MODELO PARA LA GESTIÓN DEL RIESGO DE CUMPLIMIENTO PARA PROVEEDORES

CMD-PR-37001

Primera Edición
2023-02-03

Este documento fue desarrollado por
Certification Management & Development SAS
CMD Certification SAS
Basado en la norma ISO 37001:2016
2023
Documento registrado en la Dirección Nacional del Derecho de Autor en Colombia

Documento disponible en www.cmdcertification.com

0. INTRODUCCIÓN

Un Sistema de Gestión Cumplimiento permite que los colaboradores, directivos, accionistas, proveedores y contratistas de una organización, actúen diligentemente en la gestión de los riesgos de corrupción, no cumplimiento, lavado de activos, financiación del terrorismo, vulneración de los derechos humanos y en general, frente a conductas, acciones o decisiones que impliquen posibles delitos.

En los últimos años se han publicado diversos modelos de gestión aplicables a la administración integrada del cumplimiento, incluso en algunos países existen obligaciones legales frente a los Programas de Transparencia y Ética Empresarial, además de disposiciones expresas frente a la Seguridad en la cadena de suministro para la prevención del narcotráfico y el contrabando, la prevención del lavado de activos y otros delitos de interés trasnacional.

1. OBJETO Y CAMPO DE APLICACIÓN

Este documento especifica los requisitos para establecer, implementar, mantener, revisar y mejorar un sistema de gestión simplificado para el Cumplimiento de proveedores de bienes y servicios, donde sus clientes les soliciten una adecuada gestión del riesgo de Cumplimiento. El documento puede ser aplicado voluntariamente por proveedores que deseen demostrar a organizaciones que cuentan con un sistema de gestión simplificado que contribuye a la gestión del riesgo de Cumplimiento.

Este documento puede ser empleado por organizaciones proveedoras, como modelo de gestión para el Cumplimiento, también puede ser aplicado con propósitos de obtener una puntuación a partir de una evaluación realizada por CMD Certification.

2 REFERENCIAS NORMATIVAS

Norma internacional ISO 37001:2016.

3 TÉRMINOS Y DEFINICIONES (Tomadas de ISO 37001:2016)

Para los fines de este documento, se aplican los siguientes términos y definiciones.

3.1
Soborno
Oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor (que puede ser de naturaleza financiera o no financiera), directamente o indirectamente, e independientemente de su ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación con el desempeño (3.16) de las obligaciones de esa persona

3.2
Organización.
Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus objetivos (3.11)

Nota 1 a la entrada: El concepto de organización incluye, entre otros, un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, organización caritativa o institución, o una parte o combinación de estas, ya sea de responsabilidad limitada o compartida o de otra índole, públicas o privadas.

Nota 2 a la entrada: Para organizaciones con más de una unidad operativa, una o más de una unidad de operación se puede definir como una organización.

3.3
Parte interesada
Persona u organización (3.2) que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.

Nota 1 a la entrada: Parte interesada puede ser interna o externa de la organización.

3.4
Requisito
Necesidad que está establecida y es obligatoria.

Nota 1 a la entrada: La definición esencial de “requisito” en normas ISO de sistemas de gestión es “necesidad o expectativa establecida, generalmente implícita u obligatoria”. La parte de “generalmente implícita” de esta definición no es utilizada en este documento.

Nota 2 a la entrada: "Generalmente implícita" significa que es una costumbre o una práctica común de la organización o partes interesadas de que la necesidad o expectativa bajo consideración es implícita.

Nota 3 a la entrada: Un requisito específico es aquel que es establecido, por ejemplo en la información documentada.

3.5
Sistema de gestión
Conjunto de elementos de una organización (3.2) interrelacionados o que interactúan para establecer políticas (3.10) y objetivos (3.11) y procesos (3.15) para lograr estos objetivos.

Nota 1 a la entrada: Un sistema de gestión puede considerar una sola disciplina o varias disciplinas.

Nota 2 a la entrada: Los elementos del sistema incluyen la estructura de la organización, los roles y las responsabilidades, la planificación y la operación, la evaluación del desempeño y la mejora.

Nota 3 a la entrada: El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

3.6
Alta dirección
Persona o grupo de personas que dirige y controla una organización (3.2) al más alto nivel.

Nota 1 a la entrada: La alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización.

Nota 2 a la entrada: Si el alcance del sistema de gestión (3.5) comprende solo una parte de la organización, entonces la alta dirección se refiere a quienes dirigen y controlan esa parte de la organización.

