biblioteca COMPLIANCE

WORLD COMPLIANCE ASSOCIATION

biblioteca COMPLIANCE

03

HERRAMIENTA DE GESTIÓN DE RIESGOS PARA ORGANIZACIONES DEL TERCER SECTOR

Febrero 2022

GA_P Gómez-Acebo & Pombo

BUREAU VAN DIJK A Moody's Analytics Company

EQS GROUP

La **World Compliance Association (WCA)** es una asociación internacional sin ánimo de lucro formada por profesionales y organizaciones interesadas en el mundo del *compliance.* La asociación tiene, entre sus objetivos, la promoción, reconocimiento y evaluación de las actividades de cumplimiento en las organizaciones (con independencia de su forma jurídica), así como el desarrollo de herramientas y procesos para una correcta protección frente a determinados delitos/infracciones cometidas por sus empleados, colaboradores o cualquier otra persona relacionada con ella.

La **Biblioteca Compliance** es un proyecto que tiene por objetivo desarrollar contenidos bajo un enfoque práctico a través de documentos de buenas práctica sobre cinco ejes principales alrededor del *compliance*:

biblioteca COMPLIANCE BUEN GOBIERNO

biblioteca COMPLIANCE GESTIÓN DE RIESGOS

biblioteca COMPLIANCE TECNOLOGÍA

biblioteca COMPLIANCE REGULACIÓN

biblioteca COMPLIANCE SECTORIAL

Todos los documentos están disponibles en
www.worldcomplianceassociation.com

biblioteca COMPLIANCE
GESTIÓN DE RIESGOS

HERRAMIENTA DE GESTIÓN DE RIESGOS PARA ORGANIZACIONES DEL TERCER SECTOR

Febrero 2022

Laura Gonzalvo Diloy
DIRECTORA DE AUDITORÍA INTERNA Y CONTROL DE RIESGOS EN FIIAPP

Jorge Pelegrín Sáenz
TÉCNICO DE ORGANIZACIÓN Y CALIDAD

Dolores García Villaverde
EXPERTA EN COMPLIANCE DEL TERCER SECTOR

WORLD COMPLIANCE ASSOCIATION biblioteca COMPLIANCE

WORLD® COMPLIANCE ASSOCIATION

HERRAMIENTA DE GESTIÓN DE RIESGOS PARA ORGANIZACIONES DEL TERCER SECTOR

A todas las Entidades del Tercer Sector para que este documento pueda servirles de ayuda para perder el miedo y las dudas y conseguir así dar sus primeros pasos hacia el Compliance como una herramienta para el cambio.

El cambio es siempre el resultado de un buen aprendizaje.

Desde la World Compliance Association, se ha desarrollado una herramienta para facilitar la gestión de los riesgos de las entidades del tercer sector.

Está herramienta es gratuita para todas las entidades del tercer sector y se puede solicitar a la asociación.

Te invitamos a formar parte de la **Red Mundial para el Cumplimiento.**

La World Compliance Association (WCA) es una asociación internacional sin ánimo de lucro formada por profesionales y organizaciones interesadas en el mundo del compliance. La asociación tiene, entre sus objetivos, la promoción, reconocimiento y evaluación de las actividades de cumplimiento en las organizaciones (con independencia de su forma jurídica), así como el desarrollo de herramientas y procesos para una correcta protección frente a determinados delitos/infracciones cometidas por sus empleados, colaboradores o cualquier otra persona relacionada con ella.

La pertenencia a la WCA muestra por sí misma un interés y un compromiso real con el mundo del compliance. Está abierta a personas y organizaciones con interés en participar, impulsar y ampliar su conocimiento y red de trabajo y colaboración en el mundo del compliance corporativo.
Además nuestro socios profesionales están cubiertos por un Seguro de Responsabilidad Civil en sus actividades como compliance officer, consultor y/o auditor de compliance.

01 | CONTENIDOS EXCLUSIVOS

02 | PARTICIPACIÓN PRIVILEGIADA

03 | CRECIMIENTO PROFESIONAL

04 | PRIVILEGIOS EXCLUSIVOS

Y VENTAJAS ADICIONALES PARA ASOCIADOS CORPORATIVOS

CUOTA DE ADHESIÓN

Categoría Socio	Profesional		Corporativo
	Fuera de España	España (seguro RC)	
Cuota Semestral	70 €	110 €	195 €
Cuota Anual	120 €	195 €	295 €

WORLD® COMPLIANCE ASSOCIATION

WCA Internacional
Paseo Castellana 79, 7ª Planta (Lexington Center)
28046 Madrid - España Tlf: +34 917 91 66 16
info@worldcomplianceassociation.com
www.worldcomplianceassociation.com

WCA está acreditada por IAS para la certificación de ISO 37001:2016

ÍNDICE

1. INTRODUCCIÓN 9
2. CONTEXTO ORGANIZATIVO 10
3. CATÁLOGO DE RIESGOS 13
4. CRITERIOS DE VALORACIÓN DE RIESGOS 15
5. EVALUACIÓN DE RIESGOS 18
6. MATRIZ DE RIESGOS Y CONTROLES 21

QUÉ ES UN MAPA DE RIESGOS

Un mapa de riesgos ayuda a las organizaciones a identificar y priorizar aquellos riesgos a los que está expuesta.

Un mapa de riesgos es una herramienta que ayuda a las organizaciones a identificar y priorizar aquellos riesgos a los que está expuesta, teniendo en cuenta el contexto de la organización, el cual es dinámico en el tiempo.

