GUÍA DE HERRAMIENTAS PARA LA IMPLEMENTACIÓN DEL SISTEMA DE CONTROL INTERNO (HISCI)

COMPONENTE II:
EVALUACIÓN DE RIESGOS

COMPONENTE II: EVALUACIÓN DE RIESGOS

Este componente identifica los posibles riesgos asociados con el logro de los objetivos de la organización:

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
Evaluación de riesgos	**6.** La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.	**Objetivos Operativos:** ✓ Refleja las elecciones de la administración. ✓ Considera la tolerancia al riesgo. ✓ Incluye las metas de desempeño operativo y financiero. ✓ Constituye una base para confiar los recursos.
		Objetivos de Reporte Financiero Externo: ✓ Cumple con los estándares contables aplicables. ✓ Considera la materialidad. ✓ Refleja las actividades de la entidad.
		Objetivos de Reporte no Financiero Externo: ✓ Cumple con los estándares y marcos externos establecidos. ✓ Considera los niveles de precisión requeridos. ✓ Refleja las actividades de la entidad.

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
		Objetivos de Reporte interno: ✓ Refleja las elecciones de la administración. ✓ Considera el nivel requerido de precisión. ✓ Refleja las actividades de la entidad.
		Objetivos de Cumplimiento: ✓ Refleja las leyes y regulaciones externas. ✓ Considera la tolerancia al riesgo.
	7. La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determinar cómo se deben gestionar.	Incluye la entidad, sucursales, divisiones, unidad operativa y niveles funcionales. La organización identifica y evalúa los riesgos a nivel de la entidad, sucursales, divisiones, unidad operativa y niveles funcionales relevantes para la consecución de los objetivos.
		Evalúa la consideración de factores externos e internos en la identificación de los riesgos que puedan afectar a los objetivos.
		Involucra a los niveles apropiados de la administración. La dirección evalúa si existen mecanismos adecuados para la identificación y análisis de riesgos.
		Analiza la relevancia potencial de los riesgos identificados y

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
		entiende la tolerancia al riesgo de la organización.
		Determina la respuesta a los riesgos. La evaluación de riesgos incluye la consideración de cómo el riesgo debería ser gestionado y si aceptar, evitar, reducir o compartir el riesgo.
	8. La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.	Considera varios tipos de fraude: La evaluación del fraude considera el Reporting fraudulento, posible pérdida de activos y corrupción.
		La evaluación del riesgo de fraude evalúa incentivos y presiones.
		La evaluación del riesgo de fraude tiene en consideración el riesgo de fraude por adquisiciones no autorizadas, uso o enajenación de activos, alteración de los registros de información, u otros actos inapropiados.
		La evaluación del riesgo de fraude considera cómo la dirección u otros empleados participan en o justifican acciones inapropiadas.

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
	9. La organización idéntica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.	Evalúa cambios en el ambiente externo. El proceso de identificación de riesgos considera cambios en los ambientes regulatorio, económico, y físico en los cuales la entidad opera.
		Evalúa cambios en el modelo de negocios. La organización considera impactos potenciales de las nuevas líneas del negocio, composiciones alteradas dramáticamente de las líneas existentes de negocios, operaciones de negocios adquiridas o de liquidación en el sistema de control interno, rápido crecimiento, el cambio de dependencia en geografías extranjeras y nuevas tecnologías.
		Evalúa cambios en liderazgo. La organización considera cambios en administración y respectivas actitudes y filosofías en el sistema de control interno.

Evaluación de riesgos

Toda organización debe hacer frente a una serie de riesgos de origen tanto interno como externo, que deben ser evaluados. Estos riesgos afectan a las entidades en diferentes sentidos como en su habilidad para competir con éxito, mantener una posición financiera fuerte y una imagen pública positiva. Por ende se entiende por riesgo cualquier causa probable de que no se cumplan los objetivos de la organización. De esta manera la organización debe prever, conocer y abordar los riesgos con los que se enfrentan, para establecer mecanismos que los identifiquen, analicen y disminuyan. Este es un proceso dinámico e iterativo que constituye la base para determinar cómo se gestionaran los riesgos.

