INTOSAI GOV 9100

Las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) son emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI). Para más información visite *www.issai.org*

INTOSAI

Guía para las normas de control interno del sector público

INTOSAI Professional Standards Committee

PSC-Secretariat

Rigsrevisionen • Landgreven 4 • P.O. Box 9009 • 1022 Copenhagen K • Denmark

Tel.:+45 3392 8400 • Fax:+45 3311 0415 • E-mail: info@rigsrevisionen.dk

I N T O S A I

EXPERIENTIA MUTUA

OMNIBUS PRODEST

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

INTOSAI

INTOSAI

Guía para las normas de control interno del sector público

GUÍA PARA
LAS NORMAS DE CONTROL INTERNO
DEL SECTOR PÚBLICO

Comité de normas de control interno

Fr. VANSTAPEL
Primer Presidente del Tribunal
de Cuentas de Bélgica

Regentschapsstraat 2
B-1000 BRUSELAS
BÉLGICA

Tel: ++32 (2) 551 81 11
Fax: ++32 (2) 551 86 22
E-mail: internalcontrol@ccrek.be

Guía para las normas de control interno del sector público

INTOSAI

Secretariado general de INTOSAI - RECHNUNGSHOF
(Tribunal de Cuentas de Austria)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-mail: intosai@rechnungshof.gv.at:
http://www.intosai.org

Contenido

Guía para las normas de control interno del sector público

Prefacio

La Guía de INTOSAI de 1992 para las normas de control interno fue concebida como un documento vital que refleja la visión de que se deben promover las normas para el diseño, implantación y evaluación del control interno. Esta visión involucra un esfuerzo continuo por mantener esta guía actualizada.

En la 17 reunión INCOSAI (Seúl 2001) se reconoció la existencia de una fuerte necesidad de actualizar la guía de 1992 y se acordó que debía ser considerado para esta tarea el marco integrado para control interno del *Committee on Sponsoring Organisations of the Treadway Commission's* (COSO). Los esfuerzos de reuniones subsecuentes resultaron en recomendaciones adicionales cuyas directrices se dirigen a valores éticos y dan más información sobre los principios generales de las actividades de control relacionadas con el procesamiento de la información. La guía revisada toma en cuenta estas recomendaciones y debe facilitar la comprensión de nuevos conceptos relacionados con el control interno.

Esta guía revisada también debe ser considerada como un documento vital que deberá ser actualizada y perfeccionada suficientemente para involucrar el impacto de los nuevos avances, como el marco COSO Gestión de Riesgo de Empresa[1].

Esta actualización es el resultado del esfuerzo conjunto de los miembros del Comité de INTOSAI para las normas de control interno. La actualización ha sido coordinada por un grupo de trabajo conformado por los miembros del comité y por los representantes de las instituciones fiscalizadoras

[1] Coso, *Enterprise Risk Management Integrated Framework*, www.coso.org, 2004.

superiores de Bolivia, Francia, Hungría, Lituania, Holanda, Rumania, Gran Bretaña, Estados Unidos y Bélgica.

Un plan de acción para la actualización de la Guía fue entregado para su aprobación por el directorio actual en la 50° versión de su reunión (Viena, octubre 2002). El directorio actual fue informado del progreso de este trabajo en la reunión 51° (Budapest, octubre 2003). El borrador fue discutido y aceptado en general por la reunión del comité en Bruselas en febrero del 2004. Después de la reunión del comité el mencionado borrador fue enviado a todos los miembros de la INTOSAI para su comentario final.

Los comentarios recibidos fueron analizados y se han aportado los cambios estimados necesarios.

Quisiera agradecer a todos los miembros del Comité de INTOSAI para las normas de control interno sus esfuerzos y su cooperación para realizar este proyecto. Se agredezca especialmente a los miembros del grupo de trabajo.

La *Guía para las normas de control interno del sector público* será sometida a la aprobación del XVIII INCOSAI a Budapest 2004.

Franki VANSTAPEL
Primer Presidente del Tribunal de Cuentas de Bélgica
Presidente del Comité de INTOSAI para las normas de control interno.

Introducción

En 2001 la INCOSAI decidió actualizar la guía de la INTOSAI de 1992 sobre las Normas de Control Interno para tomar en cuenta todos los avances significativos y recientes en control interno y para incorporar conceptualmente en el documento de la INTOSAI al Informe COSO titulado Control Interno – marco integrado en el documento de la INTOSAI.

Implementando el modelo COSO a las directrices, el comité no sólo busca actualizar el concepto de control interno, sino que trata de contribuir a la comprensión común del control interno en las EFS. Queda claro que este documento toma en cuenta las características del sector público. Esto motivó al comité a considerar algunos cambios y temas adicionales.

Comparado con la definición del informe COSO y con la guía de 1992, el aspecto ético de las operaciones ha sido adicionado. Su inclusión en los objetivos del control interno está justificada, al igual que la importancia de la conducta ética y la prevención y detección del fraude y la corrupción en el sector público que han tenido mayor énfasis desde los 90[2]. Las expectativas generales son que los servidores públicos deben servir los intereses públicos con cuidado y administrar los recursos públicos apropiadamente. Los ciudadanos deben recibir tratamiento imparcial sobre la base de la legalidad y la justicia. Por lo tanto la ética pública es un prerequisito y un soporte para la confianza pública y una clave para el buen gobierno.

Dado que los recursos en el sector público generalmente involucran dinero público y su utilización en el interés público generalmente requiere un cuidado especial, la importancia de la salvaguarda de los recursos en el sector público necesita ser fortalecida.

Además, la contabilidad del presupuesto sobre la base del efectivo sigue siendo una práctica común en el sector público pero no provee la suficiente seguridad relacionada con la adquisición, uso y disposición de los recursos. Como resultado, muchas organizaciones del sector público no siempre tienen un inventario de sus bienes, lo cual las hace más vulnerables. Por lo tanto, la salvaguarda de los recursos ha sido juzgada como un objetivo importante del control interno.

---

[2] XVI INCOSAI, Montevideo, Uruguay, 1998.

Así como el control interno en 1992 no estaba limitado a la visión tradicional del control administrativo financiero e incluía un concepto más amplio del control de la administración, este documento también resalta la importancia de la información no financiera.

Dado el extensivo uso de los sistemas de información en todas las organizaciones públicas, los controles de la tecnología de la información (TI) han ido logrando cada vez mayor importancia, lo que justifica un párrafo separado en esta guía. Los controles de la tecnología de la información se relacionan con cada uno de los componentes del proceso de control interno de la entidad incluyendo al entorno de control, la evaluación del riesgo, las actividades de control, la información y comunicación, al igual que el seguimiento. De cualquier modo, para propósitos de presentación, éstos se discuten en el capítulo "actividades de control".

El objetivo del comité es desarrollar directrices para establecer y mantener una control interno efectivo en el sector público. La administración gubernamental es por lo tanto un importante destinatario de esta guía. La administración gubernamental puede utilizar esta guía como base para la implantación y la ejecución del control interno en sus organizaciones.

Dado que la evaluación del control interno está generalmente aceptada como una norma de campo en la auditoría pública[3], los auditores pueden usar las directrices como una herramienta de auditoría. La guía para las Normas de Control Interno que comprenden el modelo COSO puede por lo tanto ser utilizada tanto por la administración gubernamental[4] como ejemplo de un marco sólido de control interno para las organizaciones, y por los auditores como herramienta para alcanzar el control interno. De cualquier modo, estas directrices no tienen la intención de sustituir a las Normas de Auditoría del INTOSAI o cualquier otra norma relevante de auditoría.

Este documento define un marco recomendado para el control interno en el sector público y presenta una base para que el control interno pueda ser evaluado. El anticipo puede ser aplicado a todos los aspectos operacionales de una organización. De todas maneras, no intenta limitar o

[3] Normas de Fiscalización de INTOSAI.

[4] Personal operativo que no está específicamente mencionado como grupo clave. Pese a que son afectados por el control interno y toman acciones que juegan un papel importante dentro del control, ellos, a diferencia de la gerencia, no son los últimos responsables por todas las actividades de la organización relacionadas con el sistema de control interno. El capítulo 3 de esta guía describe roles y responsabilidades individuales.

interferir el trabajo de las autoridades relacionadas con el desarrollo de la legislación, de quiénes hacen las reglas o de quiénes tienen la potestad de establecer políticas en una organización.

El control interno en las organizaciones del sector público debería ser entendido dentro del contexto de las características específicas de estas organizaciones, es decir su enfoque para lograr objetivos sociales o políticos; la utilización de los fondos públicos; la importancia del ciclo presupuestario; la complejidad de su funcionamiento (esto llama a hacer un balance entre los valores tradicionales como la legalidad, integridad y transparencia, y los modernos valores gerenciales como eficiencia y eficacia) y el gran espectro correspondiente de su responsabilidad pública.

