4

GESTIÓN DEL RIESGO DE INTEGRIDAD


VLTRA

4.1 INTRODUCCIÓN

Un sistema de gestión de riesgos se define como el conjunto de acciones destinadas a dirigir y controlar los riesgos propios de una organización. Su finalidad es definir un marco de acción para saber qué aspectos gestionar y cómo hacerlo, sobre todo teniendo en cuenta que la gestión debe partir de la cuantificación de aquellos riesgos[12].

La gestión de estos riesgos en el marco de la integridad busca, en primer lugar, identificar todos aquellos posibles comportamientos o eventos futuros inadecuados, en un margen temporal previsible, que podrían producirse en el desarrollo de la actividad de la organización, tal y como está diseñada, y que pueden comprometer la consecución de sus objetivos y el respeto de los principios y normas que la inspiran.

En segundo lugar, la gestión de riesgos pretende establecer medidas que, conforme a los criterios y definiciones establecidos por los códigos o normativas de referencia, imposibiliten o, al menos, dificulten la ocurrencia de tales comportamientos o que minimicen sus consecuencias.

Un sistema de gestión de riesgos debe contemplar los procedimientos de prevención, detección y de respuesta a los riesgos. Asimismo, es un instrumento que permite evaluar la efectividad y debilidades de los controles internos de gestión, por lo que permite revisar los sistemas de control interno establecidos.

4.2 MARCO DE REFERENCIA DE LA GESTIÓN DEL RIESGO

El propósito del marco de referencia de la gestión del riesgo es asistir e intentar implicar a la organización en integrar la gestión del riesgo en todas sus actividades y funciones significativas.

Los componentes del marco de referencia y la manera en la que trabajan juntos han de adaptarse a las necesidades de la organización y se analizan en detalle en el anexo 4.2.

4.2.1 Marco normativo

Puede entenderse que en la actualidad la Administración General de Estado ya se ha dotado de un marco jurídico completo e integrado que define y aborda los escenarios

12 Definiciones en anexo 4.1.

y figuras relativas a la ética e integridad en el ejercicio de cargos públicos, en todas las componentes documentales que constituyen los instrumentos administrativos para su gestión, es decir, la explicativa, la dispositiva y, teniendo en consideración la materia objeto de estudio, los correspondientes códigos penológicos aplicables en los diversos niveles en los que puedan ser aplicables en virtud de su tipicidad y su carga de antijuridicidad.

El objetivo de la actuación propuesta pretende incidir en la componente explicativa de las diversas figuras típicas cuya comisión deriva en acciones contrarias a la ética y la integridad en el ejercicio de funciones públicas. Se asume que las componentes dispositivas y los diversos regímenes penológicos aplicables, por todos ampliamente conocidos, detallan, sin solución de continuidad, tanto su *iter* procedimental como, si fuera el caso, el procesal, para gestionar los supuestos de hecho de dichas acciones que constituyan presuntos incumplimientos, así como las empleadas y empleados públicos que gozan de las habilitaciones especiales para proceder con competencia debida, y llegada la circunstancia, para la tramitación, investigación y puniciones que procedieren.

Por todo ello, es necesario explicitar el marco normativo de referencia en materia de ética e integridad públicas que, bien entendido, toda unidad, organismo público, departamento y, en su totalidad la Administración General del Estado, deben asumir tanto en los códigos éticos, como en los modelos de gestión de riesgos y en la gestión de dichos riesgos cuando se materialicen las contingencias consistentes en la vulneración, por acción o por omisión y en el grado de comisión que sea.

Dicho marco normativo es la infraestructura que dota de homogeneidad necesaria en una materia. De este conjunto de normas se tomará la parte explicativa, como ya se ha adelantado.

En el ámbito de comisión con alcance administrativo, cuyo tratamiento penológico es el de falta administrativa:

a) Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Artículos 52 a 54. (Deberes de los empleados públicos. Código de Conducta). Artículos 93 a 98, especialmente el 95 (Régimen disciplinario).

b) Reglamento de Régimen Disciplinario de los funcionarios de la Administración del Estado, aprobado por Real Decreto 33/1986, de 10 de enero. Artículos 7-13, exceptuando el art. 6 que se rige por el TREBEP.

c) IV Convenio único para el personal laboral de la Administración General del Estado, registrado y publicado por Resolución de 13 de mayo de 2019, de la Dirección General de Trabajo. Artículos 99 y 100 (principios y responsabilidad disciplinaria). Artículos 101 a 104 (faltas).

d) Ley 53/1984, de 26 de diciembre, de Incompatibilidades del personal al servicio de las Administraciones Públicas.

e) Real Decreto 598/1985, de 30 de abril, sobre incompatibilidades del personal al servicio de la Administración del Estado, de la Seguridad Social y de los Entes, Organismos y Empresas dependientes.

f) Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

g) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (artículos 26 a 29).

En el ámbito de comisión con alcance penal, cuyo tratamiento penológico es el de delito:

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal:

a) Delitos contra las personas y agravadas en caso de cometerlas una empleada o empleado público en funciones o prevaliéndose de su condición y también de fuerza en las cosas: Arts. 167, 169-172, 173.1 (Acoso Laboral) 174-176; 177. bis.5; 178-183 (183.5); 184 (Acoso sexual y por razón de sexo); 188.2.c); 196; 198; 204; 205-216; 222; 233.2.

b) Delitos contra el patrimonio: 234-244.

c) Defraudaciones: estafa (248-251); administración desleal (252); apropiación indebida (253-256); frustraciones de ejecución-alzamientos de bienes (257-258); alteración de precios en concursos y subastas públicas (262); daños (263-267); corrupción en negocios (286 ter); daños a cosas de utilidad social (289); blanqueo de capitales (303); contra la Hacienda Pública y contra la Seguridad Social (306); contra los derechos de los trabajadores (311-318); contra los derechos de los ciudadanos extranjeros (318.bis.4); ordenación del territorio y el urbanismo y patrimonio histórico (320, 322-324); contra los recursos naturales y el medio ambiente (329); de riesgo catastrófico. relativos a la energía nuclear y a las radiaciones ionizantes (341-345); de los estragos (346-347); de riesgo provocados por explosivos y otros agentes (448-350); contra la salud pública (362.quater. 1.ª; 369.1. 1.ª; 372).

d) De las falsedades documentales (390-394; 397-398); usurpación de funciones públicas y del intrusismo (402-403).

e) Delitos contra la Administración Pública. De la prevaricación de los funcionarios públicos y otros comportamientos injustos (404-406); del abandono de destino y de la omisión del deber de perseguir delitos (407-409); de la desobediencia y denegación de auxilio (410-412); de la infidelidad en la custodia de documentos y de la violación de secretos (413-418; del cohecho (419-427 bis); del tráfico de influencias (428-431); de la malversación (432-435 bis); de los fraudes y exacciones ilegales (436-438); de las negociaciones y actividades prohibidas a los funcionarios públicos y de los abusos en el ejercicio de su función (439-444).

4.2.2 Marco organizativo

La norma UNE-ISO 31000 sobre gestión de riesgos establece en su marco de referencia la necesidad de que la alta dirección y los órganos de supervisión aseguren que la gestión del riesgo está integrada en todas las actividades de la organización y demuestren el liderazgo y compromiso en la puesta en marcha de la política de riesgos. Además, deben asegurar que la determinación de los roles para la rendición de cuentas

y la supervisión de la gestión del riesgo, como partes integrales de la gobernanza, se asignen adecuada y eficazmente.

Por su parte, el Manual sobre Integridad Pública de la OCDE también expresa claramente que la dirección tiene la responsabilidad primaria de crear y mantener un entorno de control que enfatice la integridad y establezca pautas positivas. Además, el compromiso de alto nivel contribuye a concienciar sobre los riesgos de integridad y ayuda a mejorar la puesta en marcha de las actividades de control.

Son numerosos los factores que inciden en la toma de decisiones sobre la gobernanza del sistema de gestión de riesgos (tamaño, organización del control interno, complejidad de los riesgos, análisis del contexto interno o externo, etc.). En todo caso, como se indica en el Manual de la OCDE, independientemente del enfoque que se adopte, resulta esencial que la entidad o función tenga líneas de notificación directas con la alta dirección, dada la responsabilidad general de esta última en la gestión de los riesgos de integridad.

