Consello de Contas
de Galicia

METODOLOXÍA PARA A ADMINISTRACIÓN DE RISCOS

ÍNDICE

I. INTRODUCIÓN

O documento *Estratexia en materia de prevención da corrupción* aprobado pola Sección de Prevención do Consello de Contas establece como obxectivo que tódalas entidades públicas desenvolvan unha estratexia que permita a implantación de modelos de organización e xestión que contemplen:

- O establecemento dunha política de integridade institucional.
- A identificación, avaliación e análise de riscos de corrupción.
- A adopción de medidas de supervisión e control.

A plasmación por escrito da estratexia integrada polos tres elementos anteriores (medidas xerais organizativas e de funcionamento dunha política de integridade, a avaliación de riscos, e as medidas específicas para evitalos) determina a estrutura e o contido do plan de prevención da corrupción.

Baixo a denominación "metodoloxía para a administración de riscos" abórdase neste documento técnico a descrición do proceso de identificación, avaliación e análise de riscos, en especial os de corrupción, que constitúe o segundo elemento desa estratexia.

O modelo de avaliación de riscos que se propón contempla un enfoque global e amplo que abarque a totalidade dos riscos de xestión, nos que se enmarcan, ademais dos relacionados coa corrupción e integridade, os de cumprimento normativo en xeral, de boa administración e de adecuada presentación da información financeira.

Con carácter xeral, entendemos por administración de riscos o proceso sistemático que deben realizar as institucións para avaliar os riscos aos que están expostas no desenvolvemento das súas actividades, mediante a análise dos distintos factores que poden provocalos e coa finalidade de definir as estratexias que permitan controlalos.

Trátase en primeiro lugar de identificar as áreas de actividade da entidade e os riscos que afectan a estas actividades, para, a partir da avaliación daqueles, elaborar mapas de riscos que recollan os aspectos aos que se debe prestar especial atención, así como as medidas correctoras a implantar.

Nas entidades públicas –nas que xa existe un marco normativo que regulan as infraccións e as sancións de tipo administrativo ou penal para os casos de incumprimento- o valor engadido que supón a implantación de modelos de xestión de riscos está na súa operatividade para adaptar o enfoque xeral das disposicións legais tanto aos diferentes tipos de entidades como aos contextos cambiantes nos que estas operan.

Os potenciais beneficios dunha adecuada xestión de riscos serán os seguintes:

- Proporciona unha visión obxectiva e realista para determinar as áreas especialmente sensibles de incorrer en riscos de xestión, incluídos os de corrupción.

- Permite prestar especial atención a aquelas actividades con máis risco.

- Posibilita detectar onde se están producindo controis innecesarios e reorientalos cara onde sexan máis necesarios.

- Axuda a visualizar o risco que se asume nas actuacións que implican relacións con terceiros.

- Identifica oportunidades de actuacións máis eficientes, non só no ámbito do control senón tamén na actividade diaria da entidade.

- Favorece a sensibilización en materia de prevención da corrupción, a toma de decisións éticas no ámbito público e, como consecuencia de todo isto, unha maior confianza da cidadanía nas institucións.

II. OBXECTIVOS

Son os xestores os que, en base ao coñecemento da organización e a información de que dispoñen das distintas fontes ao seu alcance, deben apreciar os distintos factores de risco e a identificación e valoración dos mesmos.

A avaliación de riscos compete polo tanto ás propias organizacións públicas. Este documento pretende servir de guía aos xestores respecto dos elementos clave para esa administración de riscos, así como orientalos respecto do contido que se espera que conteñan os programas de prevención da corrupción respecto deste compoñente do control interno. Constitúe, polo tanto, unha ferramenta para que os centros xestores realicen unha descrición e valoración dos principais riscos de xestión, incluídos os de corrupción.

As vulnerabilidades e as áreas ás que pode afectar a avaliación de riscos variarán substancialmente en función do tipo de entidade, de aí que o que se persegue sexa unicamente ofrecer certas pautas que orienten a cada entidade na busca do modelo e a metodoloxía máis adecuados ás súas peculiaridades, priorizando o contido sobre a forma de presentalo.

Trátase, en definitiva, de axudar a formular as preguntas adecuadas e obter as mellores respostas posibles, así como de sensibilizar ás entidades que integran o sector público autonómico sobre a importancia de identificar e xestionar adecuadamente os riscos de integridade e corrupción aos que se enfrontan.

III. ENFOQUE E METODOLOXÍA

A avaliación de riscos contémplase cun enfoque amplo que abarca a totalidade dos riscos de xestión, nos que se tratan de incluír os riscos de corrupción e infraccións á integridade, e constitúe un instrumento para a xestión do risco como axuda á planificación, ao proceso de toma de decisións e a execución das súas actividades.

Tal e como se indica no documento *Estratexia en materia de prevención da corrupción,* a metodoloxía segue o marco xeral e as orientacións sobre a xestión de riscos do modelo COSO, deseñado para mellorar a xestión pública e reducir o alcance do fraude nas organizacións.

Tamén se toma como referencia a norma ISO 31000:2009, que establece os principios básicos de carácter xenérico sobre a xestión de riscos, aprobada co obxectivo de axudar ás organizacións de todo tipo a administrar os riscos de xestión con efectividade.

Este marco de referencia define a xestión de riscos como a posibilidade de que ocorra un evento que afecte negativamente aos obxectivos da entidade (COSO 2004), e resulta aplicable á avaliación de todo tipo de riscos en función dos obxectivos establecidos.