Nota 3 a la entrada: Las organizaciones pueden ser organizadas de acuerdo a su tamaño, sector, etc. Algunas organizaciones poseen tanto un órgano de gobierno (3.7) como una alta dirección (3.6), mientras que en algunas organizaciones no se dividen las responsabilidades en varios órganos. Estas variaciones, tanto en lo que se refiere a la organización y responsabilidades pueden ser consideradas cuando se aplican los requisitos en el capítulo 5.

3.7
Órgano de gobierno
Grupo u que tiene en últimas la responsabilidad y autoridad fundamental sobre las actividades, la gobernabilidad y las políticas una organización (3.2), y al que la alta dirección (3.6) le informa y al que la alta dirección le rinde cuentas.

Nota 1 a la entrada: No todas las organizaciones, especialmente las organizaciones pequeñas, tendrán un órgano de gobierno independiente de la alta dirección (véase 3.6, Nota 3 a la entrada).

Nota 2 a la entrada: Un órgano de gobierno puede incluir pero no está limitado a una Junta directiva, comités de la junta, consejo de vigilancia, administradores y supervisores.

3.8
Función de cumplimiento (Adaptado de ISO 37001)
Persona(s) con responsabilidad y autoridad para el funcionamiento del sistema de gestión (3.5) simplificado del Cumplimiento (3.33).

3.9
Eficacia
Grado en el cual se realizan las actividades planificadas y se logran los resultados planificados.

3.10
Política
Intenciones y dirección de una organización (3.2), como las expresa formalmente su alta dirección (3.6) o de su órgano de gobierno (3.7)

3.11
Objetivo
Resultado a lograr.

Nota 1 a la entrada: Un objetivo puede ser estratégico, táctico u operativo.

Nota 2 a la entrada: Los objetivos pueden referirse a diferentes disciplinas (tales como financieras, ventas y marketing, compras, de salud y seguridad y ambientales), se pueden aplicar en diferentes niveles (tales como estratégicos, para toda la organización, para proyectos, productos y procesos (3.15)).

Nota 3 a la entrada: Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, un objetivo de cumplimiento, o mediante el uso de términos con un significado similar (por ejemplo, finalidad, meta u objetivo).

Nota 4 a la entrada: En el contexto de sistemas de gestión de cumplimiento, la organización establece los objetivos de cumplimiento, en concordancia con la política de cumplimiento, para lograr resultados específicos.

3.12
Riesgo
Efecto de la incertidumbre sobre los objetivos (3.11)

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un suceso, su consecuencia o su probabilidad.

Nota 3 a la entrada: Con frecuencia el riesgo se caracteriza por ser referido como eventos potenciales (según se define en la Guía ISO 73:2009, 3.5.1.3) y consecuencias (según se define en la Guía ISO 73:2009, 3.6.1.3), o a una combinación de estos.

Nota 4 a la entrada: Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad (según se define en la Guía ISO 73:2009, 3.6.1.1) asociada de que ocurra.

3.13
Competencia
Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

3.14
Información documentada
Información que una organización (3.2) tiene que controlar y mantener, y el medio que la contiene.

Nota 1 a la entrada: La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

Nota 2 a la entrada: La información documentada puede hacer referencia a:

- El sistema de gestión (3.5), incluidos los procesos (3.15) relacionados;
- La información generada para que la organización opere (documentación);
- La evidencia de los resultados alcanzados (registros).

3.15
Proceso
Conjunto de actividades mutuamente relacionadas que interactúan, que transforma los elementos de entrada en elementos de salida

3.16
Desempeño
Resultado medible.

Nota 1 a la entrada: El desempeño puede relacionarse con hallazgos cuantitativos o cualitativos.

Nota 2 a la entrada: El desempeño se puede relacionar con la gestión de actividades, procesos (3.15), productos (incluidos servicios), sistemas u organizaciones (3.2).

3.17
Contratación externa
Establecer un acuerdo mediante el cual una organización (3.2) externa realiza parte de una función o proceso (3.15) de una organización.

Nota 1 a la entrada: Una organización externa está fuera del alcance del sistema de gestión (3.5), aunque la función o proceso contratado externamente forme parte del alcance.

