MAPA DE RIESGO PLAN DE MANEJO Y MONITOREO 2014

PROCESO: **Participación**

OBJETIVO DEL PROCESO: **Brindar espacios donde los ciudadanos se puedan instruir, capacitar y desarrollar su potencial y talento, por medio de la promoción del cumplimiento de los derechos culturales a través del diseño, fomento y ejecución de políticas, programas y proyectos culturales que tiendan a fortalecer la convivencia y la reconciliación, apoyados por redes de servicios que contienen información de los diferentes agentes e instituciones culturales.**

ÁREA: **OFICINA ASESORA DE PLANEACIÓN -SINIC**

									SEGUIMIENTO I SEMESTRE 2014				SEGUIMIENTO II SEMESTRE				
RIESGO	**FACTOR INTERNO**	**ZONA DE RIESGO**	**OPCIONES DE MANEJO / ACCIONES**	**Peso Porcentual**	**INDICADORES**	**META #**	**CRONOGRAMA**	**RESPONSABLE**	**ACCIÓN DE CONTINGENCIA**	**AVANCE %**	**ANÁLISIS DE DATOS**	**EVALUACIÓN**	**ZONA DE RIESGOS**	**AVANCE %**	**ANÁLISIS DE DATOS**	**EVALUACIÓN**	**ZONA DE RIESGOS**	**EVALUACIÓN**
Perdida, daños y/o exposición de información protegida	* Falta de capacitación y concienciación del personal en cuanto a la protección y entrega de información a terceros, sin las debidas medidas de seguridad.	64%	* Diseñar y realizar una capacitación de Seguridad Informática para usuarios antiguos y nuevos, que contenga información acerca de la normatividad existente, consecuencias jurídicas y videos alusivos al tema.	30%	Dos (2) capacitaciones al año. (de rutina y específica, para personal antiguo y nuevo). Incluir este tema en las jornadas de inducción y reinducción programadas por Gestión Humana.	100%	Primer trimestre y cuarto trimestre de cada año.	Coordinador SINIC	Se podrá incluir el tema referente a seguridad informática en las capacitaciones relacionadas con los sistemas de información y que se realizan con las áreas del ministerio.	50%	Se realizaron jornadas de sensibilización y capacitación en seguridad de la información para usuarios antiguos y nuevos los días: 25mar/14; 27mar/14; 28mar/14; 23abr/14; 24abr/14 y 9jun/14. Estas capacitaciones se incluyeron durante las jornadas realizadas en referencia a los sistemas de información que se llevan a cabo con las diferentes dependencias del Ministerio y durante la segunda jornada de inducción general de contratistas, organizada por el grupo de Gestión Humana.	54%	Zona de Riesgo Extrema	100%	Para el segundo semestre de 2014 se contrató por medio de la Oficina de Planeación con la supervisión del grupo de Sistemas el proceso de implantación del SGSI, lo cual cubria la parte de capacitación. Dentro de las funciones del contrato, esta persona realizó estas capacitaciones por medio de la intranet y protectores de pantalla, cubriendo esta actividad al 100%.	52%	Zona de Riesgo Alta	En la identificación del riesgo se evidencia ha sido determinada de forma adecuada, incluso la valoración inicial, después de controles y la valoración proyectadas resultan acordes con las posibilidades de manejo del riesgo. Respecto a la etapa de tratamiento, se percibe que las acciones propuestas coinciden con la mitigación de los factores internos y externos identificados, sin embargo las acciones referentes al ajuste estructural de la asignación de claves y al diseño de la política de control representan acciones parciales, en tanto se reflejan en indicadores documentales que no permiten evidenciar su implementación total, como se puede verificar en el análisis de datos presentados para el primer y segundo semestre, donde en el caso de las claves de acceso esta acción no se pudo llevar a cabo y para el caso del protocolo solo se implementó para el SIG quedando sin implementar en los demás sistemas de información manejados por el Ministerio (SINIC, SIREC, SIPA, entre otros). Se considera que se deben reevaluar los resultados finales del riesgo ya que las acciones son parciales y como tal no aseguran que la zona de riesgo cambie. Adicionalmente se señala que de acuerdo con la zona de riesgo proyectada, la zona de riesgo resultante debería seguir siendo extrema, lo cual indica que la casilla de zona de riesgo para el segundo semestre está clasificada inadecuadamente.
	* Claves de acceso asignadas por los usuarios son muy débiles, por lo tanto pueden ser descifradas fácilmente por un tercero.		* Modificar la longitud y estructura de la asignación de las claves en el sistema, con el fin de aumentar el número de caracteres y exigir la inclusión de caracteres especiales y alfanuméricos.	50%	Procedimiento para asignar claves, luego de que se modifique el algoritmo de asignación en el sistema.	100%	Segundo trimestre de 2014.		Aseguramiento y calidad de las contraseñas. Que el sistema solicite el cambio de contraseña periódicamente.	50%	Se está analizando el impacto de mitigar este riesgo, dado que este afectará a todos los usuarios del Ministerio, incluyendo a las directivas, para las cuales se está diseñando un proceso de capacitación y explicación del porque se realiza este cambio, para que de esta manera no genere tanto traumatismo la nueva parametrización de las claves de acceso.			50%	Dadas las prioridades de trabajo de la persona que hace mantenimiento al SIG no fue posible realizar este tema en el 2014. Ahora, con el paso de esta actividad al grupo de Sistemas e Informática, así como las priorizaciones dadas con la implementación del SGSI, se espera poder llevar a cabo este proceso en el 2015.			