Cando se fala de obxectivos da entidade estámonos a referir non só a obxectivos operativos (eficacia e eficiencia), senón tamén de cumprimento normativo, de boa xestión financeira, de adecuada información, e tamén aos obxectivos de integridade (comportamentos conforme aos principios e valores dunha boa administración) e de prevención da corrupción (posibilidade de que, por acción ou omisión, se abuse do poder para obter un beneficio privado, directo ou indirecto).

Búscase así unha cultura de cumprimento, na que a prevención de riscos constitúe un proceso relevante para a mellora da xestión pública de cara á súa eficacia, eficiencia e calidade dos servizos, e a avaliación de riscos de corrupción constitúe ademais un obxectivo primordial de cara á salvagarda dos recursos públicos e á recuperación da confianza da cidadanía nas institucións.

A metodoloxía contida neste documento intentará achegar ferramentas que permitan ás entidades que integran o sector público autonómico:

- Impulsar o deseño de obxectivos institucionais coa suficiente claridade, que sirvan de guía para a avaliación de riscos.
- Identificar as áreas de actividade especialmente vulnerables.

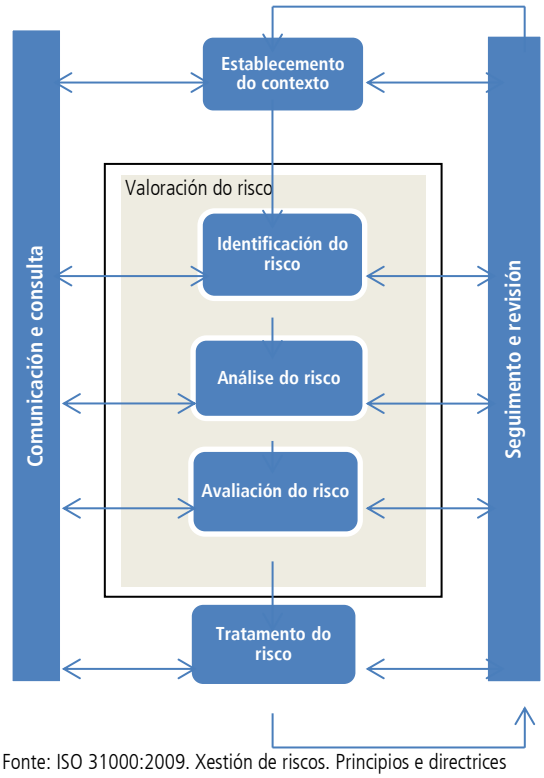
• Identificar os eventos que constitúen os riscos, considerando a posibilidade de fraude e corrupción, e avaliar a súa probabilidade e o seu impacto.

• Determinar como deben tratarse eses riscos, elaborando unha matriz de riscos que permita identificar os aspectos aos que se debe prestar especial atención e as respostas ou medidas correctoras a implantar.

IV. DESCRICIÓN DO PROCEDEMENTO DE ADMINISTRACIÓN DE RISCOS

Seguindo a norma *ISO 31000:2009 Xestión de riscos. Principios e directrices*, os procesos de avaliación de riscos desenvolveranse de acordo co establecido no seguinte esquema:

Cadro 1. Proceso de xestión do risco



Fonte: ISO 31000:2009. Xestión de riscos. Principios e directrices

Nos seguintes apartados desenvólvense as fases de identificación, análise, avaliación e tratamento dos riscos. En cada unha destas etapas deberán establecerse mecanismos de comunicación e coordinación que fomenten a implicación de tódolos afectados.

1. DEFINICIÓN DO CONTEXTO

1.1. Establecemento do contexto

Para aplicar con éxito calquera metodoloxía de avaliación de riscos é importante dotar ás organizacións de certas condicións previas de carácter normativo e institucional e, así mesmo, asegurarse de que o proceso contará co compromiso da dirección e cos medios suficientes para levalo a cabo.

O contorno no que cada unha das entidades que integran o sector público autonómico desempeña as súas funcións é diferente, e consecuentemente os riscos aos que están expostas non poden xeneralizarse, sen prexuízo da consideración dalgúns deles como comúns ou máis habituais nas distintas áreas de xestión.

Cada entidade deberá definir de xeito individual o seu propio contexto e os seus propios riscos, coa finalidade de que as estratexias que desenvolva para xestionalos sexan adecuadas e efectivas. Neste sentido, o coñecemento particularizado da propia organización, da súa estrutura interna, e das interaccións que realiza co exterior contribuirá a determinar cales son, en cada caso, as principais debilidades e fortalezas.

No ámbito interno, será necesario ter en conta o funcionamento xeral da entidade e os obxectivos e metas que persegue, considerando:

- A planificación estratéxica
- A cultura da organización en relación coa integridade e os valores éticos
- A estrutura orgánica da entidade e o xeito de asignar responsabilidades
- Os sistemas de información e os procesos de toma de decisións
- As normas, directrices e modelos adoptados pola entidade

En xeral, será relevante considerar calquera factor que asegure que o enfoque atribuído á xestión de riscos é apropiado ás circunstancias, á organización e aos riscos que afectan o logro dos obxectivos de cada entidade.

No relativo á corrupción, o principal risco procedente do ámbito externo será a existencia de persoas ou organizacións que poidan ter interese en ofrecer beneficios ilexítimos aos servidores públicos a cambio dunha acción ou omisión.

Os riscos máis comúns derivarán das debilidades da entidade nas funcións de supervisión, control e auditoría interna; da xestión inadecuada dos seus contratos e das súas relacións cos provedores; e por último, de factores de carácter individual que poidan predispoñer aos empregados públicos a cometer accións inapropiadas, como a insatisfacción no traballo ou as presións políticas.