Nota 2 a la entrada: El texto esencial de las normas ISO de sistemas de gestión contiene una definición y un requisito en relación con la contratación externa, el cual no es utilizado en este documento, ya que proveedores externos están incluidos en la definición de socio de negocios (3.26)

3.18
Seguimiento
Determinación del estado de un sistema, un proceso (3.15) o una actividad.

Nota 1 a la entrada: Para determinar el estado puede ser necesario verificar, supervisar u observar en forma crítica.

3.19
Medición
Proceso (3.15) para determinar un valor

3.20
Auditoría
Proceso (3.15) sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

Nota 1 a la entrada: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).

Nota 2 a la entrada: Una auditoría interna es conducida por la organización o por una parte externa que actúe en su nombre.

Nota 3 a la entrada: “Evidencia de auditoría” y “criterios de auditoría” se definen en ISO 19011.

3.21
Conformidad
Cumplimiento de un requisito (3.4)

3.22
No conformidad
Incumplimiento de un requisito (3.4)

3.23
Acción correctiva
Acción para eliminar la causa de una no conformidad (3.22) y para evitar que vuelva a ocurrir.

3.24
Mejora continua
Actividad recurrente para mejorar el desempeño (3.16).

3.25
Personal
Directores, oficiales, empleados, empleados o trabajadores temporales y voluntarios de la organización (3.2).

Nota 1 a la entrada: Diferentes tipos de personal plantean diferentes tipos y grados de riesgo (3.12) de no cumplimiento y, por lo tanto, pueden ser tratados de manera diferente por los procedimientos de evaluación de riesgo de cumplimiento y de gestión de riesgos de cumplimiento de la organización.

Nota 2 a la entrada: Véase el apartado 8.5 para guiarse sobre los empleados o trabajadores temporales.

3.26
Socio de negocios
Parte externa con la que la organización (3.2), tiene o planea establecer algún tipo de relación comercial.

Nota 1 a la entrada: Socio de negocios incluye, pero no se limita a los clientes, consumidores, empresas conjuntas, socios de empresas conjuntas, los socios del consorcio, la externalización de los proveedores, contratistas, consultores, subcontratistas, proveedores, vendedores, asesores, agentes, distribuidores, representantes, intermediarios e inversionistas. Esta definición es deliberadamente amplia y debe ser interpretada de acuerdo con el perfil de riesgo (3.12) del no cumplimiento de la organización para aplicar a los socios de negocios que puedan exponer razonablemente a la organización a riesgos de cumplimiento.

Nota 2 a la entrada: Diferentes tipos de socio de negocios plantean diferentes tipos y grados de riesgo de cumplimiento, y una organización (3.2) tendrá diferentes grados de capacidad para influir en diferentes tipos de socio de negocios. Por lo tanto, diferentes tipos de socio de negocios pueden ser tratados de manera diferente por los procedimientos de evaluación de riesgo de cumplimiento y de gestión de riesgos de cumplimiento de la organización.

Nota 3 de entrada: La referencia a "negocio" en este documento puede interpretarse en sentido amplio para significar a aquellas actividades que son relevantes a los efectos de la existencia de la organización.

3.27
Funcionario público
Toda persona que ocupe un cargo legislativo, administrativo o judicial, ya sea por designación, elección o sucesión, o cualquier persona que ejerza una función pública, incluso para un organismo

público o una empresa pública, o cualquier funcionario o agente de una organización nacional o internacional público o cualquier candidato para un cargo público.

3.28
Tercera parte
Persona u organismo que es independiente de la organización.

Nota 1 a la entrada: Todos los socios de negocios (3.26) son tercera parte, pero no todas las terceras partes son socios de negocios.

3.29
Conflicto de intereses
Situación en donde los intereses de negocios, financieros, familiares, políticos o personales podrían interferir con el criterio de las personas al realizar sus obligaciones para la organización (3.2).

3.30
Gestión del riesgo con nivel de riesgo residual inaceptable
Proceso (3.15) para evaluar con mayor detalle la naturaleza y alcance del riesgo de cumplimiento (3.12) y ayudar a las organizaciones (3.2) a tomar decisiones en relación con operaciones, proyectos, actividades, socios de negocios y personal específicos.

3.31
Lavado de activos (Tomado de UNODC)
El Lavado de Activos es un delito, que consiste en dar una apariencia de origen legítimo o lícito a bienes - dinerarios o no, que en realidad son productos o "ganancias" de delitos graves como: Tráfico ilícito de drogas, Trata de Personas, Corrupción, secuestros y otros.

