. H. (1997). *METODOLOGÍA DELA INVESTIGACIÓN.* Mexico, Mexico: MCGRAW-HILL.

Symantec. (2013). *Data Breach Risk Calculator*. Recuperado el 18 de 3 de 2015, de DataBreachcalculator.com: http://www.databreachcalculator.com/Calculator/#

Universidad de Sevilla. (s.f.). *COEFICIENTE DE CORRELACIÓN LINEAL DE PEARSON* . Recuperado el 18 de 03 de 2015, de http://www.us.es/: http://personal.us.es/vararey/adatos2/correlacion.pdf

Valdez, M. (4 de 12 de 2012). *Planificar la respuesta a los riesgos*. Recuperado el 18 de 03 de 2015, de Administración de Proyectos: http://itsm-admon-proy.blogspot.com/2012/12/planificarla-respuesta-los-riesgos.html

WikiBooks. (s.f.). Obtenido de http://en.wikibooks.org/wiki/ITIL_v3_%28Information_Technology_Infrastructure_Library%29/Service_Design

Wikipedia. (s.f.). *http://es.wikipedia.org/wiki/Basilea_II*. Recuperado el 04 de 2014, de Wikipedia: http://es.wikipedia.org/wiki/Basilea_II

Wikipedia. (s.f.). *http://es.wikipedia.org/wiki/Coeficiente_de_correlaci%C3%B3n_de_Pearson*. Recuperado el 15 de 03 de 2015, de http://es.wikipedia.org: http://es.wikipedia.org/wiki/Coeficiente_de_correlaci%C3%B3n_de_Pearson

ANEXOS

Anexo 1 - Minutas entrevistas

MINUTA	
Nombre del proyecto: Metodología de gestión de riesgos de operación para un servicio de TI Tema: **Entender de manera ejecutiva la visión y esquema actual de la gestión de riesgos en la organización**	**Lugar y Fecha:** Oficina Marco Fonseca, 03/Feb/14 **Hora:** 5:00PM A 6:00 PM

1. Presentes:

Nombre	Área
Marco Fonseca (MFonseca)	GPRO
Jorge Betancourth (JBetancourth)	GRSI

2. Ausentes:

Nombre	Área

3. Agenda de la reunión:

Hora	Tema	Responsable	Resultado esperado
5:00 PM	Alcance y objetivos de Proyecto ajustados	Mfonseca	Informar propósito y cambios
5:30 PM	Visión del Sponsor	Jbetancourth	Entender situación actual
5:45 PM	Áreas de enfoque	Jbetancourth	Entender Preocupacion

			es, necesidades y recomendaciones

4. Acuerdos:

Tema	Acuerdo	Tomado por:
Visión del Sponsor	Analizar documentación entregada por el Sponsor (Manual de curso Gestión de Riesgos Operativos) en la etapa de análisis del proyecto.	Presentes
Áreas de enfoque	Abordar dentro de la investigación las siguientes preocupaciones del sponsor: A. Empirismo metodología actual (no es un ejercicio guiado paso a paso sino resultado de un proceso de lluvia de ideas donde cada quien documenta según su imaginación y experiencia) B. Identificación de riesgos de la dimensión personas asumidos por actos de Dios (agentes externos) C. Evaluación de los riesgos no es consistente si lo hacen dos personas diferentes, altamente sujeto a interpretación (poca predictibilidad)	Presentes
Áreas de enfoque	Considerar dentro del análisis y propuesta, una práctica que ha resultado exitosa en el pasado y es la identificación de riesgos de manera conjunta y no individual.	Presentes
Áreas de enfoque	Considerar dentro del análisis y propuesta la eliminación de ambigüedades (por ejemplo, hoy en día la metodología dice revisión exhaustiva una vez	Presentes

	al año. No se especifica ni aclara que significa exhaustivo)	
Áreas de enfoque	Cuestionar dentro del análisis si realmente el proceso de gestión de riesgos es costo efectivo dado que es muy complejo	Presentes
Áreas de enfoque	Revisar si existe un desenfoque en la identificación y clasificación de riesgos. Por ejemplo: 1. Se han detectado como riesgos principales situaciones que no corresponden a tal criticidad (Riesgos de Caja Chica) 2. Incidentes mayores que se han materializado no estaban declarados como riesgos 3. El volumen de riesgos detectados por un área es alto (>4000)	Presentes

5. Compromisos adquiridos

Tema tratado	Compromiso	Responsable	Fecha de compromiso
Alcance y Objetivos del Proyecto	Solicitar aprobación al CIO de revelación de información contenida dentro del objetivo específico 2) Analizar las prácticas actuales de gestión de riesgos en la organización para determinar las brechas que existen en comparación con las mejores prácticas de gestión de riesgos de la industria.	MFonseca	16/Feb/2014
Alcance y Objetivos del Proyecto	Analizar la factibilidad de analizar norma de Basilea II en sustitución de COBIT 5	Presentes	24/Feb/2014

	dado que CRISC, CGEIT y COBIT 5 todos provienen de ISACA		

6. Otros temas:

Anexo 1: Documentos

20140203 Anteproyecto MFonseca vFinal.d

MINUTA	
Nombre del proyecto: Metodología de gestión de riesgos de operación para un servicio de TI Tema: **Entender de manera ejecutiva la visión y esquema actual de la gestión de riesgos en la organización**	**Lugar y Fecha:** Oficina Marco Fonseca, 12/Feb/14 **Hora:** 2:00PM A 3:15 PM

1. Presentes:

Nombre	Área
Marco Fonseca (MFonseca)	GPRO
Daniel Iván Chacón (DChacón)	GRSI

2. Ausentes:

Nombre	Área

3. Agenda de la reunión:

Hora	Tema	Responsable	Resultado esperado
2:00 PM	Alcance y objetivos de Proyecto	Mfonseca	Informar propósito proyecto
2:15 PM	Visión General	Dchacon	Entender visión general gestión de riesgos en la organización
2:30 PM	Áreas de enfoque	DCHacon	Entender Preocupaciones, necesidades y recomendaciones

4. Acuerdos:

Tema	Acuerdo	Tomado por:
Visión General	Existen tres componentes claves a nivel de documentación que se deben abarcar: 1. Lineamiento de Gestión de Riesgos Operativos (se resume en la reserva que debe hacer la organización para afrontar cualquier riesgo materializado) 2. Proceso Evaluar y administrar los Riesgos (PO9) 3. Proceso Evaluación y gestión de Riesgos Tecnológicos (PO9)	Presentes

Áreas de enfoque	La propuesta a realizar debe buscar la eliminación de la subjetividad en el uso de las herramientas de gestión	Presentes
Áreas de enfoque	La propuesta debe considerar los instrumentos necesarios puesto que lo que se tiene en este momento es el vehículo o marco de trabajo general pero no es específico. Actualmente se está planteando un borrador de un checklist que puede analizarse	Presentes
Áreas de enfoque	Analizar cómo hacer un uso eficiente del tiempo de las personas invertido en la gestión de riesgos (“Lo que está escrito no promueve esta efectividad”)	Presentes
Áreas de enfoque	Considerar la eliminación de incentivos perversos (por ejemplo, se bajan puntos en la evaluación de las personas si no se identifican una cantidad mínima de riesgos en iteración)	Presentes
Áreas de enfoque	Revisar las siguientes debilidades dentro del análisis: 1. No están documentado los argumentos para asignar o transferir la propiedad de un riesgo una vez identificado 2. Las áreas de negocio no son propietarias de riesgos tecnológicos en la actualidad 3. Debe mejorarse la sincronía del estado de los planes de RT y RO	Presentes

5. Compromisos adquiridos

Tema tratado	Compromiso	Responsable	Fecha de compromiso
Áreas de enfoque	Remitir copia del Checklist Borrador que se está construyendo	DCHacon	16/Feb/2014

Áreas de enfoque	Remitir presentaciones utilizadas para las capacitaciones de Riesgo Operativo	Dchacon	14/Feb/2014

6. Otros temas:

Anexo 1: Documentos

Anexo 2 – Encuesta Evaluación Metodología Gestión de Riesgos TI BAC

Evaluación Metodología de Gestión de Riesgos de TI BAC Credomatic

La presente encuesta es realizada por el Ing. Marco Fonseca Aragón como parte de una investigación que forma parte de los requisitos para el Proyecto de Graduación de la Maestria en Administración de Tecnología (MATI) de la Universidad Nacional.

Esta investigación cuenta con el patrocinio del Sr. Jorge Betancourth (Gerente Regional de Seguridad y Riesgos) y cuenta con la aprobación del Sr. Roberto López (Director de Informática).

El objetivo de esta encuesta es poder recolectar información relevante para el análisis de la gestión de riesgo utilizada actualmente por la organización con el fin de determinar oportunidades de mejora comparando la ejecución actual versus el estado del arte en la gestión de riesgo en la industria financiera.

Agradecemos su tiempo para poder responde a las preguntas que se plantean a continuación.

Se estiman 15 minutos para completar el instrumento

***1. Favor elija cuáles de los siguientes conceptos corresponden a los marcos de trabajo de gestión de riesgo adoptados por su organización para implementar los procesos actuales**

- ☐ CISA
- ☐ CRISC
- ☐ PMBOK
- ☐ ISACA
- ☐ ISO 31000:2009
- ☐ COBIT
- ☐ COSO ERM
- ☐ CMMi
- ☐ M_o_R
- ☐ ISO/IEC 27000
- ☐ Basilea II
- ☐ OCTAVE
- ☐ ISO 20000
- ☐ CGEIT
- ☐ Risk IT
- ☐ ITIL

***2. Identifique al menos dos fortalezas de la metodología de gestión de riesgos utilizada actualmente por la organización**

***3. Identifique al menos dos oportunidades de mejora de la metodología de gestión de riesgos utilizada actualmente por la organización**

Page 1

Evaluación Metodología de Gestión de Riesgos de TI BAC Credomatic

***4. Indique la frecuencia con que se capturan las siguientes características al momento de identificar los riesgos asociados a servicios de TI .**

	No se utiliza	Ocasionalmente	Siempre se utiliza
Volumen transaccional	○	○	○
Probabilidad de ocurrencia	○	○	○
Criticidad del componente involucrado	○	○	○
Frecuencia con que ocurre	○	○	○
Severidad	○	○	○
Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas)	○	○	○
Criticidad del servicio del servicio involucrado	○	○	○
Impacto regulatorio	○	○	○
Apetito de Riesgo	○	○	○
Vulnerabilidad	○	○	○
Impacto medido en costos intangibles (pe pérdidas por mala reputacion e imagen)	○	○	○
Impacto en imagen (no cuantificado monetariamente)	○	○	○

Evaluación Metodología de Gestión de Riesgos de TI BAC Credomatic

***5. Califique según su criterio el nivel de eficiencia, efectividad y/o agilidad de las siguientes variables en la gestión de riesgos de la organización.**

	Bajo	Medio	Alto
Conocimiento y experiencia del personal participantes del proceso	○	○	○
Por qué? (favor justifique)			
Procesos de la gestión de riesgos	○	○	○
Por qué? (favor justifique)			
Herramientas	○	○	○
Por qué? (favor justifique)			
Indicadores claves de gestión	○	○	○
Por qué? (favor justifique)			
Patrocinio de los Gerentes y Directores	○	○	○
Por qué? (favor justifique)			
Mecanismos para aumentar el compromiso del personal	○	○	○
Por qué? (favor justifique)			

Evaluación Metodología de Gestión de Riesgos de TI BAC Credomatic

***6. Indique cuáles características se se utilizan actualmente por la organización para priorizar la atención de los riesgos identificados**

	No se utiliza	Ocasionalmente	Siempre se utiliza
Severidad	○	○	○
Criticidad del componente involucrado	○	○	○
Impacto medido en costos intangibles (pe pérdidas por mala reputacion e imagen)	○	○	○
Probabilidad de ocurrencia	○	○	○
Impacto regulatorio	○	○	○
Vulnerabilidad	○	○	○
Frecuencia con que ocurre	○	○	○
Impacto en imagen (no cuantificado monetariamente)	○	○	○
Volumen transaccional	○	○	○
Criticidad del servicio del servicio involucrado	○	○	○
Apetito de Riesgo	○	○	○
Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas)	○	○	○

Evaluación Metodología de Gestión de Riesgos de TI BAC Credomatic

***7. Al evaluar riesgos que puedan afectar la disponibilidad de un servicio crítico, favor indicar cuáles de las siguientes variables se cuantifican o traducen a términos económicos tomando en cuenta el tiempo de afectación?**

- ☐ Impacto en participación en el mercado
- ☐ Impacto en ventaja competitiva
- ☐ Impacto en participación de mercado
- ☐ Impacto en Productividad
- ☐ Costo de la respuesta al riesgo (Planes)
- ☐ Impacto en Satisfacción del cliente
- ☐ Impacto en percepción externa (cobertura negativa en medios de comunicación masivos como prensa, televisión, revistas, redes sociales, etc)
- ☐ Incumplimiento regulatorio o legal (Prisión, pérdidas financieras, revocación de licencias para operar, multas, etc)
- ☐ Ninguno de los anteriores
- ☐ Otro (especifique)

***8. Favor indicar cuales de los siguientes elementos se cuantifican y documentan al momento de definir los planes para atender un riesgo**

- ☐ Costo de la respuesta/plan definido para atender el riesgo (Evitar/Mitigar/Tranferir)
- ☐ Ahorros tangibles por reducción/mitigación del impacto del riesgo con los planes indicados
- ☐ Ahorros tangibles por evitar un riesgo
- ☐ Ahorros intangibles (imagen, reputación, etc) por reducción/mitigación del impacto del riesgo con los planes indicados
- ☐ Ahorros intangibles (imagen, reputación, etc) por evitar un riesgo
- ☐ Ninguno de los anteriores
- ☐ Otro (especifique)

***9. Favor indique su puesto en la organización**

Anexo 3 - Resultados Encuesta

Posterior a aplicar la encuesta a las dos muestras indicadas en el Marco Metodológico, se obtuvieron los siguientes resultados:

1. Personal responsable de los procesos de gestión de riesgos

Pregunta 1: Favor elija cuáles de los siguientes conceptos corresponden a los marcos de trabajo de gestión de riesgo adoptados por su organización para implementar los procesos actuales		
Opciones de respuesta	**Porcentaje Respuestas**	**Cantidad de respuestas**
ISACA	100.0%	4
COBIT	100.0%	4
Risk IT	100.0%	4
CRISC	50.0%	2
ITIL	50.0%	2
Basilea II	50.0%	2
ISO/IEC 27000	50.0%	2
CGEIT	25.0%	1
COSO ERM	25.0%	1
CMMi	25.0%	1
CISA	0.0%	0
ISO 31000:2009	0.0%	0
M_o_R	0.0%	0
OCTAVE	0.0%	0
ISO 20000	0.0%	0
PMBOK	0.0%	0

Pregunta 2: Identifique al menos dos fortalezas de la metodología de gestión de riesgos utilizada actualmente por la organización	
Opciones de respuestas	**Cantidad de respuestas**
	4

Número	**Respuesta**
1	Esta montada sobre mejores prácticas Es de uso corporativo en todos los países.

2	Dentro del alcance de la metodología está identificar riesgos en la fase de diseño y modificación de los procesos, lo que permite identificar vulnerabilidades que propicien la materialización de algunos riesgos que si bien pueden ser inherentes al proceso, si estos superan el apetito en la fase de diseño la probabilidad que se materialice el riesgo es mucho mayor. 2. La evaluación de los riesgos tanto tecnológicos como operativos toman como objetivo de evaluación los intereses de la organización, si bien, existen bien detrás de toda aplicación, sistema o ejecución de un proceso, el apetito se determina de acuerdo a los intereses reales de la organización
3	Visibilidad de los resultado por altos niveles de la organización y Posibilidad de priorizar entre todos los riesgos con un apetito alineado con negocio
4	Procesos establecidos Poder realizar seguimiento de los planes de mitigación de riesgo con los dueños.

Resumen pregunta 2

Fortaleza	Cantidad de respuestas personal a cargo de procesos	Cantidad de respuestas ejecutores del proceso	Total
Procesos estándares, estructurados y cíclicos	2	3	5
Basada en mejores prácticas	1	1	2
Permite identificar riesgos en diferentes etapas (pe. diseño y modificación de los procesos)	1	1	2
Considera identificación proactiva de riesgos tecnológicos y operativos	1	1	2
Visibilidad de la gestión por los niveles ejecutivos	1	1	2
Priorización basado en apetito de riesgo alineado con negocio	1	1	2
Seguimiento a planes de mitigación con los dueños	1	1	2

Evita materialización de riesgos		1	1
Involucra a personal expertos en riesgo para la documentación		1	1
Existencia de indicadores de gestión		1	1

Pregunta 3:Identifique al menos dos oportunidades de mejora de la metodología de gestión de riesgos utilizada actualmente por la organización	
Opciones de respuestas	**Cantidad de Respuestas**
	4

Número	Respuesta
1	Busca ser muy exhaustiva, perdiendo foco. Debe enfocarse en lo crítico y alinearse con el cumplimiento de objetivos de negocio. Calificar riesgos toma mucho tiempo y las personas no logran ver el valor agregado. Debe ser más práctica.
2	1. La herramienta que se cuenta, es un Excel, y al momento de estimar el nivel de riesgo no considera la probabilidad de ocurrencia del evento como una variable de peso para determinar el nivel de riesgo. 2. La administración de los riesgos es manual haciendo poco eficiente el seguimiento y control de los riesgos.
3	Disminuir la complejidad de la evaluación y alinear las herramientas de mitigación con las herramientas que ya utiliza la organización (PAPs, Project Server, etc.)
4	Cambio en la herramienta que se utiliza, Excel. Planificación de checklist para identificación de riesgos, con puntos indispensables que se deben validar en la identificación de riesgos cuando se ejecuta un análisis de servicios.

