ANEXOS

Guía No. 1
Evaluación de Riesgos de las Entidades Gubernamentales

La evaluación del riesgo se enfocará en lo siguiente:

a) Identificación de Objetivos de la Entidad

Los objetivos estratégicos, operativos, de información y de cumplimiento normativo definidos en el PEI, POM y POA de la entidad, deben ser considerados para el inicio del proceso de evaluación de riesgos y priorizados de acuerdo al nivel de aporte directo a la prestación de servicios o entrega de productos de la entidad.

b) Identificación de Estrategias y Planes de Acción

Por cada objetivo priorizado, deben identificarse las estrategias, planes de acción e indicadores de desempeño.

c) Identificación de Eventos

La máxima autoridad, equipo de dirección y la unidad especializada de la entidad, identificarán todos los eventos que amenacen el alcance de objetivos priorizados y estrategias identificadas de la entidad, provenientes de fuentes internas y externas.

Dentro de los eventos derivados de fuentes Internas, podrán esquematizar y detallarse los relacionados a:

- Gestión del Recurso Humano.
- Gobernanza, Infraestructura, datos y aplicaciones de Tecnologías de Información implementadas en la entidad.
- Disponibilidad y salvaguarda de bienes del estado en propiedad de la entidad.
- Gestión presupuestaria.
- Gestión financiera y operativa.

- Cumplimiento de políticas y procedimientos.
- Cumplimiento de normativa propia de la entidad.
- Cumplimiento de requerimientos éticos y normas de conducta.
- Estructura organizacional de acuerdo a las actividades.
- Gestión de medios de comunicación efectivos.
- Resguardo de información física y digital.
- Cumplimiento de aspectos legales y
- Otros que apliquen a la entidad.

En las fuentes externas deberán esquematizar y detallarse, entre otros, los siguientes:

- Políticas públicas: normativa, acuerdos, circulares y otros emitidos por el ente rector de la legislación en el Estado.

- Economía del país: tipo de cambio, inflación, movimiento de índices económicos, presupuesto aprobado y cambios en políticas económicas.

- Sociales: crecimiento demográfico, demandas de los ciudadanos, influencia de grupos de poder, la fiscalización social y servicios hacia la población.

- Cambios en las Tecnologías de Información: tendencias, temas emergentes, obsolescencia de equipos, cambios en los marcos de gobernanza.

- Ambientales: catástrofes, estados de emergencia, cambio climático y normativa relacionada.

- Salud y seguridad: normativa de protección al trabajador, disposiciones generales de salud, suspensión de trabajo por enfermedades o accidentes, estados de calamidad por enfermedad.

- Normativos en general: cambios en leyes, exposición a incumplimientos, adhesión a convenios internacionales y otros.

Para identificar eventos podrán utilizar diferentes técnicas, dentro de estas deberán considerarse:

- Metodologías proporcionadas por el ente rector de planificación para identificar riesgos.
- Inventarios históricos de eventos y riesgos, a cargo del ente rector de gestión y prevención de desastres.
- Ejercicios del equipo de dirección, para la identificación de eventos.
- Estadísticas de ocurrencia generadas por el ente rector de información estadística y tendencias del Estado.
- Talleres de autoevaluación.
- Mapeo de procesos.
- Análisis del entorno.
- Lluvia de ideas.
- Análisis de indicadores.
- Entrevistas.
- Cuestionarios a mandos superiores y medios.
- Información de eventos de años anteriores.
- La máxima autoridad de la entidad podrá utilizar la información y conocimientos de eventos que puedan ser considerados como riesgos potenciales, proporcionados por la unidad de auditoría interna.
- Información de eventos y riesgos de proveedores y otros.
- El portafolio de eventos deberá actualizarse anualmente.

d) Evaluación de Riesgos

La unidad especializada de la entidad deberá evaluar los eventos identificados, utilizando las perspectivas de probabilidad de que un evento se materialice y su severidad o impacto negativo en los objetivos relacionados al momento de materializarse.