En el momento actual, en todos los Estados miembros de la Unión Europea se deben aplicar medidas antifraude a aquellas actuaciones financiadas con fondos del Plan de Recuperación, Transformación y Resiliencia (PRTR), con independencia de que estas medidas puedan aplicarse con posterioridad al conjunto de las actuaciones y programas, ampliando de forma paulatina su alcance objetivo y subjetivo hasta incorporar la actividad integral del organismo que se considere.

En el marco del PRTR y de la exigencia de evaluación del riesgo de fraude dentro de los planes de medidas antifraude (artículo 6 de la Orden HFP/1030/2021) se han desarrollado unas Orientaciones para el refuerzo de los mecanismos para la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses, elaboradas por la Secretaría General de Fondos Europeos (en adelante Orientaciones), que incluyen unas consideraciones organizativas. En su parte introductoria se indica que «la propuesta tiene por objeto servir como referencia y ayudar a las diferentes entidades decisoras y ejecutoras a definir un modelo/sistema de gestión del riesgo de fraude en la ejecución del Plan de Recuperación, Transformación y Resiliencia. Con esta iniciativa, con fines orientativos, se abordan consideraciones funcionales y organizativas, que se deben concretar en el plan que se defina para cada ámbito (entidad decisora/entidad ejecutora), de la manera que se considere más adecuada para el cumplimiento de los requerimientos funcionales, atendiendo a su capacidad auto organizativa».

Sobre la base de estas orientaciones, el modelo organizativo propuesto para la gestión del Sistema de Integridad de la AGE propone una distribución de responsabilidades entre las figuras de la alta dirección, los coordinadores o coordinadoras de integridad, los comités de integridad departamentales y la Comisión de integridad institucional de carácter interdepartamental que se aplica al marco de referencia para la gestión de riesgos con arreglo al siguiente esquema:

1. Titulares de órganos directivos con rango de dirección general:

    a) Definir las diferentes responsabilidades para la realización del análisis y autoevaluación de riesgos de integridad de todo el órgano.

    b) Aprobar la evaluación de riesgos del órgano, al objeto de concretar la planificación de controles de gestión en función del riesgo detectado.

c) Aprobar los planes de tratamiento del riesgo y su actualización periódica, proponiendo los indicadores de riesgo aplicables, así como su adecuada documentación, seguimiento y revisión.

d) Velar por la comunicación al personal de la organización de la aprobación y actualización de los planes de actuación y del resto de comunicaciones que en relación con los mismos y sus medidas deban realizarse.

2. Coordinadoras y coordinadores de integridad institucional de ámbito departamental:

a) Supervisar la evaluación de riesgos realizada por la dirección del órgano.

b) Validar los planes de tratamiento del riesgo y su actualización.

c) Registrar las evaluaciones y planes de tratamiento del riesgo.

d) Validar los modelos de documentos necesarios para la prevención, detección, corrección y persecución del conflicto de intereses, el fraude y la corrupción y la documentación de las actuaciones relacionadas.

e) Proponer medidas correctoras y de mejora de los procedimientos relativos a la prevención, detección, corrección y persecución del conflicto de intereses, el fraude y la corrupción.

3. Comité de integridad institucional de carácter departamental:

a) Aprobar los objetivos e indicadores departamentales anuales de acuerdo con el Plan anual de integridad institucional de la AGE, sin perjuicio de aquellos casos en los que un determinado organismo considere oportuno recurrir a la aprobación de un plan de integridad específico, siempre que se encuentre alineado con la planificación general.

b) Aprobar el informe anual de seguimiento del cumplimiento de los objetivos e indicadores departamentales.

c) Aprobar las revisiones de los objetivos e indicadores departamentales anuales.

d) Aprobar el informe anual de seguimiento del cumplimiento de los objetivos e indicadores departamentales.

4. Comisión de integridad institucional de carácter interdepartamental:

a) Aprobar la memoria anual sobre las actuaciones desarrolladas por los distintos departamentos ministeriales en aplicación del Sistema de Integridad de la AGE, para su remisión al Consejo de Ministros.

b) Aprobar las revisiones del Sistema de Integridad de la AGE que les sean elevadas por los comités de integridad institucional o que se juzguen oportunas.

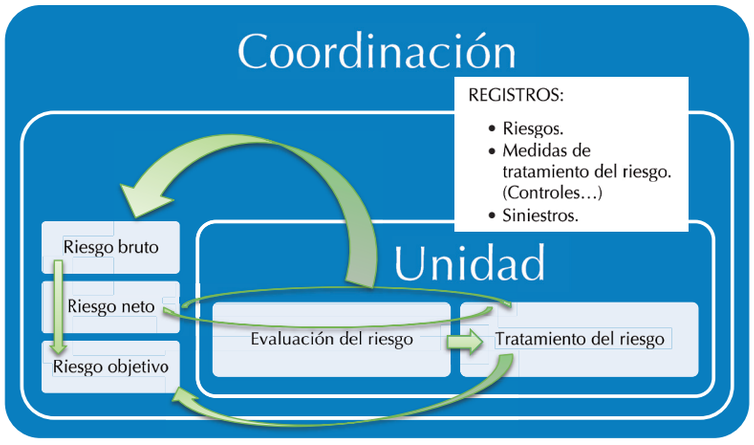
c) Aprobar el Plan anual de integridad institucional de la AGE.

Por último, ha de tenerse en cuenta que, si bien la dirección tiene la responsabilidad primaria de crear y mantener un entorno de control que enfatice la integridad y asuma la responsabilidad de la gestión de riesgos globalmente, también se precisa identificar las funciones y las responsabilidades de todas las personas que participen en el sistema y crear un equipo para evaluar los riesgos de integridad en toda la organización. La gestión de riesgos requiere la participación de una serie de personas en diferentes roles, como, por ejemplo, los superiores inmediatos, los gestores o gestoras de riesgos y los auditores internos (es decir, la primera, la segunda y la tercera línea de defensa, respectivamente). Todos ellos desempeñan un papel fundamental para garantizar la gestión de riesgos y el control interno.

4.3 MODELO PARA LA GESTIÓN DEL RIESGO

4.3.1 Esquema

El esquema de gestión de riesgos propuesto busca mantener la máxima simplicidad con el claro objetivo de que pueda ser aplicable por la AGE.



4.3.2 Fuentes

El modelo para la gestión de riesgos que se propone busca la sencillez, para facilitar su uso y va a partir, básicamente, de las siguientes fuentes, sin perjuicio del uso de otros materiales y documentación que se citan:

a) Norma UNE-ISO 31000, de marzo de 2018, sobre gestión de riesgos.

b) Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

c) Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia.

d) Ley 31/2022, de 23 de diciembre, de Presupuestos Generales del Estado para el año 2023.

e) Guía práctica de la Secretaría General de Fondos Europeos (Ministerio para la Transformación Digital y de la Función Pública) para la aplicación de la Orden HFP/55/2023, de 24 de enero.

f) Matrices de riesgo diseñadas por el Servicio Nacional de Coordinación Antifraude en su «Guía para la aplicación de medidas antifraude en la ejecución del Plan de Recuperación, Transformación y Resiliencia».

g) Principios del Marco Integrado de Control Interno. Modelo COSO III.

h) Directrices de la «Guía para las normas del control interno del sector público» de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI).

4.4 PROCESO DE GESTIÓN DEL RIESGO

El proceso de gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registros e informes de los riesgos. Este proceso debiera ser una parte integral de la gestión y de la toma de decisiones y se debería integrar en la estructura, las operaciones y los procesos de la organización. Puede aplicarse a nivel estratégico, operacional, de programas o de proyectos y sirve para la gestionar eficazmente los riesgos de integridad pública y realizar las evaluaciones de riesgo.

Se resumen a continuación algunos aspectos generales definidos en la norma ISO 31000.

4.4.1 Comunicación y consulta

El propósito de la comunicación y consulta es apoyar a las partes interesadas pertinentes a comprender los riesgos, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la concienciación y la comprensión de los riesgos, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.

4.4.2 Alcance, contexto y criterios

El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión de riesgos, para permitir una evaluación de riesgos efectiva y un tratamiento apropiado de los mismos.

4.4.3 Evaluación del riesgo

«La evaluación del riesgo es el proceso general de identificación de riesgos, análisis de riesgos y valoración de riesgos» (ISO 31000:2018). Constituye un instrumento de apoyo para la planificación y el proceso de toma de decisiones, contribuyendo así a la consecución de los objetivos de la entidad.

4.4.3.1 Identificación del riesgo

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos (ISO).

Este proceso requiere un conocimiento detallado de la entidad, que permita la identificación de los riesgos, tanto si las fuentes están bajo su control como si no es así. Por tanto, debe abordarse de forma metódica para asegurar:

a) La identificación de todas las actividades y procesos de la organización.