Resumen pregunta 3

Oportunidad	Cantidad de respuestas personal a cargo de procesos	Cantidad de respuestas ejecutores del proceso	Total

Herramienta automatizada, funcional y sencilla.	2	8	10
Proceso de Identificación, cálculo de puntaje según riesgos y criticidad. Subjetividad y Complejidad	3	2	5
Mejor seguimiento en los riesgos y planes de mitigación. Seguimiento Manual.	1	2	3
Mayor involucramiento y participación de los encargados de RO.		1	1
Capacitación		1	1
Diferencias en la evaluación riesgos operativos y tecnológicos		1	1
Generación y Visibilidad de la gestión de riesgo.		1	1
Centralización de la gestión de riesgos.		1	1
Búsqueda de riesgos alineada con el negocio	1		1

Pregunta 4: Indique la frecuencia con que se capturan las siguientes características al momento de identificar los riesgos asociados a servicios de TI.

Opciones de respuesta	No se utiliza	Ocasionalmente	Siempre se utiliza	Cantidad de respuestas
Impacto medido en costos intangibles (pe pérdidas por mala reputación e imagen)	0	4	0	4
Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas)	0	3	1	4
Volumen transaccional	0	3	1	4
Impacto en imagen (no cuantificado monetariamente)	0	2	2	4
Criticidad del servicio del servicio involucrado	0	2	2	4
Frecuencia con que ocurre	0	2	2	4
Criticidad del componente	0	1	3	4

involucrado				
Probabilidad de ocurrencia	1	0	3	4
Vulnerabilidad	0	1	3	4
Impacto regulatorio	0	0	4	4
Severidad	0	0	4	4
Apetito de Riesgo	0	0	4	4

Pregunta 5: Califique según su criterio el nivel de eficiencia, efectividad y/o agilidad de las siguientes variables en la gestión de riesgos de la organización.

Opciones de respuesta	Bajo	Medio	Alto	Cantidad de respuestas
Conocimiento y experiencia del personal participantes del proceso	0	3	1	4
Patrocinio de los Gerentes y Directores	0	3	1	4
Indicadores claves de gestión	1	2	1	4
Procesos de la gestión de riesgos	1	1	2	4
Herramientas	3	1	0	4
Mecanismos para aumentar el compromiso del personal	3	0	1	4

Pregunta 6: Indique cuáles características se utilizan actualmente por la organización para priorizar la atención de los riesgos identificados

Opciones de Respuesta	No se utiliza	Ocasionalmente	Siempre se utiliza	Cantidad de respuestas
Volumen transaccional	0	4	0	4
Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas)	0	3	1	4
Impacto medido en costos intangibles (pe pérdidas por mala reputación e imagen)	0	2	2	4
Impacto en imagen (no cuantificado	0	2	2	4

monetariamente)				
Criticidad del servicio del servicio involucrado	0	2	2	4
Criticidad del componente involucrado	0	2	2	4
Frecuencia con que ocurre	0	2	2	4
Probabilidad de ocurrencia	0	1	3	4
Vulnerabilidad	0	1	3	4
Impacto regulatorio	0	0	4	4
Severidad	0	0	4	4
Apetito de Riesgo	0	0	4	4

Pregunta 7: Al evaluar riesgos que puedan afectar la disponibilidad de un servicio crítico, favor indicar cuáles de las siguientes variables se cuantifican o traducen a términos económicos tomando en cuenta el tiempo de afectación?

Opciones de respuestas	Porcentaje respuestas	Cantidad de respuestas
Incumplimiento regulatorio o legal (Prisión, pérdidas financieras, revocación de licencias para operar, multas, etc.)	100.0%	4
Impacto en percepción externa (cobertura negativa en medios de comunicación masivos como prensa, televisión, revistas, redes sociales, etc.)	100.0%	4
Impacto en Productividad	75.0%	3
Costo de la respuesta al riesgo (Planes)	75.0%	3
Impacto en Satisfacción del cliente	25.0%	1
Impacto en participación de mercado	25.0%	1
Otro (especifique)	0.0%	0
Ninguno de los anteriores	0.0%	0
Impacto en ventaja competitiva	0.0%	0
Impacto en participación en el mercado	0.0%	0

Pregunta 8: Favor indicar cuáles de los siguientes elementos se cuantifican y documentan al momento de definir los planes para atender un riesgo

Opciones de respuesta	Porcentaje respuestas	Cantidad de respuestas
Costo de la respuesta/plan definido para atender el riesgo	50.0%	2

(Evitar/Mitigar/Transferir)		
Ahorros intangibles (imagen, reputación, etc.) por reducción/mitigación del impacto del riesgo con los planes indicados	50.0%	2
Ahorros tangibles por reducción/mitigación del impacto del riesgo con los planes indicados	25.0%	1
Ninguno de los anteriores	25.0%	1
Otro (especifique)	25.0%	1
Ahorros tangibles por evitar un riesgo	0.0%	0
Ahorros intangibles (imagen, reputación, etc.) por evitar un riesgo	0.0%	0

2. Personal ejecutor de la metodología de gestión de riesgos

Pregunta 1: Favor elija cuáles de los siguientes conceptos corresponden a los marcos de trabajo de gestión de riesgo adoptados por su organización para implementar los procesos actuales

Opciones respuestas	Porcentaje Respuestas	Cantidad respuestas
COBIT	100.0%	8
ITIL	75.0%	6
CISA	37.5%	3
Basilea II	25.0%	2
Risk IT	25.0%	2
PMBOK	12.5%	1
ISACA	0.0%	0
CGEIT	0.0%	0
CRISC	0.0%	0
COSO ERM	0.0%	0
ISO 31000:2009	0.0%	0
M_o_R	0.0%	0
OCTAVE	0.0%	0
CMMi	0.0%	0
ISO/IEC 27000	0.0%	0
ISO 20000	0.0%	0

Pregunta 2: Identifique al menos dos fortalezas de la metodología de gestión de riesgos utilizada actualmente por la organización

Opciones de respuestas	Cantidad de respuestas
	8

Número	Respuesta
1	-Colabora para evitar que se materialice el riesgo, -
2	Poder identificar riesgos en un momento específico. Poder darle seguimiento a los planes de mitigación.
3	Permite dar visibilidad a los riesgos de proyectos y de infraestructura productiva.
4	Proceso de riesgos muy claro Adecuada metodología
5	Se hace una identificación de riesgos proactiva. Se utiliza una valoración del riesgo en función de apetito de riesgo.
6	1- Participación de expertos en riesgo en la documentación de riesgos. 2- Existencia de indicadores de gestión
7	Se realiza de manera estructurada y cíclica
8	La metodología se aplica a toda la región La metodología se encuentra documentada y definida

Pregunta 3: Identifique al menos dos oportunidades de mejora de la metodología de gestión de riesgos utilizada actualmente por la organización

Opciones de respuesta	Cantidad de respuestas
	8

Número	Respuesta
1	1. Herramienta más sencilla para la evaluación del mismo. 2. Validación de los campos definidos en las plantillas de manera que sea más sencillo la documentación.
2	Mejorar la herramienta de la gestión de riesgos. Tener más participación de los encargados de RO de cada unidad en la identificación de riesgos.

3	1. Uso de mejores herramientas 2. Capacitar mas a los participantes y lideres
4	Mejora en el seguimiento Utilizar una herramienta apropiada no exceles
5	Hay riesgos no materializados que deberían atenderse y no se hace debido a que su puntaje puede ser bajo. La identificación de riesgos es muy subjetiva y depende de la visión de la persona asignada.
6	1-Creación de una herramienta automatizada donde se puedan identificar y documentar los riesgos y sean más visibles para las áreas mediante acceso para los usuarios. 2-Eliminación de la plantilla de riesgo operativo actual.
7	La evaluación de riesgos tecnológicos y operativos es muy distinta. Considero que deberían tener una base semejante y evaluar puntos particulares adicionales dependiendo el tipo de riesgo a documentar El seguimiento de la evolución del riesgo y de los planes de mitigación es muy manual Todos los riesgos se visualizan con la misma criticidad, no se clasifican, para priorizar la atención de los planes
8	Utilizar una herramienta más flexible. Generar más información hacia las diferentes áreas. Centraliza la identificación de riesgos en una sola área, que se encargue de inicio a fin de todo el proceso de identificación

Pregunta 4: Indique la frecuencia con que se capturan las siguientes características al momento de identificar los riesgos asociados a servicios de TI.

Opciones de respuesta	No se utiliza	Ocasionalmente	Siempre se utiliza	Cantidad respuestas
Impacto medido en costos intangibles (pe pérdidas por mala reputación e imagen)	0	5	3	8
Volumen transaccional	1	4	3	8
Impacto en imagen (no cuantificado	0	4	4	8

monetariamente)				
Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas)	0	3	5	8
Criticidad del componente involucrado	0	3	5	8
Probabilidad de ocurrencia	0	3	5	8
Impacto regulatorio	0	2	6	8
Severidad	1	1	6	8
Vulnerabilidad	0	2	6	8
Criticidad del servicio del servicio involucrado	0	1	7	8
Frecuencia con que ocurre	0	1	7	8
Apetito de Riesgo	0	1	7	8

Pregunta 5: Califique según su criterio el nivel de eficiencia, efectividad y/o agilidad de las siguientes variables en la gestión de riesgos de la organización.

Opciones de respuesta	Bajo	Medio	Alto	Cantidad respuestas
Patrocinio de los Gerentes y Directores	0	4	4	8
Conocimiento y experiencia del personal participantes del proceso	0	5	3	8
Procesos de la gestión de riesgos	3	2	3	8
Indicadores claves de gestión	4	2	2	8
Mecanismos para aumentar el compromiso del personal	5	1	2	8
Herramientas	8	0	0	8

Pregunta 6: Indique cuáles características se utilizan actualmente por la organización para priorizar la atención de los riesgos identificados

Opciones de respuesta	No se utiliza	Ocasionalmente	Siempre se utiliza	Cantidad respuestas
Impacto en imagen (no cuantificado	1	4	3	8

monetariamente)				
Volumen transaccional	2	3	3	8
Impacto medido en costos tangibles (pe pérdidas por transacciones no efectuadas)	1	3	4	8
Impacto medido en costos intangibles (pe pérdidas por mala reputación e imagen)	1	3	4	8
Probabilidad de ocurrencia	0	4	4	8
Frecuencia con que ocurre	2	2	4	8
Vulnerabilidad	1	2	5	8
Criticidad del componente involucrado	0	2	6	8
Severidad	1	1	6	8
Apetito de Riesgo	0	2	6	8
Criticidad del servicio del servicio involucrado	1	0	7	8
Impacto regulatorio	0	1	7	8

Pregunta 7: Al evaluar riesgos que puedan afectar la disponibilidad de un servicio crítico, favor indicar cuáles de las siguientes variables se cuantifican o traducen a términos económicos tomando en cuenta el tiempo de afectación?

Opciones de respuesta	Porcentaje respuestas	Cantidad respuestas
Incumplimiento regulatorio o legal (Prisión, pérdidas financieras, revocación de licencias para operar, multas, etc.)	87.50%	7
Impacto en Satisfacción del cliente	62.50%	5
Impacto en percepción externa (cobertura negativa en medios de comunicación masivos como prensa, televisión, revistas, redes sociales, etc.)	50.00%	4
Impacto en Productividad	37.50%	3
Costo de la respuesta al riesgo (Planes)	37.50%	3
Impacto en ventaja competitiva	12.50%	1
Impacto en participación de mercado	12.50%	1

Otro (especifique)	12.50%	1
Impacto en participación en el mercado	0.00%	0
Ninguno de los anteriores	0.00%	0

Pregunta 8: Favor indicar cuáles de los siguientes elementos se cuantifican y documentan al momento de definir los planes para atender un riesgo		
Opciones de respuesta	**Porcentaje respuesta**	**Cantidad Respuestas**
Costo de la respuesta/plan definido para atender el riesgo (Evitar/Mitigar/Transferir)	50.0%	4
Ahorros tangibles por evitar un riesgo	25.0%	2
Ahorros intangibles (imagen, reputación, etc.) por reducción/mitigación del impacto del riesgo con los planes indicados	25.0%	2
Ahorros intangibles (imagen, reputación, etc.) por evitar un riesgo	25.0%	2
Ahorros tangibles por reducción/mitigación del impacto del riesgo con los planes indicados	12.5%	1
Ninguno de los anteriores	12.5%	1
Otro (especifique)	12.5%	1

Anexo 4 – Encuesta Nivel de Satisfacción Usuarios con la Metodología Actual

La presente encuesta es realizada por el Ing. Marco Fonseca Aragón como parte de una investigación que forma parte de los requisitos para el Proyecto de Graduación de la Maestria en Administración de Tecnología (MATI) de la Universidad Nacional.

Esta investigación cuenta con el patrocinio del Sr. Jorge Betancourth (Gerente Regional de Seguridad y Riesgos) y con la aprobación del Sr. Roberto López (Director de Informática).

El objetivo de esta encuesta es poder recolectar información relevante sobre el nivel de satisfacción que tienen las partes interesadas con la metología de gestión de riesgos utilizada actualmente por la organización para efectos de plantear algunas mejoras y posterior a la ejecución de un piloto poder medir nuevamente el nivel de satisfacción.

Agradecemos su tiempo para poder responde a las preguntas que se plantean a continuación.

Se estiman 10 minutos para completar el instrumento

***1. ¿Considera Ud que las herramientas utilizadas actualmente por la metodología de gestión de riesgos de la organización permiten un uso eficiente de los recursos para el proceso de identificación y evaluación de nuevos riesgos?**

- ○ Totalmente en desacuerdo
- ○ En desacuerdo
- ○ Ligeramente en desacuerdo
- ○ Neutral
- ○ Ligeramente de acuerdo
- ○ De acuerdo
- ○ Totalmente de acuerdo

***2. ¿La identificación de nuevos riesgos es un proceso guíado, predecible y claro de forma tal que permite a los participantes concentrarse en los riesgos más relevantes para la organización?**

- ○ Totalmente en desacuerdo
- ○ En desacuerdo
- ○ Ligeramente en desacuerdo
- ○ Neutral
- ○ Ligeramente de acuerdo
- ○ De acuerdo
- ○ Totalmente de acuerdo

***3. ¿Se utilizan elementos cuantitativos (variables monetarias) además de los cualitativos (probabilidad e impacto) para efectos de priorizar/calificar los riesgos y planes de respuesta, como parte de los criterios para facilitar la toma de decisiones?**

- Totalmente en desacuerdo
- En desacuerdo
- Ligeramente en desacuerdo
- Neutral
- Ligeramente de acuerdo
- De acuerdo
- Totalmente de acuerdo

***4. ¿La metodología de gestión de riesgos actual considera, además de acciones de mitigación, alternativas como Evitar, Transferir o Aceptar el riesgo, tomando en cuenta los costos asociados a la ejecución de los planes de mitigación?**

- Totalmente en desacuerdo
- En desacuerdo
- Ligeramente en desacuerdo
- Neutral
- Ligeramente de acuerdo
- De acuerdo
- Totalmente de acuerdo

5. ¿La metodología de gestión de riesgos actual mantiene indicadores de gestión que le facilitan a Usted la toma de decisiones, el monitoreo y la detección de mejoras al proceso?