3.32
Financiación del terrorismo (Tomado de CNBS)
Cualquier forma de acción económica, ayuda o mediación que proporcione apoyo financiero a las actividades de elementos o grupos terroristas. También, es la captación y el procesamiento de activos para dotar a los terroristas con recursos que les permitan llevar a cabo sus actividades.

3.33
Cumplimiento
Obligaciones legales y voluntarias asociadas a la prevención del lavado de activos, la financiación del terrorismo y soborno (3.1), incluido el cohecho con funcionarios públicos (3.27) nacionales y trasnacionales.

4 CONTEXTO DE LA ORGANIZACIÓN

4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr su política del sistema de gestión del Cumplimiento. Estas cuestiones incluyen, pero no se limitan a, los siguientes factores:

a) el tamaño, estructura y autoridad delegada con poder de decisión de la organización;
b) los lugares y sectores en los que opera la organización o planea operar;
c) la naturaleza, escala y complejidad de las actividades y operaciones de la organización;
d) el modelo de negocio de la organización;
e) las entidades sobre las que la organización tiene el control y entidades que ejercen control sobre la organización;
f) los socios de negocios de la organización;
g) la naturaleza y alcance de las interacciones con los funcionarios públicos;
h) los deberes y obligaciones estatutarias, reglamentarias, contractuales y profesionales aplicables, y;
i) los proyectos y tipos de contratos que la organización suscribe con sus clientes.

NOTA Una organización tiene control sobre otra organización si controla directa o indirectamente la gestión de la organización.

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La organización debe determinar:

a) las partes interesadas que son pertinentes relevantes para el sistema de gestión del Cumplimiento, incluidos sus clientes y proveedores;
b) los requisitos relevantes de estas partes interesadas en cuanto al Cumplimiento.

NOTA En la identificación de los requisitos de las partes interesadas, una organización puede distinguir entre los requisitos obligatorios y las expectativas de carácter no obligatorio, y compromisos voluntarios, a las partes interesadas.

4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DEL CUMPLIMIENTO

La organización debe determinar los límites y la aplicabilidad del sistema de gestión del Cumplimiento para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas mencionadas en 4.1;
b) los requisitos mencionados en 4.2;
c) los resultados de la evaluación del riesgo de cumplimiento referenciado en 4.5.

El alcance debe estar disponible como información documentada.

4.4 SISTEMA DE GESTIÓN DEL CUMPLIMIENTO

La organización debe establecer, documentar, implementar, mantener y revisar continuamente y, cuando sea necesario, mejorar el sistema de gestión del Cumplimiento, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

El sistema de gestión del Cumplimiento contendrá medidas destinadas a identificar y evaluar el riesgo de cumplimiento, y para prevenir, detectar y responder lo relacionado a las obligaciones de cumplimiento (ver 3.33).

NOTA 1 El sistema de gestión del Cumplimiento debe ser razonable y proporcionado, teniendo en cuenta los factores mencionados en 4.3.

4.5 EVALUACIÓN DE RIESGOS DE CUMPLIMIENTO

4.5.1 La organización debe realizar regularmente evaluación(es) del riesgo de cumplimiento que deberá(n):

a) identificar el riesgo de cumplimiento (ver 3.33) que la organización podría anticipar razonablemente, dado los factores enumerados en el apartado 4.1;
b) analizar, evaluar y priorizar los riesgos de cumplimiento identificados;
c) evaluar la idoneidad y eficacia de los controles existentes de la organización para mitigar los riesgos de cumplimiento evaluados.

Nota 1: Los riesgos de cumplimiento mencionados incluyen los relacionados con soborno (ver 3.1), Lavado de Activos (3.31) y Financiación del Terrorismo (3.32).
Nota 2: La organización podría incluir riesgos relacionados con la prevención de otros delitos como la trata de personas, narcotráfico y otros.

4.5.2 La organización debe establecer criterios para evaluar su nivel de riesgo de cumplimiento, los cuales tendrán en cuenta las políticas y objetivos de la organización.

4.5.3 La evaluación de los riesgos de cumplimiento debe ser revisada:

a) de manera periódica de modo que los cambios y los nuevos datos puedan ser adecuadamente evaluados con base en los tiempos y la frecuencia definidos por la organización;
b) en el caso de un cambio significativo en la estructura o las actividades de la organización.

