ANÁLISIS DE RIESGOS INFORMÁTICOS EN LA IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIAS PARA EL SOFTWARE DE ATENCIÓN AL CLIENTE EN UNA EMPRESA DE TELECOMUNICACIONES

Lorena, Garibello Brand

Ingeniero Telemático, Ingeniero de Soporte, Heinsohn Business Tecnology, Bogotá, D.C., Colombia,

lorenagaribello@gmail.com

Elkin Alexander, Oviedo Ruiz

Ingeniero Civil, Interventor de Proyectos, Inversiones Bibo S.A.S, Bogotá, D.C., Colombia,

elkinoviedo@hotmail.com

Dairo Yesid, Sierra Joiro

Ingeniero de Sistemas, Ingeniero de Infraestructura, Claro – Outsourcing Sonda de Colombia SA, Bogotá, D.C., Colombia,

dairo.sierra.ext@claro.com.co

TUTOR

Diego Roberto, Naizaque Ospina

Ingeniero de Diseño y Automatización Electrónica, Especialista en Gerencia de Empresas de Telecomunicaciones, Líder de Proyectos, Bogotá, D.C., Colombia,

diego.naizaque@claro.com.co

RESUMEN

La indisponibilidad en la aplicación de atención al cliente, impacta la operación de la empresa, por esto, se hace un análisis de riesgos a la implementación de un plan de contingencias para gestionar adecuadamente los riesgos críticos identificados.

PALABRAS CLAVES: Gestión de riesgos, Proyectos informáticos, Gerencia de proyectos y Plan de contingencias.

1. INTRODUCCIÓN

La empresa bajo estudio[1], inició operaciones en Colombia desde el año 1994 como proveedor de telecomunicaciones de última generación, maximizando la infraestructura de red disponible, generando innovadoras estrategias comerciales y desarrollo de productos para las empresas del país. El alto nivel de inversión en tecnología que ha tenido la empresa, ha generado oportunidad de crecimiento y mejora, pero al tiempo, se asocian a este crecimiento riesgos informáticos significativos, por lo anterior en este artículo se busca identificarlos y evaluarlos a través del análisis cualitativo y al final proponer un plan de respuesta a los riesgos críticos, con técnicas de control a través de actividades específicas, que permitan alcanzar el objetivo control sobre cada caso en estudio mitigando sus efectos en caso de llegar a materializarse.

[1] Por temas de confidencialidad se reserva el nombre de la compañía objeto del análisis y se hará referencia a una empresa de telecomunicaciones

El problema antes descrito se desarrolla tomando como referencia la metodología planteada en PMI [3], no obstante también se utiliza COBIT 4.1 [4], [5]. En la primera parte del artículo se trata la identificación de riesgos, en el capítulo dos, se trata la evaluación de los riesgos, en la cual se realiza el análisis cuantitativo de los mismos, en la tercera parte se trabaja el plan de respuesta a los riesgos y por último la documentación, donde se hará referencia a las lecciones aprendidas durante el desarrollo del proyecto.

2. DESCRIPCIÓN DEL PROBLEMA

La empresa bajo estudio, se localiza en el sector de las telecomunicaciones móviles con más de 35 millones de clientes y teniendo en cuenta las cifras oficiales de activaciones de líneas de telefonía móvil al cierre del cuarto trimestre de 2012 [1], se observa que en la empresa, se ha presentado una disminución del 1,64% frente al mismo periodo del año anterior (cuarto trimestre de 2011) y los retiros aunque han bajado en un 0,15% con respecto al trimestre anterior, siguen mostrando una cifra preocupante, originada por los problemas reiterados en el servicio, tales como falencias en la atención, demoras en la solución de peticiones, quejas y reclamos, procedimientos técnicos no efectivos y visitas técnicas no conciliadas por problemas en el sistema.

El cumplimiento correspondiente a la prestación de los servicios y desarrollo de los productos ofrecidos por la empresa, el mantenimiento de la actividad operativa e incluso la continuidad del negocio, dependen del cuidado y conservación que se tenga de la base tecnológica y por supuesto, del personal que la opera. Esto

implica que cuando un usuario experimenta problemas con su servicio, se comunica a la línea de soporte, la cual realiza un diagnóstico preliminar; si no logra dar solución, se utiliza la herramienta Visitas Técnicas, para programar el desplazamiento de un técnico a terreno. El número de visitas en promedio por día para mantenimientos es de 2.700 a nivel nacional [2].

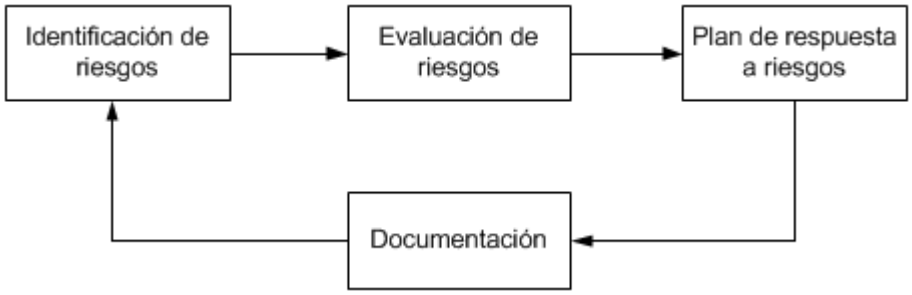
Actualmente, la compañía no cuenta con un plan de contingencia para la aplicación de atención al cliente, que permita seguir prestando el servicio, ante la ocurrencia de eventos de carácter técnico, accidental o humano con el fin de *minimizar el efecto de un riesgo sobre la operación y asegurando su continuidad*. Debido a esto la empresa se interesada en implementar dicha contingencia y así poder solucionar el problema que ocasiona no tenerlo. De este proyecto, se desprende la necesidad de analizar los riesgos informáticos en términos de los servicios que las áreas operativas ofrecen a sus clientes, sus vulnerabilidades, así como las amenazas y posibles impactos; además de identificar qué servicios de Infraestructura Tecnológica IT soportan los procesos de negocio asociados con la Aplicación de atención al cliente.