Para la *Federation of European Risk Management Associations* (FERMA), las actividades, procesos y decisiones de las entidades pueden clasificarse en distintas categorías, que incluirían las siguientes:

i. Estratégicas: Se refieren a los objetivos estratégicos a largo plazo. Pueden estar condicionadas por los riesgos políticos, los cambios legales, la reputación y los cambios en el entorno físico.

ii. Operacionales: Se refieren a los problemas cotidianos a los que se enfrenta la administración para la consecución de sus objetivos estratégicos.

iii. Financieras: Se refieren a la gestión efectiva y al control del presupuesto.

iv. Gestión del Conocimiento: Se trata de la gestión efectiva y del control de los recursos del conocimiento, la producción, protección y comunicación de los mismos. Los factores externos pueden incluir el uso sin autorización o el abuso de la propiedad intelectual, los fallos en el área de energía y la competencia tecnológica. Entre los factores internos se pueden incluir el mal funcionamiento de los sistemas o la pérdida de personal clave.

v. Conformidad: Se refiere a temas como salud y seguridad, medioambiente, descripción comercial, protección del consumidor, protección de datos, prácticas de empleo.

b) La identificación de los factores de riesgo asociados a dichas actividades y procesos.

Para identificar los factores de riesgo que afectan a cada uno de los procesos, se puede partir del conocimiento de los propios gestores o gestoras, así como de diferentes fuentes de información tales como informes internos y externos, informes de auditoría, resoluciones judiciales, denuncias, experiencias similares de otras organizaciones, entrevistas y cuestionarios.

Respecto a los factores de riesgo que afectan a la ética e integridad de la Administración Pública, se pueden señalar los siguientes:

i. Riesgo de conflicto de intereses: situación en la que una persona debe optar entre las responsabilidades de su puesto y sus propios intereses privados.

ii. Riesgo de favoritismo: trato de favor que se da a una persona en perjuicio de otras que también lo merecían en la misma o mayor medida.

iii. Riesgo de nepotismo: preferencia que se otorga a parientes para concesiones o empleos públicos.

iv. Riesgo de soborno: oferta, promesa, aceptación o exigencia de un incentivo para realizar una acción ilícita o contraria a la ética.

v. Riesgo de malversación: utilización deshonesta e ilícita de fondos y bienes públicos para fines de enriquecimiento personal.

vi. Riesgo de fraude: engaño deliberado para obtener una ventaja indebida o ilícita.

vii. Riesgo de colusión: acuerdo secreto entre partes que confabulan para engañar y defraudar y así obtener una ventaja económica ilícita.

c) La identificación de los riesgos.

El objetivo de la descripción e identificación de riesgos es mostrar los riesgos identificados de una forma estructurada, clara y precisa que permita la elaboración del mapa de riesgos de la organización.

En el siguiente cuadro se detalla la descripción del riesgo que realiza FERMA:

Nombre del riesgo.	Identificación del riesgo.
Alcance del riesgo.	Descripción cualitativa de los sucesos, su tamaño, tipo y número.
Naturaleza del riesgo.	Estratégico, operacional.
Interesados.	Interesados y sus expectativas.
Cuantificación del riesgo.	Importancia y probabilidad.
Tolerancia al riesgo.	Potencial de pérdida e impacto financiero del riesgo Probabilidad y tamaño de las pérdidas potenciales. Objetivo del control del riesgo y nivel deseado de cobertura.
Tratamiento del riesgo y mecanismos de control.	Medios por los que se gestiona el riesgo actualmente Niveles de confianza en el control existente. Identificación de protocolos de supervisión y revisión.
Acción potencial de mejora.	Recomendaciones para reducir riesgos.
Política y estrategia para desarrollar.	Identificación de la persona responsable.

4.4.3.2 Análisis del riesgo

Mediante el análisis del riesgo se determina la graduación del riesgo teniendo en cuenta su probabilidad de ocurrencia y la magnitud de las consecuencias, impacto, en caso de que llegue a producirse (riesgo = probabilidad de la amenaza x impacto).

i. Probabilidad del riesgo: Es la posibilidad de materialización del riesgo analizado.

Se trata de una probabilidad teórica puesto que el riesgo cero no existe. Por tanto, es necesario determinar dicha probabilidad a través de escalas cualitativas o cuantitativas, que cuenten con diversos escenarios.

ii. Impacto del riesgo: Es el conjunto de consecuencias (tanto económicas, como reputacionales, operativas, etc.) que tendría para la organización el hecho de que el riesgo llegara a materializarse.

Al igual que la probabilidad, el impacto se determina por medio de escalas. Cada entidad, teniendo en cuenta su metodología y objetivos definirá la tipología, número y nomenclatura del impacto.

iii. Matriz de riesgos. La matriz de riesgos muestra una escala de la gravedad de los riesgos teniendo en cuenta la probabilidad de ocurrencia y la gravedad de las posibles consecuencias. El resultado final del proceso será la priorización de los riesgos asignando a cada uno de ellos una categoría de probabilidad e impacto.

4.4.3.3 Valoración del riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:

a) No hacer nada más.

b) Considerar opciones para el tratamiento del riesgo.

c) Realizar un análisis adicional para comprender mejor el riesgo.

d) Mantener los controles existentes.

e) Reconsiderar los objetivos.

Las decisiones deberían tener en cuenta un contexto más amplio y las consecuencias reales y percibidas por las partes interesadas externas e internas.

Los resultados de la valoración del riesgo se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.

4.4.4 Tratamiento del riesgo

Después de identificar y evaluar los riesgos, el siguiente paso es determinar si se debe responder y cómo hacerlo. Esta etapa implica la evaluación de los resultados del análisis de riesgos con respecto a criterios de riesgo específicos (es decir, las tolerancias) y luego perfeccionar la estrategia de la organización para mitigar los riesgos. Los criterios de riesgo refieren al nivel de riesgo que una organización está dispuesta a aceptar. Las tolerancias son criterios que actúan como umbrales para facilitar la toma de decisiones y asegurar que los controles sean eficaces y proporcionados.

Estos criterios deben determinarse de antemano por la alta dirección antes de realizar las evaluaciones de los riesgos y deben estar en consonancia con las políticas, los reglamentos y los objetivos de la organización.

Identificar y actuar sobre todos los riesgos es poco realista. Los criterios de riesgo ayudan a la alta dirección a decidir si aceptan, evitan, reducen o comparten el riesgo. Si las medidas de control son eficaces para mantener el riesgo por debajo o en el umbral establecido por los criterios de riesgo, entonces la aceptación del riesgo residual podría ser la medida más eficaz y eficiente en función de los recursos. Si se determina que las actividades de control no logran atenuar los riesgos hasta el nivel aceptable, los administradores deberán evitar, reducir o compartir el riesgo.

Evitar el riesgo implica el cese de la política o de las operaciones vinculadas a él. Algunos riesgos son inevitables. La reducción de esos riesgos implica la adaptación de los procedimientos y las actividades de control para disminuir su probabilidad y su impacto. Por último, compartir el riesgo es más común en el contexto empresarial, pero también puede ocurrir en el sector público. Normalmente, implica la adopción de alguna medida para transferir el riesgo a un tercero, como una compañía de seguros.

El objetivo del tratamiento del riesgo es seleccionar y poner en marcha opciones para abordar el riesgo.

Por tanto, el tratamiento del riesgo implica la selección y el acuerdo para aplicar una o varias opciones para reducir la probabilidad de que los riesgos ocurran, los efectos de los riesgos, o ambas cosas, así como la implantación de estas opciones.

A continuación de esto, sigue un proceso crítico de reapreciación del nuevo nivel de riesgo, con la intención de determinar su tolerancia con respecto a los criterios previamente establecidos, para decidir si se requiere tratamiento adicional.

El tratamiento del riesgo implica un proceso iterativo de:

a) Formulación y selección de opciones para el tratamiento del riesgo.

b) Planificación y puesta en marcha del tratamiento del riesgo.

c) Evaluación de la eficacia de ese tratamiento.

d) Decisión acerca de si el riesgo residual es aceptable y, si no es aceptable, efectuar tratamiento adicional.

Los controles son medidas implementadas por las organizaciones para modificar los riesgos que posibilitan el logro de los objetivos. Los controles pueden modificar el riesgo mediante el cambio de cualquier fuente de incertidumbre (por ejemplo, haciendo más o menos posible que algo ocurra) o cambiando el rango de consecuencias posibles y dónde pueden ocurrir.

