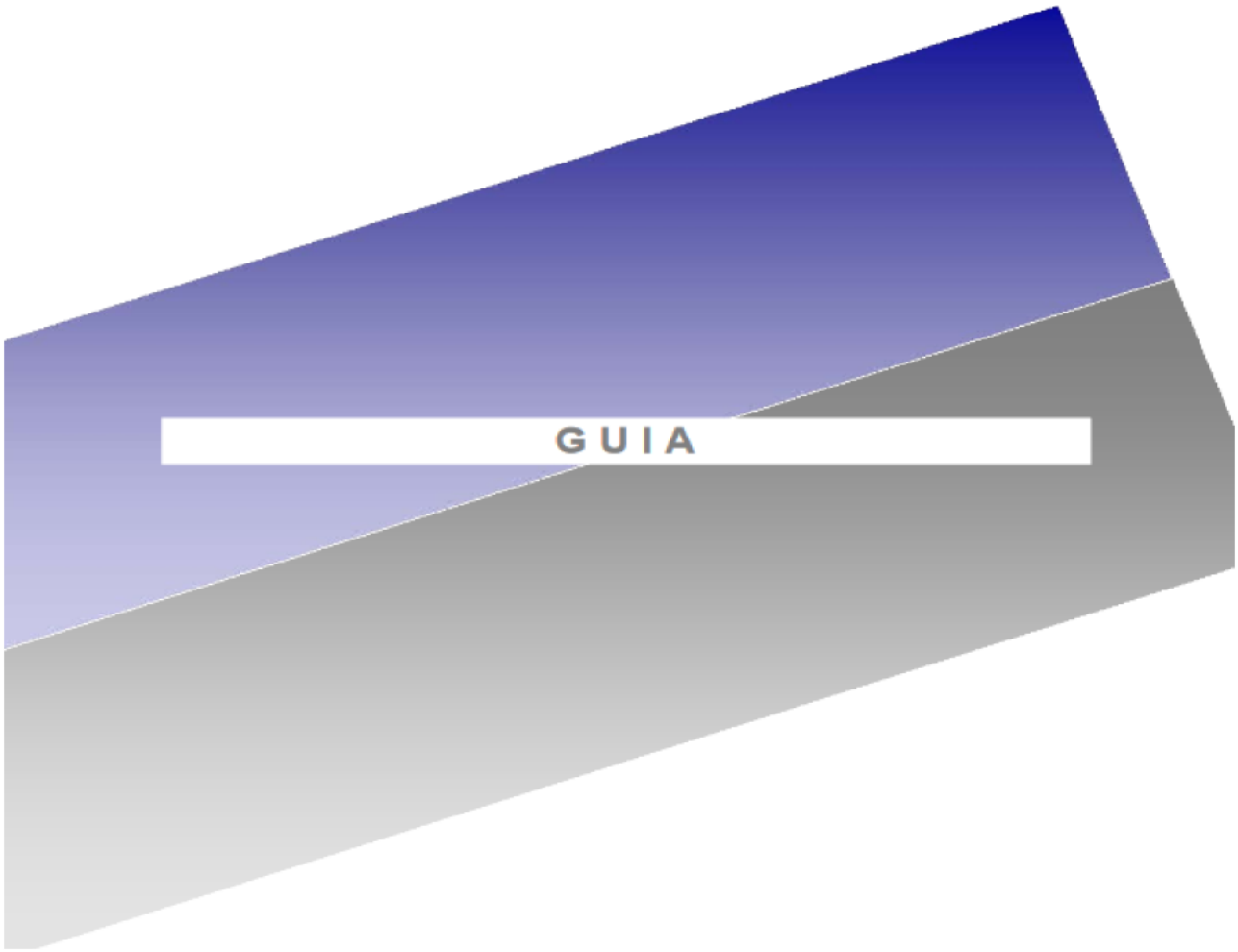
GESTIÓN DE RIESGOS DE INTEGRIDAD

para

Autoridades de Lucha contra la Corrupción (ACA)

y

Organismos de Supervisión Policiales (POB)



Traducción no oficial al castellano de: European partiers against corruption (2017, noviembre). Integrity risk management [en línea]. Disponible en: https://www.epac-eacn.org/downloads/recommendations [2018, Agosto].