4.5.4 La organización debe conservar la información documentada que demuestre que la evaluación del riesgo de cumplimiento se ha llevado a cabo, y se utiliza para diseñar o mejorar el sistema de gestión del Cumplimiento.

5 LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

5.1.1 Alta dirección
La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión del Cumplimiento:

a) asegurándose de que el sistema de gestión del Cumplimiento, que incluye la política, se establezca, implemente, mantenga y se revise que estos sean compatibles con la dirección estratégica de la organización;
b) asegurándose de la integración de los requisitos del sistema de gestión del Cumplimiento en los procesos de la organización;
c) desplegando recursos suficientes y adecuados para el funcionamiento eficaz del sistema de gestión del Cumplimiento;
d) comunicando interna y externamente lo relacionado con la política de cumplimiento;
e) comunicando internamente la importancia de la gestión eficaz de cumplimiento y la conformidad con los requisitos del sistema de gestión del Cumplimiento;
f) asegurándose que el sistema de gestión del Cumplimiento esté diseñado adecuadamente para cumplir con su política;
g) dirigiendo y apoyando al personal para contribuir a la eficacia del sistema de gestión del Cumplimiento;
h) promocionando una cultura de cumplimiento apropiada dentro de la organización;
i) promoviendo la mejora continua;
j) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo en la prevención y detección de formas de no cumplimiento que sea aplicable a sus áreas de responsabilidad;
k) fomentando el uso de los procedimientos para reportar la sospecha de delitos o delitos reales que pudieran cometerse en el marco de las actividades de la organización;
l) asegurándose de que ningún miembro del personal sufrirá represalias, discriminación o medidas disciplinarias por cuenta de los reportes hechos de buena fe o sobre la base de una creencia razonable de violación o sospecha de violación a la política de cumplimiento de la organización, o por negarse a participar en un delito, incluso si tal negativa podría dar lugar a la pérdida de negocios para la organización (excepto cuando el individuo participó en la violación);

5.2 POLÍTICA DE CUMPLIMIENTO

La alta dirección debe establecer, mantener y revisar una política de cumplimiento que:

a) prohíba cualquier práctica que conduzca al no cumplimiento (ver 3.33);
b) requiera del cumplimiento de las leyes de prevención y acción frente a acciones de no cumplimiento que son aplicables a la organización;
c) sea apropiada al propósito de la organización;
d) incluya el compromiso de cumplir los requisitos aplicables al sistema de gestión del Cumplimiento;
e) fomente el reporte en buena fe o sobre la base de una creencia razonable en confianza y sin temor a represalias;
f) incluya un compromiso de mejora continua del sistema de gestión del Cumplimiento;

La política de cumplimiento debe:

- estar disponible como información documentada;
- ser comunicada en los idiomas apropiados dentro de la organización y a los socios de negocios;
- estar disponible para las partes interesadas relevantes, según corresponda.

5.3 ROLES, RESPONSABLIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

5.3.1 Roles y responsabilidades

La alta dirección debe tener la responsabilidad general de la aplicación y el cumplimiento del sistema de gestión de cumplimiento tal como se describe en el apartado 5.1.1.

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes sean asignados y comunicados dentro y a través de todos los niveles de la organización.

Los directivos en todos los niveles deben ser responsables de solicitar que los requisitos del sistema de gestión del Cumplimiento sean aplicados y cumplidos en su departamento o función.

5.3.2 Función de cumplimiento

La alta dirección debe asignar a la función de cumplimiento la responsabilidad y autoridad para:
a) supervisar el diseño e implementación por parte de la organización del sistema de gestión del Cumplimiento;
b) proporcionar asesoramiento y orientación al personal sobre el sistema de gestión del Cumplimiento y las cuestiones relacionadas con el Cumplimiento;
c) asegurar que el sistema de gestión del Cumplimiento cumpla los requisitos de este documento;
d) informar sobre el desempeño del sistema de gestión del Cumplimiento a la alta dirección y otras funciones de cumplimiento, según corresponda.

La función de cumplimiento debe disponer de recursos suficientes y ser asignada a la persona (s) que tengan la competencia apropiada, la posición, autoridad e independencia.

La función de cumplimiento debe tener acceso directo y rápido al órgano de gobierno (si existe) y a la alta dirección en el caso de que cualquier problema o inquietud tenga que ser elevado en relación con el no cumplimiento o el sistema de gestión del Cumplimiento.