En conclusión, debe quedar claramente establecido que este documento incluye directrices para las normas. La guía no provee políticas detalladas, procedimientos o prácticas para implementar el control interno, sino que dan un amplio marco dentro del cual las entidades pueden desarrollar controles detallados. El comité obviamente no está en la posición de fortalecer las normas.

¿Cómo se ha estructurado este documento?

En el primer capítulo, se define el concepto de control interno y se define su alcance. También se establecen las limitaciones del control interno. En el segundo capítulo, los componentes del control interno son presentados y discutidos. El documento termina con un tercer capítulo de roles y responsabilidades.

En cada sección, los principios más importantes son presentados resumidamente en un cuadro azulado. Informes más detallados siguen. También se hace referencia a ejemplos concretos, que pueden encontrarse en los anexos. Además, al final del documento hay un glosario que contiene los términos técnicos más importantes.

1 Control Interno

1.1 Definición

El control interno es un proceso integral efectuado por la gerencia y el personal, y está diseñado para enfrentarse a los riesgos y para dar una seguridad razonable de que en la consecución de la misión de la entidad, se alcanzarán los siguientes objetivos gerenciales:

- Ejecución ordenada, ética, económica, eficiente y efectiva de las operaciones
- Cumplimiento de las obligaciones de respondabilidad
- Cumplimiento de las leyes y regulaciones aplicables
- Salvaguarda de los recursos para evitar pérdidas, mal uso y daño.

El control interno es un proceso integral dinámico que se adapta constantemente a los cambios que enfrenta la organización. La gerencia y el personal de todo nivel tienen que estar involucrados en este proceso para enfrentarse a los riesgos y para dar seguridad razonable del logro de la misión de la institución y de los objetivos generales.

Un proceso integral

El control interno no es un hecho o circunstancia, sino una serie de acciones que están relacionadas con las actividades de la entidad. Estas acciones se dan en todas las operaciones de la entidad continuamente. Estas acciones son inherentes a la manera en la que la gerencia administra la organización. El control interno por lo tanto es diferente a la perspectiva que tienen algunos de él, quienes lo ven como un hecho adicionado a las actividades de la entidad, o como una obligación. El control interno debe ser incorporado a las actividades de la entidad y es más efectivo cuando se lo construye dentro de la estructura organizativa de la entidad y es parte integral de la esencia de la organización.

El control interno debe ser diseñado desde adentro, no por encima de las actividades. Al diseñar el control interno desde adentro, éste se vuelve

parte integrada de los procesos de planificación, ejecución y seguimiento de la gerencia.

Además su concepción desde adentro tiene importantes implicaciones desde la perspectiva del costo, añadir procedimientos de control que están separados de los procedimientos existentes aumenta los costos. Enfocándose en las operaciones existentes y en su contribución al control interno efectivo e integrando los diferentes controles en las actividades operativas básicas, la organización puede evitar procedimientos y costos innecesarios.

Efectuado por la gerencia y el resto del personal

La gente es la que realiza el trabajo de control interno. Éste se logra por los individuos dentro de una organización, con lo que ellos hacen y dicen. Consecuentemente el control interno es ejecutado por la gente. La gente debe conocer su rol, sus responsabilidades, y los límites de autoridad. Dada la importancia de este concepto, un capítulo completo (3) está dedicado a él.

La gente de una organización incluye a la gerencia y al resto del personal. Pese a que el primer objetivo de la gerencia es la supervisión, también establece los objetivos de la entidad, y tiene la responsabilidad del conjunto del sistema de control interno. Dado que el control interno provee los mecanismos necesarios para ayudar a comprender el riesgo en el contexto de los objetivos de la entidad, la gerencia debe implementar actividades de control, realizar su seguimiento y evaluarlas. La implantación de estas actividades requiere de mucha iniciativa de la gerencia y comunicación intensiva entre la gerencia y el personal. Por lo tanto, el control interno es una herramienta utilizada por la gerencia y directamente relacionada con los objetivos de la entidad como tal, la misma gerencia es un elemento importante del control interno. De todas maneras, todo el personal en la organización juega un papel importante en llevarlo a cabo.

Del mismo modo, el control interno es efectuado por la naturaleza humana. La guía reconoce que la gente no siempre comprende, comunica y actúa consistentemente. Cada individuo lleva a su lugar de trabajo una historia única y sus propias habilidades técnicas, teniendo así diferentes necesidades y prioridades. Estas realidades afectan, y son afectadas, por el control interno.

En consecución de la misión de la Institución

Cualquier organización está en primer lugar preocupada por la consecución de su misión. Las instituciones existen para un fin – el sector público se encuentra generalmente preocupado con la prestación de un servicio y por unos resultados beneficiosos para el interés público.

Dar respuesta a los riesgos

Cualquiera que sea la misión, su consecución se enfrentará a toda clase de riesgos. La tarea de la gerencia es identificar y dar respuesta a estos riesgos cara a maximizar la posibilidad de alcanzar la consecución de la misión. El control interno puede ayudar a enfrentarse a estos riesgos, sin embargo sólo puede proporcionar una garantía razonable sobre el logro de la misión y de los objetivos generales.

Provee seguridad razonable

No importa cuan bien diseñado y ejecutado esté, el control interno no puede dar a la gerencia seguridad completa en relación al logro de los objetivos generales. En su lugar, las directrices dicen que se puede esperar un nivel "razonable" de seguridad.

La seguridad razonable equivale a un nivel satisfactorio de confianza bajo ciertas consideraciones dadas de costo, beneficio y riesgo. Determinar cuanta seguridad es razonable requiere de juicio. Al ejercitar la capacidad de juicio, los ejecutivos deben identificar los riesgos inherentes de operaciones y los niveles aceptables de riesgo bajo diversas circunstancias, además de fijar el riesgo tanto cuantitativa como cualitativamente.

La seguridad razonable refleja la noción sobre la incertidumbre y riesgos futuros, mismos que nadie puede predecir con total certeza. Además existen factores que están fuera de control o de la influencia de la organización y pueden afectar la habilidad para lograr los objetivos. Las limitaciones también son resultado de las siguientes realidades: el juicio humano al tomar las decisiones puede ser erróneo; las crisis pueden darse por pequeños errores; los controles pueden ser eludidos si dos o

más miembros así lo deciden, o la gerencia puede eludir el sistema de control interno. Además, los compromisos en el sistema de control interno reflejan el hecho de que los controles tienen un costo. Estas limitaciones hacen que la gerencia no pueda tener seguridad absoluta de que los objetivos sean alcanzados.

La seguridad razonable reconoce que el costo del control interno no debe exceder los beneficios que de él deriven. Las decisiones sobre la respuesta al riesgo y la implantación de controles necesitan considerar los costos y los beneficios relativos. El costo se refiere a la medida financiera de recursos consumidos para lograr un propósito específico y a la medida económica de una oportunidad perdida, como ser el retraso en las operaciones, una disminución en los niveles de servicio o productividad, o el bajo nivel moral de los empleados. Un beneficio es medido por el grado en el que el riesgo de no alcanzar un objetivo determinado es eliminado. Los ejemplos incluyen un incremento en la probabilidad de detectar el fraude, desperdicio, abuso, o error, previniendo una actividad inapropiada, o aumentando el cumplimiento de las regulaciones.

El diseño de los controles internos que son benéficos respecto de sus costos al reducir el riesgo hasta un nivel aceptable, requiere que los gerentes entiendan claramente el conjunto de los objetivos a ser alcanzados. Si esto no es así, los gerentes gubernamentales pueden diseñar sistemas con excesivos controles en un área operativa que pueden afectar negativamente otras operaciones. Por ejemplo, los empleados pueden tratar de evadir los procedimientos, las operaciones ineficientes pueden causar retrasos, el exceso de procedimientos puede anquilosar la creatividad de los empleados o la capacidad de solucionar problemas y perjudicar la calidad de los servicios que se presta a los beneficiarios. Por ello, los beneficios derivados de los excesivos controles en un área pueden ser anulados por el incremento de costos en otras actividades.

Sin embargo, también se deben hacer consideraciones cuantitativas, puede por ejemplo ser importante el tener los controles adecuados sobre las transacciones en unidades monetarias de alto o bajo riesgo, tales como los salarios, viajes y gastos de representación. Los costes de los controles correspondientes pueden parecer excesivos en relación a las cantidades de dinero que se manejan en el conjunto de los gastos gubernamentales, pero pueden ser críticos a la hora de la confianza de los ciudadanos en los gobiernos y su administración.

Logro de objetivos

El control interno está dirigido hacia el logro de una serie de objetivos generales, objetivos separados pero al mismo tiempo integrados. Estos objetivos generales están implantados a través de numerosos sub-objetivos específicos, funciones, procesos y actividades.

Los objetivos generales son:

- *Ejecutar las operaciones de manera ordenada, ética, económica, eficiente y efectiva*

Las operaciones de una entidad deben ser ordenadas, éticas, económicas, eficientes y efectivas. Tienen que ser consistentes con la misión de la organización.

Ordenadamente significa que las operaciones están bien organizadas, es decir, metódicamente.

