4. GESTIÓN DE RIESGOS III

4.1 Metodología para la gestión de riesgos

La herramienta de matriz de gestión de riesgos se ha demostrado como una de las más efectivas en el desarrollo de este proceso al identificar las actividades más importantes para un proyecto, sus riesgos inherentes y los factores internos o externos relacionados con estos riesgos. La matriz de riesgos también permite evaluar la efectividad de una adecuada gestión y administración de los riesgos sobre todo financieros que pudieran impactar los resultados del proyecto u organización.

La matriz es una herramienta flexible que documenta los procesos para realizar un diagnóstico de la situación global del riesgo. Exige la participación activa de todo el equipo de proyecto y el impulso de su dirección.

4.1.1. Pasos en la generación de la matriz de riesgos

1. Identificación de los procesos: generar un mapa de interrelación de los procesos identificando dentro del sistema de calidad normalizado

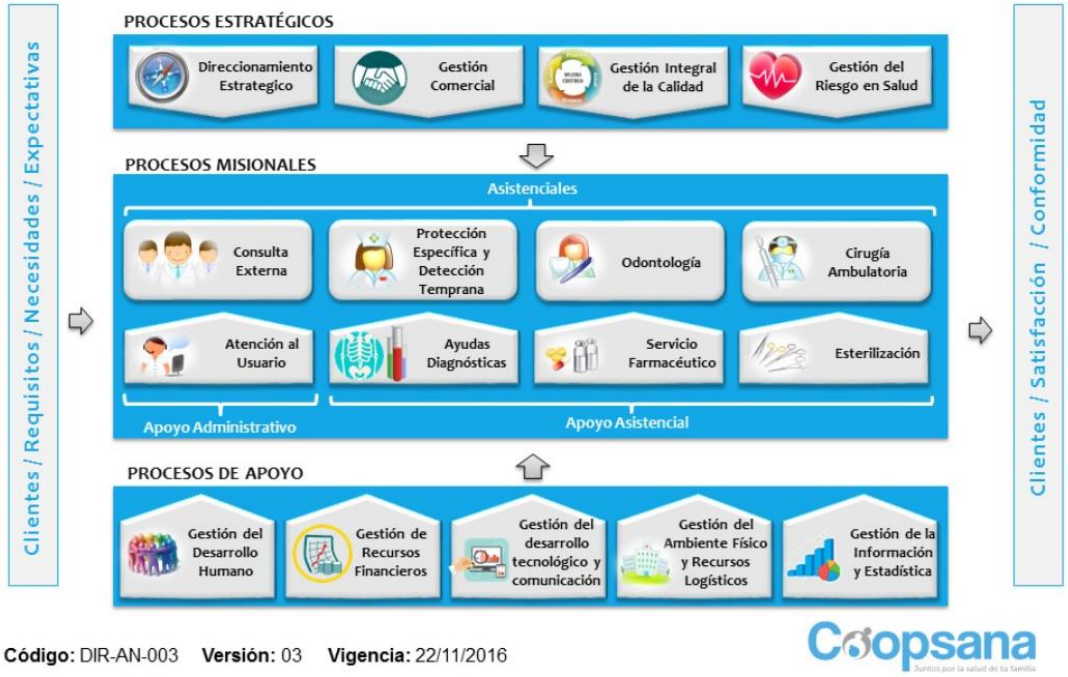

Figura 5. *Mapa de procesos de empresa salud Coopsana*

2. Identificar los riesgos posibles dentro de cada proceso, listado de todos los riesgos

En el ejemplo de Coopsana se elegirá el subproceso “asistencial administrativo” y sobre él se realizará una detección de riesgos a ser posible por un grupo que interactúe con ese objetivo. Esta lista identificará las actividades, las entradas y las salidas del proceso.

PROCESO APOYO ADMINISTRATIVO – ATENCIÓN AL USUARIO		
RIESGOS IDENTIFICADOS		
ENTRADAS	**ACTIVIDADES**	**SALIDAS**

Figura 6.

