IDENTIFICACIÓN MAPA DE RIESGOS

Código: F-OPL-026
Versión: 1
Fecha: 24/Mar/2015

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**

Id	RIESGO / DESCRIPCIÓN	CLASIFICACIÓN	Ponderación %	CAUSAS INTERNAS	CAUSAS EXTERNAS	EFECTOS O CONSECUENCIAS	IMPACTO	PROBABILIDAD DE OCURRENCIA	ZONA DE RIESGO (Evaluación)	CONTROL EXISTENTE	ZONA DE RIESGO (Evaluación después de controles)	IMPACTO ESPERADO	PROBABILIDAD DE OCURRENCIA ESPERADA	ZONA DE RIESGO ESPERADA
1	Daño y pérdida de los recursos tecnológicos	Tecnología	20%	Indebida utilización de las herramientas informáticas disponibles.	Ataques o intrusiones a los equipos activos. Factores sobre naturales. Recorte de Presupuesto	Indisponibilidad de los servicios. Afectación del rendimiento de algunos elementos informáticos.	4. Mayor	5. Ocurriría en la mayoría de las circunstancias	Zona de Riesgo extremo 80%	Manuales de Usuario Capacitaciones al personal Segmentaciones de Red Puntos de Red Deshabilitados Diagnósticos de obsolescencia, cumplimiento de norma. Monitoreo de sistemas de información, UPS, aires acondicionados, equipos activos de red y demás elementos de la plataforma. Planes de Mantenimiento Compra de equipos con garantía. - Inclusión de los elementos tecnológico en la póliza global de los seguros. Priorización y optimización de recursos PETIC - Plan Estratégico de TIC Contratos de servicios tercerizados con empresas especializadas	Zona de Riesgo Extrema 64%	4. Mayor	3. Posiblemente ocurriría	48%
			30%	Tecnología obsoleta hardware y software (cumplimiento de vida útil, perdida de garantía)										
			15%	Fallas en la administración de las instalaciones físicas (eléctricas - hidráulicas)										
			15%	Falta de asignación de Recursos económicos										
			20%	Fallas en la continuidad y cumplimiento de los contratos de mantenimiento y soporte técnico										
2	Alteración, perdida y fuga de información	Operativo	15%	Ingreso no autorizado a las bases de datos de los sistemas de información.	Ataques o intrusiones a los sistemas de información.	Investigaciones disciplinarios y de entes de control. Indisponibilidad de los sistemas de información. - Pérdida de efectividad, eficiencia de los procesos. -Información errada o inoportuna para la toma de decisiones. - Pérdida de la imagen y credibilidad en la organización.	4. Mayor	4. Probablemente ocurriría	64%	1. Cada aplicación cuenta con usuario de conexión a la base de datos. 2. Procedimiento backups. 3.Politica de control de Acceso. 4. Solución de filtro de contenidos web. 5. y 6. 7. Eliminación de cargue por Base de Datos, con desarrollo específicos en las aplicaciones. 8.Capacitaciones, manual de usuario de los sistemas de información. Se cuenta con un contrato de seguridad que cubre antivirus, detector de intrusos antispam, control de navegación a internet y firewall. Se realizan backups de acuerdo con la política establecida. Segmentación de Redes	Zona de Riesgo Extrema 48%	4. Mayor	1. Excepcionalmente ocurriría	16%
			15%	Fallas en la herramienta que ejecuta la política de backups										
			20%	Falta de implementación de políticas de acceso físico, lógico y procedimientos para la administración de la información										
			10%	Ingreso a sitios web no autorizados.										
			10%	Fallas en la asignación de los roles en los sistemas de información										
			10%	Fallas en la gestión de usuarios y de los equipos.										
			10%	Errores en el cargue y validación de la información por base de datos.										
			10%	Desconocimiento técnico en la operación, gestión de equipos y manejo de los sistemas de información.										
			15%	Mala interpretación de los términos contractuales por parte del proveedor de desarrollo de software	Cambios en lineamientos y	- Multas y sanciones por incumplimientos en los reportes a los entes de control				Procedimiento de desarrollo de software				