4.4.4.1 Selección de las opciones para el tratamiento del riesgo

La selección de las opciones más apropiadas para el tratamiento del riesgo implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos y los costes, esfuerzo o desventajas de la puesta en marcha.

Las opciones de tratamiento del riesgo no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias. Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:

a) Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo.

b) Aceptar o aumentar el riesgo en busca de una oportunidad.

c) Eliminar la fuente de riesgo.

d) Modificar la probabilidad.

e) Modificar las consecuencias.

f) Compartir el riesgo (por ejemplo: a través de contratos de seguros).

La justificación para el tratamiento del riesgo es más amplia que las simples consideraciones económicas y debería tener en cuenta todas las obligaciones de la organización, los compromisos voluntarios y los puntos de vista de las partes interesadas. La selección de las opciones para el tratamiento del riesgo debería realizarse de acuerdo con los objetivos de la organización, los criterios del riesgo y los recursos disponibles.

Al seleccionar opciones para el tratamiento del riesgo, la organización debería considerar el involucrar potencialmente a las partes interesadas y los medios más apropiados para comunicarse con ellas y consultarlas.

El tratamiento del riesgo a su vez puede introducir nuevos riesgos que necesiten gestionarse.

Si no hay opciones disponibles para el tratamiento o si las opciones para el tratamiento no modifican suficientemente el riesgo, este se debería registrar y mantener en continua revisión.

Las personas que toman decisiones y otras partes interesadas deberían ser conscientes de la naturaleza y el nivel del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y ser objeto de seguimiento, revisión y, cuando sea apropiado, de tratamiento adicional.

4.4.4.2 Preparación y puesta en marcha de los planes de tratamiento del riesgo

El propósito de los planes de tratamiento del riesgo es especificar la manera en la que se pondrán en marcha las opciones elegidas para el tratamiento, de manera tal que las personas involucradas comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado.

Los planes de tratamiento deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas. La información proporcionada en el plan del tratamiento debería incluir:

a) El fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados.

b) Las personas que rinden cuentas y aquellas responsables de la aprobación y puesta en marcha del plan.

c) Las acciones propuestas.

d) Los recursos necesarios.

e) Las medidas del desempeño.

f) Las restricciones.

g) Los informes y seguimiento requeridos.

h) Los plazos previstos para la realización y la finalización de las acciones.

Hay que determinar quién se responsabiliza de cada medida establecida, además de cuándo y cómo se tienen que llevar a cabo o preparar.

Habrá que seleccionar e implantar medidas que permitan actuar contra cada factor de riesgo y reducir, así, la probabilidad de los riesgos, así como medidas para reducir la gravedad de los efectos de los riesgos.

En los planes de tratamiento del riesgo habrá que:

a) Determinar las medidas a implantar.

b) Asignar a una persona responsable para cada medida, que será la encargada de su implantación y seguimiento, o de definirla y establecer las alertas que indicarán que hay que ponerla en marcha.

c) Hacer una previsión de los recursos necesarios para su puesta en marcha.

d) Establecer una fecha límite de esta puesta en marcha o para disponer los procesos, protocolos o herramientas necesarias para su puesta en marcha.

e) Definir la forma y periodicidad del seguimiento en cada caso.

4.4.5 Seguimiento y revisión

4.4.5.1 Consideraciones generales

El seguimiento y la revisión son dos actividades diferenciadas cuyo propósito es asegurar y mejorar la calidad y la eficacia del diseño, la puesta en marcha y los resultados del proceso.

El seguimiento considera la vigilancia rutinaria del desempeño real y su comparación con el desempeño requerido o esperado. Involucra la comprobación o investigación, la supervisión, la observación continua.

La revisión involucra la comprobación periódica o de improviso, para detectar cambios en el ambiente, en las prácticas de la industria o en las prácticas de la organización. Esta actividad se lleva a cabo para determinar la idoneidad, adecuación y

eficacia del marco de trabajo y el proceso para lograr los objetivos establecidos. Las revisiones deberían considerar las salidas de las actividades de seguimiento.

El seguimiento y la revisión están dirigidos a aportar seguridad razonable de que los riesgos se gestionan adecuadamente, a identificar deficiencias en la gestión del riesgo, a identificar oportunidades de mejora de la gestión de los riesgos y a determinar si han ocurrido cambios que precisan ajustes o actualización del marco de trabajo o de algún aspecto del proceso. Ambos son necesarios para asegurar que la organización mantiene una comprensión actualizada de sus riesgos en relación con sus criterios de riesgo, en coherencia con su actitud de riesgo. Ambos requieren un enfoque sistemático integral a los sistemas de gestión generales de la organización.

Los riesgos, sus controles y tratamientos subyacentes se pueden modificar con el tiempo, y las personas responsables de la gestión del riesgo necesitan ser conscientes de las implicaciones de estos cambios. Los fallos en los tratamientos pueden conducir a que el riesgo sea inaceptable.

El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados debería ser una parte planificada del proceso en su conjunto, con responsabilidades claramente definidas.

El seguimiento y la revisión deberían tener lugar en todas las etapas del proceso. El seguimiento y la revisión incluyen planificar, recopilar y analizar información, registrar resultados y proporcionar retroalimentación.

La responsabilidad general de las actividades de seguimiento y revisión reside en el órgano de supervisión y en la alta dirección, no en quienes proveen el aseguramiento, por ejemplo, la auditoría interna.

Los resultados del seguimiento y la revisión deberían incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.

4.4.5.2 Seguimiento

El objetivo de realizar un seguimiento periódico será valorar la efectividad de todas las medidas preventivas, así como identificar nuevos riesgos que haya que analizar, evaluar y tratar. Igualmente, el seguimiento también deberá prever la revisión y actualización, si conviene, de las medidas contingentes, así como de las alertas previamente definidas.

Los enfoques típicos para el seguimiento incluyen los siguientes:

a) Los coordinadores y coordinadoras de integridad institucional[13] pueden analizar el ambiente para supervisar los cambios de contexto. La frecuencia de esta revisión dependerá del nivel de riesgo y de la dinámica de tales cambios en el contexto. El dueño del riesgo compara los factores internos o externos pertinentes contra la declaración del contexto para determinar si ha ocurrido un cambio importante. Esto puede requerir la comunicación y consulta periódica

13 Ver 5.3.2.

con las partes involucradas para determinar si sus puntos de vista y objetivos han cambiado.

b) Los coordinadores y coordinadoras de integridad institucional también deberían supervisar los planes de tratamiento de riesgos para determinar las acciones oportunas y responder a cambios en el ambiente.

c) Los coordinadores y coordinadoras de integridad institucional son responsables del seguimiento de los controles que les han sido asignados, que pueden involucrar la comprobación periódica o el seguimiento continuo.

El seguimiento debería ser parte integral de la gestión. Los riesgos y controles se deberían asignar a las personas que tienen asignada la autoridad para gestionarlos (dueños o dueñas del riesgo), quienes son responsables de su seguimiento. Esta responsabilidad se debería registrar en las descripciones de puesto o de cargo.

La forma en que la alta dirección reacciona a los resultados del programa de seguimiento puede afectar el comportamiento de los empleados y empleadas, y es importante que la alta dirección actúe dando ejemplo como modelo a seguir.

4.4.5.3 Revisión

La alta dirección debería llevar a cabo periódicamente la revisión de procesos, sistemas y actividades para asegurar que no hayan surgido nuevos riesgos y que los controles y tratamiento de riesgos continúen siendo idóneos y eficaces. Estas revisiones se deberían programar.

Para estas revisiones se pueden usar las mismas técnicas que para el seguimiento regular, pero si las realiza alguien que no está involucrado directamente en la operación de los procesos, pueden proporcionar un análisis más objetivo. La frecuencia de la revisión se puede ver influenciada por el nivel de riesgo, el ciclo de planificación del negocio, la dinámica en el ambiente, el contexto o por el acuerdo con el órgano de gobierno que es responsable de supervisar los riesgos y la gestión de éstos.

Cuando se planifican cambios organizacionales o se detectan cambios externos, puede haber cambios en el ambiente externo o interno, o las partes involucradas y sus puntos de vista; el contexto de gestión del riesgo, los objetivos de la organización y sus criterios de riesgo; los riesgos y sus diferentes niveles; la necesidad de tratamientos para los riesgos; el efecto y la eficacia de los controles.