1.2. Obxectivos e criterios de riscos

Unha vez definidos estes contextos, e con carácter previo á fase de identificación dos riscos concretos que lle afectan, cada entidade establecerá os seus obxectivos en materia de integridade e prevención da corrupción tratando de que sexan coherentes cos obxectivos de carácter xeral da institución: o que se vai facer ou que se pretende conseguir neste ámbito; cales son os recursos dispoñibles; quen será o responsable de acadar os obxectivos fixados; como se avaliarán e informarán os resultados; e quen vai impoñer as sancións que procedan, no seu caso.

O establecemento destes obxectivos permitirá determinar o risco aceptado (risco que unha entidade está preparada para soportar antes de que se xulgue necesario actuar) e a tolerancia ao risco, entendida como a desviación aceptable por parte da entidade na consecución dos seus obxectivos.

Unha cuestión esencial desta etapa é a definición dos criterios de risco, isto é, os criterios que se aplican para avaliar a importancia dos riscos, en función das causas e consecuencias para as institucións.

2. IDENTIFICACIÓN E ANÁLISE DE RISCOS

O principal obxectivo desta fase será identificar as actividades e procesos máis vulnerables e os riscos específicos aos que están expostos.

O resultado final, cuxo éxito requirirá da implicación e participación activa de todo o persoal, consistirá na elaboración dunha lista ou inventario de procesos vulnerables que permita diferenciar entre os que están baixo control e aqueles que non o están e que, polo tanto, deberán ser xestionados.

A identificación destes procesos vulnerables realízase tanto a través da determinación dos posibles riscos inherentes ao propio proceso como a través doutros factores de vulnerabilidade da propia organización. A continuación expóñense os posibles pasos a seguir:

Paso 1. Identificación das actividades e procesos da organización

A análise de riscos debe partir da identificación das actividades ou procesos propios cada organización, diferenciando ente os procesos centrais e os procesos de apoio.

No anexo I deste documento recóllese unha sistemática para a descrición de procesos (táboa 2), e unha relación dos procesos máis vulnerables comúns no sector público elaborada pola Oficina Antifraude de Cataluña (táboa 3).

Por outra banda, nas entidades públicas existen determinadas áreas de xestión especialmente sensibles (contratación, subvencións, gastos de persoal, xestión de tesourería, de ingresos, etc.) sobre as que este Consello de Contas realizou unha identificación dos riscos máis comúns no documento *Catálogo de riscos por áreas de actividade*.

Paso 2. Consideración dos factores de risco que afectan a cada proceso ou actividade

Poden definirse como factores de risco as situacións ou circunstancias que incrementen a probabilidade de que se produzan incumprimentos, falta de fiabilidade da información, falta de eficacia nas actuacións ou prácticas corruptas propiamente ditas.

A presenza destes factores debe ser apreciada polo propios xestores en base ao coñecemento da organización ou de diferentes fontes de información, como:

- Informes internos ou externos, informes de auditoría, resolucións xudiciais ou denuncias.
- Información procedente da experiencia dos empregados da entidade, a través de entrevistas ou cuestionarios.
- Información sobre experiencias en entidades similares obtida a través de informes públicos ou páxinas web.

Un factor de risco -ao igual que o risco mesmo- pode afectar a varios obxectivos da organización e tamén a varias áreas de actividade ou de xestión.

Nas Administracións públicas adoitan identificarse distintos factores de risco de xestión, que basicamente obedecen á tipoloxía que se enumera a continuación:

- *Factores de risco externos:*

- Debilidades no marco normativo necesario para fortalecer a integridade e a loita contra a corrupción (leis en materia de conflitos de intereses, protección adecuada dos denunciantes, ou establecemento de sancións para o caso de incumprimento)
- Cambios reguladores importantes
- Cambios nos altos cargos da organización

- *Factores de risco internos ou institucionais:*

- Ausencia dunha política adecuada que promova a transparencia e o comportamento ético
- Inadecuación ou debilidade dos mecanismos internos de supervisión
- Ausencia de sistemas de alerta para o caso de que se produzan irregularidades
- Actividades con alto grao de discrecionalidade
- Procesos pouco informatizados
- Información pouco transparente
- Xestión documental deficiente

- *Factores de risco individuais:*

- Relacións inadecuadas cos clientes
- Falta de experiencia ou de formación
- Posibles presións no ambiente de traballo
- Insatisfacción dos traballadores
- Inadecuada supervisión do traballo

- *Factores de risco procedimentais:*

- Falta de manuais de procedementos
- Falta de transparencia na toma de decisións
- Falta de claridade na distribución de competencias
- Ausencia de controis verticais e horizontais dos procedementos

Como información complementaria, no anexo I deste documento recóllese unha táboa (táboa 4) con outros factores ou indicadores de riscos recollidos de distintas fontes.

Paso 3. Identificación dos riscos

O obxectivo deste paso consiste en xerar unha lista de riscos baseada en eventos que poderían obstaculizar ou retrasar o logro dos obxectivos a que está suxeita toda entidade pública.

O risco debe estar descrito de maneira clara e precisa e a súa redacción non debe dar lugar a ambigüidades ou confusións coa causa ou factores xeradores do mesmo.

Como xa se sinalou, o obxectivo final desta fase será identificar os riscos dun xeito estruturado que facilite a posterior elaboración dun mapa de riscos por parte de cada entidade.

Un estudo completo de cada risco identificado debería tomar en consideración os distintos elementos integrantes da súa descrición que se expoñen no seguinte cadro.