Índice

Introducción

Para cumplir sus responsabilidades, instituciones públicas como las autoridades de lucha contra la corrupción (ACA, para las siglas en inglés) o los organismos de supervisión policiales (POB, para las siglas en inglés) utilizan cada vez más herramientas de gestión que hasta ahora se utilizaban sobretodo en el sector privado, como la gestión de proyectos, la gestión de riesgos o la gestión de cumplimiento. Con el fin de sacar el máximo partido de estas herramientas y de aumentar la eficiencia de la administración pública, es necesario conocer los métodos, los campos de aplicación, el valor añadido y los efectos de cada herramienta.

En la 16a Conferencia Profesional Anual y Asamblea General celebradas del 15 al 17 de noviembre de 2016 en Riga, se impulsó la creación de un grupo de trabajo sobre gestión y análisis de riesgos. El grupo de trabajo comienza su actividad a principios de 2017, presidido por Austria. Lo formaban representantes de Austria, Azerbaidjan, Bulgaria, Estonia, Alemania, Hungria, Kosovo, Portugal, Moldavia, Rumania, Eslovenia y España. Entre abril y septiembre de 2017 se celebró en Austria, Eslovenia y Moldavia dos reuniones del grupo de trabajo y una reunión adicional trilateral. También se estudiaron diversas contribuciones escritas.

En la 17a Conferencia Profesional Anual y Asamblea General, celebradas del 15 al 17 de noviembre de 2017 en Lisboa, se presentó la guía sobre la gestión de riesgos de integridad para ACA Y POB, la cual fué adoptada como estándar de trabajo por las autoridades pertenecientes a la asociación EPAC/EACN.

El objetivo de esta guía es ayudar a los miembros de la EPAC/EACN, tanto ACA como POB, a luchar contra la corrupción, promover los aspectos de cumplimiento y fomentar el desarrollo de una política de riesgos común entre los miembros de la EPAC/EACN.

El grupo de trabajo "Gestión y análisis de riesgos" propone la presentación de esta guía al Grupo de Estados contra la Corrupción (GRECO) del Consejo de Europa para que se pueda aplicar en el marco de la 5ª Ronda de Evaluación de GRECO.

1. Visión general

La gestión de riesgos es la manera profesional de hacer frente a los riesgos. Comprende todas las medidas necesarias para identificar, analizar, evaluar, supervisar y controlar los riesgos.

Para las autoridades de lucha contra la corrupción (ACA) y los organismos de supervisión policiales (POB), la gestión de riesgos se puede realizar de dos formas:

- Estableciendo un sistema de gestión de riesgos integral para aumentar la eficacia de las ACA y los POB y reforzar sus objetivos *(enfoque interno);*
- Contribuyendo a la realización de las funciones de las ACA y los POB, es decir, la prevención y la lucha contra la corrupción, identificando, analizando y evaluando riesgos de corrupción *(enfoque externo).*

1.1 Gestión interna de riesgos y gestión externa de riesgos para ACA y POB

Sobretodo en épocas de muchos cambios, los organismos han de poder identificar rápidamente sus riesgos y oportunidades si quieren proteger, conservar y profundizar en sus valores. La gestión de riesgos les ayuda a conseguirlo.

Las ACA y los POB centran a menudo la atención pública por la naturaleza de sus responsabilidades. Están obligadas a cumplir su cometido demostrando un nivel máximo de ética y siguiendo estándares profesionales.

La gestión de riesgos es una herramienta de gestión que sirva para identificar, analizar y evaluar los riesgos de un organismo concreto, y para aplicarlos es necesario definir antes los objetivos, las estrategias, la cultura y la política que dominan el organismo en lo que respecta a la gestión de riesgos.

Esta guía ha de ser el punto de partida para establecer unos estándares mínimos sobre gestión de riesgos en las ACA y los POB y para establecer la gestión de riesgos y el análisis de riesgos como herramientas destinadas a facilitar el trabajo de prevención de la corrupción.

La gestión de riesgos interna tiene un alcance más amplio que la gestión de riesgos externa, porque puede cubrir todo tipo de riesgos para los POB y las ACA. La valoración externa, por otra parte, aporta a los organismos información más precisa y equilibrada a la hora de ayudarlos a gestionar sus riesgos de integridad.