Figura 6. *del subproceso elegido*[5]

[5] Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del Cliente TGE de la Empresa Assurance Controltech” – Diana Fernanda Jara Pérez – Universidad Distrital Francisco José de Caldas- 2017;

IDENTIFICACIÓN DEL RIESGO - FASE 2													
ID RIESGO	TIPO DE RIESGO	PROCESO / SUBPROCESO	RIESGO (Puede suceder que)	NÚMERO (del riesgo en el listado)	DESCRIPCIÓN DEL RIESGO	CAUSA (Debido a)	CONSECUENCIAS (Qué podría ocasionar)	FUENTE GENERADORA DE RIESGO					PROPIETARIO DEL RIESGO (Cargo)
								RH	EXT	INFRAEST. / AMBIENTAL	OP	TEC	
RSI-01	RiskSI	Call Center / Agendamiento Ventas	R-030 Pérdida de disponibilidad de la informacion por cambios de configuración	R-030	Pérdida de información por no ejecución periódica definida de backups a sistemas de información que soportan el negocio (Grabaciones de llamadas y Bases de datos con la trazabilidad de la operación)	CSI003 - Inadecuada o inexistente ejecución de copias de respaldo	Sanciones contractuales o legales	X			X	X	Director del Call center
RSI-05	RiskSI	Call Center / Agendamiento Ventas	R-007 Acciones no autorizadas sin trazabilidad en áreas seguras	R-007	Aceso no controlado al área de Contact center	CSI401 - Ausencia de control físico de acceso a áreas seguras	Fuga de información de los clientes	X				x	Director del Call center
RSI-10	RiskSI	Call Center / Agendamiento	R-012 Fuga o robo de información en servidores y/o estaciones de trabajo	R-012	Existe software no requerido en los equipos de los agentes	CSI014 - Ausencia de definición o asignación errada de roles y perfiles de acceso a sistemas de información o componentes tecnológicos	Fuga de información de los clientes					X	Director del Call center

Nota: los riesgos aquí identificados corresponden a un ejemplo no relacionado con la empresa Coopsana, la referencia puede ser encontrada en la bibliografía de este documento.

3. Categorización del riesgo en función de su probabilidad de ocurrencia y su potencial impacto

OCURRENCIA (PROBABILIDAD)				
MUY BAJA 1	BAJA 2	MEDIA 3	ALTA 4	MUY ALTA 5

IMPACTO (GRAVEDAD)				
MUY BAJO 1	BAJO 2	MEDIO 3	GRAVE 4	MUY GRAVE 5

Figura 7. *Categorización de riesgo* [2]

IDENTIFICACIÓN DEL RIESGO - FASE 2	ANÁLISIS DEL RIESGO - FASE 3					
RIESGO (Puede suceder que)	CRITERIOS DE SEGURIDAD AFECTADOS			CRITERIOS DE EVALUACIÓN DEL RIESGO		
	C	I	D	PROBABILIDAD	IMPACTO	
R-030 Pérdida de disponibilidad de la informacion por cambios de configuración		X	X	5	5	Legal
R-007 Acciones no autorizadas sin trazabilidad en áreas seguras	X			5	4	Legal
R-012 Fuga o robo de información en servidores y/o estaciones de trabajo	X			5	4	Legal

Nota: los riesgos aquí identificados corresponden a un ejemplo no relacionado con la empresa Coopsana, la referencia puede ser encontrada en la bibliografía de este documento

4. Evaluación del riesgo: Dependiendo de la categoría señalada en la matriz se debe establecer el camino a seguir con cada uno de los riesgos:

a. Zona Crítica: Requiere medidas preventivas urgentes. No se debe iniciar proceso, o actividad sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.

b. Zona Alta: Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proceso

c. Zona Moderada: Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.

d. Zona baja: se vigilará, aunque no requiere medidas preventivas de partida.