IDENTIFICACIÓN MAPA DE RIESGOS

Código: F-OPL-026
Versión: 1
Fecha: 24/Mar/2015

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**

Id	RIESGO / DESCRIPCIÓN	CLASIFICACIÓN	Ponderación %	CAUSAS INTERNAS	CAUSAS EXTERNAS	EFECTOS O CONSECUENCIAS	IMPACTO	PROBABILIDAD DE OCURRENCIA	ZONA DE RIESGO (Evaluación)	CONTROL EXISTENTE	ZONA DE RIESGO (Evaluación después de controles)	IMPACTO ESPERADO	PROBABILIDAD DE OCURRENCIA ESPERADA	ZONA DE RIESGO ESPERADA
3	Incumplimiento en oportunidad y calidad de los requerimientos de desarrollo de software	Operativo	15%	Falta de personal con el perfil correspondiente para cumplir con las necesidades de desarrollo de software del Ministerio	normatividad que no den el tiempo requerido para aplicarlos en los sistemas	- Incumplimientos de entrega de funcionalidades a clientes externos del Ministerio	3. Moderado	4. Probablemente ocurriría	Zona de Riesgo moderada 48%	Plan de acción donde se encuentran las actividades de desarrollo de software. Personal capacitado	Zona de Riesgo Moderada 24%	3. Moderado	1. Excepcionalmente ocurriría	12%
			20%	Incumplimiento de los lineamientos del procedimiento de desarrollo de software establecido	Incumplimiento de proveedores externos de desarrollo de software	-Pérdida de efectividad en el uso y la producción del software desarrollado en el Ministerio				Instructivo de requerimientos mínimos de arquitectura y de seguridad de las aplicaciones.				
			25%	Deficiencia en el levantamiento de los requerimientos del usuario		-Malgasto de los recursos del Ministerio por la duplicidad de esfuerzos en el desarrollo de software				Se cuenta con personal contratado por el Grupo de Sistemas que valida el cumplimiento de los estándares definidos para el desarrollo de software. Manuales técnico de las aplicaciones.				
			25%	Falta de documentación sobre los sistemas de información existentes, que dificulta el desarrollo de actualizaciones										
4	Comercializar o divulgar información sensible de la entidad.	Corrupción	15%	1. Falta de controles (físicos y lógicos) en los permisos de acceso.	Ataques o intrusiones a los sistemas de información.	Divulgaciòn de Informaciòn Sensible del Ministerio. Sanciones para la entidad	5. Catastrófico	5. Ocurriría en la mayoría de las circunstancias	Zona de Riesgo extremo 100%	1. Procedimientos documentados 2. Herramienta de registro de casos (Help desk). 3. Copias de seguridad. 4. Mantenimientos Preventivos y/o correctivos. 5. Monitoreos a la plataforma tecnológica. 6. Protocolos de seguridad informática. 7. Establecimiento de permisos y roles para el acceso a la red. 8. Código de ética	Zona de Riesgo extrema 60%	N:A	N:A	N:A
			15%	2. Infraestructura tecnológica Hardware y/o software de tecnología obsoleta.										
			20%	3. Políticas de seguridad de la información, inexistentes o inapropiadas										
			30%	4. Falta de ética de los profesionales asociados a los procesos de sistemas										
			20%	5. Utilización de información de los sistemas del Ministerio para beneficio de particulares										