La metodología para la valoración interna y por la valoración externa es muy semejante. Estos dos tipos de valoración tienen sus puntos fuertes y sus puntos débiles respecto de la gestión concreta de la corrupción y el fraude (mirar Anexo).

1.2. Alcance

Esta guía:

- Contribuye a sensibilizar sobre aspectos de la lucha contra la corrupción (Convención de las Naciones Unidas contra la Corrupción, UNCAC, Art. 6);
- Busca establecer unos estándares mínimos;
- Define una política de gestión de riesgos común de conformidad con la política de l'EPA/EACN;
- Se centra en el aspecto práctico de la gestión de riesgos;
- Subraya la importancia de la gestión de riesgos y del análisis de riesgos;

- Se puede aplicar como herramienta para la prevención de la corrupción y para identificar riesgos de integridad;
- Está pensada para valoraciones tanto internas como externas;
- Constituirá un punto de partida para una buena administración;
- Busca proteger contra influencias ilícitas;
- Contribuye a impedir conflicto de intereses;
- Contribuye a identificar niveles y áreas de riesgos;
- Incluye métodos;
- Debería implementarse como parte del trabajo habitual, de un plan de integridad o de planes de acción y estrategias de lucha contra la corrupción nacionales, locales o sectoriales.

1.3 Lo que no ha de ser

Ni el grupo de trabajo ni la guía tienen como objetivo simplemente describir estándares, presentar estadísticas nacionales, elaborar un manual o diseñar una carpeta o folleto. La guía no será muy compleja ni utilizará términos ambiguos o poco claros.

1.4 Grupos destinatarios

- Fuerzas del orden
- Autoridades policiales
- Autoridades de la lucha contra la corrupción
- Organismos policiales de supervisión
- Instituciones y departamentos públicos.

1.5 Condiciones previas

Es necesario cumplir las siguientes condiciones previas:

- Compromiso de la dirección para establecer una cultura de integridad en los organismos;

- Compromiso de la dirección de implementar una gestión de riesgos (marcar el objetivo desde arriba);
- Integración de la guía en la policía nacional o en otro cuerpo policial;
- Disponibilidad de recursos (presupuesto, tiempo y recursos humanos);
- Formación específica previa y adquisición previa de ciertas competencias.

1.6 Formación y competencias

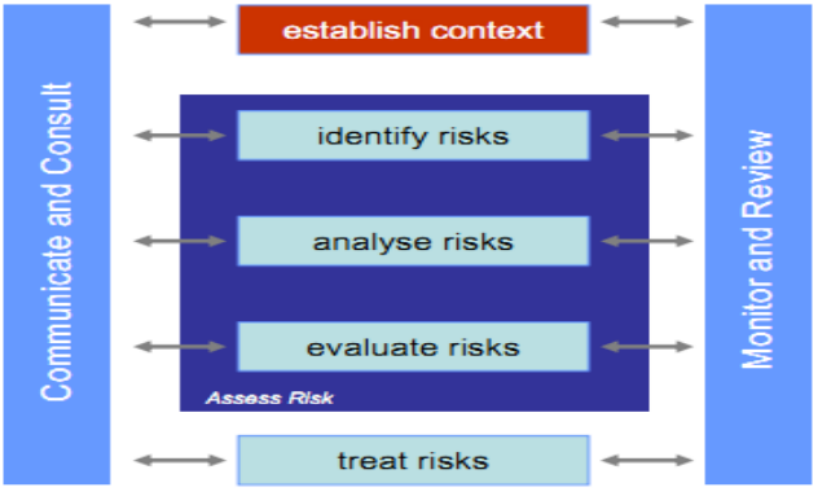
Para que funcione bien el sistema de análisis de riesgos y el sistema de gestión hace falta adquirir un conocimiento básico pero sólido de los métodos y la capacidad de aplicarlos en la práctica (ver también el capítulo 6).

2. Elementos clave de la gestión de riesgos de integridad

Para conseguir una gestión de riesgos de integridad de la calidad necesaria hace falta cumplir los elementos siguientes clave:

- Todos los principales procedimientos de trabajo en todos los campos de acción;
- Valoraciones jurídicas;
- Cultura institucional;
- Factores humanos.