La perspectiva de probabilidad, deberá considerar los niveles de valoración siguientes:

PROBABILIDAD

VALOR	CRITERIO	DESCRIPCIÓN
1	Muy Baja	Evento que se presenta históricamente, pero sin frecuencia estadística comprobada
2	Baja	Evento que se presenta históricamente, en rangos amplios de 5 a 10 años, pero sin frecuencia estadística comprobada
3	Media	Evento que se presenta con una frecuencia estadística comprobada, en rango de 3 a 5 años
4	Alta	Evento que se presenta con una frecuencia estadística comprobada, en rangos de 1 a 3 años
5	Muy Alta	Riesgo que se presenta con una frecuencia anual y soportada con información estadística o histórica

La perspectiva de severidad, deberá considerar los niveles de valoración siguientes:

SEVERIDAD

VALOR	CRITERIO	DESCRIPCIÓN
1	Muy Baja	Eventos sin impacto en la ejecución de estrategias u operaciones de la entidad
2	Baja	Evento que provoca impacto leve en la operación y áreas de apoyo de la entidad
3	Media	Evento que afecta objetivos institucionales no claves no operacionales
4	Alta	Evento que afecta objetivos institucionales y estratégicos clave, pero permite el ajuste a la estrategia, planes de acción y programas, para el cumplimiento razonable de prestación de servicios o entrega de productos de la entidad
5	Muy Alta	Evento que impacta directamente en el alcance de objetivos institucionales y estratégicos clave, provocando interrupciones de servicios o falta de entrega de productos de la entidad

La combinación de la probabilidad y la severidad representa el riesgo inherente a la ejecución de la estrategia, por lo que se aplicará la formula siguiente:

Valor de la probabilidad multiplicado por el Valor de la severidad = Riesgo Inherente.

La unidad especializada de la entidad deberá evaluar el riesgo inherente y acumular los resultados en una matriz, con el objetivo de contar con un portafolio de riesgos a ser gestionados.

e) Establecimiento de Posibles Respuestas al Riesgo

Una vez que han sido determinados los riesgos inherentes en la matriz, la unidad especializada de la entidad debe definir la posible respuesta ante el riesgo. Para ello, será necesario aplicar el criterio profesional basado en las hipótesis realizadas sobre el riesgo y en un análisis razonable de los costos asociados, con la reducción del nivel de riesgo.

La respuesta adoptada no derivará necesariamente en un menor volumen de riesgo residual, pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables, para la máxima autoridad y equipo de dirección, la unidad especializada de la entidad deberá volver a analizar y revisar la respuesta.

Un riesgo que presente severidad significativa en la entidad y con probabilidad no relevante, por lo general, no requerirá una respuesta detallada ante dicho riesgo. El riesgo que presente una mayor probabilidad de que se produzca y/o presente una severidad significativa, requerirá una mayor atención.

Las estimaciones de la importancia al riesgo, a menudo se ven determinadas por el uso de datos de eventos anteriores, que proporcionan una base objetiva respecto a las estimaciones totalmente subjetivas. Los datos generados internamente, basados en la propia experiencia de la entidad, pueden resultar más relevantes y aportar mejores resultados que los datos procedentes de fuentes externas, sin embargo, incluso en estas circunstancias, los datos externos pueden resultar de utilidad, como punto de control o para mejorar el análisis.

La unidad especializada de la entidad, al considerar la respuesta al riesgo, deberá identificar la “tolerancia de riesgo” de la entidad, esta constituye la cantidad de riesgos a la que una entidad está preparada a exponerse, antes de decidir sobre la acción que se tomará; Las decisiones sobre las respuestas al riesgo tienen que ser tomadas en forma conjunta con la identificación de la cantidad de riesgos que pueden ser tolerados.

Las respuestas a los riesgos se enmarcarán en las siguientes categorías:

I. Aceptar: No se adopta ninguna actividad de control que mitigue a la probabilidad o la severidad del riesgo. Este tipo de respuesta es seleccionada al no existir actividad de control mitigante y la máxima autoridad asume la responsabilidad de continuar con las estrategias asociadas por conveniencia a la prestación de servicios o entrega de productos institucionales.

II. Evitar: Se evita realizar las estrategias, planes de acción o programas que den lugar al riesgo, por lo que no se describe una actividad de control específica.

III. Reducir: Se adoptan medidas para reducir la probabilidad o la severidad del riesgo, o ambos. Este tipo de respuesta implica la selección de las actividades de control que se adoptan en una organización o la definición de acciones específicas, ante la ausencia de un control mitigante.

IV. Compartir: Se reduce la probabilidad o la severidad del riesgo transfiriendo o compartiendo una parte del mismo. Las respuestas implican la selección de actividades de control compartidas; habitualmente incluyen la contratación de seguros o la tercerización de una actividad, entre otros.