Cadro 2. Descrición do risco

Concepto	Descrición
Nome do risco	Identificación do risco
Alcance do risco	Descrición cualitativa dos sucesos, o seu tamaño, tipo e número
Natureza do risco	Estratéxico, operacional.....
Interesados	Interesados e as súas expectativas
Cuantificación do risco	Importancia e probabilidade
Tolerancia ao risco	Potencial de perda e impacto financeiro do risco Probabilidade e tamaño das perdas potenciais Obxectivo do control do risco e nivel desexado de cobertura
Tratamento do risco e mecanismos de control	Medios polos que se xestiona o risco actualmente Niveis de confianza no control existente Identificación de protocolos de supervisión e revisión
Acción potencial de mellora	Recomendacións para reducir riscos
Política e estratexia a desenvolver	Identificación do responsable

Fonte: Estándares de xerencia de riscos FERMA

a) Riscos en xeral. Tipoloxía

O proceso de identificación inclúe a clasificación dos riscos considerando, entre outras, as seguintes categorías:

- Estratéxicos. Asócianse aos asuntos relacionados coa misión e o cumprimento dos obxectivos estratéxicos.
- Financeiros. Relaciónanse cos recursos económicos da institución, principalmente da eficiencia e transparencia no manexo dos recursos.

- Operativos. Aqueles relacionados con fallos nos procesos, nos sistemas ou na estrutura da institución.
- Legais. Afectan á capacidade da institución para dar cumprimento á lexislación e ás obrigas contractuais.
- Tecnolóxicos. Riscos relacionados coa disfunción ou a obsolescencia do equipamento tecnolóxico.
- Á integridade. Son aquelas situacións ou eventos que, no caso de materializarse, impactarían en maior ou menor medida no contorno dos valores e principios éticos da institución.
- Reputacionais. Riscos relacionados coa reputación da entidade e a percepción que ten a cidadanía da súa eficacia.

b) Consideración dos riscos de corrupción

De acordo co modelo proposto, a avaliación de riscos formúlase cun enfoque global de control de riscos de xestión, nos que se inclúen os riscos de corrupción. Hai que destacar, non obstante, que se pretende que a esta análise atenda especialmente ao comportamento ético e á salvagarda de activos nas operacións realizadas como obxectivo máis específico, propio da política de prevención de riscos de corrupción, dando así resposta ao deseño e implantación de políticas de integridade e aos plans de prevención de riscos de corrupción a que alude a Lei do Consello de Contas.

Dentro das Administracións públicas véñense identificando como riscos máis vinculados a distintas formas de corrupción:

- Risco de conflito de intereses: situación na que unha persoa debe optar entre as responsabilidades do seu posto e os seus propios intereses privados.
- Risco de favoritismo: trato de favor que se dá a unha persoa en prexuízo doutras que tamén o merecían na mesma ou maior medida.
- Risco de nepotismo: preferencia que se outorga a parentes para concesións ou empregos públicos.
- Risco de suborno: ofrecemento, promesa, aceptación ou esixencia dun incentivo para realizar unha acción ilícita ou contraria á ética.
- Risco de malversación: utilización deshonesta e ilícita de fondos e bens públicos para fins de enriquecemento persoal.

- Risco de fraude: engano deliberado para obter unha vantaxe indebida ou ilícita.
- Risco de extorsión: utilización do poder ou de información para esixir inxustificadamente a outros colaboración ou diñeiro mediante ameazas coercitivas.
- Risco de colusión: acordo secreto entre partes que confabulan para enganar e defraudar e así obter unha vantaxe económica ilícita.

c) Consideración dos riscos penais nas entidades instrumentais do sector público

Para as entidades instrumentais con forma de sociedade mercantil pública autonómica ou fundación do sector público autonómico, dispoñer dun sistema de xestión de cumprimento de riscos penais constitúe un instrumento relevante que pode servir de eximente ou atenuante de responsabilidades da entidade neste ámbito, nos termos establecidos polo Código Penal.

Con este fin, o seu modelo de organización e xestión de cumprimento (programa de cumprimento) debe dar resposta necesariamente ás políticas de integridade e administración de riscos que se espera de tódalas entidades do sector público (riscos de xestión, incluídos os riscos de integridade ou de corrupción) e, ademais, incluír os elementos propios dun plan de prevención de delitos (riscos penais).

Considerando que os elementos básicos deses programas de cumprimento e dos plans de prevención de riscos de corrupción que prevé o artigo 5 bis da Lei do Consello de Contas son coincidentes, non debe existir ningún inconveniente para integrar dentro do plan de prevención de riscos de corrupción o propio plan de prevención de delitos, sempre coa necesaria énfase na avaliación de riscos de ilícitos penais que afectan ao contorno das actuacións desas organizacións.

Para estes efectos, a axeitada avaliación de riscos no ámbito penal debe partir dos riscos polos que pode ser declarada a responsabilidade penal das persoas xurídicas (Código Penal). Este mapa de posibles riscos penais deberá completarse e adaptarse a cada caso, tendo en consideración as particularidades de cada entidade, especialmente no que atinxe ao seu obxecto e sector no que desenvolve a súa actividade.

3. AVALIACIÓN DE RISCOS

3.1. Avaliación do risco inicial

A finalidade da avaliación é determinar a extensión coa que un evento pode afectar aos obxectivos dunha organización. Realízase desde unha dobre perspectiva: probabilidade de ocorrencia e impacto sobre os obxectivos.

Trátase, polo tanto, de determinar a gradación do risco en función da probabilidade de que o risco ocorra e do seu impacto no caso de ocorrer.

En xeral, a avaliación de riscos caracterízase por unha primeira etapa que ten como obxectivo medir o risco inherente -risco inicial antes de controis- e unha segunda etapa de contraste deses riscos cos controis establecidos, para determinar o risco actual sobre o cal decidir as medidas de tratamento.

O resultado final desta fase será a avaliación de cada risco individualmente desde esa dobre perspectiva -probabilidade e impacto- tendo en conta a natureza do risco e a magnitude das consecuencias no caso de que chegue a producirse. Os riscos máis importantes serán aqueles nos que concorran unha alta probabilidade de ocorrencia e un alto impacto.

