DEFINICIONES

Aceptar el Riesgo: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Administración de Riesgos: Conjunto de Elementos de Control que al interrelacionarse permiten a 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.

Análisis de Riesgo: Elemento de Control que permite establecer la probabilidad de ocurrencia de los 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.

Autoevaluación del Control: Elemento de Control que basado en un conjunto de mecanismos de 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.

Causas (factores internos o externos): Son los medios, las circunstancias y agentes generadores de 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, minimizar o prevenir el riesgo.

Cronograma: son las fechas establecidas para implementar las acciones por parte del grupo de trabajo.

Efectos (consecuencias): Constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la 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.

Evaluación del riesgo: Resultado obtenido en la matriz de calificación, evaluación y respuesta a los 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 ocurrido un evento en un tiempo dado.

Identificación del Riesgo: Elemento de Control que posibilita conocer los eventos potenciales, estén o no bajo 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.

Indicadores: se consignan los indicadores diseñados para evaluar el desarrollo de las acciones implementadas.

Monitorear: Comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el 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.

Probabilidad: entendida como la posibilidad de ocurrencia del riesgo; ésta puede ser medida con 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.

Reducción del Riesgo: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.

Reducción del Riesgo: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o 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 de su interacción con las demás áreas, dependerá en gran parte el éxito o fracaso de toda entidad.

Riesgos Operativos: Comprende los riesgos relacionados tanto con la parte operativa como con la técnica de 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.

Riesgos Operativos: Comprende los riesgos relacionados tanto con la parte operativa como con la técnica de 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 2011

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
ÁREA: GRUPO DE SISTEMAS

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 después de controles)
Daño y perdida de los activos.	Tecnología	Desconocimiento del debido cuidado que debe darse a los elementos informáticos. Indebida utilización de las herramientas informáticas disponibles.	Ataques o intrusiones a los equipos activos. Factores naturales y entrópicos.	Indisponibilidad de los servicios. Afectación del rendimiento de algunos elementos informáticos.	4. Mayor	3. Posiblemente ocurriría	48%	Compra de equipos con garantía. - Inclusión de los elementos en la póliza global de los seguros. Tener disponibles equipos en reserva para atender requerimientos por daño.	Con los controles existentes se disminuye la probabilidad de ocurrencia de riesgo y el impacto en caso de llegarse a materializar.	24%
Alteración, perdida y fuga de información	Operativo	Ingreso no autorizado a las bases de datos de los sistemas de información. No generación de respaldos de información de acuerdo con la política de backup establecida. Ingreso a sitios web no autorizados. Utilización de información de los sistemas del Ministerio para provecho personal o por hacer favores sin ser la persona autorizada.	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 decisiones. - Bajos índices 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.	Los controle ayudan a disminuir la probabilidad de ocurrencia del riesgo.	48%

MAPA DE RIESGO PLAN DE MANEJO Y MONITOREO 2011

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
ÁREA: GRUPO DE SISTEMAS

RIESGO	FACTOR INTERNO	ZONA DE RIESGO	OPCIONES DE MANEJO / ACCIONES	INDICADORES	META #	CRONOGRAMA	RESPONSABLE	ACCIÓN DE CONTINGENCIA	SEGUIMIENTO I SEMESTRE			SEGUIMIENTO II SEMESTRE			
									AVANCE % (Expresión PORCENTUAL del avance)	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACION	AVANCE % (Expresión PORCENTUAL del avance)	ANÁLISIS DE DATOS (Descripción del avance)	EVALUACION	CRITERIOS DE EVALUACIÓN
Daño y perdida de los activos.	Desconocimiento del debido cuidado que debe darse a los elementos informáticos.	24%	Definir una política para el buen uso de los elementos informáticos y divulgarla a todo el Ministerio.	1 política documentada y divulgada	1	jun-11	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.						24%	
	Indebida utilización de las herramientas informáticas disponibles.		Fortalecer el esquema de vigilancia a través del aumento del número de cámaras.	100 cámaras de seguridad al servicio.	100	dic-11	Coor. Grupo de Sistemas								
Alteración, perdida y fuga de información	Ingreso no autorizado a las bases de datos de los sistemas de información.	48%	Fortalecer el control de acceso a las bases de datos requiriendo la asignación de claves y mejorando las ya asignadas.	Garantizar que los sistemas de información y bases de datos tengan un usuario particular para su administración. (no aplica para archivos de trabajo en excel y Access)	100%	dic-11	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.						#¡REF!	
	No generación de respaldos de información de acuerdo con la política de backup establecida.		Monitorear la generación de los backups y administrarlos de acuerdo con la política.	Generar los backups cada tercer día	104	dic-11								0%	
	Ingreso a sitios web no autorizados.		Establecer niveles de acceso a internet de acuerdo con las necesidades de los servidores públicos y las tareas que tiene a cargo.	Niveles de acceso definidos y configurados a cada perfil.	100%	dic-11								0%	
	Utilización de información de los sistemas del Ministerio para provecho personal o por hacer favores sin ser la persona autorizada.		Definir la propuesta de protección de información para presentarla a la Secretaría General.	Propuesta definida	1	dic-11								0%	