La ética se refiere a los principios morales. La importancia de la conducta ética y la prevención y detección de fraude y corrupción en el sector público ha tenido más énfasis desde los noventa. Generalmente se espera que los servidores públicos deban servir a los intereses públicos con justicia y que administren adecuadamente los recursos públicos. Los ciudadanos deberán recibir tratamiento imparcial basado en la legalidad y la justicia. Por tal motivo la ética pública es un prerrequisito y un soporte para los dineros públicos y una clave para su buen gobierno.

Tratamiento económico sin desperdicio ni extravagancia. Significa utilizar una correcta cantidad de recursos, de la calidad correcta, entregada en el lugar y el momento precisos al costo mas bajo.

La eficiencia se refiere a los recursos utilizados para lograr los objetivos. Significa poner el mínimo de recursos para lograr una cantidad y calidad de resultados, o lograr los máximos resultados con una determinada calidad y cantidad de recursos.

La eficacia se refiere al logro de los objetivos o al grado en el que los resultados de una actividad cumplen con el objetivo o los efectos previstos de dicha actividad.

- *Satisfacer las obligaciones de respondabilidad*

Respondabilidad es el proceso en el que las organizaciones públicas y los individuos que las integran se hacen responsables por sus decisiones y acciones, incluyendo su salvaguarda de recursos públicos, imparcialidad, y todos los aspectos de su desempeño.

El proceso se ejecuta desarrollando, manteniendo, y facilitando información financiera y no financiera de confianza e importancia, y a través de la presentación de esta información en informes hechos oportunamente destinados a interesados internos y externos.

La información no financiera puede estar relacionada con la economía, eficiencia y eficacia de las políticas y operaciones (información sobre la actuación), y el control interno y su efectividad.

- *Cumplir con las leyes y regulaciones*

Las organizaciones requieren el cumplimiento de muchas leyes y regulaciones. En las organizaciones públicas las leyes y regulaciones ordenan la obtención y gasto del dinero público y la manera de operar. Los ejemplos incluyen la ley de presupuesto, tratados internacionales, leyes sobre la correcta administración, ley de contabilidad, ley de derechos civiles y protección del medio ambiente, regulaciones sobre los ingresos por impuestos y acciones que evitan el fraude y corrupción.

- *Salvaguarda de recursos contra pérdida por desperdicio, abuso, mala administración, errores, fraude e irregularidades.*

Si bien el cuarto objetivo puede ser visto como una subcategoría del primero (operaciones ordenadas, éticas, económicas, eficientes y efectivas), la importancia de la salvaguarda de los recursos del sector público necesita ser fortalecida. Esto se debe a que los recursos en el sector público generalmente involucran dinero público y su utilización en el interés público generalmente requiere cuidado especial. Además, la contabilidad del presupuesto en base de efectivo, práctica que sigue siendo muy común en el sector público, no provee suficiente seguridad relacionada con la adquisición, utilización y disposición de los recursos. Como resultado, las organizaciones en el sector público no siempre tienen registros de sus activos, lo que las hace más vulnerables. Por tal motivo, se debe adoptar controles en cada una de las actividades relacionadas con la administración de los recursos de la entidad, desde la adquisición hasta la disposición.

Otros recursos tales como la información, fuentes de documentación y archivos de contabilidad también están en peligro de ser robados, mal utilizados o destruidos. La salvaguarda de ciertos recursos y archivos se ha vuelto cada vez más importante desde la llegada de los sistemas de computación. La información sensible almacenada en medios de computación puede ser destruida o copiada, distribuida y mal usada, si no se tiene el suficiente cuidado como para protegerla.

1.2 Limitaciones de la efectividad del control interno[5]

El control interno no puede por sí mismo asegurar el logro de los objetivos generales definidos anteriormente.

Un sistema de control interno efectivo, sin importar cuan bien concebido y administrado pueda ser, puede dar sólo una seguridad razonable –no así absoluta– a la gerencia sobre el logro de los objetivos de la entidad o sobre su supervivencia. Puede dar información gerencial sobre los progresos de la entidad, o la ausencia de los mismos, hacia el logro de los objetivos. Pero el control interno no puede cambiar una gerencia inherentemente mala por una buena. Es más, los cambios en las políticas o programas gubernamentales, las condiciones demográficas o económicas están típicamente fuera del control de la gerencia.

Un efectivo sistema de control interno reduce la probabilidad de no alcanzar los objetivos. De cualquier manera, siempre habrá riesgo de que el control interno sea diseñado de manera deficiente o falle en operar como se espera.

Dado que el control interno depende del *factor humano*, es sujeto a las debilidades en el diseño, errores de juicio o interpretación, mala comprensión, descuido, fatiga, distracción, colusión, abuso o excesos.

Otro factor limitante es que el diseño del sistema de control interno se enfrente a la *disminución de recursos*. Los beneficios de los controles deben ser considerados consecuentemente en relación a su costo. Mantener un sistema de control interno que elimine el riesgo de pérdida no es realista y probablemente costaría mas que los beneficios derivados. Al determinar si un control particular debe o no ser diseñado, la probabilidad de que exista un riesgo y el efecto potencial de éste en la entidad deben ser considerados junto con los costos relacionados a la implantación del nuevo control.

Los *cambios organizacionales* y la *actitud gerencial* tienen un profundo impacto en la eficacia del control interno y el sistema en el que opera el

[5] Las limitaciones en la efectividad del control interno tienen que ser establecidas para evitar expectativas exageradas debido a la mala comprensión de su alcance.

personal. Por ello, la gerencia necesita revisar y actualizar los controles continuamente, comunicar los cambios al personal, y dar el ejemplo con la adhesión a estos controles.

2 Componentes del control interno

El control interno comprende cinco componentes interrelacionados:

- Entorno de control
- Evaluación del riesgo
- Actividades de control
- Información y comunicación
- Seguimiento

El control interno está diseñado para proveer seguridad razonable de que los objetivos generales de la entidad están siendo alcanzados. Por ello la existencia de objetivos claros son un prerrequisito para un proceso efectivo de control interno.

El entorno de control es la base para el sistema de control interno en su conjunto. Da la disciplina y la estructura además de un clima que influye en la calidad del control interno en su conjunto. Tiene una influencia general en la manera en la que se establecen las estrategias y objetivos y en la manera en que las actividades de control son diseñadas.

Habiendo establecido objetivos claros y un entorno de control efectivo, una *evaluación de los riesgos* que enfrenta la entidad en la búsqueda de lograr su misión y sus objetivos determina una base para desarrollar una apropiada respuesta al riesgo.

La mejor manera de mitigar el riesgo es a través de *actividades de control interno*. Las actividades de control pueden ser preventivas y/o detectivas. Las acciones correctivas son necesarias para complementar las actividades de control interno con la intención de lograr los objetivos. Las actividades de control y las acciones correctivas deben proveer valor por dinero. Su costo no debe exceder el beneficio que de ellas resulte (costo efectividad).

Información y comunicación efectivas son vitales para que una entidad conduzca y controle sus operaciones. La gerencia de una entidad

requiere comunicación relevante, confiable, correcta y oportuna relacionada con los eventos internos, así como con los externos. Además, la información es necesaria en toda la entidad para que ésta logre sus objetivos.

Finalmente, dado que el control interno es una actividad dinámica que tiene que ser adaptada continuamente según los cambios y riesgos que la entidad tenga que enfrentar, el seguimiento del sistema de control interno es necesario para procurar a asegurar que el control interno esté a tono con los objetivos, el entorno, los recursos y el riesgo.

Estos componentes definen un enfoque recomendable para el control interno en el gobierno y dan las bases sobre las cuales se puede evaluar el control interno. Estos componentes aplican a todos los aspectos de las operaciones de una organización.

Esta guía provee un marco general. Cuando sea implementada, la gerencia será responsable de desarrollar las políticas más detalladas y las prácticas y procedimientos para satisfacer las operaciones de su organización, para asegurar que éstas sean hechas como parte integral de esas operaciones.

Relación entre objetivos y componentes

Existe una relación directa entre los objetivos que representan lo que una entidad está tratando de conseguir y los componentes del control interno que representan cómo se pueden alcanzar esos objetivos. Esta relación está representada en una matriz tridimensional que tiene la forma de un cubo.

Los cuatro objetivos – respondabilidad (e información), cumplimiento (con las leyes y regulaciones), operaciones (ordenadas, éticas, económicas eficientes y efectivas) y salvaguarda de recursos, están representados por las columnas verticales, los cinco componentes están representados por las filas horizontales y la organización o entidad y sus departamentos están representados por la tercera dimensión de la matriz.

Cada fila de los componentes "hace un corte transversal" y aplica a cada uno de los cuatro objetivos. Por ejemplo, la información financiera y no financiera generada de fuentes internas y externas, que pertenece al componente de información y comunicación, son necesarias para manejar las operaciones, emitir informes y cumplir con los propósitos de respondabilidad y para cumplir con las leyes aplicables.