- Totalmente en desacuerdo
- En desacuerdo
- Ligeramente en desacuerdo
- Neutral
- Ligeramente de acuerdo
- De acuerdo
- Totalmente de acuerdo

***6. A nivel general, ¿cuál es el nivel de satisfacción que Usted tiene sobre la metodología y herramientas utilizadas actualmente por la organización para la gestión de riesgos tecnológicos?**

- ○ Muy insatisfecho
- ○ Insatisfecho
- ○ Ligeramente insatisfecho
- ○ Neutral
- ○ Ligeramente satisfecho
- ○ Satisfecho
- ○ Muy satisfecho

***7. Favor indique su puesto en la organización**

Anexo 5 – Catálogo de escenarios de riesgos

		Componentes del escenario del riesgo							Riesgo	Consecuencias de riesgo		Riesgo	Consecuencias de riesgo	
Número	Escenario de riesgo de Alto Nivel	Actor	Tipo de Amenaza	Evento	Activo/Recurso	Criticidad del recurso	Dimensión de Tiempo	Impacto de Riesgo	Ejemplos de escenarios negativos	Pérdida de Oportunidad	Pérdida de Valor	Ejemplos de escenarios positivos	Ganancia de valor	Preservar valor
1	Envejecimiento del software de aplicación	1. Interno	3. Falla	7. Ejecución inefectiva	Proceso (adquirir y mantener infraestructura tecnológica) Arquitectura empresarial (aplicación)	2. No Crítico	Estacionalidad (No crítico) Duración (extendida) Detección (lenta)	1. Directo	Aplicaciones o software obsoleto (por ejemplo, tecnología antigua pobremente documentada, costosa de mantener y extender, no integrada a la actual arquitectura)	X	X	Aplicaciones o software moderno, donde es fácil agregar/integrar nuevas funcionalidades o procesos	X	X
2	Selección/rendimiento de proveedores y terceros	1. Interno	3. Falla	6. Diseño inefectivo	Proceso (Administración de servicios de terceros) Personal y organización	2. No Crítico	Estacionalidad (No crítico) Duración (extendida) Detección (lenta)	1. Directo	Servicio y soporte ineficientes entregados por proveedores, no alineados con los acuerdos de niveles de servicio (SLAs) Rendimiento inadecuado de un proveedor de largo plazo de alto impacto	X	X	Un tercero que actúe como un socio estratégico	X	X
3	Robo de infraestructura	3. Interno y Externo	1. Malicioso	4. Robo	Infraestructura de TI	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Robo de portátiles/móviles con datos sensibles Robo significativo de servidores utilizados para desarrollo de aplicaciones	NA	X	N/A	NA	NA
4	Destrucción de infraestructura	3. Interno y Externo	1. Malicioso	5. Destrucción	Infraestructura	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Destrucción de data centers (sabotage, etc)	NA	X	NA	NA	NA
5	Destrucción de infraestructura	3. Interno y Externo	2. Accidental/error	5. Destrucción	Infraestructura	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Destrucción accidental de portátiles de personal clave	NA	X	NA	NA	NA
6	Personal de TI	1. Interno	3. Falla	7. Ejecución inefectiva	Proceso (administrar recurso humano de TI) Personal y organización	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (moderada)	1. Directo	Salida o indisponibilidad prolongada de personal clave de TI Personal clave de desarrollo abandona la organización Dificultad/Imposibilidad de contratar a personal calificado de TI	X	X	NA	NA	NA
7	Habilidades y expertise de TI	1. Interno	3. Falla	6. Diseño inefectivo	Proceso (administrar recurso humano de TI) Personal y organización	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Habilidades de TI ausentes o no concordantes con los requerimientos de la organización (debido a las nuevas tecnologías emergentes) Falta de conocimiento del negocio por parte del personal de TI	X	X	Atracción del personal de TI apropiado incrementa la capacidad de entrega del departamento de TI La mezcla adecuada de personal y sus habilidades aseguran la entrega de proyectos y de valor a la organización	X	X
8	Integridad del software	3. Interno y Externo	2. Accidental/error	3. Modificación	Proceso (gestión de cambios y acreditación de soluciones y cambios) Arquitectura Empresarial (software)	1. Crítico	Estacionalidad (No crítico) Duración (corta) Detección (lenta)	1. Directo	Modificación no intencional del software que genere resultados inesperados Errores no intencionales en la gestión de cambios y/o configuración	NA	X	NA	NA	NA
9	Integridad del software	3. Interno y Externo	1. Malicioso	3. Modificación	Proceso (gestión de cambios y acreditación de soluciones y cambios) Arquitectura Empresarial (software)	1. Crítico	Estacionalidad (No crítico) Duración (corta) Detección (lenta)	1. Directo	Modificación intencional del software que genere datos erróneos o acciones fraudulentas	NA	X	NA	NA	NA
10	Infraestructura (hardware)	3. Interno y Externo	2. Accidental/error	3. Modificación	Infraestructura de TI	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Configuración errónea de componentes de hardware Daño de servidores críticos en el centro de datos (accidental)	X	X	NA	NA	NA
11	Infraestructura (hardware)	3. Interno y Externo	1. Malicioso	9. Uso inapropiado	Infraestructura de TI	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Alteración o daño intencional utilizando hardware (dispositivos de seguridad)	X	X	NA	NA	NA
12	Infraestructura (hardware)	3. Interno y Externo	1. Malicioso	5. Destrucción	Infraestructura de TI	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Alteración o daño intencional utilizando hardware (dispositivos de seguridad)	X	X	NA	NA	NA
13	Rendimiento del Software	1. Interno	3. Falla	6. Diseño inefectivo	Arquitectura Empresarial (aplicaciones)	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Malfuncionamiento de una aplicación crítica por una falla en el software Problemas intermitentes con el software en un sistema importante	X	X	NA	NA	NA

14	Capacidad de los sistemas	1. Interno	3. Falla	6. Diseño inefectivo	Arquitectura Empresarial (tecnología)	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Los sistemas no pueden manejar los volúmenes transaccionales cuando la cantidad de usuarios aumenta Los sistemas no soportan la carga cuando nuevas aplicaciones o iniciativas se implementan	X	X	NA	NA	NA
15	Envejecimiento del software de infraestructura	1. Interno	3. Falla	6. Diseño inefectivo	Proceso (adquirir y mantener infraestructura tecnológica)	2. No Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Versiones no soportadas de sistemas operativos se utilizan todavía Sistemas de bases de datos obsoletos se continúan utilizando	X	NA	NA	NA	NA
16	Malware	3. Interno y Externo	1. Malicioso	6. Diseño inefectivo	Proceso (DSS Asegurar la seguridad de sistemas) Arquitectura Empresarial (aplicaciones)	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Servidores críticos infectados con malware Infección de portátiles con malware	NA	X	NA	NA	NA
17	Malware	3. Interno y Externo	2. Accidental/error	9. Uso inapropiado	Proceso (DSS Asegurar la seguridad de sistemas) Arquitectura Empresarial (aplicaciones)	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Servidores críticos infectados con malware Infección de portátiles con malware	NA	X	NA	NA	NA
18	Ataques lógicos	3. Interno y Externo	1. Malicioso	6. Diseño inefectivo	Proceso (DSS Asegurar la seguridad de sistemas) Arquitectura Empresarial (aplicaciones)	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Ataques de virus Usuarios no autorizados tratando de violar la seguridad Ataques de Denegacion de Servicios Espionaje industrial Daño a los sitios Web Ataques de phishing	NA	X	NA	NA	NA
19	Ataques lógicos	3. Interno y Externo	1. Malicioso	9. Uso inapropiado	Proceso (DSS Asegurar la seguridad de sistemas) Arquitectura Empresarial (aplicaciones)	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Ataques de virus Usuarios no autorizados tratando de violar la seguridad Ataques de Denegacion de Servicios Espionaje industrial Daño a los sitios Web Ataques de phishing	NA	X	NA	NA	NA
20	Medios de almacenamiento de información	1. Interno	3. Falla	7. Ejecución inefectiva	Proceso (administración de datos) Arquitectura Empresarial (información)	1. Crítico	Estacionalidad (No crítico) Duración (desconocida) Detección (inmediata)	1. Directo	Pérdida o revelación de dispositivos o medios que contienen datos sensibles (DVDs, USBs, discos portátiles, cintas, etc) Pérdida de medios de respaldo Revelación accidental de información sensible debido a fallas en seguir las directrices para manipulación de información	NA	X	NA	NA	NA
21	Confiabilidad de servicios de terceros	1. Interno	3. Falla	2. Interrupción	Proceso (Administrar servicios de terceros) Infraestructura	1. Crítico	Estacionalidad (desconocida) Duración (desconocida) Detección (inmediata)	1. Directo	Fallas intermitentes en los servicios de terceros (telecomunicaciones, electricidad, etc) Fallas prolongadas y frecuentes en servicios de terceros	NA	X	NA	NA	NA
22	Acciones industriales	2. Externo	1. Malicioso	2. Interrupción	Personal y organización	1. Crítico	Estacionalidad (desconocida) Duración (desconocida) Detección (inmediata)	1. Directo	Edificios no accesibles debido a huelgas y manifestaciones Personal clave no disponible debido a una acción industrial	NA	X	NA	NA	NA
23	Integridad de los datos y Bases de Datos	3. Interno y Externo	1. Malicioso	3. Modificación	Arquitectura Empresarial	2. No Crítico	Estacionalidad (desconocida) Duración (desconocida) Detección (desconocida)	1. Directo	Modificación intencional de los datos (contabilidad, información de accesos y seguridad, ventas, etc)	NA	X	NA	NA	NA
24	Integridad de los datos y Bases de Datos	3. Interno y Externo	3. Falla	3. Modificación	Arquitectura Empresarial	1. Crítico	Estacionalidad (desconocida) Duración (desconocida) Detección (desconocida)	1. Directo	Corrupción de datos (base de datos de clientes, transacciones bancarias)	NA	X	NA	NA	NA
25	Violación lógica	3. Interno y Externo	1. Malicioso	6. Diseño inefectivo	Proceso (DSS Asegurar la seguridad de sistemas) Arquitectura Empresarial (información)	1. Crítico	Estacionalidad (no crítica) Duración (extendida) Detección (lenta)	1. Directo	Usuarios evadiendo los controles de seguridad lógicos de acceso a información	NA	X	NA	NA	NA
26	Violación lógica	3. Interno y Externo	1. Malicioso	9. Uso inapropiado	Proceso (DSS Asegurar la seguridad de sistemas) Arquitectura Empresarial (información)	1. Crítico	Estacionalidad (no crítica) Duración (extendida) Detección (lenta)	1. Directo	Usuarios obteniendo acceso a información no autorizada	NA	X	NA	NA	NA
27	Violación lógica	3. Interno y Externo	1. Malicioso	1. Revelación	Proceso (DSS Asegurar la seguridad de sistemas) Arquitectura Empresarial (información)	1. Crítico	Estacionalidad (no crítica) Duración (extendida) Detección (lenta)	1. Directo	Usuarios robando información sensible	NA	X	NA	NA	NA
28	Errores Operaciones de TI	1. Interno	2. Accidental/error	3. Modificación	Proceso (gestión de cambios) Arquitectura Empresarial	2. No Crítico	Estacionalidad (Crítica) Duración (extendida) Detección (desconocida)	1. Directo	Errores de Operador (Durante respaldos, actualizaciones de sistemas, mantenimiento de sistemas, etc)	NA	X	NA	NA	NA
29	Errores Operaciones de TI	1. Interno	3. Falla	3. Modificación	Proceso (gestión de cambios) Arquitectura Empresarial	2. No Crítico	Estacionalidad (Crítica) Duración (extendida) Detección (desconocida)	1. Directo	Ingreso de información incorrecta a los procesos	NA	X	NA	NA	NA
30	Cumplimiento de acuerdos contractuales	3. Interno y Externo	3. Falla	7. Ejecución inefectiva	Proceso (asegurar el cumplimiento con requerimientos externos)	2. No Crítico	Estacionalidad (no crítica) Duración (extendida) Detección (lenta)	1. Directo	Incumplimiento con los acuerdos de licenciamiento de software (uso y/o distribución de software sin licencias, etc) Acuerdos de niveles de servicio a nivel contractual no cumplidos a los clientes	NA	X	NA	NA	NA
31	Ambiental	3. Interno y Externo	4. Natural	6. Diseño inefectivo	Proceso (administrar el ambiente físico) Infraestructura	2. No Crítico	Estacionalidad (desconocida) Duración (desconocida) Detección (desconocida)	1. Directo	Equipo utilizado no es amigable con el ambiente (consumo excesivo de energía, empaques dañinos para el ambiente, etc)	NA	X	NA	NA	NA
32	Actos de la naturaleza	2. Externo	4. Natural	5. Destrucción	Proceso (administrar el ambiente físico) Infraestructura Personal	1. Crítico	Estacionalidad (desconocida) Duración (desconocida) Detección (inmediata)	1. Directo	Terremotos Tsunamis Tormentas y huracanes Incendios Inundaciones	NA	X	NA	NA	NA

Anexo 6 – Prototipo formulario para ingreso de nuevos riesgos

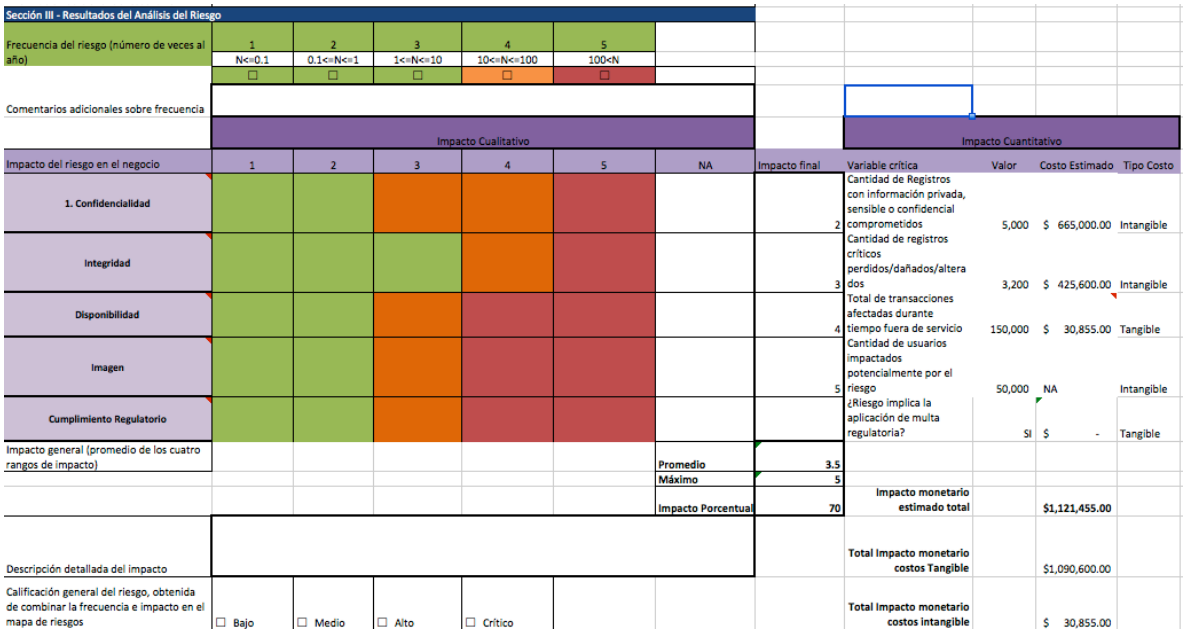
Formulario de Registro de Riesgos

Sección I - Resumen del Riesgo				
IDRiesgo	AutoGenerado			
Enunciado del Riesgo	Vista			
Dueño del Riesgo:				
Canal afectado:	Sucursal Electrónica			
Servicio afectado:	Lista			
Fecha de la última evaluación del riesgo:	Vista			
Fecha de la próxima evaluación de riesgo:	Vista			
Categoría de Riesgo:	Operacional (Operaciones de TI y entrega de servicios)			
Clasificacion de riesgo: (extraído de los resultados del análisis de riesgo)	☐ Bajo	☐ Medio	☐ Alto	☐ Crítico
Estimado impacto monetario total	Valor Monetario + la escala de evaluacion			
Estimado impacto monetario costos tangibles	Valor Monetario + la escala de evaluacion			
Estimado impacto monetario costos intangibles	Valor Monetario + la escala de evaluacion			
Respuesta a riesgo:	☐ Aceptar	☐ Transferir	☐ Mitigar	☐ Evitar
Costo Plan de Acción				
Costo acciones de respuesta (US$)				
Ahorro estimado costos intangibles ($US)				
Diferencia Estimado impacto monetario vs costo plan acción	#¡VALOR!			

Sección II - Descripción del Riesgo		
Enunciado del Riesgo		
Dueño del Riesgo:		
Canal afectado:	Sucursal Electrónica	
Servicio afectado:		
Escenario de riesgo de alto nivel (tomado del catálogo de escenarios de riesgo)		
Descripción detallada del escenario (componentes del escenario)	Actor	
	Tipo de Amenaza	
	Evento	
	Recurso/Activo	
	Tiempo	
Información adicional del escenario		

Información adicional del escenario	

Sección III - Resultados del Análisis del Riesgo						
Frecuencia del riesgo (número de veces al año)	1	2	3	4	5	
	N<=0.1	0.1<=N<=1	1<=N<=10	10<=N<=100	100<N	
	☐	☐	☐	☐	☐	
Comentarios adicionales sobre frecuencia						



Sección III - Resultados del Análisis del Riesgo											
Frecuencia del riesgo (número de veces al año)	1	2	3	4	5						
	N<=0.1	0.1<=N<=1	1<=N<=10	10<=N<=100	100<N						
	☐	☐	☐	☐	☐						
Comentarios adicionales sobre frecuencia											
	Impacto Cualitativo							Impacto Cuantitativo			
Impacto del riesgo en el negocio	1	2	3	4	5	NA	Impacto final	Variable crítica	Valor	Costo Estimado	Tipo Costo
1. Confidencialidad							2	Cantidad de Registros con información privada, sensible o confidencial comprometidos	5,000	$ 665,000.00	Intangible
Integridad							3	Cantidad de registros críticos perdidos/dañados/alterados	3,200	$ 425,600.00	Intangible
Disponibilidad							4	Total de transacciones afectadas durante tiempo fuera de servicio	150,000	$ 30,855.00	Tangible
Imagen							5	Cantidad de usuarios impactados potencialmente por el riesgo	50,000	NA	Intangible
Cumplimiento Regulatorio								¿Riesgo implica la aplicación de multa regulatoria?	SI	$ -	Tangible
Impacto general (promedio de los cuatro rangos de impacto)						Promedio	3.5				
						Máximo	5				
						Impacto Porcentual	70	Impacto monetario estimado total		$1,121,455.00	
Descripción detallada del impacto								Total Impacto monetario costos Tangible		$1,090,600.00	
Calificación general del riesgo, obtenida de combinar la frecuencia e impacto en el mapa de riesgos	☐ Bajo	☐ Medio	☐ Alto	☐ Crítico				Total Impacto monetario costos intangible		$ 30,855.00	

Sección IV - Respuesta al riesgo									
Respuesta seleccionada para este riesgo	☐ Aceptar	☐ Transferir	☐ Mitigar	☐ Evitar					
Justificación									
Descripción detallada de la respuesta (no aplica si la respuesta es Aceptar)	Acción de respuesta		Costo acciones de respuesta (US$)	Ahorro estimado costos intangibles ($US)	Nivel de Riesgo	Tasa Efectividad/ Costo	Acción a tomar	Plan de acción	Completado
	1		$ -	$ -	Vista	Alta/Baja	Campo Calculado	☐	☐
	2		$ -	$ -	Vista	Alta/Baja		☐	☐
	3		$ 1,000.00	$ 15,000.00	Vista	Alta/Baja		☐	☐
	4		$ -	$ -	Vista	Alta/Baja		☐	☐
	5		$ 500.00	$ 7,500.00	Vista	Alta/Baja		☐	☐
	6		$ -	$ -	Vista	Alta/Baja		☐	☐
	7		$ -	$ -	Vista	Alta/Baja		☐	☐
	8		$ -	$ -	Vista	Alta/Baja		☐	☐
	9		$ -	$ -	Vista	Alta/Baja		☐	☐
		Total	$ 1,500.00	$ 22,500.00				$ -	
Estatus general del plan de acción									
Principales problemas con el plan de acción									
Estatus general de las respuestas completadas									
Principales inconvenientes con las respuestas completadas									
Fecha de la última evaluación del riesgo:									
Fecha de la próxima evaluación de riesgo:									

Anexo 7 – Guía para la identificación de Riesgos

Guía para la identificación de Riesgos

El siguiente documento corresponde a una guía para apoyarle con el uso de la herramienta para identificación de riesgos y documentación de planes asociada a la metodología propuesta.