El aporte del trabajo consiste en realizar el análisis de riesgos informáticos en la implementación del plan de contingencia para la aplicación mencionada, según lo recomiendan las metodologías estándar y buenas prácticas, buscando identificar todos los riesgos asociados a la actividad y recomendar las posibles soluciones con el ánimo de mitigarlos. Esto permitirá desarrollar un procedimiento que garantice la prestación del servicio a través de la utilización de medios alternos.

3. ANÁLISIS DE RIESGOS EN LA IMPLEMENTACIÓN DE UN PLAN DE CONTINGENCIA EN UNA EMPRESA DE TELECOMUNICACIONES

Para la gestión de riesgos se ha tomado como referencia la guía PMBoK [3], complementada con el manejo de COBIT 4.1 [4], [5], definiendo la siguiente metodología: identificación de riesgos, evaluación de riesgos, plan de respuesta a riesgos y documentación como se amplía en la Figura 1:

Figura 1. Metodología de gestión de riesgos.



Fuente: Adaptado de [3], [4].

De acuerdo a la guía mencionada [3], se toma como dato de entrada el acta de constitución del proyecto (Project Charter), la cual es el preliminar del contrato de trabajo y de la misma se obtiene el cronograma, la estructura desglosada de trabajo –WBS– y el presupuesto asignado al proyecto, el cual en cifras globales asciende a 48,000 USD.

Tomando como base los entregables del proyecto se desarrolla la WBS, tal como se muestra en la Tabla 1.

Tabla 1. Work Breakdown Structure – WBS

WBS Nivel 0	WBS Nivel 1	WBS Nivel 2
Implementación plan de Contingencia	1. Hardware	1.1 Especificaciones técnicas de equipos a comprar
		1.2 Selección de proveedores de equipos
		1.3 Evaluar orden de compra
		1.4 Aprovisionar sistema operativo (SO) y storage local
		1.5 Alistamiento e instalación de equipos
	2. Software	2.1 Compra de licenciamiento de SO y aplicaciones
		2.2 Administración de los componentes
		2.3 Ejecución de pruebas de software
		2.4 Administración de la configuración
	3. Mano de Obra y/o servicios	3.1 Aprobación de ambientes y esquemas definidos
		3.2 Instalación de licenciamiento
		3.3 Ejecutar paso a producción
		3.4 Pruebas funcionales en el ambiente de producción
		3.5 Configuración de monitoreo
		3.6 Generación de manuales de usuario

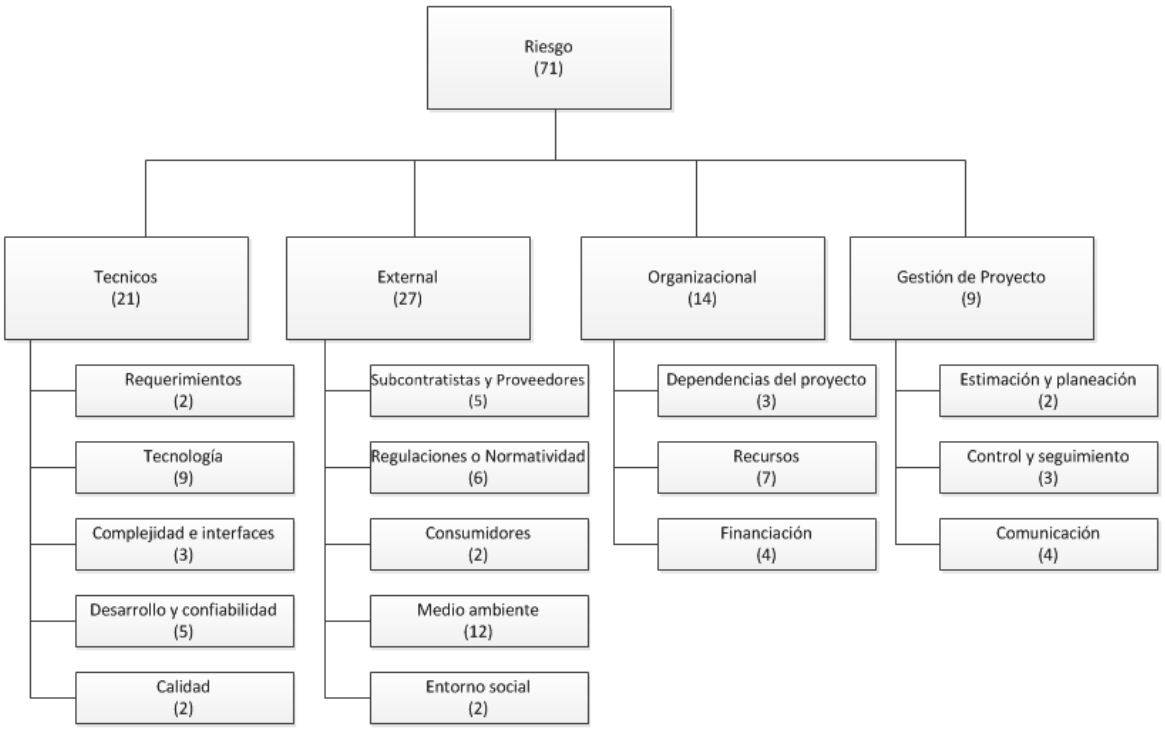
Fuente: Adaptado de [3].

