DEFINICIONES

particular.

la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar cuán frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

verificación y evaluación determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.

riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo; se pueden clasificar en cinco categorías: personas, materiales, comités, instalaciones y entorno.

Compartir el Riesgo: Cambiar la responsabilidad o carga por las pérdidas que ocurran luego de la materialización de un riesgo mediante legislación, contrato, seguro o cualquier otro medio.

Consecuencia: El resultado de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia, frente a la consecución de los objetivos de la entidad o el proceso.

Controles existentes: especificar cuál es el control que la entidad tiene implementado para combatir, trabajo.

entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Evaluación del Riesgo: Proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

riesgos.

Evento: Incidente o situación, que ocurre en un lugar determinado durante un periodo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

Frecuencia: Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha

el control de la Entidad Pública, que ponen en riesgo el logro de su Misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

implementadas.

fin de identificar posibles cambios.

Opciones de manejo: opciones de respuesta ante los riesgos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual

Pérdida: Consecuencia negativa que trae consigo un evento.

criterios de Frecuencia, si se ha materializado (por ejemplo: No. de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Probabilidad: Grado en el cual es probable que ocurra un evento, que se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.

Proceso de Administración de Riesgo: Aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la Administración del Riesgo.

su ocurrencia.

su ocurrencia.

Riesgo Estratégico: Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgo Residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

Riesgo: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos de Tecnología: Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga su necesidades actuales y futuras y soporte el cumplimiento de la misión.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad, que incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como

la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

MAPA DE RIESGO Y CONTINGENCIA - IDENTIFICACIÓN 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 / DESCRIPCIÓN	CLASIFICACIÓN	FACTOR INTERNO	FACTOR EXTERNO	EFECTOS O CONSECUENCIAS	IMPACTO	PROBABILIDAD DE OCURRENCIA	ZONA DE RIESGO (Evaluación)	CONTROL EXISTENTE	VALORACIÓN DEL RIESGO	ZONA DE RIESGO (Evaluación despúes de controles)	IMPACTO ESPERADO	PROBABILIDAD DE OCURRENCIA ESPERADA	ZONA DE RIESGO ESPERADA
Daño y perdida de los activos tecnologicos	Tecnología	Indebida utilización de las herramientas informáticas disponibles. Falta de continuidad de los contratos de mantenimiento y soporte tecnico	Ataques o instrusiones a los equipos activos. Factores naturales y antrópicos.	Indisponibilidad de los servicios. Afectación del rendimiento de algunos elementos informáticos.	4. Mayor	3. Posiblemente ocurriría	48%	Compra de equipos con garantia. - Incllusión de los elementos tecnologico en la póliza global de los seguros. Contratos con empresas especiaizadas Tener disponibles equipos en reserva para atender requerimientos por daño.	Con los controles existentes se diminuye la probabilidad de ocurrencia de riesgo y el impacto en caso de llegarse a materializar.	12%	4. Mayor	1. Excepcionalmente ocurriría	12%
Alteración, perdida y fuga de información	Operativo	Ingreso no autorizado a las bases de datos de los sistemas de información. Fallas en la herramienta que ejecuta la politica de buckus Ingreso a sitios web no autorizados. Utilización de información de los sitemas del Ministerio para beneficio de particulares	Ataques o intrusiones a los sistemas de información.	Indisponibilidad de los sistemas de información. - Pérdida de efectividad, eficiencia de los procesos. -Información errada o inoportuna para la toma de desiciones. - Bajos indices de transparencia. - Pérdida de la imagen y credibilidad en la organización.	4. Mayor	4. Probablemente ocurriría	64%	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	Los controles ayudan a disminuir la probabilidad de ocurrencia del riesgo.	32%	4. Mayor	1. Excepcionalmente ocurriría	16%
Incumplimiento en oportunidad y calidad de los requerimientos de desarrollo de software	Operativo	Mala interpretación de los terminos contractuales por parte del proveedor de desarrollo de software Falta de personal con el perfil correspondiente para cumplir con las necesidades de desarrollo de software del Ministerio Incumplimiento de los lineamientos del procedimiento de desarrollo de software estabecido Deficiciencia en el levantamiento de los requerimientos del usuario Falta de documentación sobre los sistemas de información existentes, que dificulta el desarrollo de actualizaciones	Cambios en lineamientos y normatividad que no den el tiempo requerido para aplicarlos en los sistemas Incumplimiento de proveedores externos de desarrollo de software	- Multas y sanciones por incumplimientos en los reportes a los entes de control - Incumplimientos de entrega de funcionalidades a clientes externos del Ministerio -Pérdida de efectividad en el uso y la producción del software desarrollado en el Ministerio -Malgasto de los recursos del Ministerio por la duplicidad de esfuerzos en el desarrollo de software	3. Moderado	4. Probablemente ocurriría	48%	Se cuenta con un procedimiento de desarrollo de software Se cuenta con un plan de acción donde se encuentran las actividades de desarrollo de software Se cuenta con los manuales del software desarrollado por el Ministerio Se cuenta con personal contratado por el Grupo de Sistemas que valida el cumplimiento de los estándares definidos para el desarrollo de software	Los controles ayudan a disminuir la probabilidad de ocurrencia del riesgo.	24%	3. Moderado	1. Excepcionalmente ocurriría	12%