Insumos y requisitos para utilizar el servicio:

1. Catálogo de riesgos (integrado a la herramienta)
2. Expertos con conocimiento del servicio
3. Listado de incidentes del último año
4. Acceso a la herramienta publicada en la siguiente dirección http://crcordwhshpnt1.bacnet.corp.redbac.com/DBA/AdminRiesgo/SiteAssets/Riesgo.aspx
5. Navegador Internet Explorer 10 o superior, Firefox 36 o superior, Safari 8 o superior
6. Listado de riesgos identificados para el canal de Banca Electrónica con la metodología actual

Actividades:

Fase Identificación de Riesgos

El objetivo de esta fase es orientar a la persona que participa en la identificación de riesgos de forma que utilice un procedimiento ordenado y sistemático para la identificación de riesgos facilitando el proceso creativo y la lluvia de ideas.

Paso 1 – Revisión del Catálogo de Escenarios de Riesgos

El catálogo de escenarios de riesgos es un inventario de diferentes situaciones genéricas de riesgo que sirven como punto de partida para la identificación de riesgos específicos asociados a un servicio de TI.

Cada escenario está compuesto de un conjunto de variables cuyas combinaciones permiten diferenciar una situación de otra.

En el siguiente gráfico se muestra la composición de un escenario de riesgo y las variables que intervienen.

El catálogo a utilizar ha sido precargado con cerca de 30 escenarios genéricos propuestos por ISACA. Sin embargo, no está limitado a los riesgos actuales y puede expandirse a más alternativas.

Utilice el catálogo de escenarios de riesgos como punto de partida, para efectos de que pueda analizar cada uno de los escenarios que ahí se listan con el fin de determinar si alguna de las situaciones corresponde a un riesgo que deba identificar y documentar dentro de la herramienta.

Si encuentra coincidencia con alguno, documente el enunciado del riesgo, el servicio afectado y el escenario de riesgo en la “Sección II – Descripción del Riesgo” de la herramienta y continúe con la documentación del riesgo. Al concluir

la documentación vuelva a revisar el catálogo de riesgo a partir del punto donde lo dejó. Una vez que haya finalizado el catálogo completo, determine si existe algún escenario que no esté documentado y que Usted considera necesario incorporar. En caso de existir una sugerencia de inclusión diríjase al Analista de Riesgos que conduce la sesión para que pueda solicitar la incorporación del nuevo escenario.

Una vez finalizado el paso anterior, favor continúe con el siguiente paso.

Paso 2 – Revisión del historial de incidentes

Analice el historial de incidentes asociados al servicio/canal analizado con el fin de identificar si dentro de los eventos que se han presentado en la historia del último año, existe algún riesgo que deba documentarse dentro de la herramienta.

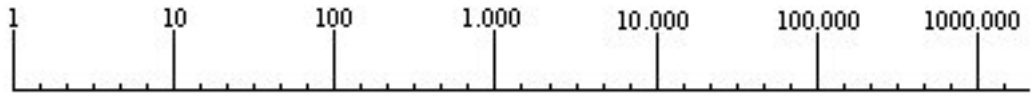
Si encuentra coincidencia con alguno, documente el enunciado del riesgo y proceda con la fase de evaluación.

Fase evaluación de Riesgos:

El objetivo de esta fase es determinar la frecuencia del riesgo, además del impacto cualitativo y cuantitativo que genera para el negocio.

Paso 1 – Determinar la frecuencia del incidente

Una vez enunciado el riesgo y asociado el canal, servicio y escenario al que pertenece, corresponde asignar la frecuencia del riesgo. La frecuencia del riesgo se identifica dentro de una escala logarítmica que clasifica las veces que el evento puede ocurrir en un período de un año.



Adicionalmente existen otras variables que pueden afectar la frecuencia con la que ocurre el evento como son la explotabilidad y la exposición de la vulnerabilidad identificada en el riesgo, considere estas otras variables para seleccionar la calificación de la frecuencia.

Considere también, en caso de tener la información, la frecuencia con la que han ocurrido incidentes similares al riesgo que se está documentando en el pasado pues puede brindarle información más exacta sobre la calificación a elegir.

Calificación de frecuencia	Veces que ocurre al año	Exposición	Explotabilidad
1	0.01	Vulnerabilidad poco conocida, presente en pocas ubicaciones	Se requiere alto grado de conocimiento y/o esfuerzo de la amenaza para poder explotar la vulnerabilidad
2	0.1		
3	1	Vulnerabilidad es accesible por las amenazas de forma limitada, está presente en varias localizaciones pero no es muy conocida.	La amenaza requiere un grado intermedio de conocimiento y/o un esfuerzo significativo para poder explotar la vulnerabilidad.
4	10		
5	100	Vulnerabilidad fácilmente accesible por las amenazas, presente en muchas ubicaciones o es muy conocida	La amenaza no requiere de conocimiento especializado para explotar la vulnerabilidad

			y/o no necesita de un esfuerzo considerable para explotarla.

Una vez que haya definido la frecuencia del riesgo, documéntela en la “Sección III - Resultados del Análisis del Riesgo” en el campo “Frecuencia del riesgo” y continúe con el siguiente paso.

Paso 2 – Determinar el impacto cualitativo del riesgo

El impacto cualitativo del riesgo se determina estimando el grado de afectación que tiene el riesgo para el negocio analizando cada una de las siguientes variables:

6. Confidencialidad
7. Integridad
8. Disponibilidad
9. Imagen
10. Cumplimiento Regulatorio

Esta evaluación cualitativa es la misma que utiliza la metodología de riesgos actual y no se consideró necesario hacer ningún tipo de ajuste o variación a la forma en que se calcula.

Utilizando el juicio experto y el conocimiento que Usted tiene sobre el servicio, en este paso debe definir, para cada una de las variables anteriores, el nivel de afectación correspondiente. En caso que la variable no aplique se debe seleccionar la opción de No Aplica (NA).

Cada variable se puede definir entre 5 diferentes niveles de afectación según se detalla a continuación.

Criterio	Niveles de afectación
Confidencialidad	1: Existe exposición de información de tipo pública que no representa perjuicio para la institución 2: Existe exposición de información protegida internamente y no afecta los intereses de la institución. 3: Existe exposición de información confidencial y puede producir un uso malicioso en contra del negocio 4: Existe exposición de información restringida que puede producir un uso malicioso en contra del negocio 5: Existe exposición de información restringida que puede producir un uso malicioso en contra del negocio así como la afectación de los intereses de la institución.
Integridad	1: Implica que de existir una alteración o pérdida de la información esta no afecta los servicios, ya que existen controles que lo detectarán y/o lo corregirán. 2: Implica que de existir una pérdida de información, esto está dentro de los umbrales aceptados de los servicios afectados (Recovery Point Objective, RPO). 3: Implica que de existir una pérdida de información, esta sobrepasa los umbrales de los servicios afectados (Recovery Point Objective, RPO), sin embargo el evento sólo afecta un servicio que no es crítico, o, se presenta una alteración de información que no es crítica para el negocio.

	4: Implica que de existir una pérdida de información, esta sobrepasa los umbrales de los servicios afectados (Recovery Point Objective, RPO), afectando como máximo un servicio crítico. De forma alternativa, se presenta una alteración de información que puede ser detectada y corregida sin afectar a clientes externos o de forma grave a procesos de negocio. 5: Implica que de existir una pérdida de información, no hay procesos que permitan reprocesarla y dicha pérdida sobrepasa los umbrales definidos para los servicios críticos (Recovery Point Objective, RPO). De forma alternativa, la alteración de información afecta a clientes externos y procesos de negocio.
Disponibilidad	1: Existe compromiso de la disponibilidad del o los componentes que puede llegar a afectar el desempeño de un servicio no crítico. 2: Existe compromiso de la disponibilidad del o los componentes que provoque la interrupción de un servicio no crítico. 3: Existe compromiso de la disponibilidad del o los componentes que puede llegar a afectar el desempeño de un servicio crítico o varios no críticos. 4: Existe compromiso de la disponibilidad del o los componentes y puede afectar gravemente un servicio crítico o varios servicios no críticos. 5: Existe compromiso de la disponibilidad del o los

	componentes y puede afectar gravemente varios servicios críticos.
Imagen	1: Impacto mínimo en la imagen o confianza pública de la organización, sin exposición a medios. 2: Impacto regular en la imagen o confianza pública de la organización sin ninguna exposición a medios 3: Impacto regular en la imagen o confianza pública de la organización con exposición limitada a medios 4: Impacto importante en la imagen o confianza pública de la organización (a nivel local), con alta exposición a medios de comunicación 5: Impacto severo o catastrófico en la imagen o confianza pública de la organización (a nivel local e internacional), con alta exposición a los medios de comunicación.
Cumplimiento Regulatorio	1: El incumplimiento no generaría un hallazgo pero si una posible observación por parte del regulador, adicionalmente no se generarían multas o sanciones 2: El incumplimiento generaría un hallazgo del regulador pero de criticidad baja, no se generarían multas o sanciones 3: El incumplimiento generaría un hallazgo importante del regulador mas no pone en riesgo el cumplimiento con la regulación, podría provocar una multa o sanción leve. 4: El incumplimiento generaría un hallazgo importante del

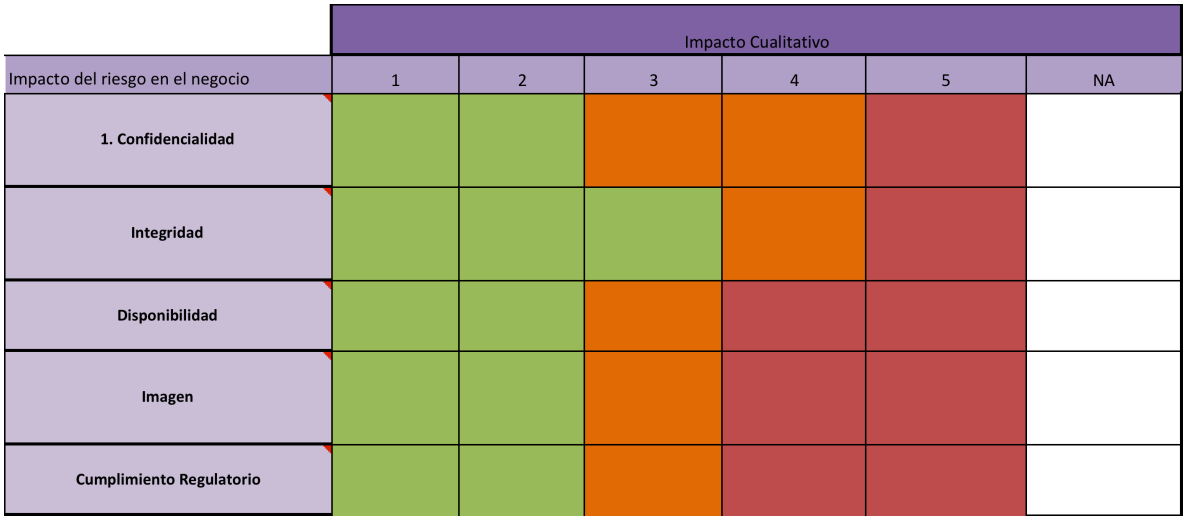
	regulador y pondría en riesgo el cumplimiento con la regulación, se generarían multas considerables o sanciones importantes. 5: El incumplimiento generaría un hallazgo crítico que generaría un incumplimiento importante de la regulación provocando la pérdida de una certificación o licencia, la aplicación de multas o sanciones que impacten significativamente al negocio.

Una vez que haya definido la aplicabilidad y/o calificación para todas las variables de impacto cualitativo, documente su respuesta en la herramienta en la “Sección III – Resultados del Análisis del Riesgo” y prosiga con el siguiente paso.

Paso 3 – Determinar el impacto cuantitativo del riesgo

El impacto cuantitativo aplica cuando en la determinación del impacto cualitativo, se seleccionan los niveles de afectación que conllevan una afectación económica a la organización, la cual puede ser estimada mediante algunas variables críticas asociadas a cada criterio, lo cual forma parte de la propuesta de esta metodología.

En el siguiente mapa de calor, se identifican en color naranja o rojo, los valores para los cuales se puede estimar un impacto cuantitativo.



En caso de que haya seleccionado alguno de los valores en naranja o rojo, a continuación se listan las variables críticas que debe documentar dentro de la herramienta con el fin de que se pueda realizar una cuantificación económica del riesgo a partir del valor que se indique.

Criterio	Variable crítica	Comentario
Confidencialidad	Cantidad de Registros con información privada, sensible o confidencial comprometidos	Se realiza una estimación de pérdidas monetarias por registro comprometido.
Integridad	Cantidad de registros críticos perdidos/dañados/alterados	Se realiza una estimación de pérdidas monetarias por datos dañados / alterados /perdidos.
Disponibilidad	Total de transacciones afectadas durante tiempo fuera de servicio	Se realiza una estimación de pérdidas monetarias por el costo de utilizar canales sustitutos para la cantidad de transacciones afectadas.

Imagen	Cantidad de usuarios impactados potencialmente por el riesgo	Esta variable es informativa, no fue posible derivar una estimación económica a partir de la misma.
Cumplimiento Regulatorio	¿Riesgo implica la aplicación de multa regulatoria?	Se cuantifica el monto correspondiente a multas por incumplimiento regulatorio.

Con el fin de facilitar la definición de algunas de las variables críticas anteriores, a continuación se resume la cantidad de transacciones que en promedio procesa cada servicio por el canal de Banca Electrónica por mes, día y hora.

Estimación de Cantidad transacciones por tipo y período

Transacción	Mensual	Diario	Hora
Consulta Consolidada	0	0	0
Consulta Banco	0	0	0
Consulta Tarjeta	0	0	0
Transf. Locales	0	0	0
Pago de Tarjeta	0	0	0
Consulta Afiliados	0	0	0
Transf. otros Bancos	0	0	0
Envío PPP	0	0	0
Consulta Préstamo	0	0	0
Pago de Préstamo	0	0	0
Transf. Regionales	0	0	0
Transf. Internacionales	0	0	0

Consulta OPC	0	0	0
Consulta Certificado	0	0	0
Consulta SFI	0	0	0
Total	**0**	**0**	**0**

Adicionalmente se incluye una tabla con la cantidad de transacciones totales realizadas por cada país a través del canal de Banca Electrónica por mes, día y hora.

Estimación cantidad transacciones por país y período, la cantidad de usuarios activos y la cantidad de usuarios creados por país.

País	Mensual	Diario	Hora	Usuarios activos	Total Usuarios existentes
CRI	0	0	0	0	0
HON	0	0	0	0	0
NIC	0	0	0	0	0
GUA	0	0	0	0	0
ESA	0	0	0	0	0
PAN	0	0	0	0	0
MEX	0	0	0	0	0
US	0	0	0		
BS	0	0	0		
Total	**0**	**0**	**0**	**0**	**0**

Una vez que haya ingresado los datos de las variables críticas para hacer las estimaciones cuantitativas en la sección “Sección III – Resultados del Análisis del Riesgo” de la herramienta, como resultado obtendrá la calificación general del riesgo y el impacto monetario estimado dividido en costos tangibles y costos

intangibles. Estas variables serán muy importantes a partir de este punto por lo que puede continuar con el siguiente paso.

Fase Respuesta al Riesgo

La planeación de la respuesta a los riesgos es el proceso de desarrollar procedimientos y acciones para maximizar las oportunidades y reducir las amenazas a los objetivos de la organización.

El objetivo de esta fase es determinar cuales acciones son las que corresponden para darle un tratamiento a cada riesgo, de forma tal que dicha decisión sea conveniente para los intereses de la organización.

Paso 1 – Determinar la respuesta seleccionada para este riesgo

Un riesgo puede recibir como respuesta cualquiera de las siguientes estrategias:

Estrategia	Significado
Aceptar	Esta estrategia se adopta debido a que rara vez es posible eliminar todas las amenazas de una organización debido a que los costos pueden resultar prohibitivos. Se puede seleccionar esta alternativa cuando no se ha podido encontrar ninguna otra estrategia de respuesta adecuada (costo/efectiva o viable). La aceptación puede ser pasiva lo cual requerirá documentar la decisión únicamente y la aceptación activa que podría considerar el establecimiento de una reserva para contingencias.
Compartir/Transferir	Implica transferir a un tercero los efectos negativos de una amenaza y la potestad de asignar una respuesta. La transferencia de un riesgo simplemente confiere a una tercera persona la responsabilidad de su gestión; no elimina el riesgo. Esta alternativa se utiliza mucho en la exposición a

	riesgos financieros. Normalmente implica el pago de una prima a la parte que asume el riesgo. Las herramientas de transferencia incluyen contratos, seguros, garantías de cumplimiento, fianzas, certificados de garantía, etc. Ejemplo seguros: 5. Contra daños directos a la propiedad (Colisión de automóviles, Cobertura de equipos/materiales del proyecto, Seguro contra incendios y desastres naturales, Seguro contra robo) 6. Contra pérdidas por consecuencia indirecta (Seguro contra daños a terceros, reemplazo de equipo) 7. Protección por responsabilidad legal, penal, civil (daños a la entidad del proyecto producto de: Errores de diseño, errores durante la ejecución, Fallas en el desempeño del proyecto) 8. Seguros relacionados con el personal (Seguro contra lesiones físicas de los empleados, Costos de reemplazo de trabajadores)
Mitigar/Reducir	Mitigar el riesgo implica reducir a un umbral aceptable la probabilidad y/o el impacto de un evento adverso de manera que se encuentre dentro los límites de tolerancia de la organización (apetito de riesgo). El nivel de riesgo resultante posterior a aplicar los planes se le conoce como riesgo residual.
Evitar	Implica cambiar el objetivo, plan o tecnología a fin de eliminar por completo la amenaza que representa el riesgo adverso. Usualmente el riesgo se anula eliminando la causa o reduciendo la probabilidad de

	ocurrencia a cero.