Por esta razón, es esencial que las organizaciones revisen sus riesgos, sus tratamientos y controles para los riesgos, cuando desarrollan o actualizan planes de negocio o planes estratégicos. Debido a que los planes de negocio y los planes estratégicos pueden crear o actualizar los objetivos de una organización, es de gran valor usar el proceso de evaluación del riesgo para enfatizar en llevar a cabo pruebas a los borradores de los planes, con el fin de asegurar que los objetivos propuestos se pueden lograr, y también para definir la medida de tratamiento de riesgos requerida para asegurar resultados satisfactorios. Quienes llevan a cabo procesos de gestión del riesgo también deberían revisar regularmente sus experiencias y resultados para identificar oportunidades de mejora.

Como parte del proceso de gestión del riesgo, los riesgos y los controles se deberían monitorizar y revisar de manera regular, con objeto de verificar que:

a) Las hipótesis establecidas en relación con los riesgos continúan siendo válidas.

b) Las hipótesis en que se ha basado la apreciación del riesgo, incluyendo los contextos externo e interno, continúan siendo válidas.

c) Si se han logrado los resultados previstos.

d) Los resultados de la apreciación del riesgo están en línea con la experiencia real.

e) Las técnicas de apreciación del riesgo se han aplicado adecuadamente.

f) Los tratamientos del riesgo son eficaces.

Las revisiones deberían incluir el examen del marco de trabajo, los procesos, los propios riesgos y los cambios en el ambiente.

Los resultados de este paso se retroalimentarán en el contexto y en otras funciones, de manera que se puedan identificar los nuevos riesgos, se puedan descubrir los riesgos existentes, y se pueda registrar el estado de ejecución del marco de trabajo, para mejora.

Si se encuentran problemas, la organización debería considerar cómo sucedieron y por qué no se detectaron antes.

4.4.6 Registros e informes

El proceso de la gestión del riesgo y sus resultados se deberían documentar e informar a través de los mecanismos apropiados. El registro e informe pretenden:

a) Comunicar las actividades de la gestión del riesgo y sus resultados a la organización.

b) Proporcionar información para la toma de decisiones.

c) Mejorar las actividades de la gestión del riesgo.

El informe es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades.

Los factores para considerar en el informe incluyen, pero no se limitan a:

a) Las diferentes partes interesadas, sus necesidades y requisitos específicos de información.

b) El coste, la frecuencia y los tiempos del informe.

c) El método del informe.

d) La pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.

e) Informar del proceso de revisión.

El informe debería aportar información a la alta dirección, a los coordinadores o coordinadoras de integridad institucional y a las partes interesadas acerca de si los riesgos de la organización están dentro de sus criterios de riesgo, o si cuenta con planes creíbles de tratamiento de riesgos que finalmente conducirán a este resultado. Adicionalmente, puede aportar información acerca de riesgos nuevos y emergentes.

Se deberían establecer procesos para asegurar que las recomendaciones sean consideradas activamente por la dirección de la organización, y las respuestas acordadas se ejecuten. Las acciones en respuesta a las revisiones se deberían informar a los coordinadores o coordinadoras de integridad institucional y supervisar rutinariamente hasta su puesta en marcha.

4.5 DOCUMENTACIÓN DE UN SISTEMA DE GESTIÓN DE RIESGO

4.5.1 Identificación de riesgos: catálogos

El autodiagnóstico de riesgos es la piedra angular del sistema preventivo, mediante cuestionarios y una estructura de desglose de riesgos.

Resulta conveniente la existencia de un catálogo que contenga los principales riesgos como base de este.

El autodiagnóstico podrá considerar las contingencias de la organización (sentencias judiciales desfavorables o pendientes de ejecución, reclamaciones de responsabilidad patrimonial, recursos, resultados de auditorías previas e informes de control e información obtenida de diversas fuentes, tales como los canales de denuncias en el caso de que ya existan).

En primer lugar, se identificarán las áreas de riesgos, a partir de información ya existente o directamente a través de entrevistas y talleres, cuestionarios y encuestas. La Orden HFP/1030/2021 contiene como medidas preventivas del fraude y de la corrupción la implantación de mecanismos adecuados de evaluación del riesgo para todas las medidas gestionadas, dejando evidencia, en busca de las partes del proceso más susceptibles de sufrir fraude, y controlarlas especialmente, sobre la siguiente base:

a) Identificación de medidas que son más susceptibles del fraude, como pueden ser aquellas con alta intensidad, alto presupuesto, muchos requisitos a justificar por la persona solicitante, controles complejos, etc.

b) Identificación de posibles conflictos de intereses.

c) Resultados de trabajos previos de auditorías internas.

d) Resultados de auditorías del Tribunal de Cuentas.

e) Resultados de auditorías de la Comisión Europea o del Tribunal de Cuentas Europeo, en su caso.

f) Casos de fraude detectados con anterioridad.

En el informe sobre integridad pública en la Administración General del Estado de junio de 2021 se identifican como áreas de riesgo en las administraciones públicas las de contratación, subvenciones, gestión económica y recursos humanos, y deja abierta la posibilidad de que los departamentos puedan identificar otras diferentes en su ámbito, si bien se pueden añadir:

a) Gestión económica y presupuestaria, tesorería, recursos financieros, prepuestos. Todos aquellos servicios cuya prestación genera una obligación de pago para las dependencias y entidades.

b) Contratación, encargos, convenios, subvenciones, etc., en materia de obra pública, o todas aquellas áreas relacionadas con la creación, mantenimiento o destrucción de construcciones.

c) Recursos humanos. Están relacionados con el reclutamiento, capacitación y pago de salario del personal.

d) Recursos materiales Consisten en la administración y distribución de bienes, insumos y servicios, así como en el manejo de almacenes a nivel general.

e) Tecnologías de información. Relacionadas con la transformación digital y la inclusión de tecnologías en la actividad de la AGE, citándose así la inteligencia artificial, *blockchain*, aplicaciones sobre base de protocolo 5G, etc.

f) Creación y corrección normativa.

g) Permisos, concesiones y autorizaciones.

h) Procedimientos sancionadores.

i) Transparencia. Son acciones enfocadas en permitir y garantizar el acceso a la información pública.

j) Inspección y auditoría. Consisten en actividades independientes, objetivas y sistemáticas que tienen el propósito de evaluar la actuación y el resultado de las entidades y todas aquellas series de acciones encaminadas a proporcionar un grado de seguridad razonable en la consecución de los objetivos y metas de la institución.

A partir de una lista de riesgos exhaustiva pero genérica, cada organización debe tener como objetivo seleccionar su propia lista. Este paso se realiza a menudo en el contexto de un ejercicio de reflexión que involucra a miembros clave del equipo de toda la organización (TI, Planificación Estratégica, Operaciones, Departamento Legal, Recursos Humanos y Seguridad). Esto no solo conduce a que se compile una lista completa, sino que también ayuda a la hora de apoyar el ejercicio. La «lista de riesgo» final, entonces debe comprobar la coherencia con la organización y los procesos de gestión de riesgos previstos[14].

14 Anexo 4.3.

4.5.2 Análisis de riesgos: mapa de riesgos

El siguiente paso en la detección de riesgos es la evaluación de los riesgos derivados de diversas situaciones. Esto implica:

a) Estimar la frecuencia de los riesgos.

b) Estimar la posible gravedad de los riesgos, por ejemplo, bajo, medio y alto.

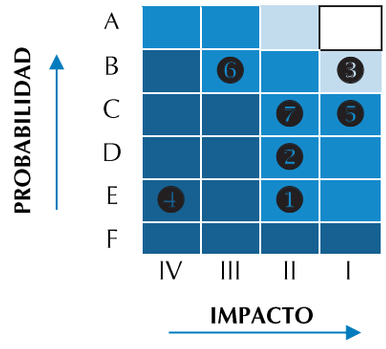
c) Tomar en cuenta los factores de contrapeso para limitar la frecuencia o la gravedad de los riesgos y comprender los posibles procesos de control.

Para esto existen diferentes herramientas.

El mapa de riesgos es una herramienta de visualización de datos para comunicar los riesgos específicos que enfrenta una organización. El objetivo de un mapa de riesgos es mejorar la comprensión de una administración de su perfil de riesgo, y pedir aclaraciones sobre la naturaleza y el impacto de los riesgos. Los mapas de riesgo pueden ser herramientas útiles para explicar y comunicar diversos riesgos para la alta dirección y las empleadas y empleados.