El riesgo tendrá que ser administrado y la entidad necesitará implantar y mantener un sistema efectivo de control interno, para mantener el riesgo en un nivel aceptable, por lo que al seleccionar la respuesta al riesgo, la máxima autoridad deberá considerar lo siguiente:

- El efecto potencial que puede tener sobre la importancia del riesgo y qué opciones de respuesta están alineadas con la tolerancia al riesgo de la entidad.
- La segregación de funciones, que permita que la respuesta adoptada logre la reducción prevista de la importancia del riesgo.
- El análisis costo/beneficio de las posibles respuestas.
-

f) Evaluación de Riesgo Residual

Una vez establecidas las respuestas al riesgo, enfocadas en reducir y compartir, para adherirlas a la matriz generada, deberá valorarse la capacidad de mitigación de las mismas, utilizando los siguientes criterios de madurez y eficiencia del control.

VALOR	CRITERIO DE MADUREZ DEL CONTROL INTERNO	DESCRIPCIÓN DE CRITERIO	CAPACIDAD DE MITIGACIÓN DE RIESGO
1	Básico	El control funciona de una forma empírica y se aplica a criterio de la autoridad a cargo del proceso	Ineficiente
2	Operativo	Control transmitido de un cargo a otro informalmente, para lograr el funcionamiento operativo y con decisiones centralizadas en la autoridad a cargo del proceso	Mínima
3	Funcional	El control es parte de documentos o instrucciones dadas por escrito a los empleados mediante la transmisión de conocimientos. Los controles buscan el funcionamiento de procesos administrativos para el alcance de objetivos operativos	Media
4	Razonable	El control se incluye formalmente en políticas y procedimientos escritos, actualizados de acuerdo a la necesidad de la entidad, enfocándose en el funcionamiento de los procesos operativos clave para el alcance de objetivos. Los controles son comunicados por escrito	Aceptable
5	Eficiente	El diseño del control permite la actualización constante, para que funcione oportuna y eficientemente en la estrategia, operaciones, así como en los procesos de registro financiero. El control es comunicado a los servidores públicos mediante capacitaciones formales por escrito. El control mitiga riesgos y permite la retroalimentación a los ejecutores para la mejora continua	Optima

Al aplicar los valores de mitigación de las respuestas al riesgo en la matriz de riesgo inherentes deberá contemplarse la siguiente fórmula para obtener el riesgo residual:

Riesgo inherente dividido entre el valor de mitigación de la respuesta al riesgo = Riesgo residual

Los resultados obtenidos deberán acumularse en la Matriz de Evaluación de Riesgos, con el objetivo de contar con un portafolio de riesgos residuales.

g) Tolerancia al Riesgo

La unidad especializada de la entidad deberá presentar los resultados en la matriz, adicionando la valoración relacionada a la tolerancia al riesgo, con rangos autorizados por la máxima autoridad de la entidad; los rangos normalmente serán definidos por la filosofía de control y buena gobernanza instituidos y de acuerdo a la cantidad de exposición al riesgo de la administración al ejecutar las estrategias.

Los rangos podrán basarse en la madurez del control de la entidad, por lo que a mayor exposición de riesgo, se determinarán rangos alejados de la valoración de riesgos, bajo un enfoque conservador; el cuadro siguiente muestra los rangos y la representación gráfica del mapa de riesgos, basada de la tolerancia recomendada. (Decisión de la máxima autoridad):

TOLERANCIA AL RIESGO

MATRIZ DE TOLERANCIA AL RIESGO			
RANGO	**CRITERIO**	**DESCRIPCIÓN**	**PRIORIZACIÓN**
1 a 10.00	Básico	Riesgo residual tolerable que no requiere atención inmediata. Es gestionado razonablemente por el control interno de la entidad	**VERDE**
10.01 a 15.00	Gestionable	Riesgo residual que puede ser gestionado a través de opciones de control adicionales o respuestas especificas al riesgo	**AMARILLO**
15.01 en adelante	No tolerable	Riesgo residual tolerable con mayor exposición a no alcanzar los objetivos, es necesario replantear la estrategia a la respuesta al riesgo. Requiere atención inmediata	**ROJO**

h) Matriz de Evaluación de Riesgos

Entidad	
Período de evaluación	

1 a 10 Torerable
10.01 a 15 Gestionable
15.01 + No Torerable

	(1)	(2)	(3)	(4)		(5)		(6)	(7)	(8)	(9)	(10)	(11)
No.	**Tipo Objetivo**	**Ref.**	**Área Evaluada**	**Eventos Identificados**	**Descripción del Riesgo**	**Evaluación**			**Riesgo Inherente**	**Valor Control Mitigador**	**Riesgo Residual**	**Control interno para mitigar (gestionar el riesgo)**	**Observaciones**
						Probabilidad	**Severidad**						
1													
2													
3													
4													
5													