2.2. Proceso de gestión de riesgos de integridad



Comunicar y consultar	Establecer contexto	Supervisar y revisar
	Identificar riesgos	
	Analizar riesgos	
	Evaluar riesgos *Valorar riesgo*	
	Tratar riesgos	

Fuente: Victorian Managed Insurance Authority (VMIA), Risk Management, de Stephen Owen (març 2010)

2.3 Identificación de riesgos de integridad

El proceso de gestión de riesgos de integridad debería de comenzar siempre por la identificación de riesgos. Por este motivo se consideran diversos métodos:

- Métodos creativos, *brainstorming*, talleres;
- Métodos de análisis de procesos;
- Análisis de escenarios posibles (creíbles) planteados en el peor de los casos;
- Análisis jurídicos;
- Estudios de caso y métodos de causas originales (Protocolo de Londres, Ishikawa, etc.);
- Métodos de mejores prácticas (ver 5.4);
- Seminarios web conducidos por las partes.

(Según ISO 31000)

2.4 Análisis y evaluación de riesgos de integridad

Una vez identificados los riesgos de integridad, deberán analizarse y evaluarse desde las perspectivas de probabilidad y consecuencia. Para facilitar este análisis, se recomienda utilizar una matriz como minino de 3x3

Probabilidad

Moderado	Mayor	Mayor
Menor	Moderado	Mayor
Menor	Menor	Moderado

Consecuencias 

Fuente: Versión adaptada de la metodología descrita en el Plan de Integridad de la Comisión para la Prevención de la Corrupción, República de Eslovenia.

El siguiente es un ejemplo de como es necesario clasificar niveles de probabilidad y consecuencia. Este modelo se puede adaptar al análisis pertinente y también se puede utilizar como base para matrices de 4 x 4, 5 x 5, etc.

Probabilidad		
1	**Muy improbable**	Una vez cada 5 años; el factor de riesgo no se ha producido nunca o solamente una vez.
2	**Probable (posible)**	Una vez al año; el factor de riesgo podría producirse en los próximos cinco años; podría repetirse varias veces.
3	**Muy probable (frecuente)**	Una vez cada seis meses; el factor de riesgo se producirá en los próximos cinco años; se repetirá varias veces.

Consecuencias		
1	**Menor**	Prácticamente no hay consecuencias.
2	**Moderado**	Las consecuencias tienen cierto impacto en la organización.
3	**Mayor (crítico a catastrófico)**	Las consecuencias son significativas.

Fuente: versión adaptada de la metodología descrita en el Plan de Integridad de la Comisión para la Prevención de la Corrupción, República d'Eslovenia.

De acuerdo con lo expuesto, un buen sistema de gestión de riesgo requiere descripciones de probabilidades y consecuencias hecho a medida en función de la especificidad de cada organismo.

2.4 Tratamiento de riesgos de integridad

Después de la identificación y el análisis de riesgos de integridad, es necesario tomar una decisión sobre la manera en que el tratamiento de riesgos tendrá en cuenta el nivel de tolerancia al riesgo del organismo. A continuación esta estrategia de tratamiento deberá ser incluida en un plan de integridad. En general, el riesgo no se elimina complemente solamente con aplicar el plan de integridad; solamente se reduce por debajo del nivel de tolerancia del riesgo.

A la hora de elegir un tratamiento de riesgos, conviene tener en cuenta la relación entre el riesgo genérico y el nivel de tolerancia del riesgo, así como el hecho de que las medidas de tratamiento del riesgo deberían ser proporcionales a las consecuencias posibles del riesgo.

Estos son los tipos más comunes de tratamiento de riesgos:

Evitar el riesgo: Cubre los procedimientos destinados a la prevención de riesgos. Básicamente, consiste en poner fin a una actividad que puede convertirse en un factor de riesgo. Como es lógico, los organismos públicos no puede optar nunca por este tipo de tratamiento, ya que sus actividades vienen determinadas por ley y no por decisiones individuales.

Traslado del riesgo: Significa que el organismo intenta encontrar un socio que se haga cargo del riesgo y también de la responsabilidad del tratamiento de riesgos, normalmente a cambio de compensación. Una forma típica es exteriorizar una

actividad determinada. Es necesario tener en cuenta, los riesgos secundarios que resultan de la externalización misma, lo que significa que, en general, la externalización no reduce el riesgo.