El tiempo estimado para la implementación del proyecto es de 4 meses y los costos están distribuidos por cada segmento de la siguiente forma: Hardware 40%, Software 20%, Mano de obra y/o servicios 30% e imprevistos con un 10% del valor aprobado para la implementación del proyecto.

3.1. IDENTIFICACIÓN DE RIESGOS:

Esta etapa consiste en identificar cuáles son los posibles riesgos en un proyecto de tecnología, determinando por la probabilidad de ocurrencia, el impacto que podría representar para empresa, en caso de llegar a materializarse. Para ese trabajo se emplea el concepto Risk Breakdown Structure (RBS), que permite identificar los riesgos según su categorización como se presenta en la Figura 2.

Figura 2. Risk Breakdown Structure – RBS



Fuente: Adaptado de [3].

Existen dos tipos de riesgos identificados, los genéricos que son una amenaza potencial para todos los proyectos de tecnología y los riesgos específicos del servicio; estos riesgos se pueden identificar sólo teniendo una visión clara de la tecnología, el personal y el entorno.

En la matriz RACI del proyecto están clasificados los roles para todos los procesos como se detalla a continuación: gerente de IT, oficial de seguridad, gerente de servicios, coordinador de redes, administrador de plataformas, coordinador de base de datos, administrador de aplicaciones, jefe de sistemas de información, coordinador de proyectos, administrador de base de datos, personal de apoyo y jefe de IT.

De acuerdo a la WBS, se genera la Tabla 2, donde se observa la Matriz RACI (Responsable, Autorizador, Consultado, Informado).

Tabla 2. Matriz RACI

Actividades	Gerente de IT	Oficial de seguridad	Gerente de Servicios	Coordinador de Redes	Coordinador de Plataformas	Jefe de compras	Administrador de Aplicaciones	Jefe de Sistemas de Información	Coorninador de proyectos	Administrador de Base de Datos	Personal de apoyo	Jefe de IT
Especificaciones técnicas de equipos a comprar	A			C	C	I	C		R	C		
Compra de equipos	I		I	I	I	R	I	I	I	I		A
Llegada de equipos comprados	I	C	I			I		I	R			C
Aprovisionar SO y storage local	C	I			R				I			A
Alistamiento e instalación de equipos	I	I			R				C			A
Compra de Licenciamiento de SO y Aplicaciones	I		I	I	C	R	C	I	I			A
Instalación de licenciamiento	I	I			R				C			A
Alistamiento de SO y Aplicaciones	C	I			R				I			A
Pruebas de funcionamiento	I	I	I	C	C		C	A	R		C	I
Aprobación de ambientes y esquemas definidos	I	I	I	C	C		C		I	R		A
Ejecutar Paso a Producción	I	I	I	C	C		C	C	R	C		A
Pruebas de usuario final	I	I	I	C	C		C	A	R		C	I
Configuración de monitoreo	I	I	I		C			C	R	C		A
Capacitación	I		A					C	R		C	

Fuente: Adaptado de [5].

A continuación se relaciona en la Tabla 3, el listado de los 71 riesgos identificados, de los cuales 15 se encuentran cubiertos por las pólizas de la compañía. Los 56 riesgos restantes se analizan a través de la matriz de Probabilidad e Impacto, teniendo en cuenta los criterios que describen en la evaluación de los riesgos.

Tabla 3. Riesgos identificados

Item	Categorización del Riesgo	Sub Categorización del Riesgo	Riesgos	Nomenclatura	Cobertura
1	Técnicos	Requerimientos	Fallas en el levantamiento de requerimientos de hardware	TREQ01	No
2	Técnicos	Requerimientos	No tener el mapa de la aplicación actualizado o que esté incompleto, llegando a afectar la adecuada implementación de la infraestructura	TREQ02	No
3	Técnicos	Tecnológicos	Fallas en la infraestructura tecnológica de Tecnologías de la Información	TTEC01	Si