Table 1 Table 1 http://itsm-admon-proy.blogspot.com/2012/12/planificarla-respuesta-los-riesgos.html

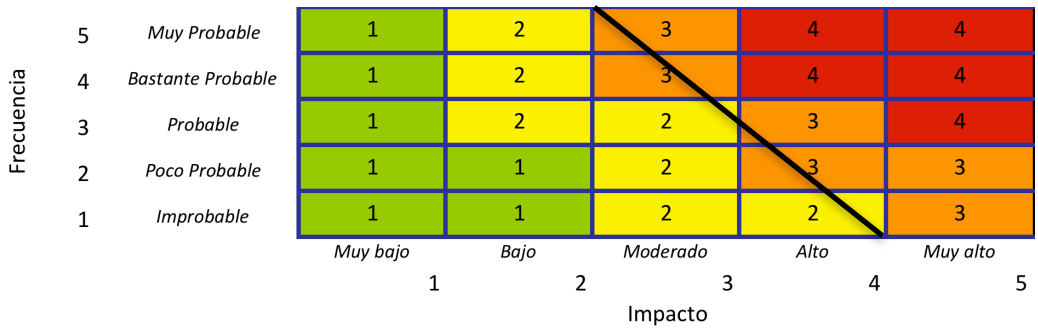
Para cada riesgo, se debe utilizar la estrategia o combinación de estrategias adecuadas (y además efectivas) y luego desarrollar acciones específicas para implementar dicha estrategia.

Se considera una buena práctica, seleccionar estrategias de apoyo o refuerzo a la estrategia primaria, y/o un plan de reserva que será activado en caso que la estrategia seleccionada no resulte ser totalmente efectiva.

Lo que va a determinar que tipo de respuesta debe darse a un plan es en primer lugar, el apetito de riesgo definido por la organización. Esto significa, cuales son los niveles de riesgo que la organización está dispuesta a tolerar.

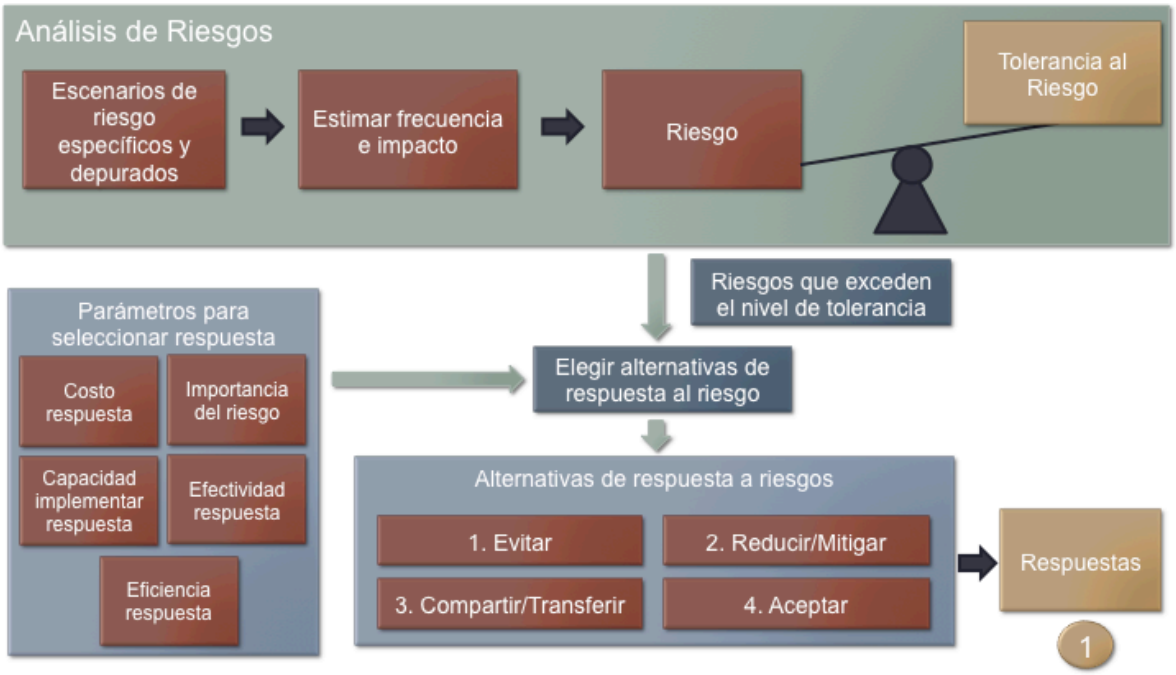
Para el caso de la institución en la cual se realiza este trabajo, el apetito de riesgo está definido hasta los colores verde y amarillo del mapa de calor de riesgos que se muestra en la siguiente figura. Es decir, los niveles de riesgo bajo y medio no requieren de definir un plan de respuesta sino que se Aceptan por definición.

En cambio, los niveles de riesgo Alto y Crítico (colores naranja y rojo) si requieren ser analizados y elegir la estrategia y plan de respuesta a considerar.



Niveles Riesgo	Descripción
1	Bajo
2	Medio
3	Alto
4	Crítico

Como se ejemplifica en la siguiente figura, una vez que conoce la calificación general de un riesgo (obtenida de combinar la frecuencia e impacto en el mapa de riesgos), si el nivel de riesgo supera el nivel de tolerancia establecido por la organización corresponde elegir una alternativa de respuesta al riesgo.



Al momento de seleccionar la alternativa de respuesta, se debe tomar en cuenta los parámetros que se describen a continuación:

Parámetros	Descripción
Costo de la respuesta para reducir la calificación del riesgo a niveles de	En el caso de elegir como estrategia la trasferencia de un riesgo, este costo

tolerancia permitidos por la organización	puede ser el valor de la prima de un seguro. En el caso de seleccionar mitigación como estrategia, correspondería al costo total de implementar las medidas de control (salarios, gastos de capital, consultorías, etc)
Importancia del riesgo	Se refiere a la posición que ocupe la calificación del riesgo dentro del mapa de calor (la cual refleja la combinación de los niveles de frecuencia e impacto). A mayor frecuencia y/o impacto, mayor relevancia tendrá la respuesta que se elija.
Capacidad de la organización para implementar la respuesta	Está relacionado directamente a las habilidades de la organización para desarrollar el plan y el nivel de madurez que la organización tenga para afrontar dicha respuesta. Cuando la empresa es inmadura en sus procesos de gestión de riesgos, varias respuestas básicas podrían ser mejores que unas pocas sofisticadas.
Efectividad de la respuesta planteada	La magnitud en que la respuesta reducirá ya sea la frecuencia o el impacto del riesgo
Eficiencia de la respuesta planteada	Los beneficios relativos de una respuesta en comparación con: otras inversiones requeridas en TI y otras respuestas a riesgos (una respuesta

	podría resolver varios riesgos, otras solamente uno)

Una vez elegidas la(s) estrategia(s) a utilizar como alternativa de respuesta, se seleccionan dentro de la herramienta en la “Sección IV - Respuesta al riesgo” en el campo “Respuesta seleccionada para este riesgo”. Opcionalmente se puede detallar la justificación del porqué se eligen estas estrategias dentro del campo “Justificación”. Una vez concluida este paso puede continuar con el siguiente.

Paso 2 – Acciones de respuesta

Con las estrategias de respuesta definidas, corresponde ahora definir las respuestas al riesgo que son planteamientos de acciones que se pueden ejecutar y que típicamente tendrán asociado un costo.

Las respuestas a los riesgos requieren muchas creatividad y análisis. A continuación se enumeran las características con las que debe cumplir una respuesta a un riesgo:

Apropiadas:	Las respuestas deben ser congruentes con la importancia del riesgo. Deben ser costo/efectivas en relación al desafío.
Ejecutables:	Ser realistas dentro del contexto de la organización e industria. Factibles técnica y legalmente.
Financiadas:	Cada respuesta debe tener un presupuesto acordado. La cantidad de tiempo, esfuerzo y dinero que se dedique al riesgo no debe exceder su presupuesto disponible.
A tiempo:	Algunos riesgos requieren acción inmediata , mientras que otros planes pueden quedar a la espera de priorización para su ejecución posterior.
Acordadas:	Estar acordadas por todas las partes implicadas y estar a cargo de una persona (“dueño”) que acepta su

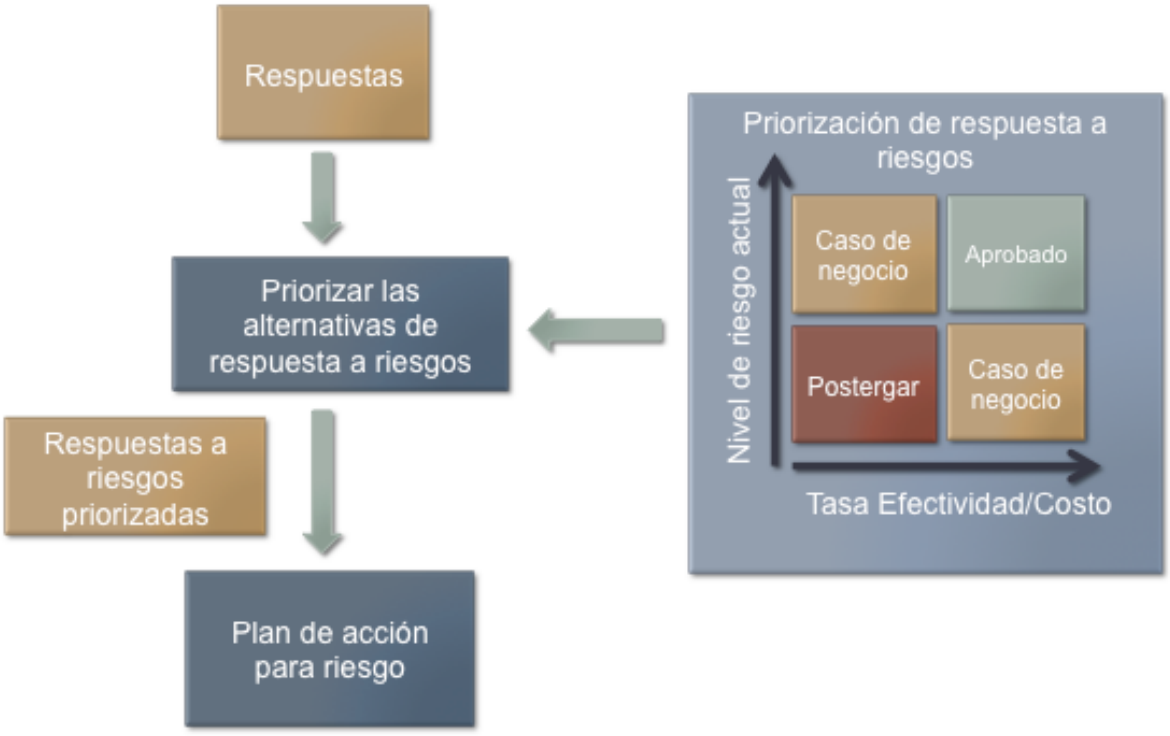
	responsabilidad respecto a la implementación.
Evaluables:	Poder analizar la efectividad posterior a su implementación, durante el seguimiento a los riesgos.

Es muy común que el esfuerzo requerido para implementar las diferentes respuestas de mitigación excedan los recursos disponibles. En este caso, será necesario realizar un ejercicio de priorización para el cual se pueden utilizar los mismos criterios que se emplearon para seleccionar la estrategia de respuesta.

Para esto se debe, ubicar las propuestas de respuesta dentro de la matriz de cuatro cuadrantes ilustrada en la siguiente figura, la cual posee tres decisiones posibles descritas dentro de la siguiente tabla.

Decisión	Nivel Riesgo	Tasa Efectividad/ Costo	Descripción
Aprobado	Alto	Alto	Este tipo de planes son victorias rápidas dado que son respuestas muy eficientes y efectivas en la atención de riesgos con una calificación alta.
Caso de Negocio	Alto	Baja	Respuestas complejas o de alto costo para atacar riesgos con calificación alta, se requiere un análisis cuidadoso y una decisión de la administración acerca de las inversiones.
Caso de Negocio	Bajo	Alta	Respuestas eficientes y efectivas para riesgos con una calificación

			baja, se requiere un análisis cuidadoso y una decisión de la administración acerca de las inversiones.
Postergar	Bajo	Baja	Respuestas costosas a riesgos con una calificación baja.



A partir de la explicación anterior, corresponde ahora documentar dentro de la "Sección IV – Respuesta al Riesgo" cada una de las acciones de respuestas, el responsable, el costo que implica desarrollar dicha acción y su tasa de efectividad/costo. Con esta información, la herramienta calculará en forma automática el ahorro estimado en costos intangibles y la acción/decisión que se recomienda para el plan.

Este insumo de priorización, le permitirá a quien documenta el riesgo elegir cuáles de las diferentes acciones de respuesta serán las que queden formalizadas como

parte del plan de acción de este riesgo, que se presentarán a la administración para someterlos a aprobación y luego integrarlos al Control de Ejecución de Planes aprobados, actividad que forma parte del Gobierno de Riesgos.

Teniendo claro lo anterior, es necesario ahora marcar dentro de la herramienta las acciones de respuesta que se identifiquen como parte de plan de acción. A partir de esta acción será posible cuantificar el costo del plan de acción.

Finalmente, el último paso corresponde a hacer una comparación entre el estimado de impacto monetario del riesgo versus el costo del plan de acción. Utilice la siguiente una tabla para definir la siguiente acción:

Nivel de Riesgo	Estimado impacto monetario Total	Costo del plan de acción	Acción a tomar
Bajo	Mayor	Menor	Plan de acción aprobado
Bajo	Menor	Mayor	Revisar las acciones y en caso de no poder encontrar mejores alternativas someter la propuesta a un caso de negocio.
Bajo	Igual	Igual	Plantear el caso de negocio
Alto	Mayor	Menor	Plan de acción aprobado
Alto	Menor	Mayor	Plantear el caso de negocio
Alto	Igual	Igual	Plan de acción aprobado

Fin del documento.

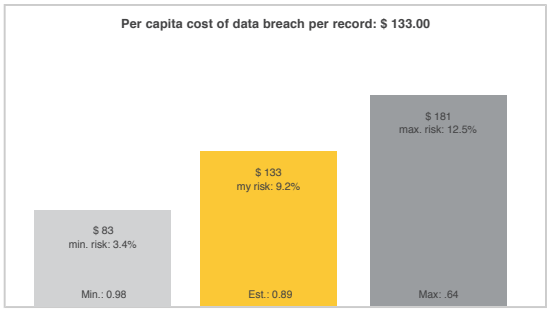
Anexo 8 – Reporte de Violación de Datos Personalizado

Symantec

Data Breach Risk Report

For BAC

From Symantec and The Ponemon Institute

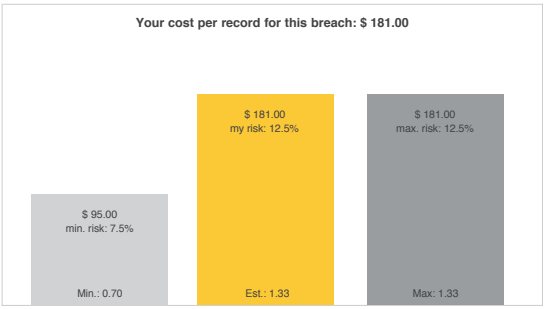


Data breach continues to be a very costly event for organizations. The average organizational cost of a data breach was millions of dollars in our study. The most expensive data breach event included in this year's study cost a company nearly $21 million to resolve. The least expensive total cost of data breach for a company included in our study was over half a million dollars. The largest data breach incident involved nearly 100,000 lost or stolen records. As in prior years, data breach cost appears to be linearly related to the size or magnitude of the breach event. Responses to questions 10-13 do not appear in this report as they were used to calculate results and to inform future updates to the Data Breach Calculator.

#1: What is your organization's industry classification?

Answer Selected:

Financial Services

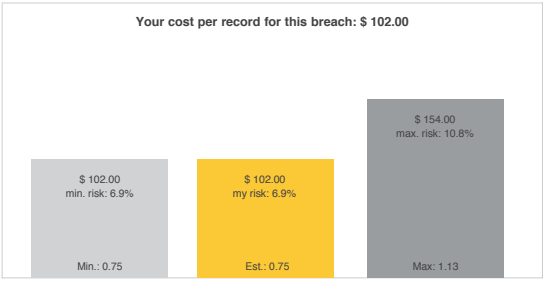


Our research finds organizations in highly trusted industries such as financial services and healthcare are more likely to experience a data breach with high abnormal churn rates. In contrast, retailers and companies with less direct consumer contact seem to experience a lower overall data breach cost. Other cost components of a data breach appear to have stabilized.

