

ANEXO 4.1

DEFINICIONES DEL ESQUEMA DE GESTIÓN DE RIESGOS

Se exponen en este epígrafe las definiciones del esquema de gestión de riesgos.

Riesgo.

(RAE) Contingencia o proximidad de un daño.

(ISO) Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas. Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles. Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

Riesgo de corrupción.

Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Impacto del riesgo.

(SNCA) Impacto o coste (tanto económico como de reputación, operativo, u otros) que tendría para la organización la materialización del riesgo.

Probabilidad del riesgo.

(SNCA) Probabilidad de que el riesgo se materialice.

(ISO) Posibilidad de que algo suceda. En la terminología de gestión del riesgo, la palabra «probabilidad» se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado).

Nivel de riesgo.

Es el resultado de correlacionar el impacto y la posibilidad, con los controles internos existentes.

Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Riesgo bruto. Riesgo inherente.

Nivel de riesgo propio de la actividad. Es aquel al que se enfrenta una entidad en ausencia de acciones para modificar su probabilidad o impacto.

(SNCA) Nivel de riesgo de cada uno de los riesgos y de los indicadores asociados a ellos. Se calcula a partir del impacto y de la probabilidad definidos de forma inicial, sin tener en cuenta el efecto de los controles existentes o previstos en el futuro.

Riesgo neto.

(SNCA) Nivel de riesgo de cada uno de los riesgos y de los indicadores asociados a ellos. Se calcula a partir del impacto y de la probabilidad de cada riesgo una vez valorada la existencia y la eficacia de los controles implementados en la entidad para cada uno de los indicadores.

Riesgo objetivo o residual.

Nivel de riesgo que permanece después de tomar medidas de tratamiento de riesgo (SNCA) Nivel de riesgo de cada uno de los riesgos y de los indicadores asociados a ellos. Se calcula teniendo en cuenta el efecto de los controles previstos por la entidad para reducir el riesgo neto.

Indicador de riesgo.

(SNCA) Hecho que revela información cualitativa o cuantitativa formada por uno o varios datos basados en hechos, opiniones o medidas, constituyéndose en indicadores o señales de alarma de la posibilidad de que exista el riesgo.

Control.

Medida que permite reducir o mitigar un riesgo.

(SNCA) Controles diseñados e implantados para mitigar el riesgo de los indicadores de cada uno de los riesgos.

(ISO) Medida que mantiene y/o modifica un riesgo. Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo. Los controles no siempre pueden producir el efecto de modificación previsto o asumido.

Plan de acción.

(SNCA) Controles a poner en marcha por la entidad para reducir el riesgo neto a unos niveles de riesgo objetivo aceptables.

Gestión del riesgo.

(ISO) Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.

Fuente de riesgo.

(ISO) Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.

Factores internos y externos que, solos o en combinación con otros, pueden producir la materialización de un riesgo.

Mapa de riesgos.

Representación gráfica de uno o más riesgos que permite vincular la probabilidad de ocurrencia y su impacto de forma clara y objetiva.

Seguimiento.

Recolección regular y sistemática sobre la ejecución del plan, que sirven para actualizar y mejorar la exposición a riesgos.

Incertidumbre.

Falta de seguridad para saber de antemano la exacta probabilidad o impacto de eventos futuros.

Evaluación de riesgos.

Proceso de identificación y análisis de los riesgos relevantes para el logro de los objetivos de la entidad y para determinar una respuesta apropiada.