Del mismo modo, si vemos los objetivos, cada uno de los cinco componentes es relevante a cada objetivo. Tomando un objetivo, como la eficiencia y eficacia de las operaciones, queda claro que cada uno de los componentes es aplicable e importante para su logro.

El control interno no sólo es relevante para toda la entidad, sino para sus unidades individuales. Esta relación está representada por la tercera dimensión, misma que representa organizaciones, áreas y unidades. Por ello uno puede enfocarse hacia cualquiera de las celdas de la matriz.

Mientras el marco del control interno es relevante y aplicable a todas las organizaciones, la manera en la que la gerencia lo aplica variará ampliamente de acuerdo con la naturaleza de la entidad, y depende de cierto número de factores específicos. Estos factores incluyen la estructura organizacional, el perfil del riesgo, el ambiente operativo, el tamaño, la complejidad, las actividades y grado de regulación, entre otros. Considerando la situación específica de cada entidad, la gerencia deberá formular una serie de alternativas relacionadas con la complejidad de los procesos y las metodologías desplegadas para aplicar los componentes del marco del control interno.

A continuación, cada uno de los componentes antes mencionados está presentado de manera concisa con comentarios adicionales.

2.1 Entorno de control

El entorno de control establece el tono de una organización, teniendo influencia en la conciencia que tenga el personal sobre el control. Es el fundamento para todos los componentes de control interno, dando disciplina y estructura.

Los elementos del entorno de control son:

(1) La integridad personal y profesional y los valores éticos de la gerencia y el resto del personal, incluyendo una actitud de apoyo hacia el control interno todo el tiempo a través de la organización;

(2) Competencia;

(3) El "tono de los superiores" (es decir la filosofía de la dirección y el estilo gerencial);

(4) Estructura organizacional;

(5) Políticas y prácticas de recursos humanos.

Integridad personal y profesional, y valores éticos de la gerencia y del personal

La integridad personal y profesional y los valores éticos de la gerencia y del personal determinan sus preferencias y sus juicios de valor, mismos que se traducen en las normas de conducta. Deben observar una actitud de apoyo hacia el control interno todo el tiempo en la organización.

Cada persona involucrada con la organización – entre los gerentes y los empleados – tiene que mantener y demostrar integridad personal y

profesional y valores éticos, y tiene que cumplir todo el tiempo con los códigos de conducta aplicables. Esto podría incluir la declaración de intereses financieros personales, cargos externos o regalos (por ejemplo ser electos como oficiales o servidores públicos de mayor rango), y reportar conflictos de intereses.

Además, las entidades públicas tienen que mantener y demostrar integridad y valores éticos y tienen que hacerlos visibles al público en su misión y valores centrales. Además, sus operaciones tienen que ser éticas, ordenadas, económicas, eficientes y efectivas. Tienen que ser consistentes con la misión.

Competencia

La competencia incluye el nivel de conocimiento y habilidades necesarias para ayudar a asegurar una actuación ordenada, ética, económica, eficaz y eficiente, al igual que un buen entendimiento de las responsabilidades individuales relacionadas con el control interno.

La gerencia y los empleados deben mantener un nivel de competencia que les permita comprender la importancia del desarrollo, implantación y mantenimiento de un buen control interno y practicar sus deberes para poder alcanzar los objetivos generales de control interno y la misión de la entidad. Cada uno en la organización está involucrado con el control interno con sus responsabilidades propias y específicas.

La gerencia y su personal deben, por lo tanto, mantener y demostrar un nivel de habilidades necesarias para ayudar a asegurar un desempeño efectivo y eficiente; y una suficiente comprensión del control interno, para efectivamente descargar sus responsabilidades.

La capacitación, por ejemplo, puede aumentar la conciencia de los servidores públicos sobre temas de control interno y ética, y ayudar a desarrollar las capacidades del servidor público para manejar dilemas éticos.

El tono de los superiores

El "tono de los superiores" (es decir la filosofía de la dirección y su estilo gerencial) refleja:

- Una actitud de apoyo permanente hacia el control interno, la independencia, la competencia y de liderazgo con el ejemplo.
- Un código de conducta establecido por la gerencia y evaluación del asesoramiento y del desempeño que apoyen los objetivos de control interno y, en particular, de las operaciones de signo ético.

La actitud establecida por la alta gerencia está reflejada en todos los aspectos de las acciones de la gerencia. La entrega, el involucramiento y el apoyo de los directores establecen "el tono de los superiores" que debe generar una actitud positiva y son cruciales para mantener una actitud de apoyo positiva hacia el control interno de una organización.

Si la alta gerencia cree que el control interno es importante, los demás miembros de la organización sentirán esta actitud y responderán observando concientemente los controles establecidos. Por ejemplo, la creación de una unidad de control interno como parte del sistema de control interno es un signo importante por parte de la gerencia de que el control interno es importante.

Por otra parte, si los miembros de la organización sienten que el control interno no es una preocupación importante para la alta gerencia y se le da la atención a medias en vez de otorgarle un soporte profundo, es casi seguro que los objetivos de control de la gerencia no sean efectivamente alcanzados.

Consecuentemente, la demostración y la insistencia en una conducta ética por parte de los ejecutivos es de vital importancia para el objetivo de control interno y en particular para el objetivo de "operaciones éticas". Al llevar a cabo este papel, la gerencia pondrá buen ejemplo a través de sus propias acciones y su conducta deberá reflejar lo que es adecuado y lo que no es aceptable. En particular, las políticas gerenciales, los procedimientos y prácticas deben promover la conducta ordenada, ética, económica, eficiente y eficaz.

La integridad de la gerencia y de su personal es, de cualquier modo, influenciada por muchos elementos. Por tal motivo, se deberá recordar al personal periódicamente sus obligaciones bajo un código operativo de conducta emitido por la alta gerencia. Las evaluaciones de asesoría y desempeño también son importantes. Las evaluaciones de desempeño deben estar basadas en una evaluación de muchos factores críticos, incluyendo el papel del empleado que efectua el control interno.

Estructura organizacional

La estructura organizacional de una entidad provee:

- Asignación de autoridad y respondabilidad;
- Delegación de autoridad y respondabilidad
- Líneas apropiadas de rendición de cuentas.

La estructura organizacional define las áreas claves de la entidad respecto de la autoridad y responsabilidad. La delegación de autoridad y la responsabilidad se relacionan con la manera en la que la autoridad y la responsabilidad son delegadas a través de la entidad. Puede no haber asignación de autoridad o una responsabilidad que no sea reportada. Por tal motivo, deben ser definidas líneas apropiadas de rendición de cuentas. En circunstancias excepcionales, otras líneas de rendición de cuentas tienen que ser posibles además de las normales, como en aquellos casos en que la gerencia está involucrada en irregularidades.

La estructura organizacional puede incluir una unidad de control interno que debe ser independiente de la gerencia y que informará directamente a la autoridad de máximo nivel dentro de la organización.

La estructura organizacional también es tratada en el capítulo 3 de roles y responsabilidades.

Políticas y prácticas de recursos humanos

Las políticas y prácticas de los recursos humanos incluyen contratación, orientación, capacitación (formal y en el sitio de trabajo), así como educación, asesoramiento y evaluación, consultoría, promoción, compensación y acciones correctivas.

El personal es un aspecto importante del control interno. Personal competente y confiable es necesario para un control efectivo. Por lo tanto, los métodos a través de los cuales se contrata a la gente, se hacen las evaluaciones, la capacitación, la promoción y la remuneración son una parte importante del entorno de control. Las decisiones de contratación deben por lo tanto contar con la seguridad de que los individuos tengan la integridad, la educación y la experiencia necesarias para llevar a cabo sus tareas y de que se provea la capacitación formal, en el trabajo y sobre la ética. Los ejecutivos y los empleados que tengan una buena

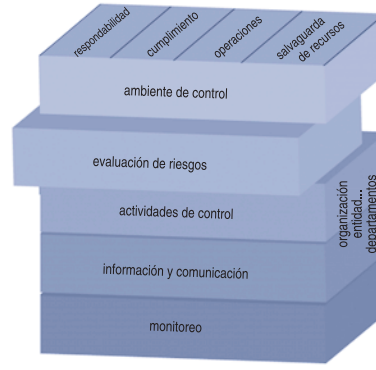
comprensión del control interno y que tengan las intenciones de asumir responsabilidades, son vitales para un control interno efectivo.

La administración de los recursos humanos también tiene un papel esencial en promover un ambiente ético desarrollando el profesionalismo y fortaleciendo la transparencia en las prácticas diarias. Esto se hace visible en los procesos de reclutamiento, evaluación, y promoción, mismos que deben estar basados en méritos. Asegurarse de una apertura en los procesos de selección publicando tanto las reglas de reclutamiento y los cargos vacantes también ayuda a tener una administración ética de los recursos humanos.

Ejemplos

El lector se referirá a los anexos para ejemplos integrados en cada uno de los objetivos y los componentes del control interno.