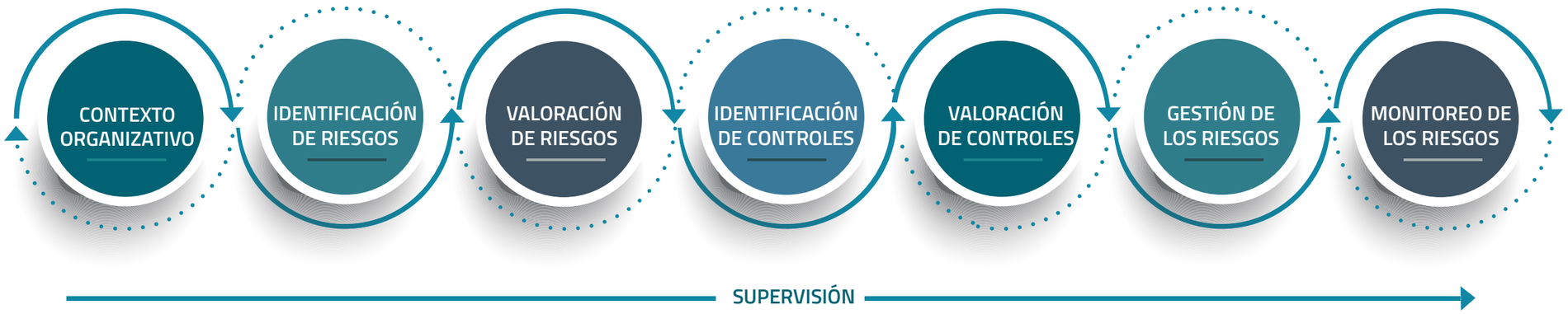
Así, el primer paso es tomar conciencia de los riesgos a los que nos enfrentamos y, el segundo, es poner la atención en la gestión de aquellos riesgos que sean más críticos y que puedan cuestionar la consecución de nuestros objetivos estratégicos y, por tanto, nuestro fin misional, ya que la capacidad y recursos de la organización son limitados.

La representación gráfica de la priorización se suele realizar a través de un mapa de riesgos o un mapa de calor, en el que quede reflejada la importancia de cada riesgo en función de la probabilidad y el impacto o daño que tendría para la organización en caso de que el riesgo se materializase.

Ver detalle completo en la Guía Compliance en el Tercer Sector publicada por la World Compliance Association en septiembre de 2020.

CONSEJOS SOBRE CÓMO HACERLO

Las fases establecidas para la elaboración de un mapa de riesgos se pueden clasificar en:



biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

HERRAMIENTA DE GESTIÓN DE RIESGOS

Desde la World Compliance Association se ha desarrollado una herramienta para facilitar la gestión de las entidades del tercer sector.

Esta herramienta, desarrollada en Excel, cuenta con las siguientes pestañas:

1. Introducción.
2. Contexto organizativo.
3. Catálogo de riesgos.
4. Criterios de valoración de riesgos.
5. Evaluación de riesgos.
6. Matriz de riesgos y controles.

Desde la World Compliance Association se ha desarrollado una herramienta para facilitar la gestión de las entidades del tercer sector.

A continuación, se explica el funcionamiento de cada una de las pestañas:

1. INTRODUCCIÓN

En la pestaña "Introducción" se muestran los distintos apartados o pestañas de la herramienta, un enlace o link a cada una de ellas, así como una breve descripción de la finalidad de cada uno de los apartados, y las tareas que se deben realizar en cada uno de ellos, de acuerdo a lo siguiente: *(ver cuadro pág.10)*

PESTAÑA	FINALIDAD	TAREAS
CONTEXTO ORGANIZATIVO	Mostrar el contexto de la organización, ya que éste condiciona su catálogo de riesgos. Se deben tener en cuenta, entre otros factores: el mapa de procesos de la organización, las obligaciones legales a las que está sujeta y cuáles son sus objetivos estratégicos.	1. Adaptar el mapa de procesos de la organización. 2. Incluir el marco normativo externo de la organización. 3. Cumplimentar los objetivos estratégicos de la organización.
CATÁLOGO DE RIESGOS	Mostrar el inventario de riesgos institucionales de la organización, clasificados según su propia clasificación o taxonomía.	Adaptar el catálogo de riesgos al contexto de cada organización, así como actualizarlo anualmente en base al mismo.
CRITERIOS DE VALORACIÓN DE RIESGOS	Desarrollar los criterios que posteriormente se utilizarán para poder evaluar los riesgos.	Cumplimentar los importes a tener en cuenta de cara al impacto inherente económico, en cada uno de los tramos, teniendo en cuenta que estos dependerán del nivel de ingresos de cada organización.
EVALUACIÓN DE RIESGOS	Realizar la evaluación de los riesgos de la organización, en base a la cual se obtendrá el mapa de riesgos, tanto inherente como residual, de la organización, que permitirá visualizar la criticidad de cada uno de los riesgos, y establecer cuáles deben ser gestionados.	Para cada uno de los riesgos identificados, asignar una puntuación al impacto inherente de acuerdo a lo establecido en la pestaña "criterios valoración riesgos".
MATRIZ DE RIESGOS Y CONTROLES	Identificar los controles existentes en la organización para prevenir y/o mitigar los riesgos a gestionar, así como aquellos que es necesario diseñar e implementar, en caso de que los existentes se consideren insuficientes o mejorables. Y determinar la efectividad de dichos controles, así como de los planes de acción.	Incluir, para cada uno de los riesgos que se decida gestionar: 1. Responsable del riesgo. 2. Controles ya existentes para prevenir y/o mitigar el riesgo: descripción del control, tipo, frecuencia y persona responsable. 3. Evaluación del control para determinar su efectividad. 4. Medidas correctivas a implementar, en el caso de que los controles se consideren insuficientes o mejorables. 5. Seguimiento de los planes de acción.

2. CONTEXTO ORGANIZATIVO

Aspectos técnicos internos y externos de los que depende el que una organización pueda desarrollar su actividad.

Entendemos por contexto todos aquellos aspectos internos y externos de los que depende que una organización pueda desarrollar su propia actividad.

El contexto de cada organización condicionará los riesgos a los que está expuesta, ya que debe tener en cuenta, entre otros factores, el mapa de procesos de la organización, las obligaciones legales a las que está sujeta y cuáles son sus objetivos estratégicos, teniendo en cuenta que uno de los objetivos fundamentales de la gestión de riesgos es asegurar su consecución, evitando que las amenazas e incertidumbres que pueden afectar a la organización se materialicen o en caso de hacerlo minimizar su impacto.