Hay una gran variedad de representaciones de los mapas de riesgo.

a) Pueden, por ejemplo, ser presentados como una matriz. Por ejemplo, se puede trazar la probabilidad de que ocurra un riesgo en el eje y, mientras que el impacto del mismo riesgo se representa en el eje x.



El «Instrumento de autoevaluación para la identificación y cobertura del riesgo» (matriz de riesgos) se centra en la identificación de los riesgos potenciales con impacto significativo, así como en la definición de mecanismos (indicadores de riesgo, controles y acciones) que permiten su gestión, seguimiento y mitigación.

La matriz de riesgos identifica una batería de riesgos que se asocian a cada uno de los instrumentos de gestión que pueden ser utilizados durante la ejecución de las actuaciones.

La matriz de riesgos puede componerse de dos instrumentos de autoevaluación de riesgos, iterativos, que se retroalimentan, y cuya utilización dependerá del momento en el que se realice la evaluación y de los agentes intervinientes: la matriz *ex ante* y la matriz *ex post*.

La matriz *ex ante* es un instrumento de carácter informador cuyo objetivo es medir, a través de un cuestionario de autoevaluación, la exposición teórica al riesgo de los métodos de gestión en virtud del histórico y de la experiencia previa de la entidad y de los procedimientos implantados a partir de los sistemas de gestión y control. En este sentido, permite determinar la probabilidad de suceso de los riesgos de una entidad y señalar los controles puestos en marcha por dicha entidad para mitigar el riesgo.

La matriz *ex post* es un instrumento que permite medir el nivel de materialización del riesgo por método de gestión. Presenta una estructura paralela a la matriz *ex ante*, es decir, incluye los mismos riesgos y banderas asociados a cada método de gestión que ya han sido evaluados previamente.

La principal referencia en lo que respecta a matrices de riesgos, la constituye la propuesta por la Comisión en sus Orientaciones para la Evaluación del riesgo de fraude (EGESIF 14-0021), a partir de la cual se han elaborado las siguientes:

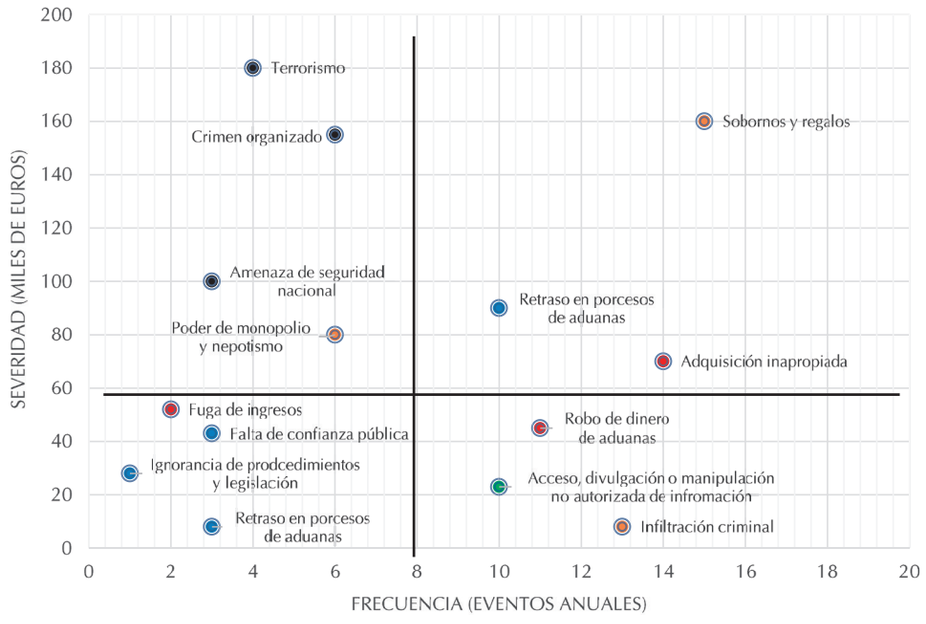
i. Instrumento de autoevaluación para la identificación y cobertura del riesgo (Matriz de riesgos) [Unidad Administradora del Fondo Social Europeo (UAFSE)] 50.

ii. Herramienta de la Guía para la aplicación de medidas antifraude en la ejecución del Plan de Recuperación, Transformación y Resiliencia.

b) Los mapas de riesgo también se pueden ilustrar con un mapa de calor, usando colores para ilustrar el nivel de riesgos al que las sucursales individuales están expuestas.

Probabilidad					
Casi seguro (5)	Medio (5)	Medio (10)	Alto (15)	Extremo (20)	Extremo (25)
Frecuente (4)	Bajo (4)	Medio (8)	Alto (12)	Alto (16)	Extremo (20)
Posible (3)	Bajo (3)	Medio (6)	Medio (9)	Alto (12)	Alto (15)
Improbable (2)	Bajo (2)	Bajo (4)	Medio (6)	Medio (8)	Medio (10)
Remoto (1)	Bajo (1)	Bajo (2)	Bajo (3)	Bajo (4)	Medio (5)
	Insignificante (1)	Menor (2)	Moderada (3)	Mayor (4)	Severa (5)
			Consecuencias		

c) Otras representaciones pueden ayudar a visualizar cómo se agrupan los riesgos y comprender la relación que existe entre los riesgos. Por ejemplo, los riesgos se muestran en una cuadrícula de gravedad y frecuencia después de la evaluación de cada riesgo. Esta tabla se utiliza para priorizar los riesgos en toda la organización. Otro mapa podría mostrar la reducción del riesgo después de que se adopta una gestión del riesgo.



Esta figura representa un ejemplo de un mapa de riesgo integral para una administración que examina la dinámica de la frecuencia y la gravedad que se refieren a cada riesgo. Mediante la asignación de probabilidad de ocurrencia contra la estimación de la magnitud futura de la posible pérdida, los administradores de riesgo pueden formar la base sobre la que una administración puede concentrarse en zonas de riesgo que tienen necesidad de acción. Por lo tanto, se pueden tomar las acciones posibles - incluyendo la cobertura de riesgos, control de riesgos y seguros. El mapa de riesgo incluye el trazado de puntos de intersección entre las medidas de frecuencia (en un eje x) y la gravedad (en un eje y). Cada punto representa la relación entre la frecuencia de la exposición y la severidad de la exposición para cada riesgo medido.

Por su amplia difusión y utilización en la AGE en el contexto del PRTR, se han elegido las matrices del SNCA como modelo para el Sistema de Integridad de la AGE[15].

15 Tal y como se ha mencionado anteriormente, en el marco del Ministerio para la Transformación Digital y de la Función Pública, el Servicio Nacional de Coordinación Antifraude SNCA ha elaborado una Guía para la aplicación de medidas antifraude en la ejecución del Plan de Recuperación, Transformación y Resiliencia de febrero de 2022, que recoge una matriz de riesgos y un sistema de banderas rojas. A título orientativo y como elemento de ayuda para la evaluación de riesgos prevista en los planes de medidas antifraude en el marco del Plan de Recuperación, Transformación y Resiliencia, se ofrece la herramienta o matriz de riesgo entendida como un instrumento de carácter informador cuyo objetivo es facilitar la evaluación de la probabilidad e impacto de determinados riesgos en los métodos de gestión más comunes aplicados en ejecución del Mecanismo de Recuperación y Resiliencia (subvenciones, contratación, convenios y encargos a medios propios), sin perjuicio de que puedan existir otros tipos de gestión y de que la herramienta pueda adaptarse teniendo en cuenta las características de cada entidad y los procedimientos implementados como consecuencia de los sistemas de control interno de gestión o de nivel 1 existentes.

Con el fin de facilitar el trabajo del equipo de evaluación de riesgos, en la citada herramienta se han definido algunos riesgos (R) que aparecen clasificados en función de que la ejecución de los fondos procedentes del Mecanismo se haya realizado a través de subvenciones (S: S. R), contratos (C: C. R), convenios (CV: CV. R) o encargos a medios propio (MP: MP. R). Para cada uno de los métodos de gestión señalados se presenta una portada en la que se recogen, a modo de resumen, los distintos riesgos y su descripción completa, detallándose después cada riesgo en su hoja correspondiente junto a un listado de posibles indicadores de riesgo y de controles propuestos de forma orientativa para cada uno de ellos. En el caso de que la entidad identifique un riesgo que no conste previamente, este nuevo riesgo deberá ser incluido en la matriz en formato de archivo Excel, añadiendo en la portada del correspondiente método de gestión una fila y una hoja específica para cada nuevo riesgo siguiendo la metodología establecida en esta Guía. De la misma manera, tanto los indicadores como los controles predefinidos en la herramienta para cada tipo de riesgo son solo ejemplos, y el equipo de evaluación puede eliminarlos si no existen, modificarlos o añadir filas si hay otros indicadores o controles en marcha para combatir los riesgos identificados.