2.2 Evaluación del riesgo



La evaluación de riesgo es el proceso de identificación y análisis de los riesgos relevantes para el logro de los objetivos de la entidad y para determinar una respuesta apropiada

Implica:

(1) Identificación del riesgo:
- Relacionado con los objetivos de la entidad;
- Comprensión
- Incluye riesgos debidos a factores externos e internos, tanto a nivel de la entidad como de sus actividades;

(2) Valoración del riesgo
- Estimación de la importancia del riesgo
- Valoración de la probabilidad de que el riesgo ocurra

(3) Evaluación de la tolerancia al riesgo de la organización;

(4) Desarrollo de respuestas:
- Cuatro tipos de respuesta al riesgo deben ser considerados: transferencia, tolerancia, tratamiento o eliminación. Entre ellos, el tratamiento del riesgo es el más relevante para esta guía porque un control interno efectivo es el mejor mecanismo para tratar el riesgo.
- Los controles apropiados involucrados pueden ser de detección o de prevención.

Dado que las condiciones gubernamentales, económicas, industriales, regulatorias y operacionales están en constante cambio, la evaluación de riesgo debe ser un proceso constante. Implica la identificación y análisis de condiciones modificadas y oportunidades y riesgos (ciclo de evaluación del riesgo) y la adaptación del control interno para dirigirlo hacia los riesgos cambiantes.

Como se enfatizó en la definición, el control interno puede dar sólo una seguridad razonable de que los objetivos de una organización sean cumplidos. La evaluación del riesgo es un componente del control interno, juega un papel esencial en la selección de las actividades apropiadas de control que se deben llevar a cabo. Es el proceso de identificar y analizar los riesgos relevantes para la consecución de los objetivos de la entidad y determinar una respuesta apropiada.

Consecuentemente, establecer los objetivos institucionales es una condición para la evaluación del riesgo. Los objetivos deben estar definidos antes de que la gerencia identifique los riesgos que pudieran afectar su consecución y ejecute las acciones para administrar esos riesgos. Esto significa tener en marcha un proceso para evaluar y dirigir el impacto del riesgo de forma que el costo sea razonable y tener personal con las habilidades necesarias para identificar y valorar los riesgos potenciales. Las actividades de control interno son una respuesta al riesgo en tanto que están diseñadas para limitar la incertidumbre del resultado que ha sido identificado.

Las entidades gubernamentales deben administrar los riesgos con mayor probabilidad de tener impacto en la prestación de servicios y en el logro de los resultados deseados.

Identificación de riesgo

Un acercamiento estratégico a la identificación de riesgo depende de la identificación de los riesgos que amenazan los objetivos clave organizacionales. Los riesgos relevantes a estos objetivos deben ser considerados y evaluados, resultando en una pequeña cantidad de riesgos clave.

La identificación de los riesgos clave no es importante sólo para identificar las áreas más importantes a las que se deben dirigir los esfuerzos de valoración, sino también para asignar responsabilidades para el manejo de dichos riesgos.

El desempeño de una entidad puede estar en riesgo debido a factores internos o externos a nivel tanto de la entidad como de sus actividades. La evaluación de riesgos debe considerar todos los riesgos que puedan darse (incluyendo el riesgo de fraude y corrupción), por ello es importante que la identificación del riesgo sea muy amplia. La identificación del riesgo debe ser un proceso permanente y muchas veces está

integrada al proceso de planificación. Es muchas veces útil considerar el riesgo con la perspectiva de una "hoja blanca de papel", y no siempre relacionarlo con una visión previa. Este tipo de acercamiento facilita la identificación de los cambios en el mapa de riesgo[6] de una organización que resulte de los cambios en el entorno económico y regulatorio, condiciones internas y externas, y de la introducción de objetivos nuevos o modificados.

Es necesario adoptar herramientas apropiadas para la identificación del riesgo. Dos de las herramientas más comúnmente utilizadas son propiciar una revisión de riesgos y una autoevaluación de riesgos.[7]

Valoración del riesgo

Para decidir cómo administrar el riesgo, es necesario no sólo identificar que un cierto tipo de riesgo existe en principio, sino valuar su importancia y valorar la probabilidad de que este riesgo se dé. La metodología para analizar riesgos puede variar, en gran parte porque muchos riesgos son difíciles de cuantificar (ejemplo: riesgos de prestigio), mientras que otros se prestan para un diagnóstico numérico (especialmente

---

[6] Una visión general o matriz de los riesgos clave que enfrenta una entidad o una unidad incluye el nivel de impacto (ejemplo: alto, medio, bajo) junto con la probabilidad de la ocurrencia del hecho.

[7] *Gestionar una revisión de riesgo*
Este es un procedimiento que va de arriba hacia abajo. Se establece un equipo para considerar todas las operaciones y actividades de una organización en relación con sus objetivos, e identificar los riesgos asociados. El equipo conduce una serie de entrevistas con miembros clave de todos los niveles de la organización para diseñar un mapa de riesgo para toda la gama de actividades en las que se identifican los campos de las políticas, actividades y funciones que pueden ser especialmente vulnerables a riesgo, (incluyendo el riesgo de fraude y corrupción).

Autoevaluación de riesgo
Este es un enfoque que va de abajo hacia arriba. Cada nivel y parte de la organización está invitada a revisar sus actividades y alimentar un diagnóstico de riesgos hacia arriba de la entidad. Esto puede hacerse a través de un enfoque de documentación (con un marco de diagnóstico establecido con cuestionarios) o a través de talleres.

Estos dos enfoques no se excluyen mutuamente y una combinación de enfoques de arriba hacia a bajo, y de abajo hacia arriba es recomendable para el proceso de valoración de riesgo y para facilitar la identificación de riesgos tanto de toda la entidad, como de cada actividad.

riesgos financieros). En el primer caso, una visión mucho más subjetiva es la única posibilidad, y en este caso la valoración del riesgo se acerca más a un arte que a una ciencia. Sin embargo, el uso de criterios de evaluación de riesgos de forma sistemática disminuirá la subjetividad del proceso, ofreciendo un marco que permitirá hacer juicios de forma coherente.

Uno de los propósitos clave de la evaluación del riesgo es informar a la gerencia sobre las áreas de riesgo donde se necesita tomar una acción y sus prioridades relativas. Por tal motivo, usualmente será necesario desarrollar algún marco de categorización para todos los riesgos, por ejemplo, dividirlos entre alto, mediano y bajo. Generalmente es mejor minimizar las categorías, ya que un refinamiento exagerado puede llevar a una separación innecesaria de niveles que en verdad no puedan ser separados con claridad.

A través de tal evaluación, los riesgos pueden tener rangos para establecer prioridades para la gerencia y presentar información para las decisiones gerenciales sobre los riesgos que necesitan mayor atención (por ejemplo aquellos que tengan un mayor potencial de impacto y una probabilidad más alta de ocurrir).

Valoración de la "tolerancia" de riesgo de una organización

Un tema importante al considerar la respuesta al riesgo es la identificación de la "tolerancia de riesgo" de una entidad. La tolerancia de riesgo es la cantidad de riesgos a la que una entidad está preparada a exponerse antes de juzgar que una acción deba ser tomada. Las decisiones sobre las respuestas al riesgo tienen que ser tomadas en forma conjunta con la identificación de la cantidad de riesgos que pueden ser tolerados.

Tanto los riesgos inherentes como los riesgos residuales necesitan ser tomados en consideración para determinar la tolerancia al riesgo. El riesgo inherente es el riesgo en una entidad en que la ausencia de acciones por parte de la dirección pueda conducir a alterar la posibilidad de riesgo o su impacto. El riesgo residual es el riesgo que permanece una vez que la la gerencia responde al riesgo.

La tolerancia de riesgo de una entidad varía de acuerdo a la importancia percibida de los riesgos. Por ejemplo, la tolerancia a la pérdida financiera puede variar de acuerdo al rango de factores, incluyendo el tamaño del presupuesto relevante, la fuente de la posible pérdida, o algunos

otros riesgos asociados tales como la publicidad adversa. La identificación de la tolerancia de riesgo es un tema subjetivo, sin embargo es una etapa importante en la formulación de la estrategia global de riesgo.

Desarrollo de las respuestas

El resultado de las acciones arriba mencionadas puede resultar en un mapa de riesgo para la organización. Habiendo desarrollado un mapa de riesgo, la organización puede entonces considerar las respuestas apropiadas.

Las respuestas al riesgo pueden ser divididas en cuatro categorías. En algunos casos, el riesgo puede ser *transferido, tolerado o eliminado*.[8] De cualquier modo, en la mayor parte de los casos, el riesgo tendrá que ser *administrado* y la entidad necesitará implantar y mantener un sistema efectivo de control interno para mantener el riesgo en un nivel aceptable.