En la herramienta se hacen referencia a los siguientes aspectos, los cuales son fundamentales a la hora de definir el contexto de una organización:

- Mapa de procesos de la organización.
- Marco normativo externo.
- Objetivos estratégicos de la organización.

Para cada uno de estos bloques en la herramienta se deben realizar las siguientes tareas:

MAPA DE PROCESOS DE LA ORGANIZACIÓN

En este punto se recomienda la elaboración de un **mapa de procesos**, entendiendo por procesos al conjunto de actividades mutuamente relacionadas que utilizan entradas para proporcionar un resultado previsto, en el que un cliente interno o externo va secuencialmente recibiendo esos resultados. Cada organización debería dibujar su propio mapa de procesos, manteniendo las categorías que se detallan a continuación. Además, es recomendable, que este mapa de procesos se revise anualmente, así como se asigne a cada proceso una persona responsable del mismo.

Un proceso es el conjunto de actividades mutuamente relacionadas que utilizan entradas para proporcionar un resultado previsto.

- Procesos estratégicos: constituyen guías y directrices para los procesos misionales y de apoyo. *Ejemplos: planificación estratégica, relaciones institucionales, voluntariado, financiación, alianzas estratégicas y rendición de cuentas, entre otros.*

- Procesos misionales u operativos: responden a la misión o fin de la organización y tienen impacto en el destinatario final. *Ejemplos: gestión de proyectos de cooperación internacional al desarrollo, de acción social y/o de ayuda humanitaria, entre otros.*

- Procesos de apoyo: dan soporte a los procesos misionales. *Ejemplos: selección y gestión del personal contratado y voluntariado, gestión de las finanzas y la contabilidad, asesoría jurídica y sistemas, entre otros.*

En la herramienta se muestra una propuesta que sirva de ejemplo para cada una de las tres categorías.

MARCO NORMATIVO EXTERNO

Debemos detallar el marco jurídico de mayor rango al que estamos sujetos como organización.

Cada organización deberá detallar el marco jurídico de mayor rango al que está sujeto. En la herramienta se ha incluido una propuesta que puede servir como ejemplo para las organizaciones del tercer sector, pero cada una de ellas debería incluir la normativa que le aplica, y que le servirá de base para la posterior identificación de riesgos, la cual vendrá condicionada por su forma jurídica y ámbito geográfico de actuación, entre otros.

TELEMÁTICA	NORMA JURÍDICA
Fundaciones	Ley 50/2002, de 26 de diciembre, de Fundaciones.
	Real Decreto 1337/2005, de 11 de noviembre, por el que se aprueba el Reglamento de fundaciones de competencia estatal.
Voluntariado	Ley 45/2015, de 14 de octubre, de Voluntariado.
Transparencia y Acceso a la Información	Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
Prevención blanqueo capitales y financiación al terrorismo	Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
	Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
Subvenciones	Ley 38/2003, de 17 de noviembre, General de Subvenciones.
Régimen Fiscal	Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos al mecenazgo.
	Real Decreto 1270/2003, de 10 de octubre, por el que se aprueba el Reglamento para la aplicación del régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo.
Protección de Datos	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
Código penal (responsabilidad penal de las personas jurídicas)	Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
Inversiones financieras temporales	Acuerdo de 20 de febrero de 2019, del Consejo de la Comisión Nacional del Mercado de Valores, por el que se aprueba el código de conducta relativo a las inversiones de las entidades sin ánimo de lucro.

OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN

La organización deberá detallar en la herramienta aquellos objetivos que se desprenden de su plan estratégico interno, que es a los que deberá ir encaminada la gestión de riesgos.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

3. CATÁLOGO DE RIESGOS

El objetivo de esta pestaña es mostrar el inventario de riesgos institucionales de la organización, clasificados según su propia taxonomía. Dicha taxonomía, así como el catálogo de riesgos deberá ser revisado periódicamente, al menos anualmente, para así confirmar aquellos riesgos que siguen siendo significativos, eliminar los que ya no apliquen e incorporar los nuevos emergentes, puesto que, como ya se remarcó al principio, el contexto en el que opera la organización y sus necesidades son dinámicos.

Para ello, se deben utilizar metodologías de recolección de información, siendo de gran utilidad las entrevistas individuales y grupales con las personas responsables de los procesos organizativos, en las que poder realizar lluvias de ideas e indagar sobre riesgos materializados en el pasado; así como hacer uso de informes y estudios nacionales e internacionales que analizan las tendencias a corto y medio plazo en materia de riesgos, tales como el informe "Risk in Focus", el cual es publicado anualmente y elaborado por un conjunto de Institutos de Auditores Internos de Europa, incluido el de España.

En la herramienta se ha incluido, a modo de ejemplo, el siguiente catálogo de riesgos, pero la organización deberá realizar su propio análisis interno, siendo fundamental que acuerden la clasificación o taxonomía de riesgos a emplear, así como el catálogo de riesgos que se desprende, detallando para todos ellos una breve descripción.

Periódicamente debemos confirmar aquellos riesgos que sean significativos en nuestro inventario.

CLASIFICACIÓ O TAXONOMÍA	RIESGO	DESCRIPCIÓN
RIESGOS ESTRATÉGICOS: asociados con los objetivos clave a largo plazo y que surgen derivados de la posición estratégica que la organización toma en el entorno en que desarrolla su actividad. Por tanto, pueden surgir de las acciones de otros grupos de interés, de las decisiones estratégicas y de los cambios en el entorno competitivo.	Posicionamiento estratégico	Ausencia de actividades de promoción tanto por inexistentes como por irrelevantes y/o inadecuadas, que permitan obtener una ventaja con el resto de organizaciones del tercer sector.
	Innovación	Dificultad de transformación y/o adaptación a los cambios en el entorno, lo que repercutiría en una pérdida de oportunidades o de posicionamiento.
	Organizativo	Falta de alineación de la estructura organizativa y/o de las personas a las prioridades estratégicas de la organización, a una inadecuada y/o insuficiente gestión y acompañamiento de las personas, y/o a una falta de liderazgo por parte de responsables de la gestión de la organización.
	Económico	Dificultad para la consecución de los objetivos financieros debido a una menor capacidad económica de nuestros actuales y/o potenciales donantes, así como a una reducción de convocatorias y/o incremento de las exigencias vinculadas a las mismas por organismos públicos y/o privados a nuestra causa.