4	Técnicos	Tecnológicos	Afectación al rendimiento del ambiente productivo, al realizar pruebas funcionales de comparación	TTEC02	No
5	Técnicos	Tecnológicos	Falta de soporte y garantía de los servidores asignados sobre los productos a instalar	TTEC03	Si
6	Técnicos	Tecnológicos	Incompatibilidad de las máquinas asignadas con los productos a instalar	TTEC04	Si
7	Técnicos	Tecnológicos	La mala manipulación de los equipos informáticos	TTEC05	No
8	Técnicos	Tecnológicos	La falla en hardware y software de respaldo de información	TTEC06	Si
9	Técnicos	Tecnológicos	La falta de mantenimiento de los equipos informáticos y redes.	TTEC07	No
10	Técnicos	Tecnológicos	La instalación de tecnología inadecuada.	TTEC08	No
11	Técnicos	Tecnológicos	Ataques informáticos.	TTEC09	No
12	Técnicos	Complejidades e Interfaces	Falta de capacitaciones para en el manejo de software	TCEI01	No
13	Técnicos	Complejidades e Interfaces	Manipulación fraudulenta de los datos	TCEI02	No
14	Técnicos	Complejidades e Interfaces	Mala configuración del sistema	TCEI03	No
15	Técnicos	Desarrollo y Confiabilidad	Perdida de información en las bases de datos	TDYC01	No
16	Técnicos	Desarrollo y Confiabilidad	Problemas de integridad de información en la Base de Datos	TDYC02	No
17	Técnicos	Desarrollo y Confiabilidad	Errores de ingreso de información al sistema	TDYC03	No
18	Técnicos	Desarrollo y Confiabilidad	Baja seguridad en el acceso a la información	TDYC04	No
19	Técnicos	Desarrollo y Confiabilidad	Perdidas de claves de acceso al sistema	TDYC05	No
20	Técnicos	Calidad	Entrega incompleta de los informes	TCAL01	No
21	Técnicos	Calidad	Baja calidad en los equipos adquiridos para el servicio.	TCAL02	Si
22	Externos	Subcontratistas y Proveedores	Interrupción en el servicio de suministro de energía por parte del proveedor	ESYP01	No
23	Externos	Subcontratistas y Proveedores	Sobrecargas en el servicio de suministro de energía por parte del proveedor	ESYP02	No
24	Externos	Subcontratistas y Proveedores	Ausencia de generadores alternos de energía eléctrica	ESYP03	No
25	Externos	Subcontratistas y Proveedores	Falta de idoneidad en el momento de ejecutar las actividades	ESYP04	No

26	Externos	Subcontratistas y Proveedores	Las fechas estimadas de liberación de los equipos no se cumplan	ESYP05	Si
27	Externos	Regulaciones o Normatividad	Falta de conocimiento de la legislación vigente colombiana	ERON01	No
28	Externos	Regulaciones o Normatividad	Cambios extraordinarios en la legislación colombiana.	ERON02	No
29	Externos	Regulaciones o Normatividad	Fallas en la aplicación de las normas de la legislación colombiana	ERON03	No
30	Externos	Regulaciones o Normatividad	Falta de entidades de control y vigilancia de las normas de la legislación colombiana	ERON04	No
31	Externos	Regulaciones o Normatividad	Retrasos en los procesos de contratación	ERON05	No
32	Externos	Regulaciones o Normatividad	Demoras en trámites de documentos según legislación colombiana	ERON06	No
33	Externos	Consumidores	Incumplimiento en el pago de usuarios por el servicio ofrecido	ECON01	No
34	Externos	Consumidores	Solicitud de cambios extraordinarios no contemplados en la planificación	ECON02	No
35	Externos	Medio ambiente	Equipos de cómputo que se encuentren defectuosos	EMEA01	Si
36	Externos	Medio ambiente	Instalaciones inadecuadas para equipos de computo	EMEA02	Si
37	Externos	Medio ambiente	Deterioro de cableado estructural	EMEA03	Si
38	Externos	Medio ambiente	Mala ubicación geográfica de las instalaciones en donde se encuentren los equipos, ejemplo: zonas costeras, zonas aledañas a fuentes hídricas o zonas de presiones geológicas.	EMEA04	No
39	Externos	Medio ambiente	Falla en sistemas de extinción de incendios dentro de las instalaciones donde están los equipos	EMEA05	Si
40	Externos	Medio ambiente	Ubicación de las instalaciones en zonas de deslizamientos de tierra	EMEA06	No
41	Externos	Medio ambiente	Ubicación de las instalaciones en zonas de ondas marinas.	EMEA07	No
42	Externos	Medio ambiente	Tormentas eléctricas en la zona donde se ubique las instalaciones donde están los equipos	EMEA08	No
43	Externos	Medio ambiente	Tormentas de polvo en la zona donde se ubique las instalaciones donde están los equipos	EMEA09	No
44	Externos	Medio ambiente	Tormentas de invierno o granizadas en la zona donde se ubique las instalaciones donde están los equipos	EMEA10	No

45	Externos	Medio ambiente	Excesivo calor en el RACK, debido a la falta de un equipo de refrigeración	EMEA11	Si
46	Externos	Medio ambiente	Excesivo frio en el RACK, debido a la falta de un equipo de calefacción	EMEA12	Si
47	Externos	Entorno social	Sabotajes continuos en el servicio	EENS01	No
48	Externos	Entorno social	Terrorismo que afecta el suministro del servicio	EENS02	No
49	Organizacional	Dependencias del proyecto	Prestación ineficiente del servicio	ODDP01	No
50	Organizacional	Dependencias del proyecto	Dificultad de adquisición de mano de obra calificada en la región	ODDP02	No
51	Organizacional	Dependencias del proyecto	Demora en los servicios logísticos de traslado de los equipos	ODDP03	Si
52	Organizacional	Recursos	Indisponibilidad del personal que presta el servicio	OREC01	No
53	Organizacional	Recursos	Demoras en los proceso de contratación de los servicios profesionales de instalación	OREC02	No
54	Organizacional	Recursos	No contar con espacio adecuado para el montaje del hardware	OREC03	No
55	Organizacional	Recursos	Robo o perdidas continuas de dispositivos	OREC04	No
56	Organizacional	Recursos	Perdida de personal clave en la compañía	OREC05	No
57	Organizacional	Recursos	Huelgas en la compañía	OREC06	No
58	Organizacional	Recursos	Falta de recursos monetarios de la compañía para prestar el servicio	OREC07	No
59	Organizacional	Financiación	Problema contractual con los proveedores	OFIN01	Si
60	Organizacional	Financiación	Crisis económica en la región	OFIN02	No
61	Organizacional	Financiación	Multas por incumplimiento del servicio prestado	OFIN03	Si
62	Organizacional	Financiación	Malas negociaciones en los procesos de adquisiciones de equipos	OFIN04	No
63	Gerencia del proyecto	Estimación y planeación	Falla en la estimación de tiempos de servicio	GPEP01	No
64	Gerencia del proyecto	Estimación y planeación	Falla en la estimación de los costos en la prestación del servicio	GPEP02	No
65	Gerencia del proyecto	Control y seguimiento	Falta de controles internos en los procesos	GPCS01	No
66	Gerencia del proyecto	Control y seguimiento	Falta de validación de la documentación en los procedimientos internos	GPCS02	No
67	Gerencia del proyecto	Control y seguimiento	Bajo nivel de satisfacción de los clientes con el servicio	GPCS03	No
68	Gerencia del proyecto	Comunicación	Falta de informes de avances del servicio	GPCO01	No