#2: Do you have a privacy and data protection security policy?

Answer Selected:

Yes, we have a formal program implemented across the entire enterprise



Our research suggests that U.S. organizations by and large take their stewardship of sensitive personal data seriously and are taking greater steps to ensure its protection from breaches. For the first time, companies participating in our annual study report that their data breaches were smaller in scale and resulted in a lower rate of churn. We conclude that companies' investment in improving their data protection practices is paying off.

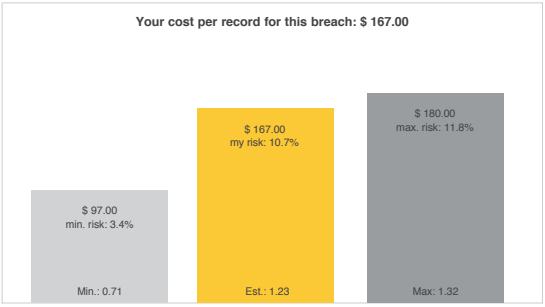
#3: What types of information do your employees handle?

Maximum Answer Selected:

Employee records

All of your selections:

1. Consumer data
2. Customer data including credit card information
3. Employee records
4. Citizen records

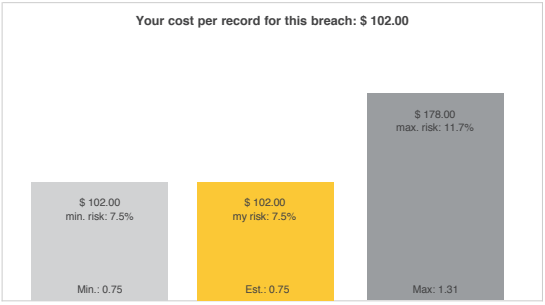


Organizations need to limit both physical and online access to data and storage devices containing sensitive customer, business and employee information. Steps should be taken to secure sensitive or confidential data both at rest and in motion. Another vulnerable area is the company-assigned laptop, smartphone or other mobile device. Ponemon Institute research has shown that one of the primary causes of a data breach is the lost or stolen mobile device that may contain sensitive information about customers, business operations, research and development and employees. However, many organizations fail to instill in their employees, contractors and business partners how critical it is to safeguard these devices.

#4: What do you think is the most likely cause of a data breach?

Answer Selected:

Negligence or mistakes

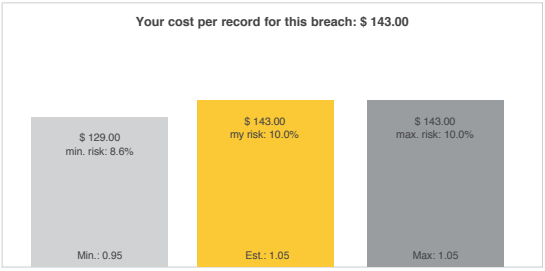


Negligent employees and malicious attracks are most often the cause of the data breach. In addition, the cost per compromised record of data breaches involving a malicious or criminal act averaged $222, 28 percent higher than breaches involving a intelligent insider ($174) and 21 percent higher than breaches from system glitches ($183). Half of those companies who experienced criminal attacks received them through electronic agents such as viruses, malware, worms, and trojans.

#5: Do your employees store sensitive data on laptops or on removable storage?

Answer Selected:

Yes

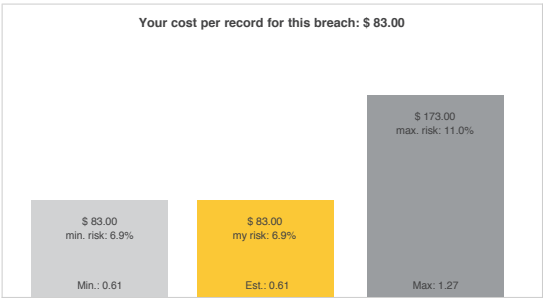


Over a third of all cases in the study involved lost or stolen mobile devices, which included laptops, smartphones, tablets, and USB drives that contained confidential and sensitive information. Specifically, in this year's study the per victim cost for a data breach involving a lost or stolen device was over $200.

#6: Is sensitive data encrypted on all laptops or removable storage?

Answer Selected:

Yes



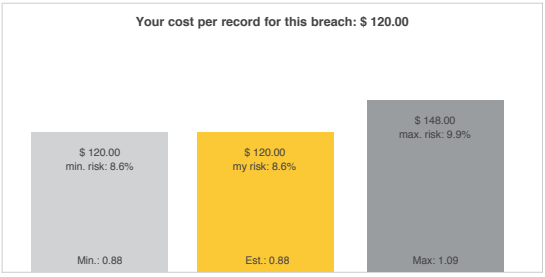
Many kinds of automated, cost-effective enterprise data protection solutions are now available to secure data both within an organization and among business partners. Some of the most popular and effective of these technologies currently available include:

- Encryption (including whole disk encryption and for mobile devices/smartphones)
- Data loss prevention (DLP) solutions
- Identity and access management solutions
- Endpoint security solutions and other anti-malware tools

#7: Does your organization have a dedicated information security leader, such as a chief information security officer (CISO)?

Answer Selected:

Yes

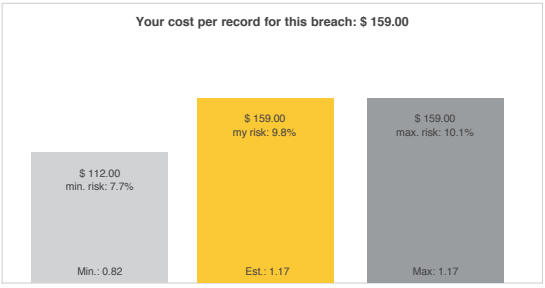


The leadership of a CISO or equivalent position substantially reduces the overall cost of data breaches. Specifically, companies with a CISO (or equivalent title) who managed data breach incidents experienced an average cost per compromised record that was over 50% less than for companies without such leadership.

#8: What is the global headcount of your organization?

Answer Selected:

Between 10,001 to 25,000

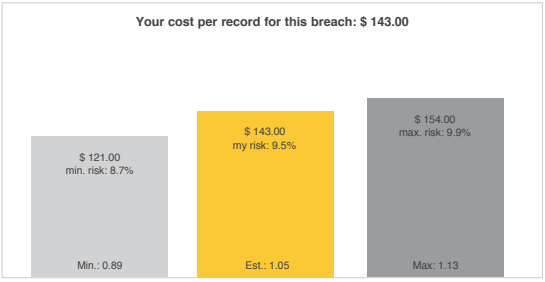


Multinational companies with thousands of employees, contractors and business partners in hundreds of locations throughout the world need to know at all times that the sensitive data they collect is protected. This can be a daunting challenge. The first step is to take an inventory of the data in your organization and determine what data is absolutely essential to supporting your business goals. The next step is to put the appropriate processes, policies and expertise in place to ensure that the data is protected and that the organization is in compliance with global regulations and laws.

#9: What is the global footprint of your organization?

Answer Selected:

Operations in many countries, in one global region



Multinational companies with thousands of locations throughout the world must devote resources to making sure they are collecting the minimum amount of sensitive data to reduce their risk of a data breach. In addition to safeguarding sensitive information, these organizations must understand the rules and regulations governing the transfer of sensitive information. Because the insider threat is considered by many to pose the greatest risk, multinationals must be diligent in making sure strict privacy and security policies are in place throughout the organization. Further that employees, contractors and business partners understand that non-compliance with these policies will be enforced.

Disclaimer

This tool is offered for illustration purposes only. The information in this report compares your answers on a high level against a compilation of market research from the Ponemon Institute. The goal of this document is to provide a personal look at the research and show how your organization may compare with organizations of a similar profile. Symantec provides the tool "as is" and does not give any warranty of any kind nor assumes any liability for the usage of the tool and its results. For a more extensive in-depth risk analysis which reflects your personal circumstances, contact your Symantec Sales or Partner representative.

More Information

Visit our website
http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.
Call toll-free: 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website.

About Symantec
Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

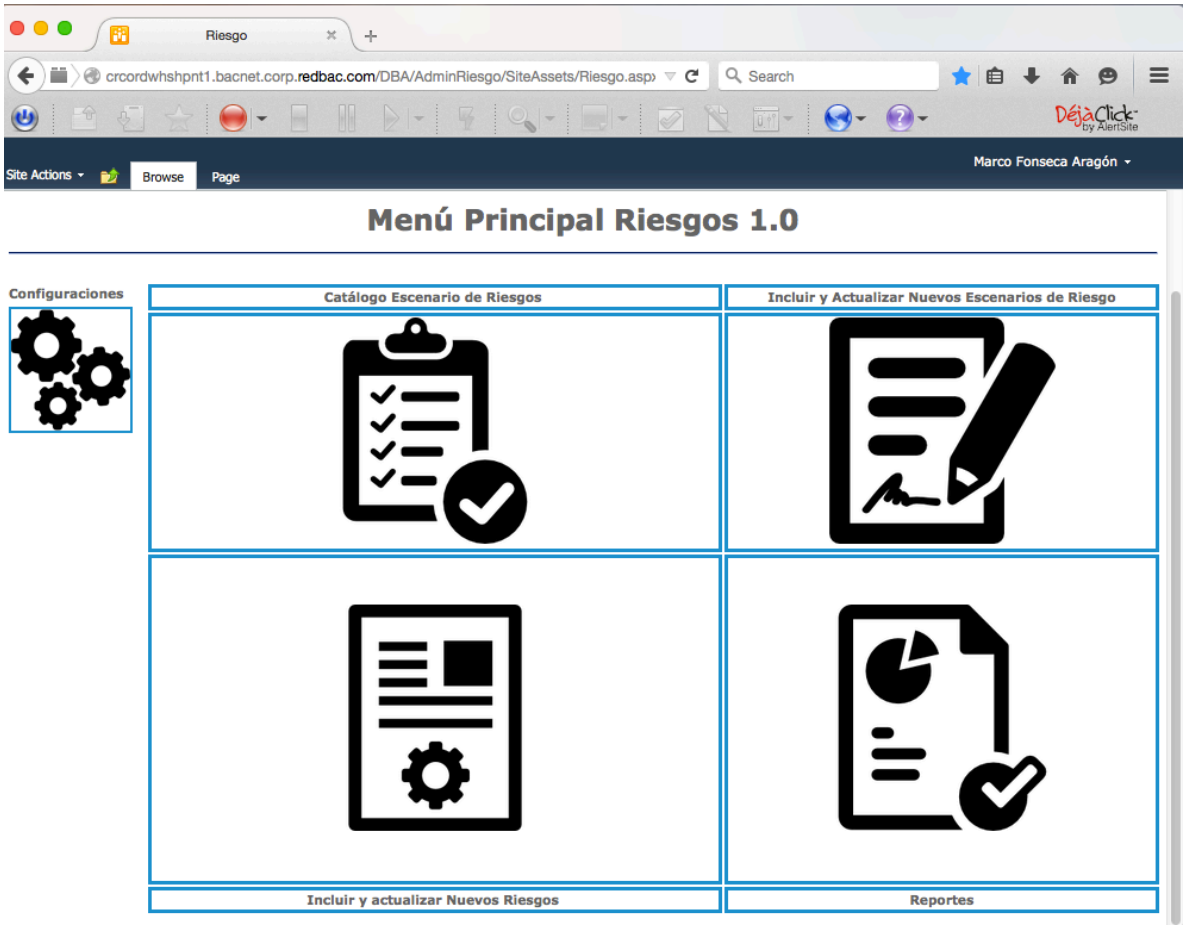
Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. Symantec helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security, and application security solutions.

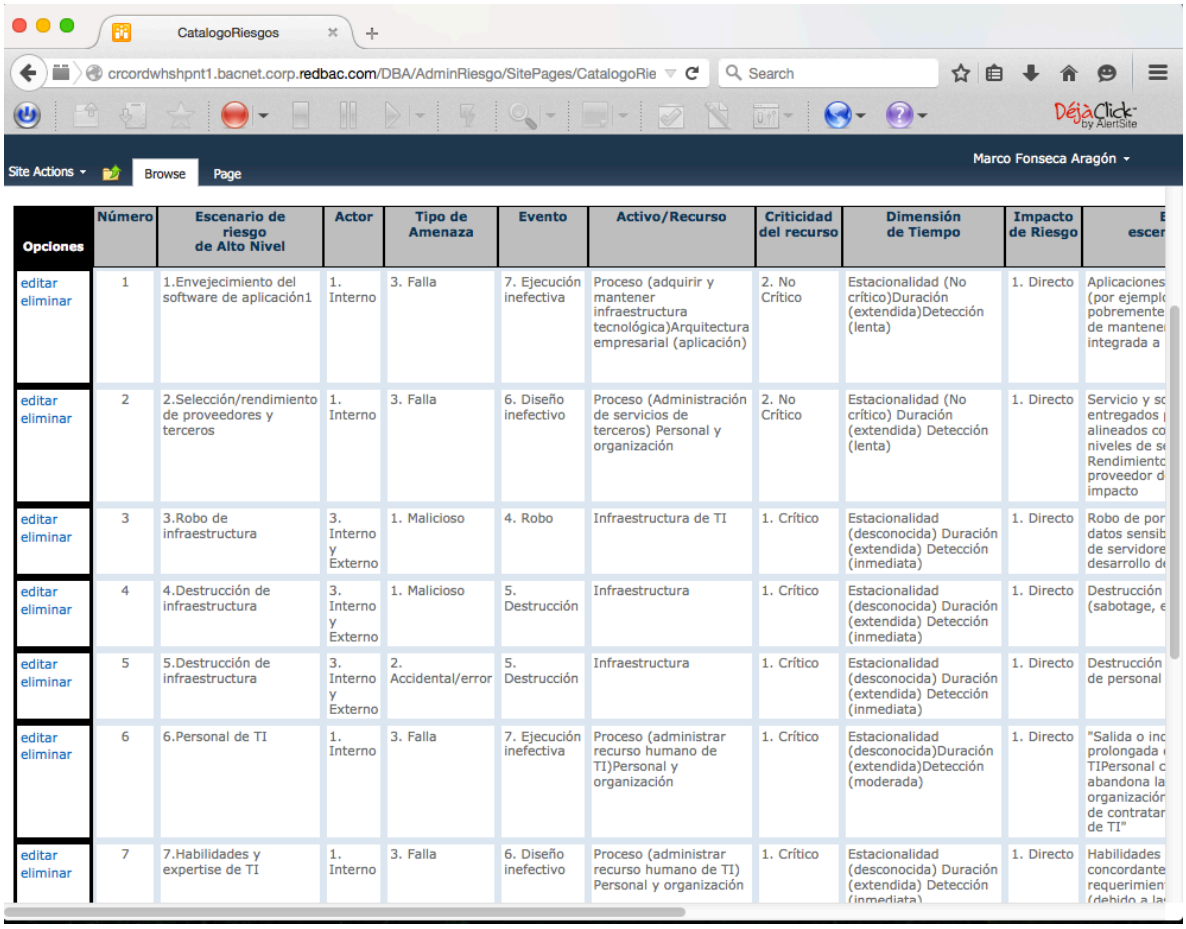
Anexo 9 – Ejemplos de Pantallas de la herramienta diseñada en Sharepoint utilizada para el Piloto

URL:
http://crcordwhshpnt1.bacnet.corp.redbac.com/DBA/AdminRiesgo/SiteAssets/Riesgo.aspx