CLASIFICACIÓ O TAXONOMÍA	RIESGO	DESCRIPCIÓN
RIESGOS OPERATIVOS: asociados con las operaciones habituales que se llevan a cabo en el desarrollo de la actividad de la organización.	Ciberseguridad	Ataques externos a la seguridad de los sistemas que supongan el acceso no autorizado a información confidencial o incapacidad para el correcto funcionamiento de estos.
	Atención a terceros	Inadecuada gestión de las consultas, sugerencias, quejas y/o denuncias remitidas por un tercero y/o ausencia de canales de comunicación eficaces que permitan una adecuada canalización y resolución de éstas.
	Formulación y seguimiento de los proyectos	No alcanzar el impacto deseado con nuestra intervención y/o que no sea sostenible en el tiempo, bien porque los proyectos no respondan a las necesidades reales de las comunidades, o bien porque no estén adaptados a la cultura local, no cuenten con su respaldo y/o apropiación y/o no se haya realizado el monitoreo adecuado.
	Entorno político	Sucesos graves que alteran el normal funcionamiento de un país, como pueden ser conflictos armados, revueltas políticas, terrorismo local o fenómenos naturales como inundaciones, terremotos, sequías, incendios o pandemias, lo cual afectaría total y/o parcialmente a la continuidad de las actividades.
	Seguridad física y laboral	Exposición incrementada en el terreno de los/as trabajadores/as en términos de riesgos laborales, así como también de seguridad al trabajar en contextos peligrosos (daños, robos, amenazas, secuestros y otras acciones perjudiciales a la integridad física).
	Identificación y monitoreo de socios locales	Ausencia de procedimientos que aseguren la idoneidad de las organizaciones con las colaboramos, así como el debido monitoreo de las obligaciones y/o compromisos alcanzados.
	Transformación digital	Ineficiencia en los procesos y/o cuestionamiento sobre la fiabilidad de la información, derivada del empleo de tecnologías de información y comunicación que no responden a las necesidades de la organización, a un mal uso de estas y/o a la existencia de procesos manuales.
RIESGOS DE CUMPLIMIENTO: incertidumbre sobre el cumplimiento de los requisitos legales, contractuales y del propio marco normativo interno de la organización.	Gestión de contratos	Incumplimiento de las obligaciones y/o compromisos que hemos adquirido con terceros (donantes, organismos públicos, empresas colaboradoras, proveedores, voluntariado, socios locales, etc.), así como de estos frente a nuestra organización, con motivo de una inadecuada gestión de los recursos, selección y/o monitoreo posterior de los terceros.
	Marco regulatorio	Asociado a la incertidumbre de los posibles cambios regulatorios en los países donde las organizaciones están presentes, los cuales suelen estar expuestos a una elevada fluctuación, y el consiguiente incumplimiento de las obligaciones a las que estamos sujetos bien por desconocimiento y/o falta de recursos.
	Gobernanza y ética	Comportamientos no éticos y/o ilícitos por parte de terceros vinculados a la organización.
	Protección de la infancia	Incumplimiento de la normativa local en materia de protección de la infancia y/o los principios recogidos en la "Convención sobre los Derechos de la Niñez", así como la comisión de delitos relacionados con menores de edad por parte de personas vinculadas a la organización.
RIESGOS REPUTACIONALES: asociados a la imagen y reputación de la organización, consecuencia de actuaciones poco éticas en el seno de esta o de terceros con los que se relaciona.	Imagen global de las ONG	Comportamientos no éticos y/o la comisión de delitos por parte de otras organizaciones y que repercuten en la imagen del tercer sector.
	Trasparencia y rendición de cuentas	Insatisfacción y/o desconocimiento por parte de los grupos de interés de la organización con motivo de una rendición de cuentas que no tiene en cuenta sus expectativas y/o necesidades.

biblioteca COMPLIANCE WORLD COMPLIANCE ASSOCIATION

4. CRITERIOS DE VALORACIÓN DE RIESGOS

Una vez que la organización ha definido su catálogo de riesgos, deberá evaluarlos, para lo cual previamente deberá establecer los criterios de valoración a emplear, los cuales se detallan a continuación:

A) IMPACTO INHERENTE

Se entiende por impacto inherente al daño que supondría para los objetivos estratégicos de la organización que el riesgo se concretara en un suceso cierto, antes de considerar cualquier control o acción mitigadora. Para ello, se considerarán los diferentes tipos de impacto, tales como económicos (reducción de ingresos, aumento de gastos y/o sanciones por incumplimientos legales), operacionales (reducción del rendimiento de la actividad y/o retrasos en la misma) y reputacionales (deterioro del valor de la marca, y/o pérdida de la imagen y confianza).

Además de identificar los riesgos, es de vital importancia contar con criterios de valoración.