69	Gerencia del proyecto	Comunicación	Mala recepción de las quejas y reclamos del servicio	GPCO02	No
70	Gerencia del proyecto	Comunicación	Falta de información hacia los trabajadores para la mejora en la prestación del servicio	GPCO03	No
71	Gerencia del proyecto	Comunicación	Actos deliberados en la divulgación de la información	GPCO04	No

Fuente: Adaptado de [3], [6].

3.2. EVALUACIÓN DEL RIESGO

Una vez identificados y clasificados los riesgos en el proyecto, se procede a desarrollar un análisis cualitativo para determinar su impacto de acuerdo a la probabilidad de ocurrencia.

3.2.1. ANÁLISIS CUALITATIVO

El análisis cualitativo del riesgo es el proceso por el cual se evalúa el impacto y la probabilidad de los riesgo identificados. Para este tipo de análisis existen diversas herramientas y técnicas para evaluar la probabilidad y las consecuencias de cada factor de riesgo; técnicas como la Lluvia de Ideas, Técnica Delphi, Entrevistas, análisis de fortalezas, oportunidades, debilidades y amenazas (FODA), permiten a un gerente de proyectos tomar decisiones frente a un nivel de riesgo, apoyándose en su juicio y experiencia.

Definición de la matriz de Riesgo: La ocurrencia de un evento tiene una implicación sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando éste se presenta, por lo que resulta necesario categorizarlos

Para determinar las probabilidades de ocurrencia de un evento, acudimos a la técnica Delphi, con el cual se maximizaron las ventajas de contar con un grupo de

expertos y minimizar inconvenientes, aprovechando la sinergia de criterios y obteniendo un consenso lo más fiable posible referente a los temas en tratamiento por parte de un grupo experto.

Para este análisis, se tomó el criterio de 5 expertos, un administrador de plataformas, un administrador de aplicaciones, un jefe de sistemas de información, un coordinador de proyectos y un jefe de IT y se estableció para un total de 100 ocurrencias, con qué frecuencia se presenta un evento de acuerdo al tipo de probabilidad tal como se muestra en la Tabla 4.

Tabla 4. Probabilidad de ocurrencia de riesgos

	Poco frecuente	Normal	Frecuente	Muy frecuente	Total ocurrencias
Experto 1	14	24	26	36	100
Experto 2	10	20	28	42	100
Experto 3	12	22	31	35	100
Experto 4	8	26	28	38	100
Experto 5	16	18	27	39	100
FRECUENCIA PROMEDIO	12	22	28	38	100
PORCENTAJE	12%	22%	28%	38%	100%

Fuente: Adaptado de [3], [6].

El resultado que se obtiene basado en el método Delphi, se ilustra a través de la Tabla 5, donde se especifica la frecuencia evaluada de manera conceptual y se ponderan las respuestas de cada experto, seleccionando los aportes con mayor grado de consenso, para determinar un valor por cada riesgo evaluado según su probabilidad de ocurrencia.

Tabla 5. Ponderación de Probabilidad de ocurrencia de un evento

Probabilidad	Frecuencia	%
Poco frecuente	Menor o igual a una vez por año	12
Normal	Menor o igual a una vez cada 6 meses	22
Frecuente	Mayor o igual a una vez por mes	28
Muy frecuente	Mayor o igual a una vez por día	38

Fuente: Adaptado de [3].

Para obtener el impacto valorado en términos económicos, también se hace uso del método Delphi, a través del cual se logra obtener el porcentaje del valor del proyecto, con el cual se clasifica el impacto que se tiene en caso de materializarse alguno de los riesgos identificados para obtener la ponderación porcentual del impacto, como se muestra en la Tabla 6.

Tabla 6. Ponderación porcentual del impacto

	Muy alto	Alto	Medio	Bajo	Muy bajo	Total ocurrencias
Experto 1	72,50%	15,63%	7,50%	3,33%	1,04%	100%
Experto 2	74,25%	14,38%	7,29%	3,13%	0,96%	100%
Experto 3	71,31%	18,13%	6,67%	2,88%	1,03%	100%
Experto 4	69,48%	19,79%	7,08%	2,67%	0,97%	100%
Experto 5	82,46%	7,08%	6,46%	3,00%	1,00%	100%
Frecuencia promedio %	74%	15%	7%	3%	1%	100%

Fuente: Adaptado de [3].

La valoración porcentual expresada en términos económicos se representa como se muestra en la tabla 7.