Mitigar riesgos: Este es el tratamiento más empleado que se puede aplicar para la mayoría de los riegos. La herramienta central para mitigar riesgos es un plan (el plan de integridad) que incluye las medidas necesarias para reducir el riesgo de manera que se mantenga por bajo del nivel de tolerancia el riesgo de la organización. Su objetivo puede ser, tanto reducir la probabilidad del riesgo, como elaborar medidas para reducir las consecuencias del riesgo.

Retener el riesgo: Este término se refiere a asumir conscientemente el riesgo. Puede ser un tratamiento útil en casos de riesgos genéricos relativamente menores o cuando el efecto previsto de otras formas de tratar los riesgos no fuera proporcionado a los gastos. También es posible, lógicamente, que el organismo simplemente no pueda hacer otra cosa que asumir el riesgo. No obstante, no hay que olvidar estos riesgos y evaluarlos periódicamente.

2.6 Opcional: Monitoreo y auditora externa

Se recomienda seguir también otros procedimiento de monitoreo y auditoria externa relativos a la aplicación de las medidas de gestión de riesgos para aumentar y garantizar su eficacia y eficiencia con parámetros e indicadores medibles.

3. Gestión de riesgos de integridad interna para ACA y POB

En el artículo 1.1. se explica la importancia de la aplicación de la gestión de riesgos para uso interno de las ACA y los POB.

Las ACA y los POB pueden implementar un sistema de gestión de riesgos con diferentes tipos de valoraciones, como por ejemplo:

- Análisis;
- Gestión de crisis y emergencias;
- Herramientas de informe y monitoreo;
- Nombramiento de una persona responsable de coordinar la gestión de riesgos;
- Herramientas de evaluación (quien controla y como? por ej. Organismos supervisores);
- Examen de la eficiencia, la idoneidad, el estado de implementación, etc . De las medidas adoptadas;

Estas valoraciones se pueden utilizar para todo tipo de riesgos (riesgos de incumplimiento, riesgos de seguridad, riesgos presupuestarios, etc.)

3.1. Marcar la tónica desde arriba

Es necesario considerar la gestión de riesgos como parte de todo liderazgo responsable, es decir, como una herramienta de gestión. Por tanto, los directivos superiores deberían poder:

- Dar ejemplo marcando la tónica desde los puestos superiores e intermedios;
- Desarrollar una política de riesgos con una estrategia y cultura determinadas;
- Definir claramente objetivos estratégicos;
- Fortalecer el organismo y hacer más seguro el entorno de trabajo;
- Sensibilizar sobre la gestión de buenas oportunidades;
- Utilizar procedimientos de trabajo establecidos como una herramienta educativa para nuevos empleados;

3.2. Riesgos de integridad

Los campos típicos en los cuales puede surgir riesgos de integridad son, por ejemplo:

- Contratación y administración de bienes;
- Conflicto de interés y favoritismo;

- Dar y recibir regalos;
- Incompatibilidades, restricciones y limitaciones;
- Restricciones post-ocupación;
- Influencias indebidas e ilícitas;
- Protección de denunciantes;
- Recursos humanos (contratación, motivación, disciplina);
- Gestión del conocimiento – pérdida de conocimientos prácticos;
- Transparencia y toma de decisiones;
- Patrocinios;
- Ámbito operativo;
- Tecnología, acceso y almacenamiento de archivos;
- TI, seguridad y protección de datos (personales);
- Irregularidades financieras;
- Propiedad intelectual;
- Recursos físicos y materiales (uso individuo, pérdida, etc.);
- Instrumentalización de las ACA y los POB (Influencias ilícitas)

3.3. Áreas de riesgo (perspectiva jurídica)

- Leyes y decretos (por ej. Delitos de corrupción y abuso de autoridad oficial, revelación de secretos oficiales, acuerdos ilegales de precios, blanqueo de dinero, fraude, apropiación indebida o malversación, derecho fiscal, etc.);
- Condiciones organizativas;
- Procedimientos de trabajo;
- Factores humanos.

3.4. Otras áreas de riesgo (si procede)

Si fuera necesario, los análisis se pueden extender a subcampos que presenten riesgos de incumplimiento y de corrupción asociados a riesgos estratégicos, operativos,

financieros, socio políticos o legales, o a riesgos medioambientales o de inversión. También se pueden aplicar en el contexto de edificios, protección contra incendios, etc.