Principio 6: Especifica objetivos relevantes

La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados a los objetivos. Antes de llevar a cabo la evaluación de riesgos, se deben establecer los objetivos asociados a los diferentes niveles de la entidad, los objetivos operativos, de información/Reporting y de cumplimiento, los cuales deben ser consistentes con la misión de la entidad.

Para determinar si los objetivos son pertinentes, la administración debe considerar:

- ✓ Alineación de los objetivos establecidos con las prioridades estratégicas.
- ✓ Articulación de la tolerancia al riesgo para los objetivos.
- ✓ Alineación entre los objetivos establecidos y las leyes, reglas, regulaciones y estándares aplicables a la entidad.
- ✓ Articulación de los objetivos en términos que sean específicos, medibles u observables, asequibles, relevantes y temporales.
- ✓ Objetivos en cascada a través de la organización y sus sub-unidades.
- ✓ Alineación de los objetivos con otras circunstancias que requieran especial atención de la entidad.
- ✓ Confirmación de la pertinencia de los objetivos dentro del proceso de establecimiento de los objetivos antes de que estos sean usados como base para la evaluación de los riesgos.

Algunos factores que influyen en la evaluación de los riesgos son:

- Políticas y procedimientos
- Aprobaciones y autorizaciones
- Conciliaciones y verificaciones
- Seguridad de activos
- Segregación de funciones
- Identificación de eventos
- Valoración de riesgos
- Respuesta al riesgo

Principio 7: Identifica y analiza los riesgos

La organización identifica los riesgos para la consecución de sus objetivos a través de la entidad y analiza los riesgos como base para determinar cómo se deben gestionar los riesgos. La administración debe considerar los riesgos en todos los niveles de la organización y tomar las acciones necesarias para responder a estos. En este proceso se consideran los factores que influyen como la severidad, velocidad y persistencia del riesgo; la probabilidad de perdida de activos y el impacto relacionado sobre las actividades de

operativas, de reporte y cumplimiento. Así mismo la entidad necesita entender su tolerancia al riesgo y su habilidad para funcionar y operar dentro de estos niveles de riesgo.

El proceso de identificación de riesgos debe ser integral y completo y considerar todas las interacciones significativas de bienes, servicios e información, internamente y entre la entidad y sus principales socios y proveedores de servicios externos.

Los riesgos pueden surgir en todos los niveles de la entidad y debido a factores tanto internos como externos. Una vez identificados estos factores se puede considerar su relevancia e importancia, y si es posible relacionarlos con riesgos y actividades específicas.

- **Riesgos externos:** Desarrollos tecnológicos que en caso de no adoptarse provocarían obsolescencia organizacional, cambios en las necesidades y expectativas de la demanda, condiciones macroeconómicas tanto a nivel internacional como nacional, condiciones microeconómicas, competencia elevada con otras organizaciones, dificultad para obtener crédito o costos elevados del mismo, complejidad y elevado dinamismo del entorno de la organización, reglamentos y legislación que afecten negativamente a la organización.

  - ✓ Riesgos económicos: Cambios que pueden impactar las finanzas, la disponibilidad de capital, y barreras al acceso competitivo.
  - ✓ Ambiente natural: Catástrofes naturales o causadas por el ser humano, o cambios climáticos que puedan generar cambios en las operaciones, reducción en la disponibilidad de materia prima, perdida de sistemas de información, resaltando la necesidad de planes de contingencia.
  - ✓ Factores regulatorios: Nuevos estándares o regulaciones y leyes que impliquen cambios en las políticas y estrategias operativas y de reporte de la entidad.
  - ✓ Operaciones extranjeras: Cambios en el gobierno o leyes de países extranjeros que afecten a la entidad.
  - ✓ Factores sociales: Cambios en las necesidades y expectativas de los clientes que puedan afectar el desarrollo de los productos, procesos de producción, servicio al cliente, precios o garantías.

