



PLAN DE MANEJO Y MONITOREO OFICINA ASESORA DE PLANEACIÓN

MAPA DE RIESGO PLAN DE MANEJO Y MONITOREO 2014

PROCESO: Proceso de Sistemas y Recursos Administrativos

OBJETIVO DEL PROCESO: Determinar, proporcionar y mantener la infraestructura necesaria para lograr la conformidad con los servicios prestados por el Ministerio de Cultura de manera eficiente, eficaz y efectiva.

ÁREA: GRUPO DE GESTIÓN DE SISTEMAS E INFORMÁTICA

RIESGO	FACTOR INTERNO	ZONA DE RIESGO	OPCIONES DE MANEJO / ACCIONES	Peso Porcentual	INDICADORES	META #	CRONOGRAMA	RESPONSABLE	ACCIÓN DE CONTINGENCIA	SEGUIMIENTO I SEMESTRE			ZONA DE RIESGOS	SEGUIMIENTO II SEMESTRE									
										AVANCE % (Expresión PORCENTUAL del avance)	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACIÓN		AVANCE % (Expresión PORCENTUAL del avance)	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACIÓN	ZONA DE RIESGOS						
Daño y pérdida de los activos tecnológicos	Indebida utilización de las herramientas informáticas disponibles.	12%	Realizar Análisis GAP	40%	Informe de análisis GAP	1%	Diciembre de 2014	Coor. Grupo de Sistemas	Proporcionar equipos de soporte para suplir el activo dañado o perdido. Informar a la aseguradora en caso de pérdida o daño por factores externos.	10%	Definición de los términos de referencia para el contrato, actualización del estudio de mercado. Pendiente designación de los recursos requeridos para realizar esta contratación.	12%	Zona de Riesgo Moderada	70%	Presupuesto no aprobado para el Análisis GAP de Seguridad de la Información, se realizó un Análisis GAP de Seguridad Informática en el marco del contrato con Digiware.	80%	Zona de Riesgo Extrema						
	Falta de continuidad de los contratos de mantenimiento y soporte técnico		Adelantar el trámite de solicitud de vigencias futuras de los contratos de mantenimiento de activos tecnológicos.	30%	Vigencias futuras aprobadas.	2	Diciembre de 2014	Coor. Grupo de Sistemas		0%	El trámite debe adelantarse en el 2 semestre de 2014.			100%	Vigencias futuras adelantadas.								
			Cumplimiento de las actividades del plan de mantenimiento definido para los activos tecnológicos.	30%	Porcentaje de Cumplimiento del Plan de Mantenimiento	100%				Documento de Análisis de Obsolescencia	1			50%	El plan de mantenimiento se está cumpliendo acorde con las fechas pactadas.			100%	El plan de mantenimiento se está cumpliendo acorde con las fechas pactadas.				
															100%			Se adelantó el análisis de obsolescencia para PCs, Impresoras y Equipos del Centro de Cómputo del Ministerio de Cultura.					
Alteración, pérdida y fuga de información	Ingreso no autorizado a las bases de datos de los sistemas de información.	32%	Implementación de herramientas para controlar el acceso a los servidores.	30%	No de herramientas. Para los sistemas de información y bases de datos tengan un usuario particular para su administración/ Total de Herramientas programadas.	100%	Diciembre de 2014	Coor. Grupo de Sistemas	Restaurar la información alterada o perdida con los Backus. Acompañar el seguimiento a la posible forma de extracción de la información.	10%	Alistamiento de los servidores donde se instalará y configurará la herramienta.	30%	Zona de Riesgo Alta	10%	En el nuevo contrato de Seguridad Informática se incluyeron las nuevas herramientas de SW para realizar un mayor control sobre los accesos a los sistemas de información.	20%	Zona de Riesgo Alta						
	Fallas en la herramienta que ejecuta la política de backus		Fortalecer el control de acceso a las bases de datos requiriendo la asignación de claves y mejorando las ya asignadas.	15%	Porcentaje de mejoramiento de asignación de claves	100%	Diciembre de 2014			Coor. Grupo de Sistemas	0%			Contratación de horas de soporte de un administrador especializado de base de datos SQL para acompañar ésta labor.	100%			Se contrató el soporte especializado SQL Server y se llevó a cabo un análisis y actualización de las bases de datos administradas por el Grupo de Sistemas.					
			Ingreso a sitios web no autorizados.	15%	Propuesta de Alternativa con Backus	1					Diciembre de 2014			Coor. Grupo de Sistemas	20%			Se adelantaron reuniones con proveedores y se enviaron correos solicitando las propuestas económicas de cada solución; insumo para el comparativo.	100%	Se realizó el análisis de alternativas de Backus existentes en el Mercado y se presentó ante el Comité de Gestión			
			Utilización de información de los sistemas del Ministerio para beneficio de particulares	Socialización de la importancia del uso adecuado del internet	20%	Campaña de socialización									1			Diciembre de 2014	Coor. Grupo de Sistemas	40%	Diseño de la estrategia de la campaña.	100%	Campaña de socialización diseñada y publicada en los protectores de campaña.
				Socialización de las políticas de acceso responsable a la información	20%	Propuesta definida									1					Diciembre de 2014	Coor. Grupo de Sistemas	40%	Diseño de la estrategia de la campaña.
			Descentralización en la administración de las bases de datos del Ministerio de Cultura.	Entrega al Grupo de Sistemas de la administración técnica de los sistemas de información y bases de datos a cargo de Planeación.		Propuesta definida									1			Diciembre de 2014	Coor. Grupo de Sistemas			0%	