3.5 Implementación.

Como se puede implementar la gestión de riesgos en su institución?

- Decide si la gestión de riesgos se implementará mediante un equipo de proyecto o siguiendo una jerárquica;
- Asignando responsabilidades y estableciendo un reglamento bien definido;
- Informando a todos los niveles de … (administración, personal);
- Visualizando los principales procedimientos de trabajo;
- Identificando riesgos (talleres, actos documentados, valoración desde el punto de vista de riesgos legales y de pérdida de reputación);
- Llevando a término una valoración de riesgos;
- Registrando y analizando incidentes y accidentes con el fin de volver a valorar los riesgos.

4. Gestión de riesgos de integridad externa a cargo de ACA y de POB

Como se explica en el artículo 1.1, la gestión de riesgos externa no es un proceso que tenga lugar totalmente fuera del organismo que ha de hacer frente a los riesgos de integridad. Al contrario, es una gestión de riesgos de integridad conducida externamente por algún evaluador externo, que suele ser una ACA o un POB, y en el cual, el organismo sometido a la valoración ha de tratar los riesgos que el evaluador ha identificado, analizado y evaluado. La gestión de riesgos de integridad externa representa sobretodo una herramienta de prevención de la corrupción utilizada normalmente por las ACA y los POB en cumplimiento de su cometido.

Visto que la metodología de la gestión de riesgos de integridad interna y la de la gestión externa es semejante, los artículos siguientes solo ilustrarán las características de la

valoración externa en los aspectos diferentes a los explicados en el capítulo 2 de esta guía.

4.1. Elección del organismo

La primera dificultad a la hora de realizar una valoración externa de riesgos de corrupción es priorizar y centrarse en organismos públicos especialmente vulnerables a al corrupción.

Los criterios para elegir un organismo para la gestión externa de riesgos de integridad podrían ser:

- Estadísticas sobre niveles de corrupción percibidos e investigados;
- Vulnerabilidad de actividades realizadas;
- Exposición al contacto directo con beneficiarios de servicios públicos;
- Aplicación insuficiente de políticas de lucha contra la corrupción nacionales y sectoriales.

4.2. Fuentes de información para la identificación de riesgos de integridad

Es muy importante confiar en fuentes de información objetivas durante el proceso de identificación de riesgos de integridad en otro organismo. Además de los métodos descritos en el artículo 2.3, otras fuentes de información pueden ser:

- Información sobre incidentes de integridad en el pasado;
- Reclamaciones de ciudadanos y otras informaciones que posean las ACA y los POB;
- Informes analíticos, encuestas, valoraciones, talleres, etc. sobre corrupción en la organización;
- Conclusiones de auditorias e inspecciones realizadas por organismos superiores y de supervisión;
- Información descubierta durante talleres;
- Prensa y otros medios.

4.3 Factores de riegos de corrupción

Al analizar los factores de la aparición de riesgos de corrupción (o los factores que la determinan), las ACA han de prestar especial atención a:

- Factores de riesgos externos;
- Factores de riesgos internos;
- Factores de riesgos operativos;
- Factores de riesgos individualizados.

4.4 Publicidad

A diferencia de la gestión interna de riesgos de integridad realizadas por las ACA y los POB que puedan cubrir un área de riesgo más amplia y que no se haga pública, la gestión externa de riesgos de integridad ha de intentar ser transparente. Es importante que el esfuerzo de lucha contra la corrupción y el fraude y de promoción de la integridad sean visibles al público.

En este sentido, un factor motivador de deseo del cambio en un organismo podría ser el reconocimiento de sus problemas de corrupción y un compromiso público para hacer crecer un clima de integridad. No obstante, la posibilidad de aplicar o no este enfoque dependerá del marco legal de cada país.

4.5 Aplicación de la guía en la formación de integridad y de lucha contra la corrupción

Esta herramienta se puede utilizar para actividades de prevención como actos informativos, seminarios, cursos de formación, *coaching* y talleres, o también para elaborar listas de peligros para la identificación de riesgos o para el análisis de riesgos con valoración, así como siempre que haya una necesidad concreta y se tengan los recursos necesarios.