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**

										SEGUIMIENTO I SEMESTRE				SEGUIMIENTO II SEMESTRE			
RIESGO	FACTOR INTERNO	ZONA DE RIESGO	OPCIONES DE MANEJO / ACCIONES	Peso Porcentual	INDICADORES	META #	CRONOGRAMA	RESPONSABLE	ACCIÓN DE CONTINGENCIA	AVANCE % (Expresión PORCENTUAL del avance)	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACION	ZONA DE RIESGOS	AVANCE % (Expresión PORCENTUAL del avance)	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACION	ZONA DE RIESGOS
Daño y perdida de los activos tecnologicos	Indebida utilización de las herramientas informáticas disponibles.	12%	Realizar Analisis 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.	30%	Se adelantó la revisión y ajustes sobre la documentación definida en procedimientos, formatos y políticas del área de Gestión de Sistemas del Ministerio	12%	Zona de Riesgo Moderada	100%	Se elaboró el documento "Manual de Gestión de TICs" que recopila las políticas para el uso y manejo de TICs en el Ministerio de Cultura y se encuentra pendiente por publicar en ISOLUCION.	12%	Zona de Riesgo Moderada
	Falta de continuidad de los contratos de mantenimiento y soporte tecnico		Adelantar el tramite de solicitud de vigencias futuras de los contratos de mantenimiento de activos tecnologicos. Cumplimiento de las actividades del plan de matenimiento definido para los activos tecnologicos.	30% 30%	Vigencias futuras aprobadas. 100%	2 100%	Diciembre de 2014	Coor. Grupo de Sistemas		40%	Se adelantaron los estudios de mercado para costear los contratos de mantenimiento no cubiertos por el presupuesto de la vigencia actual			100%	Se elaboraron todos los contratos requeridos para mantener la plataforma tecnológica y se encuentran vigentes.		
Alteración, perdida 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. Fortalecer el control de acceso a las bases de datos requiriendo la asignación de claves y mejorando las ya asignadas.	30% 15%	No de herramientas. Para los sistemas de información y bases de datos tengan un usuario particular para su administración/ Total de Herramientas programadas. Porcentaje de mejoramiento de asignasión de claves	100%	Diciembre de 2014	Coor. Grupo de Sistemas	Restaurar la información alterada o perdida con los backups. Acompañar el seguimiento a la posible forma de extracción de la información.	20%	Se adelantó un inventario de sistemas de información del Ministerio de los cuales se da soporte en el área de Sistemas, pero se detectó que en las áreas se manejan sistemas no identificados en el área. Sobre los sistemas cuyo soporte de desarrollo de software se brinda a través del área, en el segundo semestre de 2013, se realizarán los ajustes requeridos para implementar mecanismos de seguridad en el acceso.	29%	Zona de Riesgo Extrema	100%	Se actualizaron las claves de los usuarios que administran los sistemas de información cuyo soporte se brinda en el área de sistemas e informática.	16%	Zona de Riesgo Alta
	Fallas en la herramienta que ejecuta la politica de buckus		Análisis de las alternativas de generación del buckus en el mercado	15%	Propuesta de Alternativa con buckus	1	Diciembre de 2014			10%	Con el fin de poder implementar una nueva política de backup, se adelantó un análisis de alternativas para la implementación del nuevo mecanismo de backup y se solicitaron cotizaciones para definir el valor requerido para su implementación.			100%	Se implementó un nuevo esquema de backup para el Ministerio y se realizó el ajuste sobre la política de backup de acuerdo con el nuevo esquema implementado y se incluyó en el nuevo documento "Manual de Gestión de TICs"		