Conclusión:

Firma	
Nombre del Responsable	
Puesto	

No.	DESCRIPCIÓN
1	Identificar el tipo de objetivos, operacionales, estratégicos, cumplimiento y financieros.
2	Indicar el número del tipo de objetivos, ejemplo: O-1, E-1, C-1 o F-1.
3	Identificar el área que se está evaluando.
4	Describir el evento que se ha identificado como riesgo.
5	Indicar la Valoración de probabilidad del evento.
6	Indicar la valoración de la severidad del evento.
7	Colocar el resultado del riesgo inherente, el cual se origina de multiplicar el valor de la probabilidad por el valor de severidad del evento.
8	Indicar el valor del control que mitigará la severidad.
9	Colocar el resultado del riesgo residual, el cual de origina de dividir el riesgo inherente entre el valor del control mitigante.
10	Indicar los diferentes controles que mitigarán el riesgo.
11	Colocar observaciones que se deriven del análisis de la matriz y los documentos que soporten el control mitigador (digital) .

i) Plan de Trabajo en Evaluación de Riesgos

Entidad	
Período de evaluación	

	(1)		(2)	(3)	(4)	(6)	(7)	(8)	(9)	(10)
NO.	**Riesgo**	**Ref Tipo Riesgo**	**Nivel de Riesgo Residual**	**Controles Recomendados**	**Prioridad de Implimentación**	**Recursos Internos o Externos**	**Puesto Responsable**	**Fecha Inicio**	**Fecha Fin**	**Comentarios**
1										
2										
3										
4										
5										

Firma	
Nombre del Responsable	
Puesto	

No.	DESCRIPCIÓN
1	Descripción del riesgo determinado en el proceso de evaluación de riesgos.
2	El nivel de riesgo asociado a cada riesgo identificado que se determinó en el proceso de evaluación de riesgos.
3	Controles recomendados para la mitigación o transferencia del riesgo.
4	La priolridad de acción se determina sobre la base de los niveles de riesgos y los recursos disponibles.
5	Los controles seleccionados para la implementación.
6	Recursos internos y externos necesarios para la implementación de los controles determinados.
7	Lista de equipo y personas que serán responsables de implementar los controles, ya sean nuevos o mejorados.
8	Fecha de inicio para la aplicación de los controles previstos.
9	Fecha de finalización de los controles previstos aplicados.
10	Plan de mantenimiento, de revisión y evaluación de los controles, después de la implementación.

j) Mapa de Riesgos

Entidad	
Período de evaluación	

PROBABILIDAD Y SEVERIDAD

Probabilidad.					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Severidad.				

No.	Riesgos	Probabilidad	Severidad	Punteo
1				
2				
3				
4				

Niveles de Valoración

La determinación de los niveles de valoración se debe realizar utilizando los criterios de Probabilidad y Severidad incluidos en la Guía No. 1 Evaluación de Riesgos de las Entidades Gubernamentales indicados en la literal d), según las ponderaciones siguientes:

Valor	Criterio
5	Muy Alta.
4	Alta.
3	Media.
2	Baja.
1	Muy Baja.

k) Matriz de Continuidad de Evaluación de Riesgos

Entidad	
Período de evaluación	

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
No.	**Rango**	**Sub Tema**	**Nivel de Tolerancia**	**Método de Monitoreo**	**Frecuencia de Monitoreo**	**Responsable**	**Severidad del Riesgo**
1							
2							

Firma	
Nombre del Responsable	
Puesto	

No.	DESCRIPCIÓN
1	Descripción del riesgo.
2	Listados de riesgo específico por cada tipo de riesgos (E. 1. 1 . E. 1. 2)
3	Nivel de tolerancia minimo a ser aceptado.
4	Método de monitoreo para evaluar el riesgo.
5	Frecuencia de revisión.
6	Responsables del monitoreo y de informar oportunamente.
7	Severidad al pasar el limite de tolerancia.