IDENTIFICACIÓN DEL RIESGO - FASE 2	EVALUACIÓN DEL RIESGO - FASE 4															
RIESGO (Puede suceder que)	RIESGO INHERENTE	CONTROLES			EFECTIVIDAD DE LOS CONTROLES								2ª EVALUACIÓN RIESGO DESPUÉS DE CONTROLES			OPCIÓN DE TRATAMIENTO
	ZONA DE RIESGO	EXISTE CONTROL (ES)	DESCRIPCIÓN	TIPO	CALIFICACIÓN DEL CONTROL			EJECUCIÓN Y SEGUIMIENTO		PUNTAJE FINAL		PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	
					¿Está documentado y se aplica?	Naturaleza: manual o automático	¿Dispone de monitoreo oportuno que permita identificar posibles fallas?	¿Estan definidos los responsables?	¿La frecuencia de ejecución del control es adecuada?	Controles preventivos	Controles correctivos				
R-030 Pérdida de disponibilidad de la informacion por cambios de configuración	CRÍTICA	SI	CTRL067 - Sistema de respaldo periódico a sistemas de información	Preventivo: Afecta probabilidad	15 - No está documentado pero se aplica	5 - Manual	5 - No	0 - No	0 - No	25	No aplica	5	5	CRÍTICA	Riesgo crítico. Se requiere ateción inmediata de la alta dirección, Se debe reducir, evitar, compartir o transferir.
										No aplica	No aplica				
										No aplica	No aplica				

Nota: los riesgos aquí identificados corresponden a un ejemplo no relacionado con la empresa Coopsana, la referencia puede ser encontrada en la bibliografía de este documento

Figura 8. *Evaluación del riesgo*

5. encDefinición de los planes de tratamiento de cada uno de los riesgos: Se priorizarán los riesgos a tratar, la lógica impone que aquellos críticos serán los tratados en primera instancia, pero, como se ha visto anteriormente, a veces existen otros criterios (disponibilidad de recursos, por ejemplo) que hacen que se modifique la secuencia de tratamiento.

IDENTIFI-CACIÓN	EVALUACIÓN DEL RIESGO					
ID RIESGO	OPCIÓN DE TRATAMIENTO	RIESGO-SITUACIÓN OBSERVADA	ACCIÓN CORRECTIVA	RESPONSABLE	FECHA LÍMITE DOCUMENTACION DE ACC. CORRECTIVA	OBSERVACIONES DEL SEGUIMIENTO
RSI-01	Riesgo crítico. Se requiere ateción inmediata de la alta dirección, Se debe reducir, evitar, compartir o transferir.	Pérdida de información por no ejecución periódica definida de backups a sistemas de información que soportan el negocio (Grabaciones de Llamadas y Bases de datos con la trazabilidad de la operación)	Solicitar a Tecnología una estrategia de backup que garantice que la información sensible de la operación del Call Center (Grabaciones) en la planta telefónica y las bases generadas para las llamadas se encuentre respaldada periódicamente	Director Call Center Director de Tecnología		
			Solicitar a Tecnología se realice el respaldo periódico del respaldo del File Server de la operación de Call Center	Director Call Center Director de Tecnología		
			Pérdida de información por no ejecución periódica definida de Backups a sistemas de información que soportan el negocio (Grabaciones de Llamadas y Bases de datos con la trazabilidad de la operación)	Director Call Center Director de Tecnología		

Nota: los riesgos aquí identificados corresponden a un ejemplo no relacionado con la empresa Coopsana, la referencia puede ser encontrada en la bibliografía de este documento

Figura 9. *Tratamiento del riesgo*[2]

6. Comunicación y consulta: Finalizada la metodología de riesgos y la definición de los planes de acción, se ha de entregar el resultado a todos los implicados y asegurarse de que cada uno comprende su contenido y las obligaciones que se le confieren. Es responsabilidad de todos los integrantes del equipo de proyecto tanto el cumplimiento como el control de las acciones de tratamiento de los riesgos.