	* Los usuarios de ingreso a las aplicaciones no son desactivados del sistema cuando un funcionario y/o contratista no labora más en la entidad. * No se actualizan los perfiles de ingreso a las aplicaciones cuando se modifican las funciones de los funcionarios y/o contratistas del Ministerio.		* Diseñar una política de control para que los funcionarios/contratistas que se desvinculen y/o cambien de funciones en la entidad, sean reportados al grupo SINIC oportunamente, con el propósito de que sus usuarios sean inactivados o modificado su perfil de ingreso.	20%	Protocolo de desvinculación de colaboradores (contratistas/funcionarios) y de cambio de funciones de los mismos.	100%	Permanente.		Validaciones periódicas a los usuarios registrados en el sistema con los administrativos del Ministerio o quien delegue el responsable de cada área, respecto a las novedades de los colaboradores (contratistas/funcionarios) en cuanto a su continuidad con la entidad o cambio de funciones.	100%	Como política y mecanismo de control para mitigar este riesgo, relacionado en los factores internos, se diseñó el formato de solicitud y modificación de usuarios SIG, el cual cuenta con un procedimiento claro para la inclusión, asignación de perfiles, modificación y mantenimiento de los usuarios creados en el Sistema de Información Gerencial, con el fin de brindar una adecuada y oportuna gestión a los accesos que se suministran para manipular la información contenida en el mencionado sistema. Esta política se socializa en las capacitaciones que se realizan sobre seguridad de la información y sus sistemas.			100%	Se ha seguido utilizando el procedimiento igual que en el primer semestre.			
Perdida del control en la administración de los sistemas complementarios incluidos en SIPA y SINIC	* Falta de conocimiento técnico para desarrollar procesos de contratación de software por parte de las áreas administrativas. * Desconocimiento de todas las funcionalidades que actualmente tienen los sistemas del SINIC, lo que hace que estos sean subutilizados y por ende se contraten funcionalidades que ya existen. * Debilidad en la elaboración de los términos de referencia en el ámbito técnico con respecto a los entregables, metodologías de desarrollo y arquitecturas de software, sobre las cuales se requieren las implementaciones para que sean compatibles con las aplicaciones existentes. * Contratación de desarrollos de software para el SINIC por parte de otras dependencias del Ministerio, sin el acompañamiento del Grupo SINIC.	80%	* Crear protocolo de contratación de desarrollos de software en conjunto con el Grupo de Sistemas e Informática y divulgarlo a las áreas del Ministerio de Cultura interesadas.	100%	Protocolo de contratación de desarrollos de software.	100%	Permanente	Coordinador SINIC	Todo lo que tenga que ver con contrataciones de desarrollo de software, sino cumple con el protocolo establecido, no se le dará el VoBo por parte de Planeación, hasta tanto no se aplique la política establecida para este fin.		En este año no se han realizado contrataciones de desarrollos desde el SINIC, adicionalmente y por política de la entidad, de ahora en adelante todos los desarrollos deben ser aprobados por el grupo de Sistemas y ejecutados bajo el protocolo que en esta área tienen diseñado para tal fin.	80%	Zona de Riesgo Extrema	0%	En el segundo semestre de 2014 se definió que los desarrollos pasarían al grupo de Sistemas e Informática, razón por la cual este riesgo será transferido a dicha oficina.	80%	Zona de Riesgo Extrema	El riesgo identificado y todos los elementos que lo caracterizan se corresponden de manera adecuada, así mismo la acción propuesta dentro del plan de tratamiento contribuye a mitigar los factores internos. En el seguimiento se resalta que a partir de la vigencia 2014, el Grupo de Gestión de Sistemas e Informática implemento un procedimiento controlado para la contratación, seguimiento y aprobación del desarrollo de software para el Ministerio, con lo cual se establecen controles permanentes y efectivos. Es importante que desde ese proceso sea acogido este riesgo para la vigencia 2015.
Acceso indebido a los registros a nivel de base de datos	* Falta de creación de diferentes perfiles para la administración y consulta de la base de datos. * Obsolescencia del Gestor de BD que no permite la creación de diferentes perfiles y que adicionalmente ya no cuenta con soporte por parte de Microsoft.	40%	* Solicitar la adquisición de la licencia para el gestor de bases de datos SQL a la versión más actualizada existente en el mercado. A partir de la adquisición e implementación del gestor de BD crear diferentes perfiles de acceso, para optimizar el control de acceso a la BD por parte de los diferentes usuarios. * Migrar la BD a la última versión del gestor de BD.	70% 30%	* Realizar gestión ante el Grupo de Sistemas para que realicen la compra del gestor de BD. * La compra del software e implementar las actividades propuestas para la actualización de la BD expuestas en las opciones de manejo.	100%	Diciembre de 2014	Coordinador SINIC y Coordinador Grupo de Sistemas	Seguir como se está trabajando actualmente.		No se ha definido el proceso de compra, dado que aún no se sabe si el grupo SINIC pasará o no al área de Sistemas e Informática.	40%	Zona de Riesgo extrema	0%	En el segundo semestre de 2014 se definió que los procesos del SINIC en cuanto a base de datos pasan al al grupo de Sistemas e Informática, razón por la cual este riesgo es transferido a dicha oficina. Así mismo, para este período el grupo de Sistemas e Informática contrató un proceso de migración de las bases de datos del servidor Kronos a un gestor de base de datos más actualizado SQL 2012.	40%	Zona de Riesgo extrema	El riesgo identificado y todos los elementos que lo caracterizan se corresponden de manera adecuada, así mismo las acciones propuestas dentro del plan de tratamiento contribuyen a mitigar los factores internos. En el seguimiento se espera que el Grupo de Gestión de Sistemas e Informática, quien ya implemento acciones para mitigar este riesgo, lo adopte para la vigencia 2015 e incorpore los controles existentes y las acciones de mejora adicionales o complementarias que considere viables.