Tabla 7. Valoración económica del impacto

	Muy alto	Alto	Medio	Bajo	Muy bajo	Total ocurrencias
Experto 1	$ 69.600.000	$ 15.000.000	$ 7.200.000	$ 3.200.000	$ 1.000.000	$ 96.000.000,00
Experto 2	$ 71.280.000	$ 13.800.000	$ 7.000.000	$ 3.000.000	$ 920.000	$ 96.000.000,00
Experto 3	$ 68.455.000	$ 17.400.000	$ 6.400.000	$ 2.760.000	$ 985.000	$ 96.000.000,00
Experto 4	$ 66.705.000	$ 19.000.000	$ 6.800.000	$ 2.560.000	$ 935.000	$ 96.000.000,00
Experto 5	$ 79.160.000	$ 6.800.000	$ 6.200.000	$ 2.880.000	$ 960.000	$ 96.000.000,00
Frecuencia promedio	$ 71.040.000,00	$ 14.400.000,00	$ 6.720.000,00	$ 2.880.000,00	$ 960.000,00	$ 96.000.000,00

Fuente: Adaptado de [3], [5].

El análisis de riesgos va más allá de solo identificar la posibilidad de que los mismos ocurran, ya que adicionalmente se debe evaluar el impacto de cada uno, para de esta manera poderlos clasificarlos por su severidad.

De manera complementaria se puede obtener una evaluación económica del impacto en caso de que un riesgo se materializara. Dimensionar el impacto de los riesgos en cifras comparables con la inversión necesaria para su mitigación y/o control, permite determinar si los costos de implementar dichos mecanismos de control son justificables. Por ejemplo, conocer si la inversión necesaria para proteger un activo valioso, como lo es la información, es menor que el sobrecosto que acarearía su pérdida o su indisponibilidad. De esta forma se pueden priorizar las posibles incidencias y su costo potencial, desarrollando un plan de acción adecuado. En el presente caso de estudio, donde se evalúan especialmente los riesgos informáticos en la implementación de un plan de contingencia para una aplicación, se debe conocer que se quiere proteger, donde y como, asegurando que con las soluciones implementadas se mitiguen de manera efectiva las consecuencias de posibles fallas.

Para llevar a cabo la evaluación económica de los impactos se debe, por lo tanto, identificar el valor cuantitativo de los recursos a utilizar (hardware, software, personal, servicios profesionales, etc.), la cuantificación del valor de la información, así como los costos en los que se incurriría al incumplir los SLA establecidos, o las sanciones de no acogerse a las normas gubernamentales.

Después de realizar el análisis a los 56 riesgos identificados, luego de excluir los que están cubiertos por la póliza de la empresa, se encuentran 27 riesgos, en una zona crítica como se observa en la Tabla 8.

Tabla 8. Matriz Probabilidad Impacto

		Probabilidad			
		Poco Frecuente	Normal	Frecuente	Muy Frecuente
Impacto	MA: Muy Alto	10,11,23,38,40,41,42,43,44,48,54,62,68,71	53,56,60,64,69	34,49,67	65
	A: Alto	15,29,30,50,55,70	1,17		33
	M: Medio	7,13,28,58	14,18,27	32	55
	B: Bajo	9,20,22,24,47,57	4	19,63	12,31
	MB: Muy Bajo	17, 52	25, 0	2	

Fuente: Adaptado de [3].

Se toma como críticos, aquellos riesgos con impacto MA y probabilidad muy frecuente, MA, con probabilidad frecuente, MA con probabilidad normal, MA con probabilidad poco frecuente, impacto A con probabilidad muy frecuente, A con probabilidad frecuente, A con probabilidad normal, e impacto M con probabilidad muy frecuente.

Una vez se determina la criticidad de los riesgos, de acuerdo a la probabilidad de ocurrencia y su impacto, se procede a estimar a cuál de los 27 riesgos se debe hacer gestión de acuerdo al porcentaje de inversión que habría que hacer para su

mitigación, frente al costo de asumir que el riesgo se materialice, *aceptando como umbral aquellos con un porcentaje menor al 10% sobre la inversión del proyecto*, con respecto a lo cual se reduce el análisis a 7 riesgos, los cuales se relacionan a continuación:

Tabla 9. Resumen Riesgos para aplicar plan de respuesta

Categorización del riesgo	Riesgos		Costo de mitigar el riesgo	% Sobre presupuesto
Requerimientos	Fallas en el levantamiento de requerimientos de hardware	$	4.000.000	4,17%
Requerimientos	La instalacion de tecnologia inadecuada	$	19.000.000	6,86%
Requerimientos	Ataques informaticos	$	18.000.000	5,14%
Desarrollo y Confiabilidad	Problemas de integridad de informacion en la Base de Datos	$	7.000.000	1,71%
Recursos	Demoras en los proceso de contratación de los servicios profesionales de instalación	$	30.000.000	6,66%
Control y Seguimiento	Falta de validacion de la documentacion en los procedimientos internos	$	6.000.000	1,62%
Comunicación	Actos deliberados en la divulgacion de la informacion	$	200.000.000,00	3,62%

Fuente: Adaptado de [4], [6].

En la matriz de riesgos se identifican los eventos a tener en cuenta y por los cuales existe una necesidad de mitigación con el fin de disminuir el impacto.