En la herramienta se han establecido unos criterios fijos que se deben aplicar, excepto en el caso del impacto económico, que cada organización deberá establecer en función de su nivel de ingresos, el cual se desprende de la Cuenta de Resultados:

TIPO DE IMPACTO	TRAMO	DESCRIPCIÓN	VALOR
ECONÓMICO	SEVERO	Impacto superior a XX euros.	5
	MAYOR	Impacto entre XX y XX euros.	4
	MODERADO	Impacto entre XX y XX euros.	3
	MENOR	Impacto entre XX y XX euros.	2
	INSIGNIFICANTE	Impacto entre XX y XX euros.	1
OPERACIONAL	SEVERO	Implicaría el incumplimiento, retraso o cancelación de más del 10% de nuestras actividades y proyectos planificados en el ejercicio.	5
	MAYOR	Implicaría el incumplimiento, retraso o cancelación de entre un 5 y un 10% de nuestras actividades y proyectos planificados en el ejercicio.	4
	MODERADO	Implicaría el incumplimiento, retraso o cancelación de entre un 2,5% y un 5% de nuestras actividades y proyectos planificados en el ejercicio.	3
	MENOR	Implicaría el incumplimiento, retraso o cancelación de entre un 1% y un 2,5% de nuestras actividades y proyectos planificados en el ejercicio.	2
	INSIGNIFICANTE	Implicaría el incumplimiento, retraso o cancelación de menos de un 1% de nuestras actividades y proyectos planificados en el ejercicio.	1

TIPO DE IMPACTO	TRAMO	DESCRIPCIÓN	VALOR
REPUTACIONAL	SEVERO	Deterioro de la imagen de la organización que reduce significativa y permanentemente la captación de fondos de forma global.	5
	MAYOR	Deterioro de la imagen de la organización que reduce significativamente y de forma temporal la captación de fondos de forma global.	4
	MODERADO	Deterioro de la imagen de la organización que reduce de forma puntual la captación de fondos de forma global.	3
	MENOR	Deterioro de la imagen de la organización que reduce de forma puntual la captación de fondos en una zona geográfica concreta.	2
	INSIGNIFICANTE	Deterioro puntual de la imagen de la organización que provoca una reducción de la captación de fondos de forma muy residual en una zona geográfica concreta.	1

B) PROBABILIDAD INHERENTE

Se entiende por probabilidad inherente la probabilidad de que el riesgo se concrete en un suceso cierto antes de considerar cualquier control o acción mitigadora. Para ello, se considerarán factores como la ocurrencia en la organización de ese riesgo en el pasado, su frecuencia en las organizaciones del tercer sector, la complejidad del riesgo y el número de personas involucradas en la revisión y aprobación del proceso, entre otros factores.

Evaluada la probabilidad de ocurrencia, esta se categoriza en función de la matriz utilizada. En la herramienta se propone una matriz de 5x5, con los siguientes tramos:

TRAMO	DESCRIPCIÓN	VALOR
SEVERO	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad de que se materialice (90% a 100%).	5
PROBABLE	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre un 66% a un 89% de seguridad de que se materialice.	4
POSIBLE	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre un 31% a un 65% de seguridad de que se materialice.	3
IMPROBABLE	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre un 11% a un 30% de seguridad de que se materialice.	2
RARO	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene una seguridad por debajo del 11% de que se materialice.	1

Con la aplicación de estos criterios se puede determinar el valor del impacto inherente total, considerando que el peso del impacto económico es del 50%, mientras que el impacto operacional y reputacional es del 25%, pesos que cada organización podrá adaptar a lo que su órgano de gobierno estime oportuno:

biblioteca COMPLIANCE
WORLD COMPLIANCE ASSOCIATION

IMPACTO INHERENTE TOTAL = valor impacto económico x 50% + valor impacto operacional x 25% + valor impacto reputacional x 25%

Finalizada esta fase, obtendremos el riesgo inherente que, en función de la probabilidad e impacto:

RIESGO INHERENTE = probabilidad inherente x impacto inherente global

Y de esta manera, con los valores obtenidos para el riesgo inherente, de acuerdo a la siguiente tabla, se clasificarán los riesgos en un mapa de calor, teniendo en cuenta los siguientes valores:

20 a 25	CRÍTICO	Necesidad de actuar con urgencia, el riesgo es inminente
10 a 19	ALTO	Actuar con celeridad probabilidad elevada de riesgo
5 a 9	MEDIO	Poco probable a corto plazo pero probable a medio / largo plazo
3 a 4	BAJO	Posibilidad baja de riesgo, asumible por la organización
1 a 2	MUY BAJO	Posibilidad de riesgo prácticamente nula

PROBABILIDAD							
	5	CASI CIERTO	MEDIO	ALTO	ALTO	CRÍTICO	CRÍTICO
	4	PROBABLE	BAJO	MEDIO	ALTO	ALTO	CRÍTICO
	3	POSIBLE	BAJO	MEDIO	MEDIO	ALTO	ALTO
	2	IMPROBABLE	MUY BAJO	BAJO	MEDIO	MEDIO	ALTO
	1	RARO	MUY BAJO	MUY BAJO	BAJO	BAJO	MEDIO
			INSIGNIFICANTE	MENOR	MODERADO	MAYOR	SEVERO
			1	2	3	4	5
			IMPACTO				

C) NIVEL DE CONTROL

En esta pestaña de criterios también se incluyen los criterios para la evaluación de los controles que la organización tenga previamente establecidos para prevenir, mitigar y/o eliminar los riesgos previamente identificados. Una vez identificados los controles, se determinará el nivel de gestión de la organización, es decir, se evaluará la eficacia de los mismos.

El grado de efectividad de los controles determinará el grado de actuación (mitigación, eliminación…) que proporcionan sobre un determinado riesgo. En la herramienta se establecen los siguientes niveles que deben aplicarse a la hora de evaluar los controles:

TRAMO	DESCRIPCIÓN	VALOR
INSUFICIENTE	Los controles existentes son inadecuados o no es posible el control del riesgo, al estar condicionado en su totalidad por factores externos.	1
MEDIO	Los controles existentes son adecuados, pero no suficientes, ya que son mejorables.	2
SUFICIENTE	Los controles existentes son adecuados.	3

5. EVALUACIÓN DE LOS RIESGOS

INFORMACIÓN A INTRODUCIR EN LA HERRAMIENTA

En esta pestaña, una vez que la organización ha confeccionado su catálogo de riesgos y ha definido los criterios de valoración, deberá realizar una valoración de los mismos, para lo que deberá asignar una puntuación a las siguientes columnas:

- Impacto económico (columna F): de 1 a 5, de acuerdo con la estimación de impacto.
- Impacto operacional (columna G): de 1 a 5, de acuerdo con la estimación de impacto.
- Impacto reputacional (columna H): de 1 a 5, de acuerdo con la estimación de impacto.
- Probabilidad inherente (columna J): de 1 a 5, de acuerdo con la estimación de la probabilidad de ocurrencia.
- Nivel de gestión (columna L): de 1 a 3, de acuerdo con la efectividad de los controles.