El objetivo de un análisis de riesgos realizado y documentado en el marco de un taller es identificar los motivos de los riesgos, sus consecuencias y su probabilidad de aparición. El análisis deberá centrarse claramente en los riesgos de incumplimiento, es decir, en los motivos humanos y organizativos.

5. Requisitos mínimos para la gestión de riesgos y asesores de integridad

Los gestores de riesgos deberían estar integrados en el organigrama organizativo y sería necesario establecer procedimientos para el seguimiento constante de riesgos.

5.1. Competencias.

Los gestores de riesgos deberían tener conocimientos de los siguientes instrumentos de gestión del grado de cumplimiento:

- Desarrollo y aplicación de códigos de conducta y pautas de comportamiento;
- Medidas para potenciar la integridad;
- Comunicación y métodos de formación (metodología y didáctica);
- Establecimiento de un sistema de gestión del grado de cumplimiento;
- Instrumentos para implementar una cultura de integridad;
- En casos de emergencia: gestión de crisis y gestión de continuidad operativa, ej.
    - Comunicación con organismos públicos, autoridades de auditoria, departamentos de auditoria interna, auditores fiscalías y tribunales;
    - Tramitación profesional de casos.

5.2 Formación adicional

El gestor de riesgos y del grado de cumplimiento tiene la obligación de asistir periódicamente a formación adicional especializada para poder estar al día de la tecnología y la legislación del momento.

5.3. Resultado del aprendizaje y la adquisición de competencias

- Identificar, analizar, valorar, ilustrar y documentar riesgos en diferentes campos, sistemas o departamentos ministeriales;
- Comunicar a los cargos superiores las ventajas y el valor añadido de un análisis de riesgos y de un sistema de gestión de riesgos;
- Utilizar herramientas prácticas para identificar y valorar riesgos;
- Aplicar correctamente herramientas de análisis de riesgos y peligros;
- Dominar métodos de análisis de riesgos;
- Comprender y aplicar el tratamiento de errores y de herramientas de análisis de accidentes y causas (Protocolo de Londres, CIRS , ISHIKAA);
- Contribuir sustancialmente a la mejora de la transparencia en la empresa u organismo pertinente mediante una gestión de riesgos prospectiva en toda la organización.

5.4. Métodos para la formación de gestores de riesgos

- Conocimientos básicos adquiridos mediante lecturas y estudios previos;
- Conferencias;
- Ejercicios e interacción en talleres;
- Formación de comportamiento (para situaciones concretas);
- Mejores prácticas, métodos y estudios de caso;
- Discusión y reflexión.

6. Glosario básico

(1) **Riesgo:** Es el efecto de la incerteza respecto de los objetivos. Un efecto es una desviación positiva o negativa respecto a lo que estaba previsto.

(2) **Propietario del riesgo**: Es una persona o entidad a la cual se le otorga la facultad de gestionar un riesgo concreto y que asume la responsabilidad de esta gestión.

(3) **Valoración de riesgos:** Es un procedimiento que se compone en su entorno de tres procedimientos: Identificación de riesgos, análisis de riesgos y evaluación de riesgos.

(4) **Identificación de riesgos:** Es un procedimiento que implica el descubrimiento, el reconocimiento, y la descripción de riesgos que podrían afectar la consecución de los objetivos de una organización. Se utiliza para identificar posibles fuentes de riesgo además de los sucesos y circunstancias que podrían afectar al logro de los objetivos. También incluye la identificación de posibles causas y consecuencias potenciales. Resultado: lista de peligros, inventario de riesgos.

(5) **Análisis de riesgos:** Es un procedimiento que se utiliza por incluir, las fuentes y las causas de los riesgos que se han de identificar y para el cálculo estimado de niveles de riesgos. También se utiliza para estudiar el impacto y las consecuencias y para examinar los controles que existen actualmente. Los resultados se trasladan a una matriz.

(6) **Evaluación de riesgos:** Es un procedimiento que se utiliza para comparar los resultados del análisis de riesgos con criterios de riesgos con el fin de determinar si un nivel de riesgo concreto es aceptable o tolerable y que riesgos se abordarán primero.

(7) **Factor de riesgo:** Es la causa del riesgo. Suelen ser elementos que generan riesgos en el futuro. La aparición simultánea de más de un factor de riesgo puede aumentar la probabilidad do la consecuencia del riesgo, o las dos cosas.