4. PLAN DE RESPUESTA AL RIESGO

Existen varias estrategias de respuesta al riesgo. Por cada riesgo, se decide una estrategia que tenga la mayor probabilidad de ser efectiva. Luego, se deben desarrollar acciones específicas a fin de implementar dicha estrategia [3]. Esta etapa se compone de la planificación de gestión del riesgo que permite desarrollar un plan que controle cada uno de los riesgos de prioridad alta previamente identificados, resolución del riesgo y monitorización que define los indicadores que influyen en la probabilidad de que el riesgo se produzca.

La planeación de la respuesta al riesgo, se basa en definir cuál va a ser la decisión frente a cada riesgo identificado como crítico. Por esto se debe llegar a saber cómo *evitar* el riesgo, como *mitigar* el riesgo, como *transferir* el riesgo y como *aceptar* el riesgo y relacionar las acciones que respaldan cada estrategia, así como también, reflejar las fechas de cumplimiento y responsables. En la Tabla 10, se plantea el plan de respuesta definido por cada riesgo y de esta manera lograr que el tratamiento a los mismos, sea el más conveniente para los intereses de la empresa.

Tabla 10. Plan de respuesta a riesgos

Riesgos No asegurables	Decisión	Plan de contingencia	Tiempo de respuesta	Costo de respuesta	Responsable
TREQ01	Mitigar	1. Se debe realizar un dimencionamiento de trafico, IO, transacciones, usuarios conectados de forma concurentes, procesamiento, memoria y tasa de crecimiento	7 días	$ 4.000.000,00	Jefe de IT
TTEC08	Mitigar	1. Negociar recursos con gerente de otro proyecto 2. Cambiar ó repotenciar equipos a través de gestion con el proveedor	30 dias	$ 19.000.000,00	Coorninador de proyectos
TTEC09	Mitigar	1. Gestionar con el oficial de seguridad seguimiento a los ataques informáticos.	15 dias	$ 18.000.000,00	Oficial de seguridad
TDYC02	Mitigar	1. Trabajar el problema de diseño y desarrollo. 2. Realizar cambios en el software para que no se presente este tipo de inconveniente	30 dias	$ 7.000.000,00	Administrador de Base de Datos
OREC02	Mitigar	1. Validar que se cumplan los requerimientos definidos 2. Hacer seguimiento a todo el proceso de compras	20 dias	$ 30.000.000,00	Jefe de compras
GPCS02	Mitigar	Completar mapas de servicios la CMDB	15 dias	$ 6.000.000,00	Coorninador de proyectos
GPCO04	Aceptar	N/A	N/A	$ 200.000.000,00	N/A

Fuente: Adaptado de [4], [6].

5. DOCUMENTACIÓN

En cada proyecto que se aborda necesariamente se presentan situaciones que favorecen y otras que no, por lo cual se identificó y analizó lo que se puede aprender de las mismas. Tener en cuenta las lecciones aprendidas desde el inicio del proyecto hasta el final, permite documentar estas situaciones, analizar su causa raíz, el impacto que tuvieron en el proyecto y determinar qué acciones

fueron efectivas para mitigar sus efectos en el caso de las amenazas, y mejorarlos en el caso de las oportunidades. En las metodologías de gestión de proyectos, como por ejemplo el PMI, las lecciones aprendidas es un punto en los cierres de fase o proyecto, así como también al culminar cada ciclo de control (de alcance, costo, calidad, tiempo, etc.).

Para este proyecto en particular se incluyen temas relevantes dentro del desarrollo y eventos asociados a riesgos potenciales y se espera sirvan como referencia para futuros proyectos al contener un nivel de detalle suficiente para que otras personas puedan tener información suficiente sobre la cual basar sus planes de ayuda del proyecto.

En la Tabla 11 relacionada a continuación, se muestra las lecciones aprendidas del análisis de riesgos en un proyecto que pretende la implementación de un plan de contingencia para una aplicación de atención al cliente en una empresa de telecomunicaciones. Estas lecciones son categorizadas por área de conocimiento describiendo su impactos y las recomendaciones se ofrecen para su la consideración en proyectos futuros.

Tabla 11. Lecciones aprendidas

Categoría	Nombre del problema	Problema / Éxito	Impacto	Recomendación
Gestión de Compras	Requisitos del contrato	Falta de participación del gerente de proyecto en el proceso de contratación de los servicios profesionales de instalación	Todos los requisitos no fueron incluidos en la adjudicación del contrato inicial. Una modificación al contrato retrasa negativamente el proyecto	El gerente de proyecto debe participar plenamente en todos los procesos de contratación
Gestión de recurso humano	Plan de incentivos por logros	No había ningún plan para proporcionar incentivos y reconocimientos a los miembros del equipo	Al final del proyecto no hubo motivación y los miembros del equipo estaban pidiendo salir del proyecto	El proyectista deberá establecer y comunicar una entrega de incentivos (programa de reconocimiento) para cada proyecto
Gestión del alcance	Modificación del alcance	Intentos continuos de los interesados de ampliar el alcance del proyecto durante todo su ciclo de vida	El gerente del proyecto no tenía un plan para impedir el cambio del alcance y permitió incluir algunos de los requisitos solicitados, lo cual genero retraso en el cronograma del proyecto	El gerente de proyecto debe tener un proceso de aprobación de los cambios propuestos y comunicar el alcance de este proceso a todas las partes interesadas
Gestión de Calidad	Equipos para la implementación	Fallas en el levantamiento de requerimientos de hardware	Retrasos en el cronograma del proyecto a causa de tener equipos inadecuados para la implementación	Planificar siempre el listado de insumos con las especificaciones correctas y ajustada siempre a los estándares de calidad. Esto ayuda a evitar retrasos y sobrecostos
Gestión de riesgos	Accesos	Se identificó un riesgo, en cuanto a retrasos en la recepción de equipos en el DataCenter, por la aprobación de ingreso, pero fue un éxito, ya que se identificó a tiempo y fue planeado	El impacto fue mínimo debido a que el Gerente de proyectos incluyó los posibles retrasos en el cronograma del proyecto e hizo gestión para mitigar el riesgo	Tenga siempre en cuenta los efectos externos sobre el costo del proyecto y el calendario. Esta debe ser continua durante todo el ciclo de vida del proyecto

Fuente: Adaptado de [3], [6].