El resto de los valores se calcularán automáticamente, arrojando de este modo:

a) Impacto inherente total.
b) Riesgo inherente.
c) Impacto residual.
d) Probabilidad residual.
e) Riesgo residual.
f) Criticidad de los riesgos.
g) Mapas visuales de riesgos inherentes y residuales.

INFORMACIÓN GENERADA POR LA HERRAMIENTA EN BASE A LOS DATOS ANTERIORES

▪ IMPACTO INHERENTE TOTAL (A)

Como se ha indicado en el apartado anterior, se entiende por impacto inherente al daño que supondría para los objetivos estratégicos de la organización que el riesgo se concretara en un suceso cierto, antes de considerar cualquier control o acción mitigadora. El impacto inherente total de cada uno de los riesgos se calcula de acuerdo a la siguiente fórmula:

IMPACTO INHERENTE TOTAL = valor impacto económico x 50% + valor impacto operacional x 25% + valor impacto reputacional x 25%

▪ RIESGO INHERENTE (B)

Es conveniente distinguir entre el concepto de riesgo inherente y riesgo residual. Los riesgos son sucesos que aún no han ocurrido pero que se identifican previamente y de forma regular con el fin de gestionarlos adecuadamente para, o bien prevenir su ocurrencia, o bien en el caso de que se materialicen, reducir su impacto en la consecución de nuestros objetivos estratégicos. Estos riesgos de base, que se identifican antes de considerar cualquier control, son los que se llaman inherentes.

La herramienta calcula el valor automáticamente de acuerdo con la siguiente fórmula:

RIESGO INHERENTE = probabilidad inherente x impacto inherente global

▪ IMPACTO RESIDUAL (C) Y PROBABILIDAD RESIDUAL (D)

Para la estimación del impacto y probabilidad residuales de cada uno de los riesgos se utiliza un factor denominado nivel de vulnerabilidad, que es calculado por la herramienta en función del nivel de gestión de los

controles. El nivel de vulnerabilidad determina el factor reductor considerado por la implantación y aplicación de los controles previamente identificados, pudiendo oscilar su valor entre 0 y 1. Por tanto, a mayor nivel de gestión, es decir, de control del riesgo, menor nivel de vulnerabilidad.

En la herramienta se aplican los siguientes factores:

- Cuando el nivel de gestión sea insuficiente, se mantiene el impacto y la probabilidad inherente del riesgo, es decir, se multiplica por 1.
- En el caso de que el nivel de gestión sea medio, se corrige el impacto y/o la probabilidad un 20%, es decir, se multiplica por 0,8.
- En el caso de que el nivel de gestión sea suficiente, se reduce el impacto y/o la probabilidad un 40%, es decir, se multiplica por 0,6.

▪ RIESGO RESIDUAL (E)

El riesgo residual será el que queda tras el efecto de los controles que la organización ha implantado para eliminar o reducir la ocurrencia y/o las consecuencias de dichos riesgos, siendo el principal objetivo que dicho nivel de riesgo se sitúe por debajo del máximo nivel de riesgo que está dispuesta a asumir la organización (tolerancia al riesgo).

La herramienta calcula el valor automáticamente de acuerdo con la siguiente fórmula:

RIESGO RESIDUAL = probabilidad residual x impacto residual

▪ IMPORTANCIA O CRITICIDAD DE LOS RIESGOS (F)

Una vez calculado el riesgo residual de todos los riesgos que forman parte del catálogo de riesgos de la organización, la herramienta ayuda a determinar la importancia del riesgo (criticidad) de acuerdo con los siguientes tramos:

(ver cuadro pág.21)

Categoría	Valor riesgo residual	Descripción
Riesgo crítico	Superior a 20	Aquellos cuyo impacto y probabilidad residual se sitúan en el rango más alto de evaluación, superando la tolerancia al riesgo establecido, o aquellos que considere oportuno el órgano de gobierno, por su especial relevancia en la operativa de la organización.
Riesgo alto	Entre 10 y 20	Aquellos cuyo impacto y probabilidad residual se sitúen en un nivel cercano a la tolerancia máxima permitida.
Riesgo medio	Entre 5 y 10	Aquellos cuyo impacto y probabilidad residual se sitúen en un nivel intermedio de evaluación, dentro del nivel de tolerancia al riesgo establecido.
Riesgo bajo	Entre 2 y 5	Aquellos cuyo impacto y probabilidad residual se sitúen en el nivel más bajo de evaluación, dentro del nivel de tolerancia al riesgo establecido.
Riesgo muy bajo	Inferior a 3	Aquellos cuyo impacto y probabilidad residual se sitúen en el nivel más bajo de evaluación, dentro del nivel de tolerancia al riesgo establecido.

Con estos resultados la herramienta sugiere que los riesgos calificados como críticos siempre deben ser gestionados por la organización, y en el resto de los niveles debe ser la propia organización quien decida cuales de ellos quiere gestionar, puesto que puede que riesgos cuya criticidad es media, desde el punto de vista estratégico se consideren muy relevantes gestionar en el año.

▪ MAPAS VISUALES DE RIESGOS INHERENTES Y RESIDUALES (G)

Una vez cumplimentada toda la tabla se podrán ver justo debajo de la misma dos mapas visuales que muestran el riesgo inherente y el riesgo residual de cada uno de los riesgos incluidos en la taxonomía.

6. MATRIZ DE RIESGOS Y CONTROLES

Una vez la organización haya decidido los riesgos a gestionar en el año, éstos deberán volcarse a la última pestaña de la herramienta ("Matriz de riesgos y controles"), cuyos datos de la valoración de riesgos realizada previamente se volcarán de forma automática; así como el órgano de cumplimiento o en su defecto, el comité u órgano de dirección deberá nombrar a una persona propietaria de cada uno de los riesgos a gestionar.