La alta dirección puede asignar parte o la totalidad del cumplimiento de la función de cumplimiento a personas externas a la organización. Si lo hace, la alta dirección debe asegurar que personal específico tenga la responsabilidad y autoridad sobre aquellas partes externas asignadas a la función.

6 APOYO

6.1 RECURSOS

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión del Cumplimiento.

6.2 COMPETENCIA

6.2.1 Generalidades

La organización debe:
a) determinar la competencia necesaria de la(s) persona(s) que realiza(n), bajo su control, un trabajo que afecte su desempeño de cumplimiento;
b) asegurar que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas;
c) cuando sea aplicable, tomar acciones para adquirir y mantener la competencia necesaria y evaluar la eficacia de las acciones tomadas;
d) conservar la información documentada apropiada, como evidencia de la competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo, la oferta de formación, mentoría, o la reasignación de personal o socios de negocios, o el reclutamiento o la contratación de los mismos.

6.3 TOMA DE CONCIENCIA Y FORMACIÓN

La organización debe proporcionar concientización y formación de cumplimiento adecuada y apropiada para el personal. Dicha formación se debe referir a los siguientes asuntos, cuando sean apropiados, teniendo en cuenta los resultados de la evaluación del riesgo de cumplimiento (véase 4.5):

a) La política de cumplimiento de la organización, procedimientos y sistema de gestión del Cumplimiento y su deber de cumplirlos;
b) el riesgo de cumplimiento y el daño que puede resultar de acciones de no cumplimiento sobre ellos mismos y la organización;
c) las circunstancias en las que el no cumplimiento puede ocurrir en relación con sus funciones, y cómo reconocer estas circunstancias;
d) cómo reconocer y responder a las solicitudes u ofertas de no cumplimiento;
e) cómo pueden ayudar a prevenir y a evitar el no cumplimiento y reconocer indicadores de riesgo de cumplimiento;
f) su contribución a la eficacia del sistema de gestión del Cumplimiento, incluyendo los beneficios de un mejor comportamiento de cumplimiento y de reportar cualquier sospecha de no cumplimiento;
g) las implicaciones y potenciales consecuencias de no ajustarse a los requisitos del sistema de gestión del Cumplimiento;
h) cómo y a quién deben informar de cualquier asunto que genere sospecha o presunción de no cumplimiento;

i) información sobre la formación y los recursos disponibles.

Se debe proporcionar al personal toma de conciencia y formación de cumplimiento de manera periódica (a intervalos planificados determinados por la organización) según corresponda a sus funciones, los riesgos de cumplimiento a los que está expuesto, y cualquier circunstancia cambiante. Los programas de toma de conciencia y formación se deben actualizar periódicamente según sea necesario para reflejar nueva información pertinente.

Teniendo en cuenta los riesgos de cumplimiento identificados (véase 4.5), la organización debe implementar procedimientos que contemplen la toma de conciencia de cumplimiento y la formación de los socios de negocios que actúan en su nombre o en su beneficio y que pueden suponer más que un riesgo bajo de no cumplimiento a la organización. Estos procedimientos deben identificar a los socios de negocios para los cuales es necesaria la toma de conciencia y la formación, su contenido, y los medios por los cuales se debe proporcionar la formación.

La organización debe conservar información documentada sobre los procedimientos de formación, el contenido de la formación, y cuándo y quién la recibió.

NOTA 1 Los requisitos de toma de conciencia y formación para socios de negocios pueden ser comunicados a través de requisitos contractuales o similares, y ser ejecutados por la organización, el socio de negocios o por otras partes destinadas para tal fin.

6.4 INFORMACIÓN DOCUMENTADA

6.4.1 Generalidades

El sistema de gestión del Cumplimiento de la organización debe incluir:

a) la información documentada requerida por este documento;
b) la información documentada que la organización determina como necesaria para la eficacia del sistema de gestión del Cumplimiento.

NOTA 1 La extensión de la información documentada para un sistema de gestión del Cumplimiento puede variar de una organización a otra, debido a:

- El tamaño de la organización y su tipo de actividades, procesos, productos y servicios;
- La complejidad de los procesos y sus interacciones;
- La competencia del personal.

NOTA 2 La información documentada puede ser conservada por separado como parte del sistema de gestión del Cumplimiento, o se puede ser conservada como parte de otros sistemas de gestión (por ejemplo, cumplimiento, financiero, comercial, de auditoría, etc.), y sujeto a la política de retención de documentos de la organización.