	Ingreso a sitios web no autorizados.		Socialización de la importancia del uso adecuado del internet	20%	Campaña de socialización	1	Diciembre de 2014			50%	Registro del seguimiento al software de ejecución de los backups, al reporte generado por log de la herrramienta, de uso interno del área de Sistemas. Se realizaron las 52 tareas de backup del primer semestre del año.			100%	Registro del seguimiento al software de ejecución de los backups, al reporte generado por log de la herrramienta, de uso interno del área de Sistemas. Se realizaron las 52 tareas de backup del primer semestre del año.		
	Utilización de información de los sitemas del Ministerio para beneficio de particulares		Socialización de las politicas de acceso responsable a la información	20%	Propuesta definida	1	Diciembre de 2014			0%	Este tema será abordado en el documento de Gestión de Sistemas que se definirá éste año			100%	En el documento "Manual de Gestión de TICs" se incluyó el capítulo "POLITICAS DE BUEN USO DE LOS RECURSOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES" donde se estable la responsabilidad de cada colaborador del Ministerio sobre su usuario de ingreso y los equipos de cómputo a su cargo.		
Incumplimiento en oportunidad y calidad de los requerimientos de desarrollo de software	Mala interpretación de los terminos contractuales por parte del proveedor de desarrollo de software	24%	Documentar las etapas contractuales de desarrollo de sotfware siguiendo los lineamientos definidos en el procedimiento de software.		No de Actas realizadas /Reuniones planteadas.	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.	10%	Se estimaron los recursos necesarios para adelantar las labores de elaboración del Plan Estratégico Tecnológico.	21%	Zona de Riesgo Alta	100%	Se elaboró el Documento "Plan Estratégico de Tecnología"	12%	Zona de Riesgo Moderada
	Falta de personal con el perfil correspondiente para cumplir con las necesidades de desarrollo de software del Ministerio		Propuesta de mejora de la organización de personal en el área		Documento Propuesta	1				80%	Se adelantó la revisión y ajustes sobre la documentación definida en procedimientos y formatos del área de Gestión de Sistemas del Ministerio			100%	En el documento "Plan Estratégico de Tecnología" se estableció el personal y demás recursos requeridos por cada proyecto tecnológico definido.		
	Incumplimiento de los lineamientos del procedimiento de desarrollo de software estabecido		Realizar ajustes al Procedimiento		Procedimiento ajustado y divulgado	1	dic-14			0%	Este tema será abordado en el documento de Gestión de Sistemas que se definirá éste año			100%	Se publicaron los ajustes sobre la documentación definida en procedimientos y formatos del área de Gestión de Sistemas del Ministerio, en ISOLUCION		
	Deficiciencia en el levantamiento de los requerimientos del usuario					1	dic-14							100%	En el aplicativo ISOLUTION se llevo a cabo la actualización de formatos para el levantamiento de requerimientos del área usuaria lo que permite centralizar las solicitudes en el Grupo de Sistemas		
	Falta de documentación sobre los sistemas de información existentes, que dificulta el desarrollo de actualizaciones		Seguimiento al PETIC (Plan estrategico de las tic)		No de proyectos ejecutados/ Proyectos planeados con asignación de recursos	100%	Julio de 2014			20%	Se adelantó un inventario de sistemas de información del Ministerio de los cuales se da soporte en el área de Sistemas, pero se detectó que en las áreas se manejan sistemas no identificados en el área. En el segundo semestre de 2013 se adelantarán reuniones con las áreas para completar el inventario actual, dentro del ícual se encuentran la identificación de la documentación existente.			100%	Se llevo a acabo el levantamiento de información de los sistemas que apoyan la gestion de las áreas del Ministerio.		