Menú Principal de la aplicación

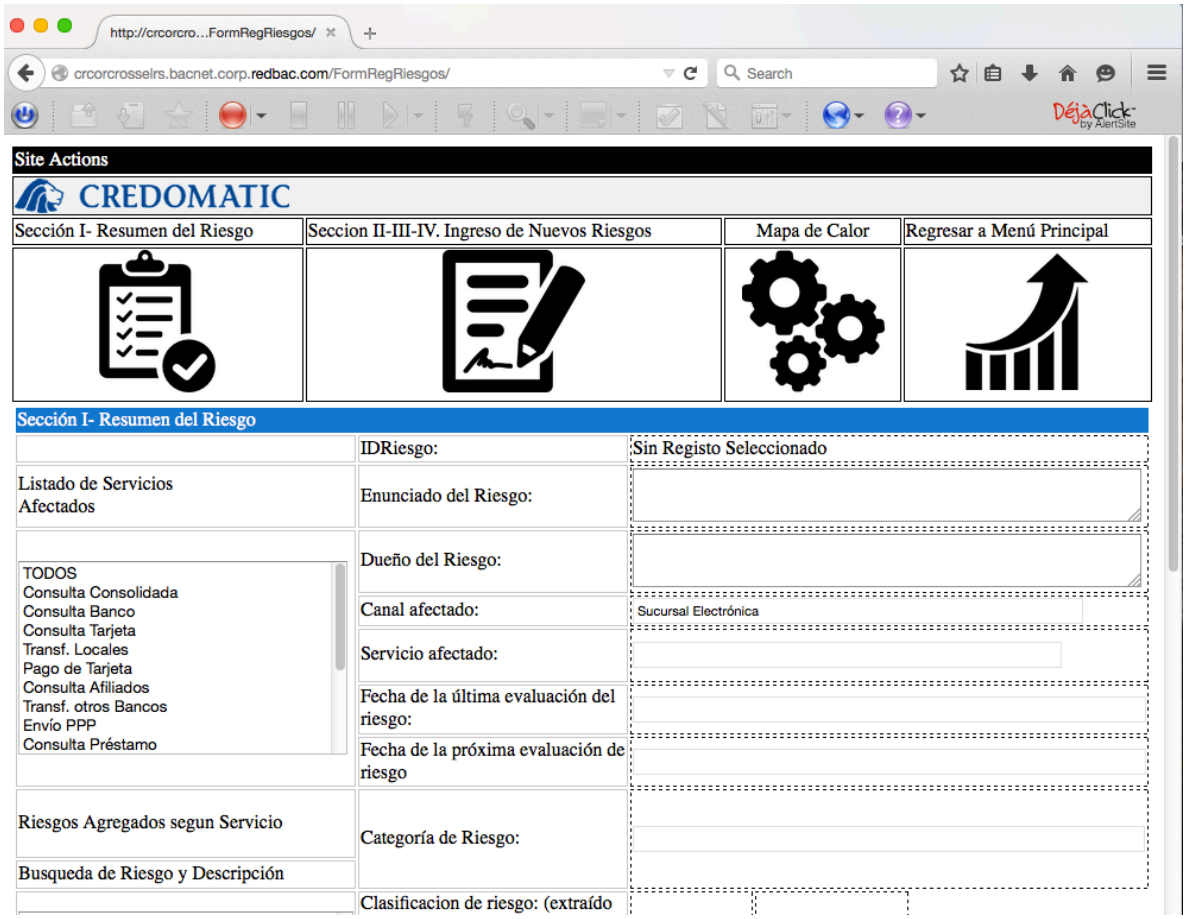


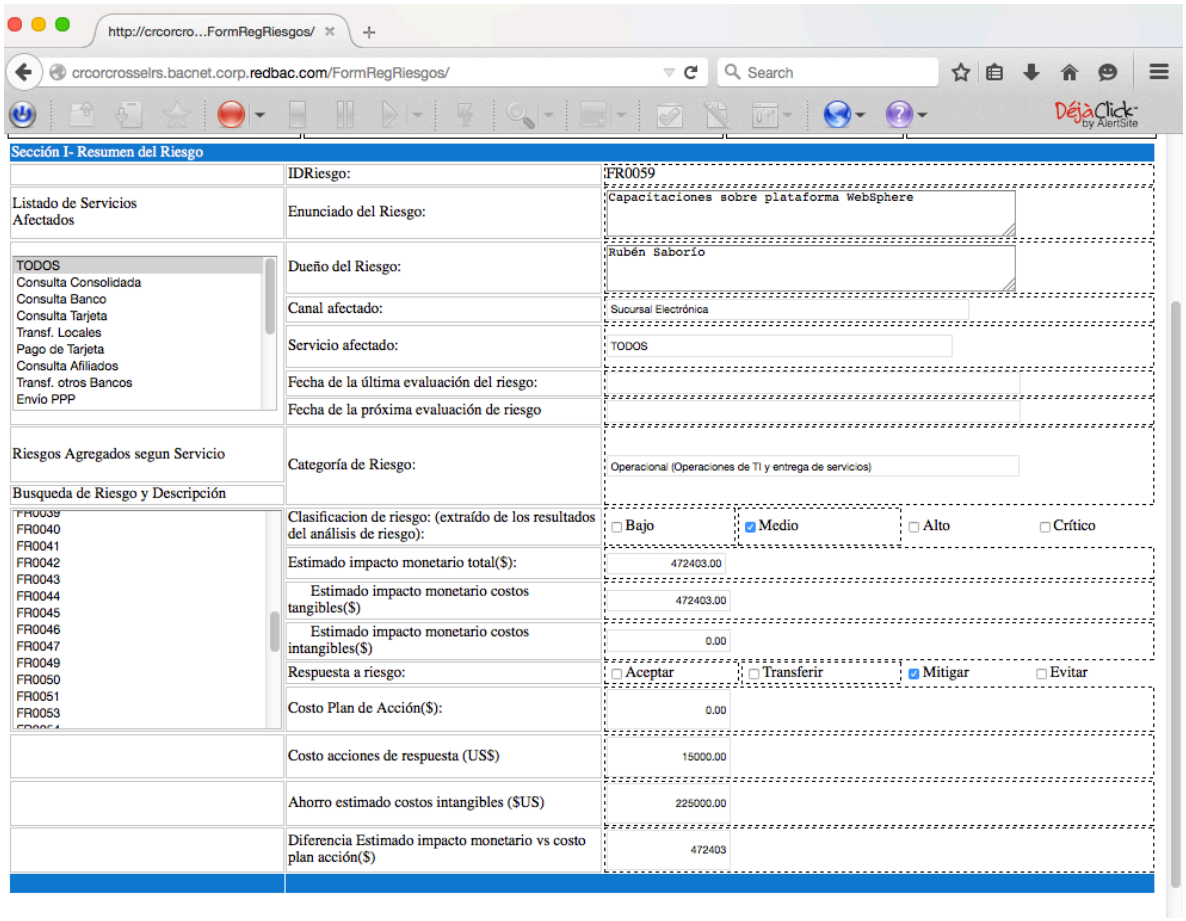
Catálogo de Escenarios de Riesgos



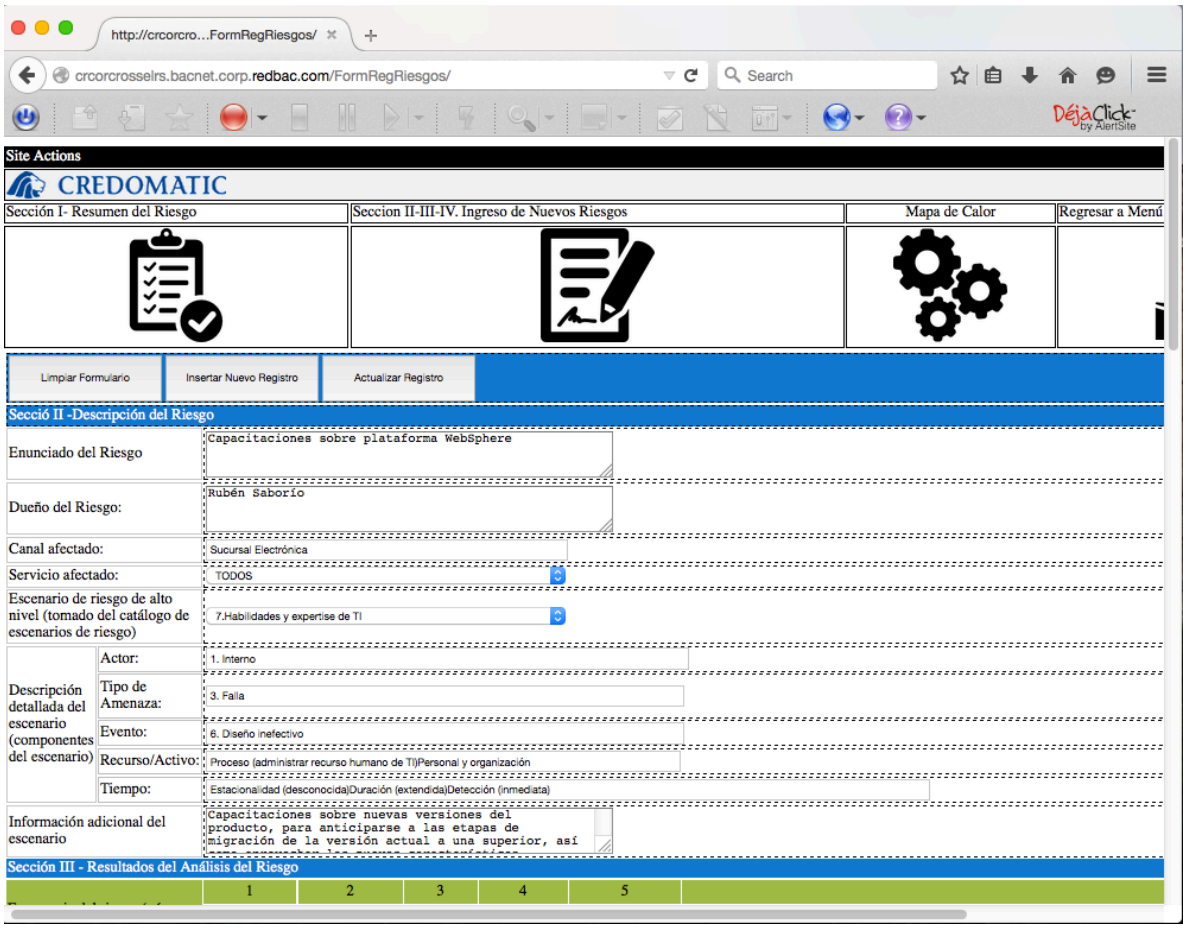
Opciones	Número	Escenario de riesgo de Alto Nivel	Actor	Tipo de Amenaza	Evento	Activo/Recurso	Criticidad del recurso	Dimensión de Tiempo	Impacto de Riesgo	E escer
editar eliminar	1	1.Envejecimiento del software de aplicación1	1. Interno	3. Falla	7. Ejecución inefectiva	Proceso (adquirir y mantener infraestructura tecnológica)Arquitectura empresarial (aplicación)	2. No Crítico	Estacionalidad (No crítico)Duración (extendida)Detección (lenta)	1. Directo	Aplicaciones (por ejemplo pobremente de mantene integrada a
editar eliminar	2	2.Selección/rendimiento de proveedores y terceros	1. Interno	3. Falla	6. Diseño inefectivo	Proceso (Administración de servicios de terceros) Personal y organización	2. No Crítico	Estacionalidad (No crítico) Duración (extendida) Detección (lenta)	1. Directo	Servicio y so entregados alineados co niveles de se Rendimiento proveedor d impacto
editar eliminar	3	3.Robo de infraestructura	3. Interno y Externo	1. Malicioso	4. Robo	Infraestructura de TI	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Robo de por datos sensib de servidore desarrollo de
editar eliminar	4	4.Destrucción de infraestructura	3. Interno y Externo	1. Malicioso	5. Destrucción	Infraestructura	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Destrucción (sabotage, e
editar eliminar	5	5.Destrucción de infraestructura	3. Interno y Externo	2. Accidental/error	5. Destrucción	Infraestructura	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Destrucción de personal
editar eliminar	6	6.Personal de TI	1. Interno	3. Falla	7. Ejecución inefectiva	Proceso (administrar recurso humano de TI)Personal y organización	1. Crítico	Estacionalidad (desconocida)Duración (extendida)Detección (moderada)	1. Directo	"Salida o inc prolongada TIPersonal c abandona la organización de contratar de TI"
editar eliminar	7	7.Habilidades y expertise de TI	1. Interno	3. Falla	6. Diseño inefectivo	Proceso (administrar recurso humano de TI) Personal y organización	1. Crítico	Estacionalidad (desconocida) Duración (extendida) Detección (inmediata)	1. Directo	Habilidades concordante requerimien (debido a la

Sección I – Formulario Identificación de Riesgos – Resumen del Riesgo

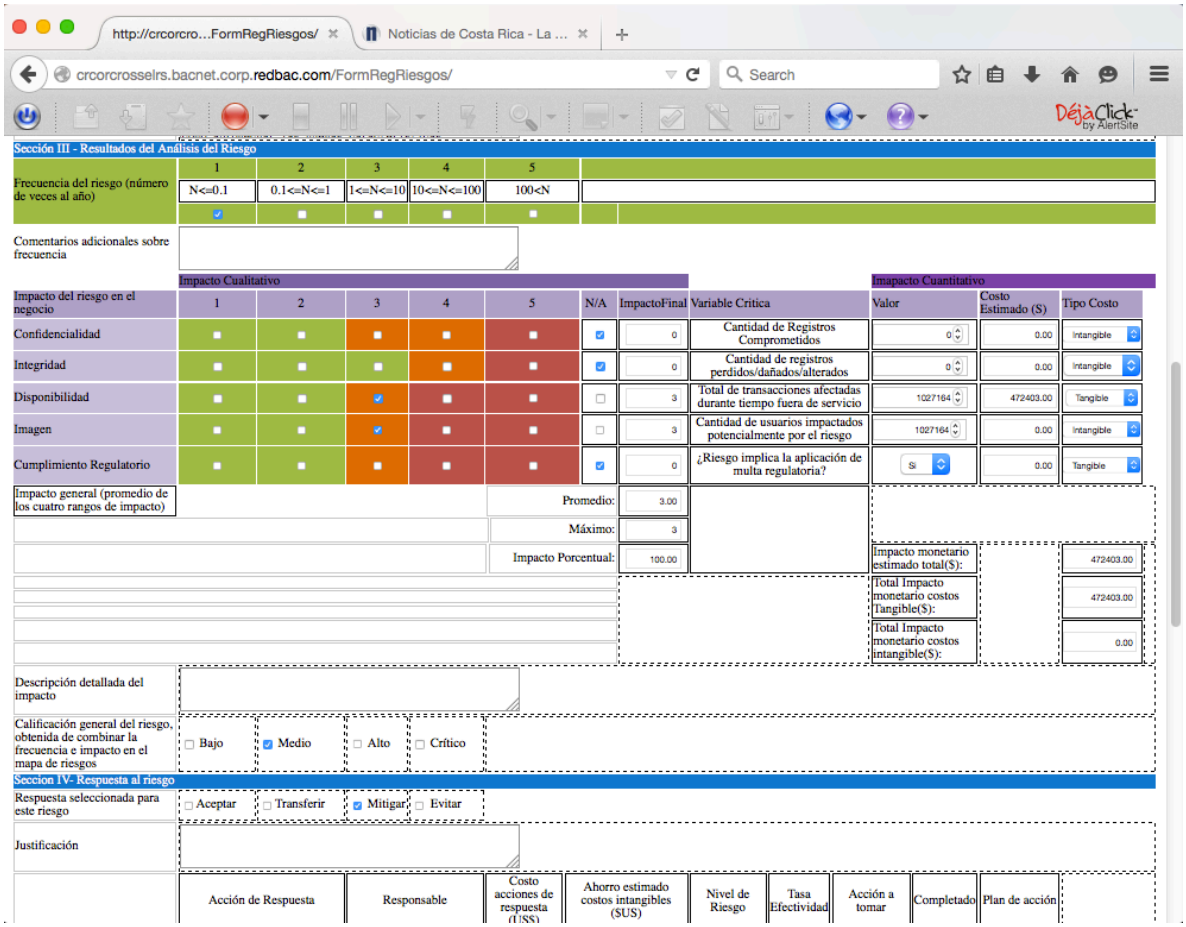



http://crcorcro...FormRegRiesgos/
crcorcrosselrs.bacnet.corp.redbac.com/FormRegRiesgos/
Search
Sección I- Resumen del Riesgo
IDRiesgo:
FR0059
Listado de Servicios Afectados
Enunciado del Riesgo:
Capacitaciones sobre plataforma WebSphere
Dueño del Riesgo:
Rubén Saborío
TODOS
Consulta Consolidada
Consulta Banco
Consulta Tarjeta
Transf. Locales
Pago de Tarjeta
Consulta Afiliados
Transf. otros Bancos
Envío PPP
Canal afectado:
Sucursal Electrónica
Servicio afectado:
TODOS
Fecha de la última evaluación del riesgo:
Fecha de la próxima evaluación de riesgo
Riesgos Agregados segun Servicio
Categoría de Riesgo:
Operacional (Operaciones de TI y entrega de servicios)
Busqueda de Riesgo y Descripción
FR0040
FR0041
FR0042
FR0043
FR0044
FR0045
FR0046
FR0047
FR0049
FR0050
FR0051
FR0053
Clasificacion de riesgo: (extraído de los resultados del análisis de riesgo):
Bajo
Medio
Alto
Crítico
Estimado impacto monetario total($):
472403.00
Estimado impacto monetario costos tangibles($)
472403.00
Estimado impacto monetario costos intangibles($)
0.00
Respuesta a riesgo:
Aceptar
Transferir
Mitigar
Evitar
Costo Plan de Acción($):
0.00
Costo acciones de respuesta (US$)
15000.00
Ahorro estimado costos intangibles ($US)
225000.00
Diferencia Estimado impacto monetario vs costo plan acción($)
472403

Sección II – Formulario Identificación de Riesgos – Ingreso de nuevo riesgo



Sección III – Formulario Identificación de Riesgos – Evaluación de riesgos



http://crcorcro...FormRegRiesgos/ | Noticias de Costa Rica - La ... | crcorcrosselrs.bacnet.corp.redbac.com/FormRegRiesgos/ | Search | DéjàClick by AlertSite

Sección III - Resultados del Análisis del Riesgo

Frecuencia del riesgo (número de veces al año)	1	2	3	4	5
	N<=0.1	0.1<=N<=1	1<=N<=10	10<=N<=100	100<N
	☑	☐	☐	☐	☐

Comentarios adicionales sobre frecuencia

Impacto del riesgo en el negocio	Impacto Cualitativo 1	2	3	4	5	N/A	ImpactoFinal	Variable Critica	Impacto Cuantitativo Valor	Costo Estimado ($)	Tipo Costo
Confidencialidad	☐	☐	☐	☐	☐	☑	0	Cantidad de Registros Comprometidos	0	0.00	Intangible
Integridad	☐	☐	☐	☐	☐	☑	0	Cantidad de registros perdidos/dañados/alterados	0	0.00	Intangible
Disponibilidad	☐	☐	☑	☐	☐	☐	3	Total de transacciones afectadas durante tiempo fuera de servicio	1027164	472403.00	Tangible
Imagen	☐	☐	☑	☐	☐	☐	3	Cantidad de usuarios impactados potencialmente por el riesgo	1027164	0.00	Intangible
Cumplimiento Regulatorio	☐	☐	☐	☐	☐	☑	0	¿Riesgo implica la aplicación de multa regulatoria?	Si	0.00	Tangible
Impacto general (promedio de los cuatro rangos de impacto)					Promedio:		3.00				
					Máximo:		3				
					Impacto Porcentual:		100.00		Impacto monetario estimado total($):		472403.00
									Total Impacto monetario costos Tangible($):		472403.00
									Total Impacto monetario costos intangible($):		0.00