4.2 Problemas en la gestión de los riesgos

Las etapas de la gestión[6] de riesgos implican cierta complejidad y total coordinación y seguimiento por parte de los equipos de proyecto u organizaciones, por ello, surgen muy a menudo problemas que la ISO 31000 ayuda a paliar:

1. En la implementación: En esta categoría, se pueden distinguir varios tipos de problemas:

    a. Resistencia al cambio: Bien sea por falta de formación o bien porque no existe un verdadero apoyo del proceso por parte de la Dirección, lo cierto es que la clave para atajar este asunto radica en la determinación del Director de Proyecto en su implantación. En este sentido, el Director de Proyecto debe convertirse en el ejemplo a seguir;

    b. Diferencia de criterios: Sucede sobre todo en las grandes empresas. Cuando los grupos de responsables tienen demasiados miembros, lo más común es que entre estas personas se presenten diferencias de criterio a la hora de implementar el plan. Esto se traduce en retrasos, reuniones excesivas y, posiblemente, nombramiento de nuevos responsables;

    c. Falta de una figura coordinadora: Del mismo modo, algunos grupos suelen notar la ausencia de una persona líder que direccione los procesos. De ahí la importancia de la elección de esa persona en los primeros pasos de la implementación;

- [6] “Metodologías para la Gestión del Riesgo” - Jorge Jhuéz, 2015;

d. Incumplimiento de plazos: Por causa de una deficiente planificación, recursos insuficientes o una comunicación deficiente entre los responsables, algunas veces los procesos de implementación de Gestión de Riesgos incurren en incumplimiento de los plazos previstos. En estos casos, el perjuicio es doble: primero, porque obstaculiza la realización del proyecto en sí mismo; y segundo, porque se pierde tiempo valioso para mitigar o gestionar riesgos que, en muchos casos, tienen carácter urgente.

e. Aplazamiento: Esto sucede cuando el plan ni siquiera llega a implementarse. Se han definido las directrices, las estrategias, los responsables y los recursos, pero por la razón que sea el plan acaba guardado en un archivo de la Dirección.

2. En el mantenimiento: En este caso, hablamos de obstáculos que surgen en la etapa de ejecución del plan de Gestión de Riesgos. Las empresas que ya han dado el paso y se encuentran en las etapas de monitorización pueden encontrarse con los siguientes problemas:

   a. Falta de recursos;

   b. Errores en el diseño del plan de gestión de riesgos: Si se han hecho cálculos erróneos en cuanto a los esfuerzos y coste de implementar las acciones de tratamiento de los riesgos, es bastante probable que estos se abandonen antes de su cumplimiento. En estos casos, los procesos requieren de un replanteamiento general.

4.3 Conclusiones

La gestión de riesgos es el proceso de identificar, analizar y responder a factores de riesgo a lo largo de la vida de un proyecto de forma preventiva y proactiva y con la implicación de todos los miembros de un proyecto.

El Director de Proyecto debe creer en el proceso de gestión de riesgos y saber liderar su implantación y seguimiento, responsabilizando a todos los agentes implicados en el mismo y comunicando además sus beneficios tanto aguas arriba, a la dirección de su organización, como aguas abajo, a su equipo de proyecto.

Evaluar y gestionar los eventuales riesgos es la mejor herramienta frente a los imprevistos en los proyectos. Al analizar los procesos para detectar los potenciales problemas y al desarrollar estrategias para abordarlos, se mejorarán sustancialmente las probabilidades de éxito del proyecto.

4.4 Referencias

- "A guide to the Project Management Body of Knowledge" – PMBOK GUIDE – 6th edition, 2017 – Project Management Institute;
- "Metodologías para la Gestión del Riesgo" - Jorge Jhuéz, 2015;
- "Valoración y plan de tratamiento de riesgos de seguridad de la información para los procesos incluidos en el alcance del SGSI del Cliente TGE de la Empresa Assurance Controltech" – Diana Fernanda Jara Pérez – Universidad Distrital Francisco José de Caldas- 2017;
- "AACE's skills and knowledge of cost engineering" – 6th Edition – AACE International ®;
- Web corporativa: http://coopsana.com.co/web/quienes-somos/mapa-de-procesos/