6.4.2 Creación y actualización

Al crear y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
b) el formato (por ejemplo, idioma, versión del software, gráficos) y los medios de soporte (por ejemplo, papel, electrónico);
c) la revisión y aprobación con respecto a la idoneidad y adecuación.

6.4.3 Control de la información documentada

La información documentada requerida por el sistema de gestión del Cumplimiento y por este documento se debe controlar para asegurarse de que:

a) esté disponible y sea idónea para su uso, dónde y cuándo se necesite;
b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

- Distribución, acceso, recuperación y uso;
- Almacenamiento y preservación, incluida la preservación de la legibilidad;
- Control de cambios (por ejemplo, control de versión);
- Conservación y disposición final;

La información documentada de origen externo que la organización determina como necesaria para la planificación y operación del sistema de gestión del Cumplimiento se debe identificar, según sea apropiado, y controlar.

NOTA El acceso puede implicar una decisión en relación con el permiso solamente para consultar la información documentada, o el permiso y a la autoridad para consultar y modificar la información documentada.

7 OPERACIÓN

7.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La organización debe planificar, implementar, revisar y controlar los procesos necesarios para cumplir los requisitos del sistema de gestión del Cumplimiento, mediante:

a) el establecimiento de acciones para mitigar, evitar o tratar los riesgos de cumplimiento, cuyo nivel de riesgo residual se encuentre en zona de no aceptación.
b) el establecimiento de criterios para los procesos determinados en el sistema de gestión (ver 4.4);
c) la implementación del control de los procesos de acuerdo con los criterios;
d) la conservación de información documentada en la medida necesaria para confiar en que los procesos se han llevado a cabo según lo planificado.
e) Rastreo de dinero hasta el destinatario final real de la transacción.
d) Registro y análisis de operaciones sospechosas que indiquen posibles no cumplimientos.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario.

La organización debe asegurar que los procesos de contratación externa sean controlados.

7.2 GESTIÓN DEL RIESGO

Los métodos de evaluación del riesgo de cumplimiento deben permitir cuantificar el nivel de riesgo residual y calificar este nivel en un rango de aceptación o no aceptación.

Cuando la evaluación del riesgo de cumplimiento de la organización, realizada según 4.5, ha determinado que el nivel de riesgo residual obtenido es inaceptable, en relación con:

a) determinadas categorías de transacciones, proyectos o actividades;
b) las relaciones existentes o planificadas con categorías específicas de socios de negocios; o
c) categorías específicas del personal en determinadas posiciones.

La organización debe evaluar la naturaleza y alcance del riesgo de cumplimiento en relaciones específicas con las operaciones, proyectos, actividades, socios de negocios y personal de negocios pertenecientes a estas categorías. Este análisis incluirá cualquier acción necesaria para obtener información suficiente para evaluar el riesgo de cumplimiento.

Cuando una parte interesada represente un nivel de riesgo de cumplimiento residual inaceptable, se debe rastrear la historia comercial y antecedentes de esta parte interesada; esta información debe considerarse para la toma de decisiones de establecer relaciones comerciales con esta parte interesada.

7.3 CONTROLES FINANCIEROS

Según sea aplicable, la organización debe implementar controles financieros que gestionen el riesgo de cumplimiento, cuando el nivel de riesgo residual resulte inaceptable.

7.4 CONTROLES NO FINANCIEROS

Según sea aplicable, la organización debe implementar controles no financieros que gestionen el riesgo de cumplimiento en relación con áreas tales como compras, operaciones, ventas, comercial, recursos humanos, legal y actividades regulatorias, cuando el nivel de riesgo residual resulte inaceptable.

7**.5 COMPROMISOS DE CUMPLIMIENTO**

Para todo el personal de la organización, así como para socios de negocios que representen un nivel de riesgo residual inaceptable, la organización debe implementar procedimientos que exijan que, en la medida de lo posible:

a) personal y socios de negocios se comprometan a prevenir el no cumplimiento por, o en nombre de, o en beneficio propio o del socio de negocios en relación con la función u operación correspondiente, proyecto, actividad o relación;
b) la organización sea capaz de poner fin a la relación con el socio de negocios en el caso de no cumplimiento por parte de, o en nombre de, o en beneficio del socio de negocios en relación con la transacción correspondiente, proyecto, actividad o relación.