(8) **Nivel de tolerancia del riesgo:** Es el nivel de exposición a riesgos que presenta el organismo y sobre el cual se aplicarán contramedidas. Debería establecerlo el director del organismo y viene condicionado por la cultura institucional, la disponibilidad de fuentes y las posibilidades técnicas.

(9) **Plan de integridad:** Es un documento aprobado por el director de la organización dirigido al tratamiento de riesgos de integridad. Un plan de integridad debería contener como mínimo: medidas para tratar los riesgos de integridad, plazos, responsabilidad de la implementación e indicadores de progreso. Para que un plan de integridad tenga éxito, son necesarios el compromiso de la dirección, la rendición de cuentas sobre su aplicación, un monitoreo imparcial y supervisión.

(10) **Tratamiento de riesgos:** Es un procedimiento de modificación de riesgos. Pueden haber distintas opciones de tratamiento: evitar el riesgo, eliminar la fuente de riesgo, modificar las consecuencias, cambiar las probabilidades o simplemente retener el riesgo.

(11) **Monitoreo de riesgos:** Es un procedimiento destinado a garantizar la correcta implementación de las medidas de tratamiento de riesgos y puede ser constante o periódico.

(12) **Protocolo de Londres:** Métodos de hipótesis para analizar episodios de daños que ya se han producido, que se utilizan para identificar riesgos y sus causas.

(13) **Sistemas de gestión de riesgos:** aplicación sistemática de principios de gestión y procedimientos para comunicar, identificar, analizar, evaluar, tratar, monitorizar y controlar riesgos. No es un elemento independiente pero si que forma parte integral de todos los procedimientos organizativos. Ayuda a los responsables de decisiones a actuar a partir de la información, a priorizar medidas y a elegir entre diversas soluciones posibles.

7.- Fuentes

- Versión adaptada de la metodología descrita en el Plan de Integridad de la Comisión para la Prevención de la Corrupción, República d'Eslovenia.
- Norma austriaca ONR 192050:2013, "Sistemas de gestión de cumplimiento (CMS) - requisitos y guía de aplicación"
- Norma austriaca ONR 49000-49003:2014 "Gestión de riesgos para organizaciones y sistemas - condiciones y principios".
- Valoración de riesgos de corrupción en instituciones públicas de l'Europa sud-oriental. Investigación i metodología comparativas preparadas para la iniciativa regional contra la corrupción (RAI) 2015.
- ISO 31000:2009, "Gestión de riesgos"
- ISO 37001:2016 "Sistemas de gestión anti soborno"
- Guía metodológica para el desarrollo de un entorno de control y un sistema de gestión de riesgos integrado, Servicio de Protección Nacional, Hungria.
- Convención de Naciones Unidas contra la corrupción (UNCAC)
- Victorian Managed Insurance Authority (VMIA), Risk Management, de Stephen Owen (març de 2010)

Anexo

Puntos fuertes y débiles de la valoración interna y de la valoración externa.

Tipos de valoración	Puntos fuertes	Puntos débiles
Valoración (o autovaloración) interna	-Procedimiento de valoración o medida basado en el conocimiento "desde dentro" del entorno y de los procedimientos de trabajo internos. - Procesos de aprendizaje y de desarrollo. - Puede ayudar a generar la confianza de los cargos públicos en aquello que se está haciendo. - Realizada con recursos internos.	- Riesgo de ser simplemente una lista de tareas pendientes o de mala calidad. -Posible falta de compromiso de los directivos o del personal. - Falta de conocimiento o de experiencia para hacer la valoración. - Requiere mucho tiempo.
Valoración externa	- En principio, mayor alcance de la valoración - Conocimiento experto y experiencias en metodología de valoración. - Valoración independiente y objetiva. - Requiere menos tiempo para el organismo que está siendo valorado.	- Valoración más profunda. - Procedimiento de valoración más sólido. - Posible ocultación de determinadas características o vulnerabilidades internas a los evaluadores externos. - Conocimiento superficial o insuficiente de los procedimientos de trabajo de la institución, el sector o el proyecto que está siendo valorado.

Fuente: "Valoración de riesgos de corrupción en instituciones pública de la Europa sud-oriental". Investigación y metodología comparativas preparadas para la iniciativa regional contra la corrupción (RAI) 2015.