➢ *Probabilidade*

A gradación da probabilidade pode valorarse con base na frecuencia (por exemplo, o número de veces que se produciu o risco nos últimos anos) e tamén basearse na existencia ou ausencia de medidas para mitigar a posibilidade de risco.

No seguinte cadro preséntase unha posible valoración da probabilidade do risco tendo en conta a maior ou menor intensidade da presenza desas variables (frecuencia e medidas).

Cadro 3. Probabilidade de ocorrencia do risco

VALOR	PROBABILIDADE	FACTORES DE GRADACIÓN
9	Alta	A entidade non implantou medidas que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia inferior á anual (varias veces no ano)
8		A entidade non implantou medidas que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia anual (unha vez ao ano)
7		A entidade non implantou medidas que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia superior á anual
6	Media	A entidade conta con medidas parciais que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia inferior á anual (varias veces no ano)
5		A entidade conta con medidas parciais que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia anual (unha vez ao ano)
4		A entidade conta con medidas parciais que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia superior á anual
3	Baixa	A entidade ten implantadas medidas que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia inferior á anual (varias veces no ano)
2		A entidade ten implantadas medidas que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia anual (unha vez ao ano)
1		A entidade ten implantadas medidas que poidan previr a súa ocorrencia e o risco prodúcese cunha frecuencia superior á anual

(No documento número 5 recóllense algunhas das medidas que se poden considerar a efectos de reducir a probabilidade de ocorrencia)

Fonte: Elaboración propia

➢ *Impacto*

O impacto sobre os obxectivos valorarase tendo en conta as consecuencias para a entidade no caso de que o risco se materialice.

No seguinte cadro preséntase unha posible valoración da gravidade do risco tendo en conta a maior ou menor intensidade dos danos reputacionais dos incumprimentos (sexan na consecución dos obxectivos da entidade ou de normas tanto penais como administrativas) ou dos danos ao patrimonio público.

Cadro 4. Impacto

VALOR	GRAVIDADE	FACTORES DE GRADACIÓN
9	Alta	Uso indebido de cargos ou fondos públicos existindo ademais un beneficio particular. Indicios de infraccións penais ou administrativas graves que ocasionen danos reputacionais á institución
8		Incumprimento de obxectivos estratéxicos que afecten á imaxe institucional ou á prestación dos servizos
7		Uso irregular de cargos, fondos ou medios públicos con danos significativos ao patrimonio
6	Media	Indicios de infraccións penais ou administrativas menos graves con impacto moderado na imaxe da institución
5		Outros incumprimentos de normas administrativas
4		Uso irregular na utilización de medios públicos sen danos significativos ao patrimonio
3	Baixa	Indicios de infraccións penais ou administrativas leves que ocasionen pequenos danos na imaxe institucional reversibles a curto prazo
2		Incumprimento de obxectivos operativos
1		Irregularidades administrativas que non supoñan incumprimentos normativos nin afectación ao patrimonio

Fonte: Elaboración propia

3.2. Matriz de riscos

A matriz de riscos mostra unha escala da gravidade dos riscos tendo en conta a probabilidade de ocorrencia e a gravidade das posibles consecuencias. O resultado final do proceso será a priorización dos riscos asignando a cada un deles unha categoría de probabilidade e impacto.

A matriz debe incluír tamén as medidas a adoptar en cada caso, que serán obxecto de análise no apartado seguinte.

Cadro 5. Matriz de riscos

Probabilidade / Gravidade	Baixa	Media	Alta
Alta	Moderado	Elevado	Elevado
Media	Baixo	Moderado	Elevado
Baixa	Baixo	Baixo	Moderado

Fonte: Elaboración propia

Para a gradación de cada risco conforme a esta matriz elaborouse unha ferramenta informática que relaciona as variables consideradas.

4. TRATAMENTO DO RISCO

4.1. Concepto

A categorización do risco determinará o establecemento de prioridades sobre as que deben concentrarse os esforzos de control e a selección de actuacións a realizar (medidas de tratamento).

Trátase de analizar se o risco é aceptable en relación co custo-beneficio ao que está asociado e, polo tanto, non hai que adoptar ningunha medida; ou se pode delegarse; ou as medidas que hai que adoptar para reducir/controlar as probabilidades e consecuencias de que ocorra.

Unha vez avaliados os riscos, a entidade debe determinar as medidas que vai adoptar para evitalos ou, no seu caso, minimizalos. As posibles accións poderían ser as seguintes:

• Previr o risco. Cando un risco foi identificado e representa unha ameaza para o cumprimento dos obxectivos estratéxicos da entidade, deberán adoptarse medidas dirixidas a diminuír a probabilidade de ocorrencia (accións de prevención) e o seu impacto (accións de continxencia), tales como actuacións específicas de control interno ou mellora dos procedementos dentro dos órganos xestores ou o reforzamento das actuacións dos órganos de control (como as Intervencións)

• Aceptar o risco. No caso de riscos de baixo impacto e baixa probabilidade de ocorrencia, pode optarse por non adoptar ningunha medida cando se chegue á conclusión de que non se está en condicións de mitigalo razoablemente. A tolerancia ao risco pode complementarse coa planificación da continxencia para manexar os impactos que se presentarían de se manifestar o risco.

• Transferir o risco. Supón trasladar ou compartir o risco cun terceiro, por exemplo a través da contratación de seguros. Esta opción será útil para determinados tipos de riscos, como os financeiros ou os derivados da subcontratación de actividades, pero non será aplicable a outros riscos, como por exemplo os de carácter reputacional.