6. CONCLUSIONES

Más allá de lo expuesto a lo largo de este documento, no se debe olvidar que los riesgos cohabitan continuamente en el ciclo de vida de los proyectos, y que su eliminación absoluta es un escenario utópico, principalmente cuando todas las organizaciones tienen limitantes de tiempo, costo o recursos. Por este motivo, lo que se debe buscar es generar planes que permitan mitigar al máximo los efectos de los mismos o reducir en la mayor medida posible la probabilidad de que sucedan.

Es importante destacar que el proceso de gestión de riesgos puede implicar tareas o inversiones adicionales dentro de un proyecto, por ejemplo en nuestro caso de estudio, conllevó a que los costos relacionados con el plan de contingencia para

software de atención al cliente en una empresa de telecomunicaciones, sean mayores que los inicialmente planeados. En algunos casos pueden ser necesarias, por ejemplo, inversiones en equipos y enlaces redundantes, además de sistemas de backup y recuperación, y hasta una planta mayor de personal de monitoreo y soporte especializado. Aun así, los costos adicionales necesarios para mitigar los riesgos, aunque altos, son indispensables para evitar pérdidas o gastos que en buena medida serán mucho mayores a las inversiones realizadas.

Se encontró que los riesgos que generan un mayor impacto económico son aquellos que afectan la disponibilidad de la información, debido a que logran paralizar parcial o totalmente los procesos del negocio, e incluso puede causar pérdida definitiva de datos valiosos para la compañía, lo cual resulta en una amenaza para la facturación y los ingresos de cualquier organización. Por otro lado, se observa mayor severidad en los riesgos que influyen en la demora y prestación correcta del servicio ya que la probabilidad de que se presenten es mayor y su impacto sobre los acuerdos del servicio que se tengan con los clientes es alto, siendo críticos, no solo porque las quejas pueden generar multas o compensaciones, sino porque además el detrimento que causan a la imagen corporativa puede llegar a ser importante e irreversible.

Es fundamental documentar los resultados de los análisis de riesgos, a fin de manejar una memoria histórica de hechos y lecciones aprendidas que pueda ser consultada fácilmente en un futuro para evitar que se repitan análisis similares, invirtiendo recursos y tiempo en algo que ya ha sido solucionado. Así mismo, una correcta documentación facilitará los procesos de seguimiento, mejoras y ajustes,

y podrá utilizarse como base para la formulación de los planes y procedimientos de contingencia y control.

7. BIBLIOGRAFÍA

[1] Ministerio de Tecnologías de la Información y las Comunicaciones. Boletín Trimestral de las TIC. (2012, Dic.). Disponible en: http://www.mintic.gov.co/index.php/cifras.

[2] Empresa de telecomunicaciones. Reporte de visitas técnicas por mantenimiento (2013).

[3] Guía de los Fundamentos de la Dirección de Proyectos PMBOK, 4ª ed., Project Management Institute, 4a ed., Newtown Square, PA, 2008.

[4] Cobit 4.1 IT Governance Institute (2007). PO9 Evaluar y administrar los riesgos de TI

[5] Cobit 4.1 IT Governance Institute (2007). PO1 Definir un plan estratégico de TI

[6] Empresa de telecomunicaciones. Manual de Metodología para la Gestión de Riesgos (2012)

[7] A. Blanco, Formulación y evaluación de proyectos, 4a.ed, 2004

[8] J. Gaspar, Planes de Contingencia la Continuidad del Negocio en las Organizaciones, Ediciones Díaz de Santos, Editorial UOC, 20011

[9] J. Rodríguez, Gestión de proyectos informáticos: métodos, herramientas y casos, Editorial UOC, 2011

[10] G. Maza, Plan de contingencia informático y seguridad de información, aplicado en la Universidad Nacional de Piura, , Edición electrónica gratuita

[11] Instituto Nacional de Estadística e Informática. (2001), Guía Práctica Para el Desarrollo de Planes de Contingencia de Sistemas de Información, Disponible en: http://www.ongei.gob.pe/seguridad/seguridad2_archivos/Lib5131/Libro.pdf

[12] R.Craig, S.Jaskiel, Systematic Software Testing, Artech House, Norwood, MA, 2011

[13] J.Hoffer, Plan de continuidad del negocio, Backing Up Business - Industry Trend or Event, Health Management Technology, 2011

[14] I.Ortiz, V. Rosales, Diseño de Indicadores en Proceso relacionado con la Dirección de Proyectos, Madrid: Escuela Técnica Superior, 2004

[15] G. Stoneburner, A. Goguen, Alexis Feringa, Risk Management Guide for Information Technology Systems, National Institute of standards and Technology, 2004

[16] Ministerio de Administraciones Públicas, Magerit, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”. Madrid. Catálogo general de publicaciones oficiales, Versión 2, 2006