7.6 REGALOS, HOSPITALIDAD, DONACIONES Y BENEFICIOS SIMILARES

La organización debe implementar procedimientos que estén diseñados para prevenir la oferta, el suministro o la aceptación de regalos, hospitalidad, donaciones y beneficios similares, en los que la oferta, el suministro o la aceptación sean o puedan ser razonablemente percibidos como no cumplimiento o un soborno.

7.7 PLANTEAMIENTO DE INQUIETUDES Y DENUNCIAS

La organización debe implementar procedimientos, para:
a) fomentar y facilitar a las personas reportar en buena fe o en base de una sospecha razonable la intención, la sospecha y el no cumplimiento real, o cualquier violación o debilidad en el sistema de gestión del Cumplimiento, a la función de cumplimiento o al personal apropiado (ya sea directamente o a través de una tercera parte apropiada);
b) salvo en la medida necesaria para que una investigación avance, solicitar que la organización trate los informes de forma confidencial con el fin de proteger la identidad del informante y de otras personas que participen o a las que se haga referencia en el informe;
c) permitir el reporte anónimo;
d) prohibir represalias, y proteger a los que realicen el reporte de represalias, después de que ellos en buena fe o sobre la base de una creencia razonable plantearon o reportaron una preocupación por intento, real o supuesta no cumplimiento o violaciones de la política de cumplimiento o del sistema de gestión del Cumplimiento;
e) permitir que el personal reciba el asesoramiento de una persona apropiada sobre qué hacer si se enfrentan a un problema o situación que podría involucrar el no cumplimiento.

La organización debe asegurarse de que todo el personal esté al tanto de los procedimientos de reporte, y que sean capaces de utilizarlos, y sean conscientes de sus derechos y protecciones bajo los procedimientos.

NOTA 1 Estos procedimientos pueden ser los mismos, o formar parte de los, que se utilizan para el reporte de otros asuntos de interés (por ejemplo, seguridad, negligencia, delito o de otro riesgo grave).

NOTA 2 La organización puede usar un socio de negocios para gestionar el sistema de información en su nombre.

7.8 INVESTIGACIÓN Y LUCHA CONTRA EL NO CUMPLIMIENTO

La organización debe implementar procedimientos para:

a) requerir una evaluación y, cuando sea apropiado, la investigación de algún no cumplimiento, o el incumplimiento de la política de cumplimiento o el sistema de gestión del Cumplimiento, que sea reportado, detectada o sobre el cual existe una sospecha razonable;
b) requerir medidas apropiadas en caso de que la investigación revele algún no cumplimiento, o el incumplimiento de la política de cumplimiento o del sistema de gestión del Cumplimiento;
c) empoderar y facilitar a los investigadores;
d) requerir la cooperación en la investigación realizada por el personal pertinente; y
e) requerir que el estado y los resultados de la investigación sean reportados a la función de cumplimiento y otras funciones de cumplimiento, según corresponda.
f) requerir que la investigación se lleve a cabo de forma confidencial y que los resultados sean confidenciales.

La investigación debe ser llevada a cabo y reportada al personal que no sea parte del papel o función que está siendo investigado. La organización puede nombrar a un socio de negocios para llevar a cabo la investigación y reportar los resultados al personal que no forman parte del papel o función que está siendo investigado.

8 MEJORA

8.1 NO CUMPLIMIENTOS Y ACCIONES CORRECTIVAS

Cuando ocurre un no cumplimiento, la organización debe:

a) reaccionar inmediatamente ante el no cumplimiento, y según sea aplicable:
1) tomar acciones para controlarlo y corregirlo,
2) hacer frente a las consecuencias;
b) evaluar la necesidad de acciones para eliminar las causas del no cumplimiento, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:
1) la revisión y el análisis del no cumplimiento,
2) la determinación de las causas del no cumplimiento, y
3) la determinación de si existen no cumplimientos similares, o que podrían ocurrir;
c) implementar cualquier acción necesaria;
d) revisar la eficacia de cualquier acción correctiva tomada;
e) si fuera necesario, hacer cambios al sistema de gestión del Cumplimiento.

Las acciones correctivas deben ser apropiadas a los efectos de los no cumplimientos encontrados.

La organización debe conservar información documentada adecuada, como evidencia de:

- La naturaleza de los no cumplimientos y cualquier acción tomada posteriormente;
- Los resultados de cualquier acción correctiva.

El tratamiento y reporte de los no cumplimientos debe ser consistente con las obligaciones legales aplicables al respecto.