- ✓ Factores tecnológicos: Desarrollos que pueden afectar la disponibilidad y uso de la información, costos de infraestructura y la demanda de los servicios basados en la tecnología.

- **Riesgos internos:** Riesgos referentes a la información financiera, sistemas de información defectuosos, pocos o cuestionables valores éticos del personal, problemas con las aptitudes y actitudes, y comportamiento del personal.

  - ✓ Infraestructura: Decisiones sobre el uso de recursos de capital que pueden afectar las operaciones y la disponibilidad de la infraestructura.
  - ✓ Estructura de la administración: Cambio en las responsabilidades de la administración que pueda afectar los controles que se llevan a cabo en la organización.
  - ✓ Personal: Calidad del personal contrato y los métodos de capacitación y motivación que puedan influir en el nivel de control de conciencia dentro de la entidad, y vencimiento de contratos que puedan afectar la disponibilidad de personal.
  - ✓ Acceso a los activos: Naturaleza de las actividades de la entidad y acceso de empleados a los activos, que puedan contribuir a la malversación de activos.
  - ✓ Tecnología: Alteraciones en los sistemas de información que puedan afectar los procesos de la entidad.

Los riesgos deben ser claramente identificados y se realiza mediante un mapeo de riesgos que incluye la especificación de los procesos claves de la organización, la identificación de los objetivos generales y particulares, y las amenazas y riesgos que pueden impedir que estos se cumplan. También es necesario llevar a cabo una evaluación de riesgos a nivel de transacciones, permitiendo así tener un nivel aceptable de riesgo en la entidad.

Después de identificar riesgos tanto a nivel de la entidad como de transacciones, se lleva a cabo el análisis de riesgos. Este proceso debe incluir la evaluación de la probabilidad de que ocurra un riesgo, el impacto que causaría y la importancia del riesgo. Es importante estimar la probabilidad de ocurrencia de los riesgos identificados con el fin de calcular posibles pérdidas. Esta estimación comprende entonces tres variables, probabilidad, impacto y velocidad; con estas consideraciones se puede construir una matriz de riesgos para determinar los riesgos prioritarios.

La importancia de cada riesgo en su control interno se basa en la probabilidad de manifestación y en el impacto que puede causar en la organización. La velocidad del riesgo se refiere a la rapidez con la que el impacto se evidenciara en la entidad. El impacto está referido a perdida de activos y de tiempo, disminución de la eficiencia y eficacia de las actividades, efectos negativos en los recursos humanos, y alteración de la exactitud de la información de la organización, entre otras. El impacto debe estar expresado en una única unidad que puede ser monetaria.

El riesgo comprende barreras que se imponen a la organización en su crecimiento o inclusive para su supervivencia. Eliminar completamente el riesgo es una situación hipotética, porque los factores a considerar son demasiados en un entorno donde el dinamismo es una constante. Sin embargo existen muchas acciones para reducir el riesgo de que la organización sea afectada, una de estas es la implementación de un adecuado sistema de control interno.

Debido a que las condiciones económicas, industriales, legislativas y operativas cambian constantemente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados. En una organización no existe forma de reducir los riesgos a cero, debido a esto se pueden distinguir dos tipos de riesgos, riesgos inherentes y el riesgo residual. El riesgo inherente es el riesgo para el cumplimiento de los objetivos de la entidad en la ausencia de las acciones de la administración para modificar su probabilidad o impacto; y el riesgo residual es el que permanece después de que la administración lleva a cabo sus respuestas a los riesgos.

Finalmente, luego de evaluar los riesgos significativos la administración debe considerar como van a ser manejados. Esto implica el uso del juicio y un análisis razonable de costos asociados con la reducción de los niveles de riesgo. Las respuestas a los riesgos se organizan en las siguientes categorías:

Categoría	Descripción
Aceptación	Ninguna acción es tomada para modificar la probabilidad o impacto del riesgo.
Anulación	Salida de actividades que dan lugar a riesgos.
Reducción	Acciones tomadas para reducir la probabilidad o impacto del riesgo.
Compartir	Reducir la probabilidad o impacto del riesgo, transfiriéndolo o compartiendo una parte del riesgo.