Descripción detallada del impacto

Calificación general del riesgo, obtenida de combinar la frecuencia e impacto en el mapa de riesgos: ☐ Bajo ☑ Medio ☐ Alto ☐ Crítico

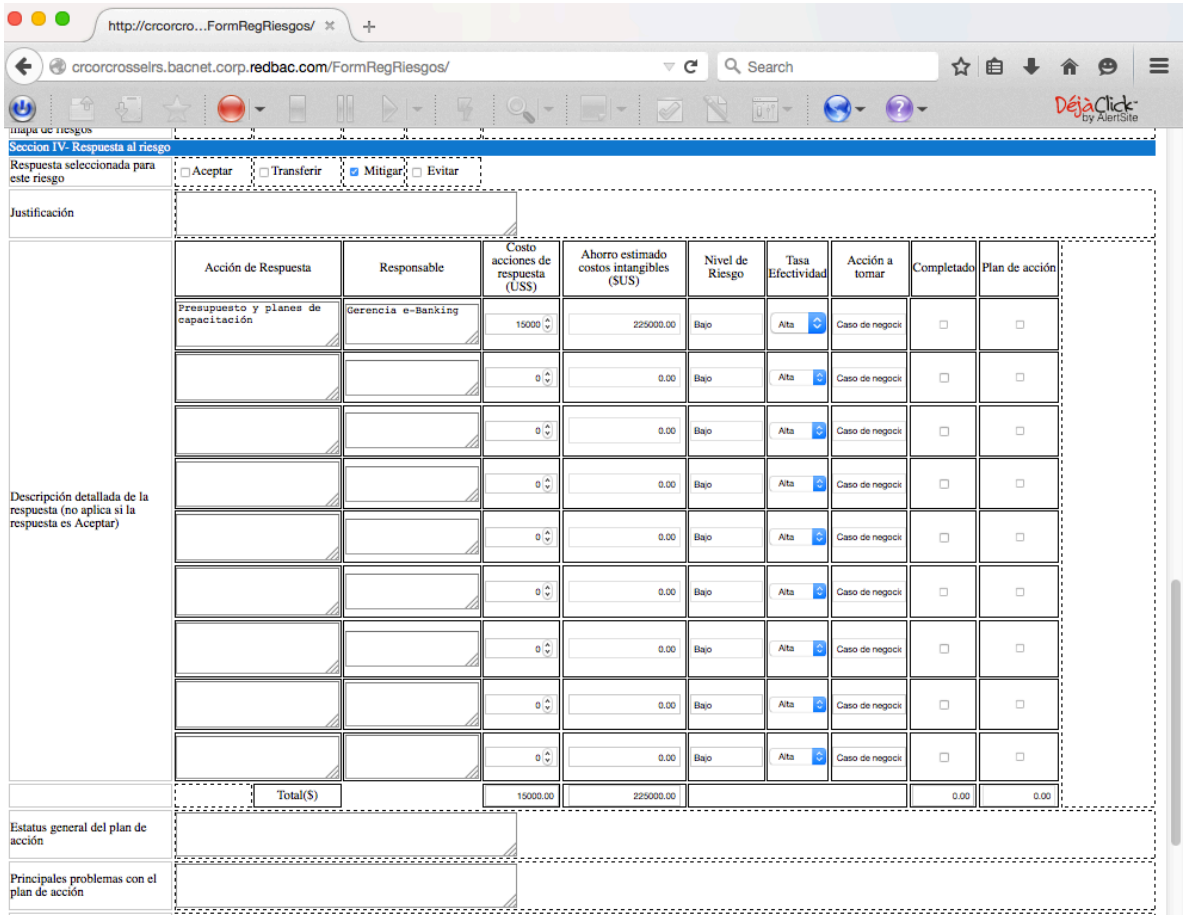
Seccion IV- Respuesta al riesgo

Respuesta seleccionada para este riesgo: ☐ Aceptar ☐ Transferir ☑ Mitigar ☐ Evitar

Justificación

Acción de Respuesta	Responsable	Costo acciones de respuesta (US$)	Ahorro estimado costos intangibles ($US)	Nivel de Riesgo	Tasa Efectividad	Acción a tomar	Completado	Plan de acción

Sección IV – Formulario Identificación de Riesgos – Respuesta a Riesgos



Seccion IV- Respuesta al riesgo

Respuesta seleccionada para este riesgo: ☐ Aceptar ☐ Transferir ☑ Mitigar ☐ Evitar

Justificación

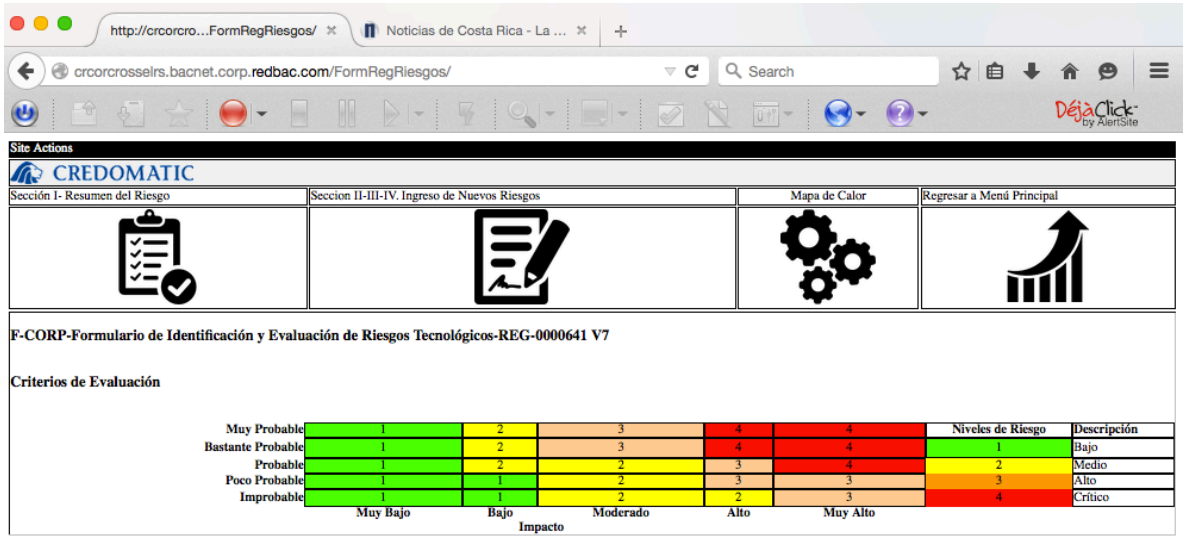
Descripción detallada de la respuesta (no aplica si la respuesta es Aceptar)

Acción de Respuesta	Responsable	Costo acciones de respuesta (US$)	Ahorro estimado costos intangibles ($US)	Nivel de Riesgo	Tasa Efectividad	Acción a tomar	Completado	Plan de acción
Presupuesto y planes de capacitación	Gerencia e-Banking	15000	225000.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
		0	0.00	Bajo	Alta	Caso de negocio	☐	☐
Total($)		15000.00	225000.00				0.00	0.00

Estatus general del plan de acción

Principales problemas con el plan de acción

Mapa de Calor



Anexo 10 - Campos Sección I – Resumen del Riesgo

Campo	Descripción
ID de Riesgo	Identificador único del riesgo generado por la herramienta
Enunciado del Riesgo	Descripción detallada del riesgo documentado
Dueño del Riesgo:	Persona a la que se le asigna la responsabilidad sobre este riesgo y el seguimiento de las acciones de respuesta.
Canal afectado:	Se puede listar Agencias, Banca Telefónica, Banca Móvil, etc. Para este ejercicio, únicamente se utilizará la banca electrónica pues corresponde al alcance de esta investigación.
Servicio afectado:	Lista de los diferentes servicios que se prestan a través del canal de Banca Electrónica a los cuales se les asocia el riesgo identificado. Por ejemplo, transferencias locales, interbancarias, internacionales, consultas de saldo, consultas de estados de cuenta, etc. Existe una opción donde se puede seleccionar un impacto a todos los servicios en caso que el riesgo afecte por completo el canal de Banca Electrónica.
Fecha de la última evaluación del riesgo:	Se utiliza para documentar cuando fue la última vez que se evaluó el riesgo.

Fecha de la próxima evaluación de riesgo:	Se utiliza para documentar cuando corresponde revaluar nuevamente el riesgo puesto que su calificación se considera que caducó. Es una buena práctica revalidar la calificación de los riesgos cada cierto tiempo.
Categoría de Riesgo:	Se pueden identificar riesgos en las agrupaciones de riesgos: Entrega de Valor de TI, Entrega Proyectos y Programas de TI y Operacional. Para este ejercicio, únicamente se utilizará Operacional pues corresponde al alcance de esta investigación.
Calificación del riesgo: (extraído de los resultados del análisis de riesgo)	Identifica cual es la calificación general que obtuvo el riesgo con base a las variables de frecuencia e impacto cualitativo. Las opciones posibles son: Bajo, Medio, Alto o Crítico.
Estimado impacto monetario total	Suma del estimado de impacto monetario en costos tangibles más costos intangibles.
Estimado impacto monetario costos tangibles	Sumatoria de costos tangibles que pudieron asociarse al impacto del riesgo descrito.
Estimado impacto monetario costos intangibles	Sumatoria de costos intangibles que pudieron asociarse al impacto del riesgo descrito
Respuesta a riesgo:	Identifica la(s) estrategia(s)

	seleccionadas para dar una respuesta al riesgo, la cual puede corresponder a: Aceptar, Transferir, Mitigar o Evitar.
Costo Plan de Acción	Sumatoria del costo de las acciones que fueron seleccionadas como parte del plan de acción para afrontar el riesgo.
Costo acciones de respuesta (US$)	Sumatoria del costo de todas las acciones de respuesta documentadas para afrontar el riesgo.
Ahorro estimado costos intangibles ($US)	Estimación general de ahorros generados por invertir en prevención.
Diferencia Estimado impacto monetario vs costo plan acción	Cálculo simple para confirmar si el valor de la inversión en el plan de acción cubre la estimación de impacto monetario realizado.

Anexo 11 – Campos Sección II – Descripción del Riesgo

Campo	Descripción
Enunciado del Riesgo	Descripción detallada del riesgo y la posible afectación que puede generar a los servicios/canal identificado.
Dueño del Riesgo:	Persona a la que se le asigna la responsabilidad sobre este riesgo y el seguimiento de las acciones de respuesta.
Canal afectado:	Se puede listar Agencias, Banca Telefónica, Banca Móvil, etc. Para este ejercicio, únicamente se utilizará la banca electrónica pues corresponde al alcance de esta investigación.
Servicio afectado:	Lista de los diferentes servicios que se prestan a través del canal de Banca Electrónica a los cuales se les asocia el riesgo identificado. Por ejemplo, transferencias locales, interbancarias, internacionales, consultas de saldo, consultas de estados de cuenta, etc. Existe una opción donde se puede seleccionar un impacto a todos los servicios en caso que el riesgo afecte por completo el canal de Banca Electrónica.
Escenario de riesgo de alto nivel (tomado del catálogo de escenarios de riesgo)	Identifica el escenario de riesgo de alto nivel al cual está relacionado el riesgo que se documenta.

Descripción detallada del escenario (componentes del escenario)	Una vez que se selecciona el escenario de riesgo en el campo anterior, la aplicación toma del catálogo de riesgos los elementos más relevantes asociados al escenario de riesgo. Estos elementos consideran los campos: Actor, Tipo de Amenaza, Evento, Recurso/Activo y Tiempo.
Información adicional del escenario	Es un campo de texto opcional para realizar cualquier aclaración ampliación sobre el riesgo actual.

Anexo 12 – Niveles de afectación para cada dimensión

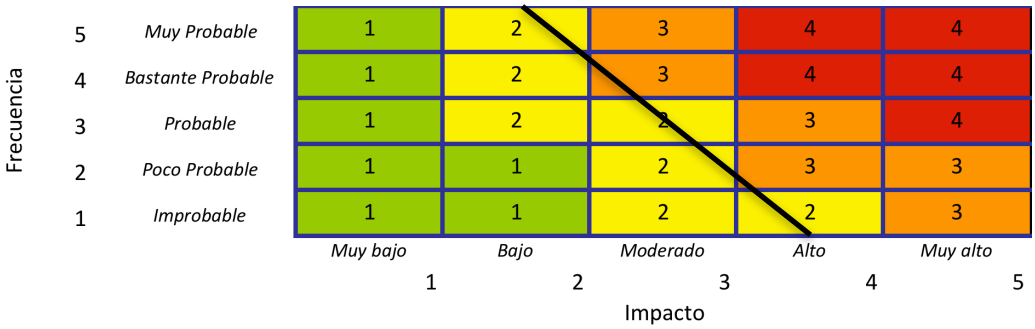
Criterio	Niveles de afectación
Confidencialidad	1: Existe exposición de información de tipo pública que no representa perjuicio para la institución 2: Existe exposición de información protegida internamente y no afecta los intereses de la institución. 3: Existe exposición de información confidencial y puede producir un uso malicioso en contra del negocio 4: Existe exposición de información restringida que puede producir un uso malicioso en contra del negocio 5: Existe exposición de información restringida que puede producir un uso malicioso en contra del negocio así como la afectación de los intereses de la institución.
Integridad	1: Implica que de existir una alteración o pérdida de la información esta no afecta los servicios, ya que existen controles que lo detectarán y/o lo corregirán. 2: Implica que en caso de existir una pérdida de información, la misma se encuentra dentro de los umbrales de tolerancia aceptados por el negocio para los servicios afectados. Esta métrica se conoce en continuidad como RPO (Recovery Point Objective). 3: Implica que de existir una pérdida de información, ésta sobrepasa los umbrales de tolerancia aceptados por el

	negocio para los servicios afectados. . Esta métrica se conoce en continuidad como RPO (Recovery Point Objective). Sin embargo, el evento sólo afecta un servicio que no es crítico, o, se presenta una alteración de información que no es crítica para el negocio. 4: Implica que de existir una pérdida de información, ésta sobrepasa los umbrales de tolerancia aceptados por el negocio para los servicios afectados. Esta métrica se conoce en continuidad como RPO (Recovery Point Objective). El evento provoca la afectación de máximo un servicio crítico. De forma alternativa, se presenta una alteración de información que puede ser detectada y corregida sin afectar a clientes externos o de forma grave a procesos de negocio. 5: Implica que de existir una pérdida de información, no hay procesos que permitan reprocesarla y dicha pérdida sobrepasa los umbrales definidos para los servicios críticos. Esta métrica se conoce en continuidad como RPO (Recovery Point Objective). De forma alternativa, la alteración de información afecta a clientes externos y procesos de negocio.
Disponibilidad	1: Existe compromiso de la disponibilidad del o los componentes que puede llegar a afectar el desempeño de un servicio no crítico. 2: Existe compromiso de la disponibilidad del o los componentes que provoque la interrupción de un servicio no crítico. 3: Existe compromiso de la disponibilidad del o los

	componentes que puede llegar a afectar el desempeño de un servicio crítico o varios no críticos. 4: Existe compromiso de la disponibilidad del o los componentes y puede afectar gravemente un servicio crítico o varios servicios no críticos. 5: Existe compromiso de la disponibilidad del o los componentes y puede afectar gravemente varios servicios críticos.
Imagen	1: Impacto mínimo en la imagen o confianza pública de la organización, sin exposición a medios. 2: Impacto regular en la imagen o confianza pública de la organización sin ninguna exposición a medios 3: Impacto regular en la imagen o confianza pública de la organización con exposición limitada a medios 4: Impacto importante en la imagen o confianza pública de la organización (a nivel local), con alta exposición a medios de comunicación 5: Impacto severo o catastrófico en la imagen o confianza pública de la organización (a nivel local e internacional), con alta exposición a los medios de comunicación.
Cumplimiento Regulatorio	1: El incumplimiento no generaría un hallazgo pero si una posible observación por parte del regulador, adicionalmente no se generarían multas o sanciones

	2: El incumplimiento generaría un hallazgo del regulador pero de criticidad baja, no se generarían multas o sanciones 3: El incumplimiento generaría un hallazgo importante del regulador mas no pone en riesgo el cumplimiento con la regulación, podría provocar una multa o sanción leve. 4: El incumplimiento generaría un hallazgo importante del regulador y pondría en riesgo el cumplimiento con la regulación, se generarían multas considerables o sanciones importantes. 5: El incumplimiento generaría un hallazgo crítico que generaría un incumplimiento importante de la regulación provocando la pérdida de una certificación o licencia, la aplicación de multas o sanciones que impacten significativamente al negocio.

Anexo 13 – Mapa de calor Riesgos



Los niveles de riesgo están definidos por la siguiente escala.

Niveles Riesgo	Descripción
1	Bajo
2	Medio
3	Alto
4	Crítico

Anexo 14 – Indicadores de medición propuestos

Indicador	Medición	Meta
Correlación de Riesgos vs Incidentes materializados	Correlación de la distribución de los riesgos relevantes identificados con la distribución de los incidentes materializados según su criticidad	Utilizando el coeficiente de correlación de Pearson lograr una correlación de los riesgos versus los incidentes que sea superior a 0.8
Nivel de satisfacción de clientes con la metodología (usuarios)	Evaluación del nivel de satisfacción a través de una encuesta	Lograr una calificación superior a 60% en la nota promedio de satisfacción de todos los criterios evaluados.
Identificación de costos (tangibles / intangibles) asociados a los riesgos	Porcentaje de riesgos identificados que incorporan la cuantificación de costos económicos (pérdidas, ahorros, etc.)	Lograr que el 60% los riesgos identificados con la nueva metodología contengan variables monetarias.