Incumplimiento en oportunidad y calidad de los requerimientos de desarrollo de software	Mala interpretación de los términos contractuales por parte del proveedor de desarrollo de software	24%	Documentar las etapas contractuales de desarrollo de software siguiendo los lineamientos definidos en el procedimiento de software.	25%	Contratos con actividades definidas / No de Contratos realizados	100%	Diciembre de 2014	Coor. Grupo de Sistemas	Realizar un diagnóstico del software suministrado al Ministerio y definir, de acuerdo con los puntos críticos detectados, las acciones a seguir en su corrección.	100%	Una vez se actualizó el procedimiento de desarrollo de software, se comenzó a incluir en todos los relacionados con Sistemas de información, la actividad del cumplimiento con lo definido en ISOLUCION	17%	Zona de Riesgo moderada	100%	Adelantada en su totalidad en el I semestre de 2014	12%	Zona de Riesgo Moderado
	Falta de personal con el perfil correspondiente para cumplir con las necesidades de desarrollo de software		Propuesta de mejora de la organización de personal en el área	25%	Documento Propuesta	1				100%	Se revisaron las actividades realizadas por el personal del área y se planteó un organigrama de la organización interna del área en el documento Manual de Gestión de Tics publicado en ISOLUCION.			100%	Adelantada en su totalidad en el I semestre de 2014		
	Incumplimiento de los lineamientos del procedimiento de desarrollo de software		Realizar ajustes al Procedimiento	25%	Procedimiento ajustado y divulgado	1	dic-14			100%	Se adelantaron las reuniones para revisar el procedimiento actualmente publicado, se definieron los ajustes, se realizaron y se publicó una nueva versión del procedimiento.			100%	Adelantada en su totalidad en el I semestre de 2014		
	Deficiencia en el levantamiento de los requerimientos del usuario						dic-14										
	Falta de documentación sobre los sistemas de información existentes, que dificulta el desarrollo de actualizaciones		Seguimiento al PETIC (Plan estratégico de las tic)	25%	No de Actas realizadas / Reuniones de seguimiento mensuales	100%	Diciembre de 2014			50%	Presentación y aprobación del PETIC en el comité institucional de desarrollo administrativo del 5 de mayo y publicación en el ISOLUCION. El seguimiento se ha venido realizando mensualmente.			100%	Presentación de los logros del PETIC en el 2014, ante el comité de Gestión Administrativa.		

EVALUACIÓN

La identificación y clasificación del riesgo es adecuada y contribuye a asegurar el cumplimiento de los objetivos del Ministerio.
Respecto a los controles y la valoración generada después de controles se observa que si bien estos controles minimizan el riesgo, las acciones de manejo propuestas indican que el impacto y la probabilidad del riesgo aun es significativa, teniendo en cuenta la posible obsolescencia de los equipos, adicionalmente se considera importante que se evalúe como consecuencia la pérdida de información, dado que los daños en dichos activos (tales como: servidores, discos duros, entre otros equipos) podrían significar tal pérdida .
Por otra parte, es evidente que se necesita un nuevo proceso de identificación y seguimiento para este riesgo dado que se materializo en la vigencia 2014, con lo cual se demostró que los controles no son del todo efectivos, por lo cual se entiende que la evaluación final de la zona de riesgo sea extrema.

El riesgo identificado corresponde con las necesidades del proceso, igualmente los factores internos señalados evidencian que se realizó el ejercicio de identificación, sin embargo, teniendo en cuenta que los controles existentes no le apuntan a mitigar todas las causas se considera alta la disminución de 2 niveles de la probabilidad de ocurrencia en la valoración después de controles. Respecto a las acciones propuestas se destaca la ejecución de la mayoría de ellas, sin embargo su ejecución no genera controles efectivos que aseguren que se disminuye la probabilidad de ocurrencia del riesgo, ya que si se estudió la posibilidad de implementar una herramienta alternativa para llevar los Backup, esta aun no se ha implementado y por su parte las socializaciones realizadas son actividades que van en la línea de mitigar el riesgo, sin embargo no son controles efectivos ni permanentes que aseguren la disminución de la probabilidad del riesgo, para lo cual se recomienda emplear controles adicionales al ingreso a sitios web y a la utilización indebida de la información del Ministerio.

Frente a la acción relacionada con fortalecer el control de acceso a las bases de datos requiriendo la asignación de claves y mejorando las ya asignadas, la descripción de las actividades adelantadas no permite verificar si se dio este fortalecimiento y si el indicador se cumplió. Se recomienda mejorar la descripción general de las acciones de manera que den cuenta del cumplimiento de los indicadores propuestos para evidenciar la eficacia y/o eficiencia de las acciones propuestas.
Por lo anterior, se concluye que la valoración final de este riesgo no corresponde, aunque se hayan presentado avances significativos en la gestión del mismo.

La formulación e identificación general del riesgo es adecuada y corresponde con los objetivos del proceso, así mismo las acciones propuestas van encaminadas a la disminución de la probabilidad del riesgo, sin embargo se considera reconsiderar la valoración del riesgo tanto en la etapa de valoración después de controles como después de ejecutadas las acciones dado que no se evidencia la implementación de las acciones propuestas, sino la actualización propia de la documentación, por ejemplo en la descripción de los avances no se evidencia que en los contratos de desarrollo de software queden registradas las etapas de desarrollo y tampoco se evidencia cuáles fueron los controles incorporados e implementados en el procedimiento para mejorar el control del riesgo, como tampoco se observan los avances respecto a este tema como producto del seguimiento e implementación del PETIC.