Los pasos fundamentales para el uso de la herramienta, que se detallan a continuación, son:

a) La estimación cuantitativa del riesgo de que se produzca un tipo de fraude, corrupción, conflicto de intereses o doble financiación determinado, basada en la valoración de su probabilidad y de su impacto (riesgo bruto).

b) La valoración de la eficacia de los controles que tiene actualmente la entidad en marcha para paliar el riesgo bruto.

c) La valoración del riesgo neto, tras tener en cuenta la efectividad y el efecto de los controles que pueda haber en marcha (es decir, la situación tal como es en el momento de la evaluación).

d) La valoración del efecto sobre el riesgo neto que pueden tener los controles atenuantes que se planee establecer.

e) Valoración del riesgo objetivo, es decir, del nivel de riesgo que se considera admisible tras la puesta en marcha de controles efectivos.

La herramienta de evaluación tiene un carácter semafórico, clasificando cada riesgo en aceptable (verde), significativo (amarillo) o grave (rojo), y el equipo de evaluación debe rellenar únicamente las casillas en gris.

Como punto de partida y de forma meramente orientativa, a cada riesgo expuesto en la matriz le han sido asociados uno o varios indicadores de riesgo a efectos de facilitar la supervisión del nivel de riesgo identificado y el funcionamiento de los controles. Por indicador de riesgo se entiende aquel 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. El punto de partida, conforme al planteamiento en tres etapas de análisis del riesgo (identificación, análisis y valoración) es la identificación, que se detalla en la descripción del riesgo en cinco aspectos.

Categoría	Aspectos	Observaciones
DESCRIPCIÓN DEL RIESGO	Referencia del riesgo (Ref. del riesgo).	Se trata de una clave identificativa única.
	Denominación del riesgo.	
	Descripción del riesgo.	
	¿A quién afecta este riesgo? (Entidad decisora (ED)/Entidad ejecutora (EE)/ Beneficiarios (BF)/Contratistas (C)/ Terceros (T)…)	
	¿Es el riesgo interno, externo o resultado de una colusión?	

La unidad efectúa el análisis y la valoración del riesgo al evaluar conforme a tablas de intensidades la probabilidad y el impacto del riesgo identificado.

Categoría	Aspectos	Observaciones
RIESGO BRUTO	Impacto del riesgo BRUTO.	Daño o perjuicio causado por la ocurrencia del siniestro (materialización del riesgo): 4 Impacto grave. 3 Impacto significativo. 2 Impacto medio. 1 Impacto limitado.
	Probabilidad del riesgo BRUTO.	Probabilidad de ocurrencia del siniestro (materialización del riesgo): 1 Va a ocurrir en muy pocos casos. 2 Puede ocurrir alguna vez. 3 Es probable que ocurra. 4 Va a ocurrir con frecuencia.
	Puntuación del riesgo BRUTO.	Definición convencional de riesgo como producto de probabilidad por impacto (medidos conforme a las tablas de intensidades): {1,2,3,4,6,8,9,12,16}.

Una vez realizada la evaluación del riesgo se pasa a la fase de tratamiento que empieza por la valoración de los controles previstos o existentes, conforme a tablas de valoración.

Categoría	Aspectos	Observaciones
CONTROLES EXISTENTES	Ref. Control.	Se trata de una clave identificativa única.
	Descripción del control.	
	¿Hay constancia de la implementación del control?	Respuesta sí/no.
	¿Qué grado de confianza merece la eficacia de este control?	Respuesta: Alta/Media/Baja.
	Efecto combinado de los controles sobre el IMPACTO del riesgo BRUTO, teniendo en cuenta los niveles de confianza.	Respuesta: bajada del nivel del impacto que supone el control (-1,-2,-3,-4).
	Efecto combinado de los controles sobre la PROBABILIDAD del riesgo BRUTO, teniendo en cuenta los niveles de confianza.	Respuesta: bajada de la probabilidad que supone el control (-1,-2,-3,-4).

La valoración de los riesgos brutos minorados por los efectos de los controles establecidos da lugar al riesgo neto. Sus valores son calculados automáticamente en virtud del riesgo bruto y los controles.

Categoría	Aspectos	Observaciones
RIESGO NETO	Impacto del riesgo NETO.	Daño o perjuicio causado por la ocurrencia del siniestro (materialización del riesgo): 4 Impacto grave. 3 Impacto significativo. 2 Impacto medio. 1 Impacto limitado.
	Probabilidad del riesgo NETO.	Probabilidad de ocurrencia del siniestro (materialización del riesgo): 1 Va a ocurrir en muy pocos casos. 2 Puede ocurrir alguna vez. 3 Es probable que ocurra. 4 Va a ocurrir con frecuencia.
	Puntuación del riesgo BRUTO.	Definición convencional de riesgo como producto de probabilidad por impacto (medidos conforme a las tablas de intensidades): {1,2,3,4,6,8,9,12,16}.

Categoría	Aspectos	Observaciones
RESULTADO DE LA AUTOEVALUACIÓN	COEFICIENTE TOTAL RIESGO NETO.	Riesgo resultante de la aplicación de las minoraciones debidas a las valoraciones dadas a los controles.
	COEFICIENTE TOTAL RIESGO OBJETIVO.	El riesgo objetivo es el nivel de riesgo tolerado o deseado. Cuando el riesgo neto supera el umbral del riesgo objetivo, será preciso establecer planes de acción (en general nuevos controles) que permitan alcanzarlo).

Cuando se establece un plan de acción han de fijarse los datos que permitan su seguimiento y valorar el efecto que las nuevas acciones tendrán sobre el riesgo para conseguir el riesgo objetivo.

Categoría	Aspectos	Observaciones
PLAN DE ACCIÓN	Nuevo control previsto.	
	Persona/unidad responsable.	
	Plazo de aplicación.	
	Efecto combinado de los nuevos controles previstos sobre el IMPACTO del riesgo NETO.	Respuesta: bajada del nivel del impacto que supone el control (-1,-2,-3,-4).
	Efecto combinado de los nuevos controles previstos sobre la PROBABILIDAD del riesgo NETO.	Respuesta: bajada de la probabilidad que supone el control (-1,-2,-3,-4).

La valoración de los riesgos netos minorados por los efectos del plan de acción da lugar al valor del riesgo objetivo. Sus valores son calculados automáticamente en virtud del riesgo neto y el plan de acción.

Categoría	Aspectos	Observaciones
RIESGO OBJETIVO	Impacto del riesgo OBJETIVO.	Daño o perjuicio causado por la ocurrencia del siniestro (materialización del riesgo): 4 Impacto grave. 3 Impacto significativo. 2 Impacto medio. 1 Impacto limitado.
	Probabilidad del riesgo OBJETIVO.	Probabilidad de ocurrencia del siniestro (materialización del riesgo): 1 Va a ocurrir en muy pocos casos. 2 Puede ocurrir alguna vez. 3 Es probable que ocurra. 4 Va a ocurrir con frecuencia.

Categoría	Aspectos	Observaciones
	Puntuación del riesgo OBJETIVO.	Definición convencional de riesgo como producto de probabilidad por impacto (medidos conforme a las tablas de intensidades): {1,2,3,4,6,8,9,12,16}.

La eficacia de la gestión del riesgo dependerá de su integración en la gobernanza de la organización, incluyendo la toma de decisiones. Esto requiere la implicación de las partes interesadas, particularmente de la alta dirección.

Estas matrices se refieren a los sectores de la contratación, encargos, subvenciones y convenios.

Para el resto de las áreas de riesgos debería adaptarse la metodología empleada identificando los riesgos propios de cada sector.

La existencia de catálogos de riesgos predefinidos puede facilitar la tarea inicial de evaluación del riesgo facilitando la identificación de riesgos propios a través de la búsqueda en el catálogo.

Por otra parte, la recomendación, que más adelante se hace, de mantener registros tanto de los riesgos detectados y gestionados como de su posible materialización en un siniestro pueden servir de base a las revisiones ulteriores de los riesgos al poder modificar la probabilidad, en su caso, por las frecuencias registradas y los impactos, en su caso, por los perjuicios o daños efectivamente sufridos.