El propósito del tratamiento no es necesariamente obviar el riesgo, sino mantenerlo bajo control. Los procedimientos que una organización establece para tratar el riesgo se llaman actividades de control. La valoración del riesgo deberá jugar un rol central en la selección apropiada de actividades de control a llevarse a cabo. Una vez más, es importante repetir que no es posible eliminar los riesgos y que el control interno puede solamente dar seguridad razonable de que los objetivos de la organización sean cumplidos. De cualquier modo, las entidades que activamente identifican y manejan los riesgos tienen mejores probabilidades de estar bien preparadas para responder rápidamente cuando las cosas salen mal y responder a cualquier cambio en general.

---

[8] En el caso de algunos riesgos, la mejor respuesta puede ser *transferirlos*. Esto se puede hacer por seguros convencionales, dándole a una tercera parte la tarea de tomar el riesgo en una forma diferente, o puede hacerse a través de estipulaciones contractuales.

La habilidad para hacer algo para evitar los riesgos puede ser limitada, o el costo de tomar algunas acciones puede ser desproporcionado con relación al potencial beneficio. En estos casos, la respuesta puede ser *tolerar* los riesgos.

Algunos riesgos sólo serán tratados o detenidos en niveles aceptables *eliminando* la actividad. En el sector público, la opción de eliminar las actividades puede ser severamente limitada comparando con el sector privado. Ciertas actividades son llevadas a acabo en el sector gubernamental porque los riesgos asociados son tan grandes, que no existe otra manera en la que el resultado, que es requerido para beneficio público, sea logrado.

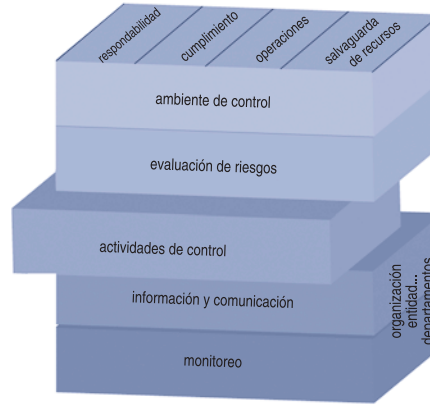
Al diseñar un sistema de control interno, es importante que las actividades de control establecidas sean proporcionales al riesgo. Aparte del resultado extremo indeseable, normalmente es suficiente diseñar un control que dé una seguridad razonable de poder limitar las pérdidas al riesgo aceptable de la entidad. Cada control tiene un costo asociado y la actividad de control debe ofrecer valor por su costo en relación al riesgo al que se está dirigiendo.

Dado que las condiciones gubernamentales, económicas, industriales, regulatorias y operativas cambian continuamente, el entorno de control de cualquier organización también está en constante cambio, y las prioridades de los objetivos y la consecuente importancia de riesgos deben adaptarse y cambiar. Algo fundamental para la evaluación de riesgos es la existencia de un proceso permanente para identificar el cambio de condiciones y tomar las acciones necesarias. Los perfiles de riesgo y controles relacionados tienen que ser regularmente revisados y reconsiderados para asegurar que el mapa del riesgo sigue siendo válido, que las respuestas al riesgo siguen siendo apropiadamente escogidas y proporcionadas, y que los controles para mitigarlos siguen siendo efectivos en la medida en la que los riesgos cambian con el tiempo.

Ejemplos

El lector se referirá a los anexos para obtener ejemplos de cada uno de los objetivos y de los componentes.

2.3 Actividades de control



Las actividades de control son políticas y procedimientos establecidos para disminuir los riesgos y lograr los objetivos de la entidad.

Para ser efectivas, las actividades de control deben ser apropiadas, funcionar consistentemente de acuerdo a un plan a lo largo de un período, y tener un costo adecuado, que comprenda muchos aspectos, ser razonables y estar relacionadas directamente con los objetivos de control.

Las actividades de control se dan en toda la organización, en todos los niveles y en todas las funciones. Incluyen una gama de actividades de control de detección y prevención tan diversas como por ejemplo:

1. Procedimientos de autorización y aprobación;
2. Segregación de funciones (autorización, procesamiento, archivo, revisión);
3. Controles sobre el acceso a recursos y archivos;
4. Verificaciones;
5. Conciliaciones;
6. Revisión de desempeño operativo;
7. Revisión de operaciones, procesos y actividades;
8. Supervisión (asignaciones, revisiones y aprobaciones, dirección y capacitación).

Las entidades deben alcanzar un balance adecuado entre la detección y la prevención en las actividades de control.

Las acciones correctivas son un complemento necesario para las actividades de control en la búsqueda del logro de los objetivos.

Las actividades de control son las políticas y procedimientos establecidos y ejecutados en dirección a los riesgos y para lograr los objetivos de la entidad.

Para ser efectivas las actividades de control necesitan:

- Ser apropiadas (esto significa el control correcto en el lugar correcto y proporcional al riesgo involucrado);
- Funcionar consistentemente de acuerdo a un plan a lo largo de un período (esto significa que deben haber sido cumplidas cuidadosamente por todos los empleados involucrados en el proceso y no hechas apresuradamente cuando el personal clave esté ausente o esté con sobrecarga de trabajo);
- Tener un costo adecuado (es decir, el costo de la implantación del control no debe exceder los beneficios que del proceso puedan derivarse);
- Ser entendibles y razonables y estar relacionadas directamente con los objetivos de control.

Las actividades de control incluyen un rango de políticas y procedimientos tan diversos como:

1. Procedimientos de autorización y aprobación

La autorización y ejecución de transacciones y eventos deben ser hechas sólo por personas que estén dentro del rango de autoridad. La autorización es el principal medio para asegurar que sólo transacciones y eventos válidos sean iniciados según las intenciones de la gerencia. Los procedimientos de autorización, que tienen que ser documentados y claramente comunicados a los gerentes y empleados, deben incluir condiciones específicas y términos bajo los cuales se puedan hacer las autorizaciones. Conformidad con los términos de autorización significa que los empleados actúan en concordancia con las directivas y dentro de las limitaciones establecidas por la gerencia o la legislación.

2. Segregación de funciones (autorización, procesamiento, archivo y revisión)

Para reducir el riesgo de error, el desperdicio o las actividades incorrectas y el riesgo de no detectar tales problemas, no debe haber un solo individuo o equipo que controle todas las etapas clave de una transacción o evento. Mas bien, los deberes y responsabilidades deben estar

asignados sistemáticamente a un cierto número de individuos para asegurar la existencia de revisiones efectivas. Las funciones clave incluyen autorización y archivo de transacciones, procesamiento y revisión o auditoría de las transacciones. La colusión entre personas, sin embargo, puede reducir o destruir la efectividad de esta actividad de control interno. Una organización pequeña probablemente tiene muy pocos empleados como para llevar a cabo satisfactoriamente esta actividad de control. En tales casos, la gerencia debe ser consciente de este riesgo y compensarlo con otras actividades de control. La rotación de empleados puede ayudar a asegurar que una sola persona no sea responsable de todos los aspectos clave de las transacciones o eventos por un excesivo período de tiempo. También es aconsejable que se propicien o pidan vacaciones anuales, eso ayudará a reducir el riesgo porque significa una rotación temporal de funciones.

3. Controles sobre el acceso a los recursos y archivos

El acceso a recursos o archivos debe ser limitado a individuos autorizados que sean responsables por la custodia y/o utilización de los mismos. La respondabilidad en cuanto a la custodia se pone en evidencia por la existencia de recibos, inventarios y otros registros otorgando la custodia y registrando las transferencia de la custodia. La restricción de acceso a los recursos reduce el riesgo de la utilización no autorizada o la pérdida y ayuda a lograr las directivas gerenciales. El grado de restricción depende de la vulnerabilidad de los recursos y el riesgo que se percibe de pérdida o utilización incorrecta, y debe ser periódicamente valorado. Cuando se determina la vulnerabilidad de un bien, deben ser considerados su costo, portabilidad y posibilidades de cambios.

4. Verificaciones

Las transacciones y eventos significativos deben ser verificados antes y después de ser procesados, ejemplo: cuando los bienes son entregados, el número de bienes provistos es verificado con el número de bienes pedidos. Después, el número de bienes facturados es verificado con el número de bienes recibidos. El inventario es verificado también realizando revisiones al almacén.

5. Conciliaciones

Los archivos son conciliados con los documentos apropiados sobre una base regular, ejemplo: los archivos de contabilidad relacionados con las cuentas bancarias son conciliados con los estados bancarios correspondientes.

6. Revisión de desempeño operativo

El desempeño de las operaciones es revisado a la luz de las normas sobre una base regular, valorando la efectividad y eficiencia. Si los análisis de gestión determinan que las acciones existentes no alcanzan los objetivos o normas establecidas, los procesos y las actividades establecidas para alcanzar los objetivos deberían ser objeto de análisis para determinar si son necesarias mejoras.

7. Revisión de operaciones, procesos y actividades

Las operaciones, los procesos y las actividades deben ser periódicamente revisadas para asegurar que cumplen con los reglamentos, políticas, procedimientos en vigor y con el resto de lso requisitos. Este tipo de revisión de las operaciones actuales de una organización debe ser claramente distinguido del seguimiento del control interno que se discute por separado en la sección 2.5.