• Evitar o risco. Supón abandonar as actividades ou eliminar os factores xeradores de riscos. Porén, este tipo de estratexia é máis limitada no sector público que no sector privado. Hai que ter en conta que determinadas actividades son levadas a cabo desde a esfera pública a pesar de que os riscos asociados son elevados pero non existe outro xeito de acadar o resultado que redunda no beneficio público.

4.2. Selección de opcións e mapa de riscos

A selección da opción máis adecuada para o tratamento do risco deberá ter en conta non só as vantaxes que proporciona senón tamén os custos que supón, tomando en consideración os requisitos legais, regulamentarios ou doutro tipo. Á súa vez, o fallo ou ineficacia das medidas de tratamento do risco pode constituír un novo risco, polo que haberá que asegurarse, a través do oportuno seguimento, de que as opcións elixidas son eficaces.

O formato do modelo de mapa de riscos pode ser o seguinte:

Cadro 6. Mapa de riscos

Identificación do Servizo/Unidade administrativa					
Actividades	**Riscos**	**PO**	**GC**	**GR**	**Medidas de prevención**

PO. Probabilidade da ocorrencia: 1,2,3 = Baixa; 4,5,6 = Media; 7,8,9 = Alta
GC. Gravidade da consecuencia: 1,2,3 = Baixa; 4,5,6 = Media; 7,8,9 = Alta
GR. Gradación do risco: 1 = Baixo; 2 = Moderado; 3 = Elevado

Fonte: Elaboración propia

ANEXO I. INSTRUMENTOS DE APOIO

TÁBOA 1. ESQUEMA DAS ACTUACIÓNS A REALIZAR EN CADA FASE DO PROCESO

ACTUACIÓNS PARA A ADMINISTRACIÓN DE RISCOS	
FITOS	
FASE PREPARATORIA	1. Acordo da dirección para a realización da avaliación de riscos (con divulgación)
	2. Designación do responsable da avaliación
	3. Definición do ámbito da avaliación
	4. Definición do método de avaliación *Xestionar unha revisión de risco: Este é un procedemento que vai de arriba cara abaixo. Establécese un equipo para considerar todas as operacións e actividades dunha organización en relación cos seus obxectivos, e identificar os riscos asociados. O equipo conduce unha serie de entrevistas con membros clave de todos os niveis da organización para deseñar un mapa de risco para toda a gama de actividades, nas que se identifican os campos das políticas, actividades e funcións que poden ser especialmente vulnerables a risco, (incluíndo o risco de fraude e corrupción).* *Autoavaliación de risco: Este é un enfoque que vai de abaixo cara arriba. Cada nivel e parte da organización está convidada a revisar as súas actividades e alimentar un diagnóstico de riscos cara arriba da entidade. Isto pode facerse a través dun enfoque de documentación (cun marco de diagnóstico establecido con cuestionarios) ou a través de talleres. Estes dous enfoques non se exclúen mutuamente, e unha combinación de enfoques de arriba cara abaixo e de abaixo cara arriba é recomendable para o proceso de valoración de risco e para facilitar a identificación de riscos, tanto de toda a entidade como de cada actividade.*
	5. Selección de participantes dos grupos de traballo
FASE DE AVALIACIÓN	
FASES	**FITOS**
DEFINICIÓN DO ENTORNO	1. Definir o contexto da organización: obxectivos e parámetros internos e externos a ter en conta na xestión do risco
	2. Establecer os criterios de risco tendo en conta os derivados das normas legales (criterios de cumprimento normativo e prevención da corrupción)
IDENTIFICACIÓN DE RISCOS	3. Determinar os procesos claves da organización e os procesos de apoio (Ver táboa 2 e táboa 3 na que se achega un listado dos procesos máis vulnerables nas organizacións públicas)
	4. Valorar a presenza de factores de risco que determinan a vulnerabilidade nos procesos da organización. Valoración dos sistema de control interno (Cuestionario de control interno)
	5. Considerar os acontecementos adversos (RISCOS) que poderían presentarse nos procesos
	6. Nos procesos vulnerables comúns, contrastar coa relación dos riscos achegada polo Consello de Contas. Na táboa 4 móstrase unha relación dos factores de risco a considerar nalgúns procesos.
ANÁLISE E AVALIACIÓN DE RISCOS	7. Determinar o nivel de risco inicial para cada un dos eventos identificados e consideralas medidas xa existentes para mitigalos
	8. Graduar os riscos en función do seu impacto e probabilidade de ocorrencia e clasificar a gradación do risco como nivel baixo, moderado ou elevado. Matriz de riscos
TRATAMENTO DOS RISCOS	9. Determinar as medidas a poñer en práctica para que o risco non ocorra ou sexa minimizado no caso de ser imposible evitalo. As medidas preventivas do risco son de natureza diversa:• Evitar o risco, eliminando a súa causa • Previr o risco, procurando minimizar a súa probabilidade de ocorrencia ou do seu impacto negativo • Aceptar o risco e os seus efectos • Transferir o risco a terceiros
	10. Establecer as medidas de prevención por risco

TÁBOA 2. DESCRICIÓN DOS PROCESOS

PROCESOS CENTRAIS

Podemos identificar os *procesos centrais* con aqueles relacionados cos deberes derivados do mandato legal da organización ou dos obxectivos contemplados na planificación aprobada. Non se pode facer unha clasificación destes procesos ao ser altamente específicos para cada tipo de organización. Como exemplo no Consello de Contas considéranse procesos centrais: a fiscalización, a prevención de riscos de corrupción e o asesoramento.