Los mapas de riesgo constituyen una herramienta valiosa de documentación de un sistema de gestión de riesgos pues representan las dos dimensiones del riesgo y permiten ver gráficamente su evolución antes de y después la aplicación de las actuaciones de tratamiento (controles, etc.).

4.5.3 Análisis de riesgo: banderas rojas, alertas y puntos críticos de control

Por bandera roja se entiende aquel hecho que revela información cualitativa o cuantitativa formada por uno o varios datos basados en hechos, opiniones o medidas, que permiten supervisar el nivel del riesgo identificado y el funcionamiento de los controles. Son «indicadores» o señales de alarma de la posibilidad de que pueda existir el riesgo.

Se trata de un elemento o una serie de elementos que son de carácter atípico o difieren de la actividad normal. Constituyen, por tanto, una señal de que algo se sale de lo habitual y necesita ser examinado con más detenimiento.

La presencia de indicadores de alerta[16] deberá obligar al personal y a las personas responsables a permanecer vigilantes y a adoptar las medidas necesarias para confirmar o negar que existe un riesgo de fraude. Es de suma importancia reaccionar ante estos indicadores de alerta. Las autoridades de gestión tienen la responsabilidad de descartar cualquier duda que suscite una bandera roja. Cabe señalar que la existencia de ban-

16 Anexo 4.4.

deras rojas no significa que se haya producido un fraude o que pueda producirse, sino que la situación debe ser verificada y supervisada con la diligencia debida.

a) Fraude en la contratación pública. Recopilación de indicadores de alerta y mejores prácticas (Ref.: Ares (2017) 6254403, de 20/12/2017) [OLAF].

b) Detección de conflictos de intereses en los procedimientos de contratación pública en el marco de las acciones estructurales. Guía práctica para las personas responsables de la gestión [OLAF].

c) Detección de documentos falsificados en el ámbito de las acciones estructurales. Guía práctica para las autoridades de gestión [OLAF].

d) Compendio de casos anónimos Acciones Estructurales [OLAF].

e) Banderas rojas en la lucha contra el fraude (Anexo IV de la Descripción de Funciones y Procedimientos de la Autoridad de Gestión del FEDER) [Subdirección General de Gestión del FEDER].

f) Nota informativa sobre indicadores de fraude para el FEDER, FSE y el FC (COCOF 09/0003/00).

g) Listado de códigos AFIS y códigos CIC (Nota: Tipos de irregularidades catalogados por la Comisión para su notificación y que por tanto se pueden asemejar a indicadores de fraude).

h) Banderas rojas por procesos de gestión de fondos: Ver riesgos y controles definidos en la Herramienta de evaluación del riesgo de fraude EGESIF_14-0021-00. Banderas rojas por instrumentos de gestión: Ver Catálogo de riesgos y banderas (Anexo II).

4.5.4 Informe

Con objeto de que queden documentados los riesgos, el proceso de evaluación del riesgo se debe documentar junto con los resultados de la evaluación. Los riesgos se deben concretar en términos acordes con el área administrativa que se evalúa, y los parámetros en que se expresa el nivel de riesgo deben ser claros.

La extensión del informe dependerá de los objetivos y del campo de aplicación de la evaluación, pero en líneas generales debe incorporar la siguiente información:

a) Los objetivos y el campo de aplicación.

b) La descripción de las partes pertinentes del sistema y sus funciones.

c) Los criterios de riesgo aplicados y la justificación de estos; las limitaciones, los supuestos y la justificación de las hipótesis.

d) La metodología aplicada en la evaluación.

e) Los resultados de la identificación del riesgo.

f) Los resultados del análisis del riesgo y su evaluación.

g) Los supuestos críticos y otros factores sobre los que se necesita hacer seguimiento.

h) Las conclusiones y recomendaciones.

Si la evaluación del riesgo sirve de apoyo al proceso continuo de gestión del riesgo, dicha evaluación se debe realizar y documentar de manera que se pueda mantener durante todo el ciclo de vida del sistema, de la organización, del equipo o de la actividad, para lo que es necesario hacer un registro del riesgo. La evaluación se debe actualizar cuando se disponga de nueva información significativa y de cambios en el contexto, de acuerdo con las necesidades del proceso de gestión.

El proceso de evaluación del riesgo debe dar importancia al contexto y a otros factores de los que se espera que pudiesen variar con el tiempo y, por tanto, cambiar o invalidar la evaluación del riesgo. Estos factores se deben identificar específicamente para que sean objeto de seguimiento y revisión, de manera que la evaluación del riesgo se pueda actualizar cuando sea necesario.

También se deberían identificar y recopilar los datos de los que se ha hecho seguimiento con objeto de mejorar la evaluación del riesgo.

Igualmente se debe hacer seguimiento y documentar la eficacia de los controles con objeto de disponer de datos para su uso en el análisis del riesgo. Se deberían definir las responsabilidades para la creación y la revisión de la evidencia y la documentación.

4.5.5 Registro de riesgos

El proceso de la gestión del riesgo y sus resultados se deben documentar e informar a través de los mecanismos apropiados. El registro pretende:

a) Comunicar las actividades de la gestión del riesgo y sus resultados a lo largo de la organización.

b) Proporcionar información para la toma de decisiones.

c) Mejorar las actividades de la gestión del riesgo.

d) Asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

La realización de un registro de riesgos en cada departamento ministerial establece la introducción de un eje vertebrador común para consolidar la evaluación de riesgo de fraude en las actividades administrativas, que debe tener su correlación con la realización de un registro de los siniestros.

4.5.6 Registro de siniestros

Dentro del registro de riesgos de cada departamento ministerial y como subapartado del mismo se debe realizar un registro de siniestros, con el fin de tener registrados los que ocurran, que servirá de referencia a las posibles actuaciones relacionadas con el ámbito disciplinario que se deban llevar a cabo por la Inspección de Servicios (rea-

lización de informaciones reservadas, tramitación propiamente dicha de expedientes disciplinarios, remisión de actuaciones al Ministerio Fiscal en caso de posibles responsabilidades penales, etc.).

En el caso de acaecimiento de siniestros en actividades administrativas derivadas de la ejecución de Fondos de la Unión Europea, este registro servirá de referencia para el seguimiento de los casos para el Servicio Nacional de Coordinación Antifraude de la Intervención General de la Administración del Estado, que pondrá en conocimiento de las actuaciones irregulares a la Oficina Europea de Lucha contra el Fraude, conforme a las previsiones de la normativa comunitaria.

4.5.7 Coordinación e intercomunicación de registros

La información contenida tanto en los registros de riesgos como en el registro de siniestros de cada departamento ministerial podría ser compartida en una red que sirviera de puesta en común de las prácticas desarrolladas por cada departamento ministerial y posibilite el *benchmarking* entre las iniciativas realizadas al respecto por todos ellos.

En esta intercomunicación de registros se debería contar con la colaboración y el apoyo de la Intervención General de la Administración del Estado (IGAE) como órgano de control interno en la Administración General del Estado.

4.6 BUENAS PRACTICAS SECTORIALES

En relación con la diferenciación entre «factores», «sectores» o «circunstancias específicas» cabe fundamentar que en materia de ética e integridad públicas no existen especificidades ni desde un punto de vista orgánico, en un ámbito departamental, ni desde el punto de vista funcional, en los diversos departamentos ministeriales.

Por todo ello, el marco de referencia del anexo 4.2 se presenta como una guía completa e íntegra para todos los sectores de la AGE, cuyas figuras[17] constituyen un mínimo necesario imprescindible como fundamento de un código ético y de integridad pública, así como para una guía de buenas prácticas.

4.6.1 Estado del arte en materia de integridad y ética públicas

Sobre la base del Informe de Integridad Pública de la Subdirección General de la Inspección general de servicios de la AGE de junio 2021, debe aplicarse la «Matriz de figuras de código e integridad públicas» que se adjunta como anexo 4.6, tanto para completar aquellos supuestos de códigos y manuales de buenas prácticas que no reúnan con plenitud el cuadro de figuras expuesto en ella, como en los supuestos donde deban construirse partiendo de cero dichos códigos y manuales.

Ha de entenderse que las presuntas especificidades que puedan plantearse desde un punto de vista funcional no resultan *per se* en figuras independientes que requieran un tratamiento diferenciado ni desde el punto de vista de los procedimientos de gestión, ni desde el de la investigación, detección, prevención, paliación, como de la recuperación o persecución, por cuanto de existir alguno habría que colegir una carencia de integridad en los códigos penológicos de corrección que, hoy por hoy, no se detectan.

17 Anexo 4.5.