8. Supervisión (valoración, revisión y aprobación, dirección y capacitación)

La supervisión competente ayuda a asegurar que los objetivos de control interno sean alcanzados. La asignación, revisión y aprobación del trabajo de un empleado comprende:

- La comunicación clara de las funciones, responsabilidades y respondabilidad asignada a cada miembro del personal;
- La revisión sistemática del trabajo de cada miembro hasta donde sea necesario:
- La aprobación del trabajo en puntos críticos para asegurarse de que marcha como se quiere.

La delegación de trabajo de un supervisor no debe disminuir la responsabilidad del supervisor por estas responsabilidades y funciones. Los supervisores además deberán dar a los empleados la suficiente guía y capacitación para ayudar a asegurarse de que los errores, desperdicio y actividades incorrectas sean minimizados y que las directivas de la gerencia sean entendidas y cumplidas.

La lista antes mencionada no es exhaustiva pero enumera las actividades más comunes de control preventivo y de detección. Las actividades de control 1-3 son preventivas, 4-6 son de detección, mientras que 7-8 son tanto preventivas como de detección. Las entidades deben alcanzar un balance adecuado entre la detección y la prevención en las actividades

de control; por esta razón frecuentemente se utiliza una mezcla de estos controles para compensar desventajas particulares de controles individuales.

Una vez que una actividad de control es implantada, es esencial que se obtenga seguridad sobre su efectividad. Consecuentemente, las acciones correctivas son un complemento necesario para las actividades de control. Más aún, debe quedar claro que las actividades de control forman sólo un componente del control interno. Deben estar integradas a los otros cuatro componentes.

Ejemplos

El lector se referirá a los anexos para ejemplos integrados de cada uno de los objetivos y sus componentes.

2.3.1 Actividades de control de información tecnológica

Los sistemas de información implican actividades de control de tipo específico. Por tal motivo, los controles de información tecnológica consisten en dos grandes grupos:

(1) Controles generales
Controles generales son la estructura, políticas y procedimientos que aplican a todo un gran segmento de la información de la entidad y ayudan a asegurar su correcta operatividad. Estos crean el medio en el que operan los sistemas de aplicación y los controles.

Las más grandes categorías de controles generales son: (1) programas de seguridad de planificación y gerencia, (2) controles de acceso, (3) controles de desarrollo, mantenimiento y cambio en la aplicación del software, (4) controles en el sistema de software, segregación de funciones, y (6) continuidad en el servicio.

(2) Aplicación de controles
La aplicación de controles son la estructura, políticas y procedimientos que aplican por separado a los sistemas de aplicación individual, y están directamente relacionados a las aplicaciones individuales computarizadas. Estos controles están generalmente diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas de información.

Los controles generales y de aplicación están interrelacionados y ambos son necesarios para ayudar a un procesamiento adecuado y completo de la información. Dado que la tecnología de la información cambia muy rápidamente, los controles relacionados deben evolucionar constantemente para seguir siendo efectivos.

Conforme la tecnología de la información ha ido avanzando, las organizaciones se han vuelto cada vez más dependientes de los sistemas computarizados de información para llevar a cabo sus operaciones y para procesar, mantener y reportar información esencial. Como resultado, la confiabilidad y seguridad de información computarizada y la de los sistemas que procesan, mantienen y reportan esta información son una importante preocupación tanto de la gerencia como de los auditores de

las organizaciones. Aunque los sistemas informáticos implican tipos específicos de actividades de control, la informática no es un tema de control independiente. Es una parte integral de la mayor parte de las actividades de control.

La utilización de sistemas automatizados para procesar la información implica varios riesgos que necesitan ser considerados por la organización. Estos riesgos van desde, entre otras cosas, uniformar el procesamiento de las transacciones, sistemas de información que inicien las transacciones automáticamente, incremento potencial de errores no detectados; existencia, integridad y volumen de pistas de auditorías; la naturaleza del hardware y software utilizados y archivo de transacciones inusuales o no rutinarias. Por ejemplo, un riesgo inherente al uniformar los procesos de transacciones es que cualquier error emergente de la programación de computación ocurrirá consistentemente en transacciones similares. Controles tecnológicos efectivos de información pueden dar a la gerencia seguridad razonable de que la información procesada por el sistema cumple con los objetivos de control deseados, tales como asegurar que la información sea completa, ordenada en el tiempo, válida y que preserva la integridad.

Los controles tecnológicos de información consisten en dos grandes grupos: controles generales y controles de aplicación.

Controles generales

Los controles generales están constituidos por la estructura, políticas y procedimientos que se aplican a todos o a una gran cantidad de los sistemas de información de una entidad, tales como minicomputadoras y redes y ayudan a asegurar su correcta operación. Crean el medio en el cual los sistemas de aplicación y controles operan.

Las categorías más importantes de los controles generales son:

(1) *El programa de planificación y gerencia de seguridad de toda la entidad* provee un marco y ciclo continuo de actividad para el riesgo gerencial, desarrollando políticas de seguridad, asignando responsabilidades y realizando el seguimiento de la correcta operación de los controles relacionados con las computadoras.
(2) *Los controles de acceso* limitan o detectan el acceso a los recursos de las computadoras (información, programas, equipos y facilidades), protegiendo así estos recursos contra modificaciones no autorizadas, pérdida y exposición no deseada.

(3) *Los controles de desarrollo, mantenimiento y cambio de la aplicación del software* previenen la utilización de programas no autorizados y/o modificaciones a los programas existentes.
(4) *Los controles de sistema de software* limitan y realizan el seguimiento del acceso a programas potentes y archivos sensibles que controlan el hardware de las computadoras y aseguran las aplicaciones apoyadas por el sistema.
(5) *La segregación de funciones* implica que las políticas, procedimientos y estructura organizacional están establecidos para prevenir que un individuo controle los aspectos clave de las operaciones de las computadoras y pueda así conducir acciones no autorizadas u obtenga acceso no autorizado a los bienes o los archivos.
(6) *La continuidad en el servicio* sirve para asegurar que cuando ocurren eventos inesperados, las operaciones críticas continúen sin interrupción o sean reemprendidas rápidamente y la información crítica o sensible sea protegida.

Controles de aplicación

Los controles de aplicación son la estructura, políticas, y procedimientos que aplican a sistemas de aplicación individual separados – tales como cuentas por pagar, inventarios, rol de pagos, garantías o préstamos – y están diseñados para cubrir el procesamiento de información dentro de aplicaciones específicas de software.

Estos controles son generalmente diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas de información.

Los controles de aplicación y la manera en la que la información fluye a través de los sistemas de información pueden ser categorizados en tres fases de un ciclo del proceso:

- Entradas: la información es autorizada, convertida a una forma automática e introducida a la aplicación de manera exacta, completa y puntual;
- Procesamiento: la información es correctamente procesada por la computadora y los archivos son actualizados de manera apropiada, y
- Salidas: los archivos y reportes generados por la aplicación reflejan transacciones y eventos que han ocurrido y reflejan los resultados del procesamiento. Sus reportes son controlados y distribuidos a usuarios autorizados.

Los controles de aplicación también pueden ser categorizados por los objetivos de tipos de control a los que se relacionan, incluyendo si las transacciones y la información es autorizada, completa, exacta y válida. Los controles de autorización conciernen a la validez de las transacciones y ayudan a asegurar que las transacciones representen eventos que hayan ocurrido durante un determinado período. Los controles que indican que los eventos o transacciones están completos, se relacionan con el control de si todas las transacciones válidas son archivadas y clasificadas adecuadamente. Los controles de exactitud tienen que ver con el hecho de que las transacciones sean archivadas correctamente y todos los elementos de la información sean exactos. Los controles sobre la integridad del procesamiento de los archivos de información, si son deficientes, pueden anular cada uno de los antes mencionados controles de aplicación y permitir la ocurrencia de transacciones no autorizadas, además de contribuir para que la información sea incompleta e inadecuada.

Los controles de aplicación incluyen actividades de control programadas, tales como emisiones automáticas y seguimiento manual de las salidas generadas por la computadora, tales como revisiones de reportes que identifiquen ítems rechazados o inusuales.

Los controles generales o de aplicación sobre los sistemas de computación están interrelacionados

La efectividad de los controles generales es un factor significativo al determinar la efectividad de los controles de aplicación. Si los controles generales son débiles, entonces disminuye notoriamente la confiabilidad de los controles asociados con las aplicaciones individuales. Cuando no hay controles generales efectivos, la aplicación de controles puede volverse poco efectiva por exageración, confusión o modificación. Por ejemplo las revisiones diseñadas para evitar que los usuarios ingresen horas de trabajo irrazonablemente grandes a un sistema de procesos de pago de nóminas pueden ser una aplicación efectiva de control. De cualquier modo, no se puede confiar en este control si los controles generales permiten modificaciones no autorizadas al programa que puedan permitir algunas transacciones excepcionales que salgan de este marco.