PLAN DE MANEJO Y MONITOREO

Código: F-OPL-027
Versión: 1
Fecha: 24/Mar/2015

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**

								SEGUIMIENTO I SEMESTRE				SEGUIMIENTO II SEMESTRE			
RIESGO	CAUSAS INTERNAS	ZONA DE RIESGO	OPCIONES DE MANEJO / ACCIONES	Medio de verificación	CRONOGRAMA	RESPONSABLE	ACCIÓN DE CONTINGENCIA	AVANCE %	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACIÓN	ZONA DE RIESGOS	AVANCE %	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACIÓN	ZONA DE RIESGOS
Daño y pérdida de los recursos tecnológicos	Indebida utilización de las herramientas informáticas disponibles.	Zona de Riesgo Extrema 64%	Revisión y documentación de los controles	Controles debidamente documentados y alineados con la normatividad vigente	Novembre de 2015	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.								
	Tecnología obsoleta hardware y software (cumplimiento de vida útil, perdida de garantía)		Seguimiento a las acciones de mejora propuestas en isolución	100% de cumplimiento	Diciembre de 2015	Coor. Grupo de Sistemas y Asesora.									
	Fallas en la administración de las instalaciones físicas (eléctricas - hidráulicas)		Diagnostico de DATA CENTER sede Palacio Echeverry. Efectuar reunión con administrativa que permita desarrollar plan de mejora para el control de plagas, mantenimiento de instalaciones electricas y otros de acuerdo a diagnostico del área	Diagnotico acta de reunión con plan de mejora.	Diciembre de 2015	Asesora Administrativa, Asesora planeación - Asesor sistemas									
	Falta de asignación de Recursos económicos		Presentar informe de avances de destinación de recursos y usos	Informe a comité de desarrollo administrativo											
	Fallas en la continuidad y cumplimiento de los contratos de mantenimiento y soporte técnico		Gestionar con el área de contratos los acuerdos de nivel de servicio, y clausulas por incumplimiento de estos. Preveer desde el Plan de Accion la actividades para la continuidad de los contratos de soporte y mantenimiento	Contratos con inclusión de acuerdos de nivel de servicios. Plan de acción	Diciembre de 2015	Coor. Grupo de Sistemas y Asesora.									
Alteración, perdida y fuga de información	Ingreso no autorizado a las bases de datos de los sistemas de información.	Zona de Riesgo Extrema 48%	Levantar inventario de Usuarios administradores. Realizar la documentación (instructivo) para el manejo de las claves de los usuario que administran las bases de datos.	Inventario Instructivo documentado	Agosto 14 de 2015	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.								
			Revisar con las partes interesadas la claves de acceso a base de datos que se encuentran quemadas en las aplicaciones.	Informe de Análisis de alternativas para el fortalecimiento de la cadena de conexión de aplicaciones a base de datos.	15 de diciembre de 2015										
	Fallas en la herramienta que ejecuta la política de backups		Renovar contrato de backups en la nube. Modificar procedimiento de backups	Contrato renovado. Procedimiento actualizado.	Agosto 20 de 2015										
	Falta de implementación de políticas de acceso físico, lógico y procedimientos para la administración de la información		Revisar la política de control de acceso e incluir políticas de operación para el ingreso y retiro de los funcionarios. Revisar el cumplimiento de esta.	Procedimiento estandarizado.	Julio 30 de 2015										
	Ingreso a sitios web no autorizados.		Fomentar la importancia del uso adecuado del internet	Campaña de socialización	Diciembre de 2015										
	Fallas en la asignación de los roles en los sistemas de información		Documentar actividades en el procedimiento de accesos, que mitiguen estas causas	Procedimiento											
	Fallas en la gestión de usuarios y de los equipos.														
	Errores en el cargue y validación de la información por base de datos.		Identificar y definir plan de desarrollo para automatizar los cargues que se realizan a través de la aplicación	Plan de trabajo	Diciembre 20 de 2015										
	Desconocimiento técnico en la operación, gestión de equipos y manejo de los sistemas de información.		Inventario de Manuales determinando grado de actualización. Notificar a las áreas la actualización de los manuales de Usuario	Inventario Notificaciones a área	Diciembre 20 de 2015										

PLAN DE MANEJO Y MONITOREO

Código: F-OPL-027
Versión: 1
Fecha: 24/Mar/2015

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**

								SEGUIMIENTO I SEMESTRE				SEGUIMIENTO II SEMESTRE			
RIESGO	CAUSAS INTERNAS	ZONA DE RIESGO	OPCIONES DE MANEJO / ACCIONES	Medio de verificación	CRONOGRAMA	RESPONSABLE	ACCIÓN DE CONTINGENCIA	AVANCE %	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACIÓN	ZONA DE RIESGOS	AVANCE %	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACIÓN	ZONA DE RIESGOS
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%	Reuniones periodicas de seguimiento de los contratos de desarrollo de software, verificando que cumplan con lo especificado contractualmente.	Infomes de seguimiento Periodicos.	Diciembre de 2015	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.								
	Falta de personal con el perfil correspondiente para cumplir con las necesidades de desarrollo de software del Ministerio		Terminar con la Propuesta de mejora de la organización de personal en el área	Documento Propuesta	Agosto de 2015										
	Incumplimiento de los lineamientos del procedimiento de desarrollo de software establecido		Realizar ajustes al Procedimiento	Procedimiento ajustado y divulgado	dic-15										
	Deficiencia en el levantamiento de los requerimientos del usuario														
	Falta de documentación sobre los sistemas de información existentes, que dificulta el desarrollo de actualizaciones		Seguimiento al cumplimiento de PETIC (Plan estratégico de las tic), el cual se revisa en presentación al comité de desarrollo administrativo	Acta de comité. Seguimiento 100% de cumplimiento de actividades planteadas a diciembre del 2015.	Diciembre de 2015										
Comercializar o divulgar información sensible de la entidad.	1. Falta de controles (físicos y lógicos) en los permisos de acceso.	60%	Fortalecer las politicas de seguridad en los elementos de hardware y software de la plataforma tecnologica.	Politicas de seguridad de la información actaulizadas y aplicadas tecnologicamente.	Diciembre de 2015	Coord. De grupo de sistemas	Investigación Disciplinaria								
	2. Infraestructura tecnológica Hardware y/o software de tecnología obsoleta.														
	3. Políticas de seguridad de la información, inexistentes o inapropiadas														
	4. Falta de ética de los profesionales asociados a los procesos de sistemas		Desarrollar estrategia de sensibilización del Código de Ética	Jornada de sensibilización código de Ética	Noviembre de 2015	Comité de Ética									
	5. Utilización de información de los sistemas del Ministerio para beneficio de particulares														