PROCESOS DE APOIO

Podemos definir *os procesos secundarios* como os procesos que directa ou indirectamente facilitan os procesos centrais ou primarios. Son exemplos típicos destes a xestión de recursos humanos, a xestión financeira, a xestión da información ou a xestión das instalacións.

Estes procesos poden dividirse, á súa vez, en procesos subsidiarios:

- Xestión de persoal (recursos humanos): a) recrutamento e selección, b) capacitación, c) remuneración, d) clima organizacional (condicións de traballo, saúde e seguridade).
- Xestión financeira: a) orzamentación, b) contabilidade, c) xestión de fondos.
- Xestión da información: a) desenvolvemento de sistemas de información, b) mantemento dos sistemas de información, c) acceso/continuidade dos sistemas de información, d) colección de datos, entrada, almacenamento e distribución.
- Xestión das instalacións: a) administración do complexo de instalacións, b) abastecemento de bens e servizos, equipamento e instalacións de tecnoloxías de información, c) transporte.

PROCESOS DE GOBERNANZA

Tamén podemos falar de *procesos de gobernanza* para referirnos a aqueles que están intimamente relacionados cos procesos de xestión e control. Existen moitas definicións posibles para a xestión interna e o control.

A xestión interna pode definirse como o proceso de dirixir unha organización para alcanzar os obxectivos da política establecidos. A un nivel organizacional, isto implica:

1) o deseño da estrutura organizacional;

2) o deseño e implementación do ciclo de planificación nos niveis estratéxico, táctico e operativo;

3) comunicación con axentes externos.

Fonte: Manual para a condución de autoavaliacións da integridade nas Entidades Fiscalizadoras Superiores (INTOSAI)

TÁBOA 3. PROCESOS MÁIS VULNERABLES COMÚNS NAS ADMINISTRACIÓNS PÚBLICAS

Administración de recursos públicos

- Contratación de obras e servizos por importe significativo
- Proxectos de concesión de obra pública por importe significativo
- Encargos de informes ou ditames a profesionais, despachos, bufetes e consultarías externas
- Outorgamento de subvencións, axudas, avais e créditos a empresas e organizacións
- Outorgamento de axudas, bolsas, subsidios ou outros beneficios a individuos
- Actuacións de asignación discrecional de recursos a organizacións
- Xestión de tesourería e contas correntes
- Xestión de caixa con manexo de efectivo
- Vendas e cobramentos en metálico
- Ingresos con recadación de impostos, taxas e prezos públicos
- Convenios con organizacións privadas
- Alleamentos ou permutas de patrimonio

Funcións de regulación, inspección e sanción

- Elaboración de normativas reguladoras de sectores de actividade
- Emisión de licenzas e autorizacións
- Determinación do importe a aboar por impostos, taxas e prezos públicos
- Imposición ou reconsideración de multas e sancións; condonacións ou adiamento de débedas
- Exercicio de funcións de autoridade, en xeral
- Inspección sobre o cumprimento de normas
- Exercicio de funcións de fe pública, auditoría e control financeiro, en xeral

Autorizacións urbanísticas, de actividades e outras

- Decisións urbanísticas en xeral e, en especial, recualificacións de solo
- Inspección ou avaliación do cumprimento de normas e estándares en locais, vivendas, empresas e organizacións, maquinaria e equipos, vehículos e produtos

Provisión de servizos públicos aos cidadáns

- Provisión de servizos públicos nos que a demanda supera a oferta (cuantitativa ou cualitativamente)
- Atención a persoas en situacións de especial debilidade
- Emisión de documentos acreditativos

Xestión de persoal

- Selección de persoal fixo ou temporal (funcionario, interino, laboral ou eventual)
- Avaliación e promoción de persoal
- Supervisión e asignación de tarefas a outros empregados
- Xestión de nóminas, horas extras, dietas, axudas sociais e anticipos e outros complementos retributivos
- Exercicio simultáneo doutros postos de traballo ou realización de tarefas profesionais para outros organismos, empresas ou particulares
- Obtención dun posto de traballo no sector privado despois de ocupar un cargo público

Relacións con entes externos

- Actividades comerciais de empresas públicas e organismos autónomos
- Aceptación de invitacións ou agasallos
- Acordos de patrocinio
- Constitución e xestión de empresas mixtas e outras iniciativas público-privadas
- Tratos habituais co sector empresarial privado
- Relacións con organizacións e profesionais que representan intereses privados (lobbies)

Outros ámbitos e situacións

- Emisión de informes, ditames ou peritaxes necesarias para decisións administrativas ou xudiciais
- Xestión de información confidencial relevante sobre persoas e organizacións
- Delegación de competencias en órganos subordinados
- Situacións nas que se produce un conflito de intereses entre a persoa e as súas funcións públicas
- Uso de tarxeta de crédito institucional
- Uso de patrimonio público fóra das instalacións e en horarios non habituais (coche oficial, ordenador, teléfono móbil ou despachos)

Fonte: Documento "Identificar e xestionar os riscos de corrupción. Orientacións para directivos públicos". Oficina Antifraude de Cataluña

TÁBOA 4. FACTORES E INDICADORES DE RISCO

1. RELATIVOS Á ESTRUCTURA ORGANIZATIVA E MARCO NORMATIVO
1.1 Organización nova.
1.2. Organización descentralizada
1.2 Lexislación cambiante
1.3 Forte crecemento ou redución da organización
1.4 Privatizacións
1.5 Subcontratacións
1.6 Reorganizacións, cuestionamento da necesidade da organización ou do traballo realizado
1.7 Presión externa sobre o desempeño/resultados, desequilibrio dos recursos en consideración das tarefas a cargo