Para responder a los riesgos debemos decidir entre aceptarlos, evitarlos, reducirlos o transferirlos a terceros.

Dicha persona tendrá la responsabilidad de proponer los controles ya existentes y planes de acción asociados a su riesgo, informar sobre la eficacia de los controles existentes y la implementación de los planes de acción definidos, así como custodiar la documentación soporte que acredite el nivel de gestión de los riesgos asignados durante un plazo de diez años.

Por tanto, en la herramienta se deberá agregar para cada uno de los riesgos, los datos de la persona propietaria asignada, esto es: nombre y apellidos, así como área, equipo o departamento al que pertenece.

RESPUESTA A LOS RIESGOS

En primer lugar, debemos tener en cuenta las opciones para el tratamiento de los riesgos a gestionar:

- Aceptar el riesgo, lo que implica no hacer nada, ya sea porque no se puede dado el carácter del riesgo o porque este se encuentra dentro de los niveles aceptables.
- Evitar el riesgo, es decir, no proceder con la actividad que genera el riesgo.
- Reducir el riesgo, lo que implica implementar acciones dirigidas a reducir el impacto o la vulnerabilidad del riesgo hasta un nivel aceptable.
- Transferir el riesgo a terceros, cambiando la responsabilidad sobre el mismo hacia un externo a la organización.

El tratamiento de riesgos se define en un plan, donde se detalla la respuesta a dar a los riesgos que se han priorizado, así como las medidas para que se mantengan en umbrales aceptables y, por tanto, no superen el apetito de riesgo establecido por el órgano de gobierno de la organización, entendiendo este como el riesgo que está dispuesto a asumir una organización en sus actividades.

En dicho plan de gestión, se establecen los controles ya existentes y aquellas mejoras necesarias para mejorar el nivel de gestión, puesto que es posible que se identifiquen debilidades en nuestro entorno de control.

Para su correcta implementación, es importante la asignación de responsables para cada control, el establecimiento de un cronograma donde se defina la periodicidad de cada control y la planificación de los recursos humanos y técnicos necesarios para la implementación de las medidas.

De forma adicional, es recomendable que la organización defina, para aquellos riesgos que se han priorizado, indicadores cuantitativos y/o cualitativos (Key Risk Indicators) que permiten monitorizar la posible materialización de los riesgos, para los cuales se establecerá una tolerancia. Así, en caso de que un indicador supere la tolerancia fijada, será la persona propietaria del riesgo quien deberá analizar las causas y proponer un plan de contingencia para dar respuesta a dicha situación, informando debidamente al órgano de cumplimiento.

El plan de gestión deberá ser elaborado por las personas propietarias de los riesgos, previamente asignadas, siendo estos debidamente reportados al órgano de cumplimiento o en su defecto al comité u órgano de dirección para contar con una visión corporativa; siendo adicionalmente recomendable que sean ser aprobados por el órgano de gobierno de la organización.

Todo este proceso se puede realizar con ayuda de la última pestaña de la herramienta ("Matriz de riesgos y controles", que consta de cuatro fases, las cuales desarrollamos a continuación:

- Identificación de controles existentes.
- Valoración de los controles: monitoreo y supervisión.
- Identificación de mejoras correctivas/planes de acción.
- Seguimiento de los planes de acción.

IDENTIFICACIÓN DE CONTROLES EXISTENTES

En esta última pestaña de la herramienta la organización identificará, para aquellos riesgos que haya decidido gestionar y en su caso, reducir el riesgo, mediante el conocimiento y análisis de la organización -preferiblemente a través de sus procesos documentados- los controles ya implementados. Estos controles permitirán, en última instancia, o bien reducir la probabilidad de ocurrencia de un suceso o, si este se produce, minimizar su impacto. Estos controles pueden ser muy

variados y se ajustan mucho a las características y necesidades de cada riesgo, pero, en general, consisten en pautas de trabajo vinculadas a los procesos de la organización, que deseablemente deberían estar recogidas en protocolos o procedimientos internos, con el fin de asegurar su debido funcionamiento.

Los controles pueden ser muy variados y se ajustan a las características y necesidades de cada proceso.

Un ejemplo podría ser, para prevenir y/o mitigar el posible riesgo de fraude al que está expuesta una organización, disponer de, entre otros:

- Unos criterios de selección de personas vinculadas a la organización que garanticen altos estándares éticos, atendiendo a criterios de idoneidad y de honorabilidad.

- Un código de conducta que recoja los estándares éticos que se esperan de las personas vinculadas a dicha organización y que incluya un régimen disciplinario al que poder acogerse en caso de identificar una conducta contraria al mismo.

- Un canal de denuncias realmente eficaz y accesible a todos los grupos de interés de la organización, como herramienta fundamental para destapar este tipo de conductas.

La herramienta está preparada para que se incluyan hasta cinco controles por cada riesgo, aun cuando puede haber un control que sirva para prevenir y/o mitigar más de un riesgo, en cuyo caso se deberá detallar nuevamente. Para cada uno de los controles que se incluya en la herramienta se deberá recoger la siguiente información:

- Descripción del control.

- Tipo de control: se debe elegir si se trata de un control preventivo (antes de que ocurra el suceso) o reactivo (una vez que el suceso se ha materializado).

- Frecuencia: en este caso se elegirá del desplegable una de las opciones en las que se indique la frecuencia con la que se aplica el control: por transacción / diaria / semanal / mensual / trimestral / semestral / anual.

- Responsable del control: se debe identificar a la persona responsable de cada uno de los controles, detallando el nombre y apellidos, así como el área, equipo o departamento al que pertenece.

VALORACIÓN CONTROLES (MONITOREO Y SUPERVISIÓN)

En el siguiente bloque lo que se busca es poder realizar un análisis de la efectividad de los controles, con el fin de concluir si estos realmente se están implementando y en caso de hacerlo, si están adecuadamente diseñados para prevenir y/o mitigar el riesgo. Para ello, de cada uno de los controles se deberá indicar:

- Documentación soporte aportada, sobre la evidencia de la ejecución del control: a cumplimentar por la persona responsable del control.