Tolerancia al Riesgo

La Tolerancia al Riesgo se refiere al nivel aceptable de variación en el desempeño relativo al cumplimiento de los objetivos. Es decir la cantidad máxima de un riesgo que una organización puede aceptar para lograr los objetivos. Funcionar y operar dentro de la tolerancia al riesgo le proporciona a la administración la seguridad del cumplimiento de los objetivos de la entidad.

Principio 8: Evalúa el riesgo de fraude

La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos. La administración debe considerar los posibles actos de corrupción ya sean del personal de la entidad o de los proveedores de servicios externos, que afectan directamente el cumplimiento de los objetivos.

El Marco Integrado de Control Interno establece la necesidad de considerar el riego de fraude potencial que pueda afectar a la consecución de los objetivos de la organización. Por lo tanto se definen varios tipos de fraude, enfatizando así el análisis y gestión del fraude.

- Reporting fraudulento.
- Custodia de activos.
- Corrupción.

El reporte fraudulento se presenta cuando los estados financieros son preparados inadecuadamente con omisiones y declaraciones erróneas y falsas. Esto sucede por diferentes irregularidades que se presenten en la entidad. El sistema de control interno debe prevenir o detectar oportunamente cualquier omisión o información errónea en los estados financieros por fraude o error.

La evaluación de riesgos debe considerar el riesgo potencial de fraude en las áreas de:

- Reporte financiero fraudulento.
- Reporte no financiero fraudulento.
- Malversación de activos.
- Actos ilegales.

Como parte del proceso de valoración de riesgos, la organización debe identificar las diversas maneras como puede ocurrir la presentación fraudulenta de reportes considerando:

- El sesgo de la administración.
- Grado de estimados y juicios en la presentación de reportes externos.
- Esquemas de fraude y escenarios comunes para los sectores de industria y los mercados en los cuales la entidad opera.
- Regiones geográficas donde la entidad hace negocios.
- Incentivos que pueden motivar el comportamiento fraudulento.
- Naturaleza de la tecnología y capacidad de la administración para manipular la información.

- Transacciones inusuales o complejas sujetas a influencia importante de la administración.
- Vulnerabilidad ante la incapacidad de la administración para eludir controles y esquemas potenciales para eludir las actividades de control existentes.

La custodia de activos se refiere a la protección de la entidad contra la adquisición, uso y disposición sin autorización o engañosa de los activos para el beneficio de un individuo o grupo, y que puede estar relacionado con mercados ilegales, robo de activos y propiedad intelectual, transacciones tardías y lavado de dinero.

Los riesgos de corrupción pueden afectar los objetivos de cumplimiento y el entorno de control. El análisis de estos riesgos debe considerar los incentivos y presiones para alcanzar los objetivos de la entidad. La administración debe estipular los niveles esperados de desempeño y estándares de conducta a través contratos y desarrollo de actividades de control que supervisen las acciones de las terceras partes.

Factores que intervienen en el Riesgo Fraude:

- Incentivos y presiones.
- Oportunidad.
- Actitudes y justificaciones.

Principio 9: Identifica y analiza cambios importantes

La organización identifica y evalúa cambios que podían impactar significativamente el sistema de control interno. Este proceso se desarrolla paralelamente a la evaluación de riesgos y requiere que se establezcan controles para identificar y comunicar los cambios que puedan afectar los objetivos de la entidad.

- Cambios en el ambiente externo.
- Cambios físicos del ambiente.
- Cambios en el modelo del negocio.
- Adquisiciones y ventas de activos significativas.
- Operaciones extranjeras.
- Crecimiento rápido.
- Nuevas tecnologías.
- Cambios significativos de personal.