2. RELATIVOS AO PERSOAL
2.1 Presión sobre o desempeño/resultados, ingresos dependentes do rendemento
2.2 Falta de recoñecemento profesional/baixas perspectivas de crecemento profesional
2.3 Remuneración fortemente dependente de resultados
2.4 Condicións de traballo inadecuadas
2.5 Cargas de traballo elevadas
2.6 Ter outros intereses (persoal con outras actividades fóra do sector público)

3. RELATIVOS A CIRCUNSTANCIAS DE INESTABILIDADADE FINANCEIRA
3.1.Deficiencias nos controles orzamentarios
3.2. Privatizacións.
3.3. Externalización de actividades públicas
3.4. Asociacións público privadas
3.5. Programas sen fondos ou recursos suficientes
3.6. Redución de orzamentos sen correlativa redución de expectativas de servizos
3.7.Operacións suxeitas a investigación

4. RELATIVOS A PROGRAMAS OU ACTIVIDADES
4.1. Actividades ou operacións complexas
4.2. Actividades con manipulación de efectivo
4.3. Actividades consideradas tradicionalmente susceptibles de corrupción
4.4. Contratos con repercusións políticas sensibles
4.5. Subvencións directas
4.6. Realización de actividades urxentes
4.7. Compra e venda de inmobles
4.8. Autorización de contratos entre partes vinculadas

5. OUTROS INDICADORES DE RISCOS
5.1 Reparos dos órganos de control interno non corrixidos
5.2 Informes internos ou externos de control xurídico ou auditoría con incorreccións significativas
5.3 Medidas impostas á institución desde instancias superiores
5.4 Resolucións xudiciais en contra de decisións da institución
5.5 Medidas disciplinarias en contra da institución ou dos seus empregados
5.6 Existencia de queixas ou denuncias sobre actuacións da organización

Fonte: Manual autoavaliación integridade nas Entidades Fiscalizadoras Superiores (INTOSAI)

TÁBOA 5. FERRAMENTA PARA A VALORACIÓN DE RISCOS

RISCOS	PROBABILIDADE. FACTORES DE GRADACIÓN						VALOR PROBAB.		GRAVIDADE. FACTORES DE GRADACIÓN									VALOR GRAVID.		GRADACIÓN DO RISCO		MATRIZ DE RISCO
	EXISTENCIA DE MEDIDAS			FRECUENCIA																		
	Sen medidas	Medidas parciais	Con medidas	Varias veces no ano	Anual	Superior ao ano			Indicios corrupción / fraude	Obxectivos estratéxicos / imaxe	Uso irregular medios	Infraccións impacto moderado	Incumprim. normativos	Abuso utilización medios públicos	Danos recuperables curto prazo	Obxectivos non estratéxicos	Irregularidades administr.					
Risco 1																						
Risco 2																						
Risco 3																						
Risco ...																						
Risco ...																						
Risco ...																						
Risco ...																						
Risco ...																						
Risco ...																						
Risco ...																						

ANEXO II. GLOSARIO DE TERMOS

Control interno. Proceso que ten como fin proporcionar un grao de seguridade razoable na consecución dos obxectivos da institución.

Seguridade razoable. Escenario no que a posibilidade de que se materialice o risco diminúe e a posibilidade de lograr os obxectivos increméntase.

Incerteza. Falta de seguridade para saber de antemán a exacta probabilidade ou impacto de eventos futuros.

Economía. Termos e condicións baixo os que se adquiren os recursos, na cantidade e calidade apropiada e ao menor custo posible, para realizar unha actividade determinada coa calidade requirida.

Eficacia. Cumprimento dos obxectivos e metas establecidos en lugar, tempo, calidade e cantidade.

Eficiencia. Logro dos obxectivos e metas programadas coa menor cantidade de recursos posible.

Evento. Situación ou circunstancia futura con probabilidade de ocorrencia e potencial impacto negativo na consecución dos obxectivos dunha organización.

Risco. Incidencia da incerteza sobre a consecución dos obxectivos dunha organización.

Risco inherente. Aquel ao que está exposta unha entidade en ausencia de accións para modificar a súa probabilidade ou impacto.

Risco residual. Aquel que permanece despois de que se desenvolvan as accións de resposta ao risco.

Risco aceptable. Cantidade de riscos a que unha entidade está preparada para expoñerse antes de que unha reacción se xulgue necesaria.

Avaliación de riscos. Proceso de identificación e análise dos riscos relevantes para o logro dos obxectivos da entidade e para determinar unha resposta apropiada.

Tolerancia ao risco. Variación relativa aceptable na consecución dos obxectivos.

Factor de risco. Circunstancia ou situación interna e/ou externa que aumenta a probabilidade de que un risco se materialice.

Impacto. Consecuencias negativas que se xerarían na entidade no caso de materializarse o risco.

Categoría de risco. Puntuación utilizada para clasificar a magnitude do risco combinando as puntuacións dadas á probabilidade de ocorrencia e á gravidade da consecuencia.

Mapa de riscos institucional. Representación gráfica dun ou máis riscos que permite vincular a probabilidade de ocorrencia e o seu impacto de forma clara e obxectiva.

Matriz de risco. Táboa que reflicte o diagnóstico xeral dos riscos dunha entidade.

Nivel de risco. Resultado de correlacionar o impacto e a probabilidade cos controis internos existentes.

Valoración do risco. Fase da administración de riscos que consta da identificación, análise e determinación do nivel de risco.

Sistemas de información. Conxunto de procedementos ordenados que, ao ser executados, proporcionan información para apoiar a toma de decisións e o control da institución.

Seguimento. Control regular e sistemático sobre a execución dun plan, que serve para actualizar e mellorar a exposición aos riscos.

Revisión. Actividade que se realiza para determinar a idoneidade, adecuación e eficacia do traballo realizado para conseguir os obxectivos establecidos.