- Evaluación de la efectividad del control: a cumplimentar por la persona propietaria del riesgo y validada por la función de Auditoría Interna, en caso de haberla. En este caso, se deberá seleccionar, en base a los resultados arrojados por las auditorías interna y/o externas, si se considera que el nivel de efectividad de cada control es:

Insuficiente: los controles existentes son inadecuados o no es posible el control del riesgo, al estar condicionado en su totalidad por factores externos.

Medio: los controles existentes son adecuados, pero no suficientes, ya que son mejorables.

Suficiente: los controles existentes son suficientes.

Por tanto, esta evaluación de los controles de la organización difiere de la realizada previamente, ya que en este caso consiste en una evaluación pormenorizada de cada uno de los controles, y ésta no se hace en base a una estimación, sino en una revisión real de la eficacia del control con el fin de concluir si éste realmente se realiza, y en caso afirmativo, si el control está bien diseñado para reducir y/o mitigar el riesgo.

Así, el grado de efectividad del control determinará el grado de reducción que proporciona ese control sobre un determinado riesgo. Es decir, si al valorar un control existente en la organización vemos que es insuficiente, eso significará que tiene poca efectividad para reducir la probabilidad de ocurrencia y/o el impacto de dicho riesgo.

Con estas valoraciones de la efectividad de cada uno de los controles la herramienta calcula la efectividad promedio de los controles de cada uno de los riesgos, y compara esta efectividad promedio con la evaluación del nivel de gestión que se había indicado en la pestaña anterior, para así tener un análisis sobre la comparativa entre la estimación de la efectividad del nivel de gestión de la organización y la real. Para ello, se tienen en cuenta los siguientes valores:

NIVEL DE EFECTIVIDAD DE LOS CONTROLES	VALORACIÓN
Superior al nivel de gestión anterior	Ha mejorado
Igual al nivel de gestión anterior	Se mantiene
Inferior al nivel de gestión anterior	Ha empeorado

IDENTIFICACIÓN DE MEDIDAS CORRECTIVAS/PLANES DE ACCIÓN

En esta fase, es importante únicamente considerar los controles que la organización ya tiene implementados, de forma que una vez se concluya el análisis y prioricemos los riesgos sobre los que centrar nuestra gestión, será el momento de identificar controles adicionales y/o planes de acción que se van a tener que diseñar e implementar en el futuro para reducir el nivel de riesgo hasta un nivel aceptable por la organización.

Por tanto, si los controles no son suficientes o son mejorables para la gestión de los riesgos, se deberá elaborar un plan de acción, el cual sería recomendable que sea aprobado por el órgano de cumplimiento de la organización, o en su defecto por el comité u órgano de dirección de la organización, con el fin de que exista una visión estratégica e integral de las medidas de mejora a adoptar. La herramienta permite sistematizar los planes de acción, en los que se debe detallar:

- Descripción del plan de acción.
- Responsable del plan de acción: nombre y apellidos, así como área, equipo o departamento al que pertenece.
- Fecha límite de implementación (dd/mm/aa).

SEGUIMIENTO DE PLANES DE ACCIÓN

Una vez definidos los planes de acción es importante realizar un seguimiento de la implementación de estos. Para ello, en la herramienta se deberá incluir, para cada una de las medidas definidas:

- A cumplimentar por la persona responsable de diseñar e implementar el plan de acción:

  Estado de situación: se debe seleccionar el estado del desplegable "En proceso / Pendiente / Finalizado", según corresponda.

  Documentación soporte aportada: evidencia de los avances realizados.

- A cumplimentar por la persona propietaria del riesgo, y validada por la función de Auditoría Interna, en caso de haberla:

  Evaluación de la efectividad del plan de acción para prevenir y/o mitigar el riesgo: se debe seleccionar de las opciones del desplegable "Suficiente / Medio / Insuficiente".

  ¿Se ha implementado en tiempo y forma, y es efectivo?: Sí / No.

Como se ha indicado anteriormente, para garantizar que el sistema de gestión de riesgos sea sólido y eficaz, la revisión se debe realizar al menos una vez al año, o con mayor frecuencia en caso de cambios significativos en el contexto de la organización. De esta forma, nos aseguramos de que la gestión de riesgos que estamos llevando a cabo está adaptada a las necesidades y la realidad de la organización.

Un sistema de gestión de riesgos sólido y eficaz debe ser revisado al menos, una vez al año.

BUREAU VAN DIJK
A Moody's Analytics Company

Some see just a business

To us it's a subsidiary that's part of a corporate group
with 712 entities, linked to 2 PEPs,
and "sanctioned by extension"

orbis

compliance catalyst²

Winner "Best Entity Data Solution"
2 years running

Welcome to the business of certainty

Register for your free trial:
bvdinfo.com
madrid@bvdinfo.com

World Compliance Association
Paseo de la Castellana, 79, 7º planta · 28046 Madrid · España
Tel.: 91 791 66 16 · www.worldcomplianceassociation.com

Diseño y maquetación: Equipo de diseño **WCA**

© **World Compliance Association. 11·02·2022**. Todos los derechos reservados.

Se permite la reproducción total o parcial y la comunicación pública de la obra, siempre que no sea con finalidades comerciales, y siempre que se reconozca la autoría de la obra original. No se permite la creación de obras derivadas.

WORLD
COMPLIANCE
ASSOCIATION

biblioteca COMPLIANCE

La labor realizada por las organizaciones del Tercer Sector es imprescindible como actores clave para la transformación de la sociedad, como garantes de la defensa y protección de los derechos humanos. Para ello es imprescindible velar por su integridad, buen hacer y legitimidad; solo así se garantizará su continuidad. El compliance se constituye como un instrumento esencial para construir y fortalecer la confianza en ellas y su sostenibilidad, velando de este modo por el cumplimiento de los compromisos adquiridos con las partes interesadas y, por ende, alcanzar su fin fundacional.

GA_P Gómez-Acebo & Pombo
BUREAU VAN DIJK A Moody's Analytics Company
EQS GROUP