Mientras los objetivos básicos de control no cambien, los cambios rápidos en la tecnología de la información requieren que los controles evolucionen para seguir siendo efectivos. Cambios como un incremento en la confiabilidad de las redes, computadoras con mayor potencia que

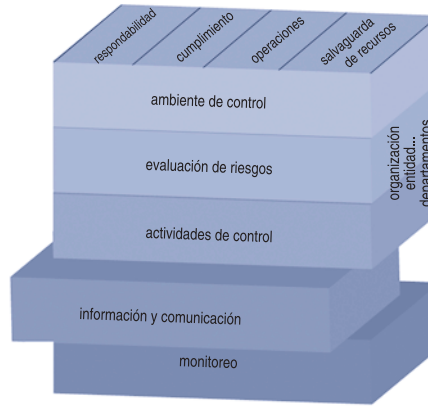
ponen responsabilidad del procesamiento de información en las manos del usuario, comercio electrónico y el internet pueden afectar la naturaleza y la implantación de actividades específicas de control.

Más información sobre las actividades de control informático puede ser encontrado en la Asociación para el control y la auditoría de los sistemas informáticos (ISACA, en sus siglas inglesas), especialmente en el marco de referencia de los Objetivos de control para la informática y tecnologías conexas (COBIT, en sus siglas inglesas) y las actas del Comité para la Auditoría de los sistemas informáticos de INTOSAI.

Ejemplos

El lector puede referirse a los anexos para obtener ejemplos integrados de cada uno de los objetivos y sus componentes del control interno.

2.4 Información y comunicación



La información y la comunicación son esenciales para ejecutar todos los objetivos de control interno.

Información

Una precondición para que la información de transacciones y hechos sea confiable y relevante, es archivarla rápidamente y clasificarla correctamente. La información pertinente debe ser identificada, capturada y comunicada de una manera y en cierto límite de tiempo que permita que el personal lleve a cabo su control interno y sus otras responsabilidades (comunicación puntual a la gente adecuada). Por tal motivo, el sistema de control interno como tal y todas las transacciones y eventos significativos deben estar apropiadamente documentados.

Los sistemas de información producen reportes que contienen información operacional, financiera y no financiera, información relacionada con el cumplimiento y que hace posible que las operaciones se lleven a cabo y se controlen. La misma no sólo tiene que ver con datos generados internamente, sino con información sobre eventos externos, actividades y condiciones necesarias que permite la toma de decisiones y el reporte.

La habilidad de la gerencia para tomar decisiones apropiadas es afectada por la calidad de la información, lo que implica que ésta debería ser apropiada, puntual, actual, exacta y asequible.

La información y la comunicación son esenciales para la realización de todos los objetivos de control interno. Por ejemplo, uno de los objetivos de control interno es cumplir con las obligaciones de respondabilidad pública. Esto puede lograrse desarrollando y manteniendo información financiera y no financiera confiable y relevante, y comunicando esta información a través de la exposición de reportes puntuales. La información y comunicación relacionada con el trabajo de la organización creará la posibilidad de evaluar orden, ética, economía, eficiencia y eficacia de las operaciones. En muchos casos, cierta información tiene que ser emitida, o el proceso de la comunicación tiene que llevarse a cabo para cumplir con las leyes y regulaciones.

La información se necesita a todos los niveles de la organización para tener un control interno efectivo y lograr los objetivos de la entidad. Por tal motivo un conjunto de información pertinente, confiable y relevante debe ser identificado, capturado y comunicado en la forma y período de tiempo que permita que la gente lleve a cabo su control interno y sus otras responsabilidades. Una precondición para que la información sea confiable y relevante es el archivo oportuno y correcta clasificación de los hechos y las transacciones.

Las transacciones y hechos deben ser archivados oportunamente cuando hayan ocurrido, si la información es relevante y valiosa para la gerencia al momento de controlar las operaciones y tomar decisiones. Esto aplica al proceso completo o al ciclo de vida de una transacción o evento, incluyendo la iniciación y autorización, todas las etapas mientras dure el proceso, y su clasificación final en los archivos. También aplica a la actualización oportuna de toda la documentación para que siga siendo relevante.

La clasificación correcta de las transacciones y hechos es también necesaria para asegurar que la información confiable sea asequible a la gerencia. Esto significa organizar, categorizar y formatear la información con la que se preparan reportes, planes de trabajo y estados financieros.

Los sistemas de información generan reportes que contienen información operacional, financiera y no financiera, información relacionada con el cumplimiento y que hace posible que se lleve a cabo y controle una operación. Los sistemas no sólo tienen que ver con formas cualitativas o cuantitativas de datos generados internamente, sino con información sobre hechos externos, actividades y condiciones necesarias para la toma de decisiones y su reporte.

La habilidad de la gerencia para tomar decisiones apropiadas está afectada por la calidad de información, lo que implica que la información sea:

- apropiada (¿está toda la información necesaria?);
- oportuna (¿está ahí cuando se la necesita?)
- actualizada (¿se tiene lo producido más recientemente?)
- exacta (¿es correcta?)
- accesible (¿puede ser obtenida fácilmente por las partes relevantes?)

Para ayudar a asegurar la cualidad de la información y la rendición de cuentas, llevar a cabo las actividades de control interno y las responsabilidades, y hacer que el seguimiento sea más efectivo y eficiente, el sistema de control interno, al igual que todas las transacciones y eventos significativos deben ser correctos y claramente documentados (ejemplo: diagramas de flujo y narrativos). Esta información además debe estar lista y asequible para ser examinada).

La documentación del sistema de control interno debe incluir la identificación de la estructura de una organización, sus políticas, sus categorías operacionales, sus objetivos relacionados y sus procedimientos de control. Una organización debe haber evidenciado por escrito los componentes del proceso de control interno, incluyendo sus objetivos y actividades de control.

La extensión de la documentación del control interno de una entidad varía de acuerdo al tamaño de la entidad, complejidad y factores similares.

Comunicación

La comunicación efectiva debe fluir hacia abajo, a través de y hacia arriba de la organización, tocando todos los componentes y la estructura entera.

Todo el personal debe recibir un mensaje claro de la gerencia superior sobre la seriedad con la que deben tomarse las responsabilidades. Es necesario que entiendan su propio rol en el sistema de control interno, al igual que la manera en la que sus actividades individuales se relacionan con el trabajo de los demás.

También se necesita que haya comunicación efectiva con las partes externas.

La información es la base de la comunicación, misma que debe cumplir con las expectativas de grupos e individuos, permitiéndoles llevar a cabo sus responsabilidades de forma efectiva. La comunicación efectiva debe darse en todas las direcciones, fluir hacia abajo, a través y hacia arriba en la organización, tocando todos los componentes de la estructura entera.

Uno de los canales de comunicación más críticos es aquel entre la gerencia y el personal. La gerencia debe estar bien actualizada en cuanto a la actuación, desarrollo, riesgos y funcionamiento del control interno y otros temas y eventos relevantes. Del mismo modo, la gerencia debe comunicar a su personal la información que requiere retroalimentación y dirección. La gerencia también debe proveer comunicación específica y dirigida, relacionada con las expectativas de conducta. Esto incluye afirmaciones claras de la filosofía de control interno de la entidad, relacionamiento y delegación de autoridad.

La comunicación debe elevar la conciencia sobre la importancia y la relevancia de un control interno efectivo, comunicar la tolerancia al riesgo de la entidad, y hacer que el personal esté consciente de su rol y responsabilidades al efectuar y apoyar los componentes del control interno.

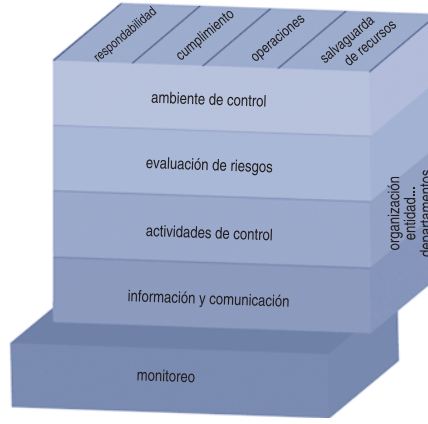
Además de las comunicaciones internas, la gerencia debe asegurar que existan medios adecuados de comunicarse y obtener información de partes externas, dado que las comunicaciones externas pueden servir como entradas que tengan un alto impacto de significado en la medida en la que la organización logre sus objetivos.

Basándose en las comunicaciones internas y externas recibidas, la gerencia debe dar los pasos necesarios para realizar acciones puntuales de seguimiento.

Ejemplos:

El lector puede referirse a los anexos para obtener ejemplos integrados de cada uno de los objetivos y los componentes del control interno.

2.5 Seguimiento



Los sistemas de control interno deben ser objeto de seguimiento para valorar la calidad de la actuación del sistema en el tiempo. El seguimiento se logra a través de actividades rutinarias, evaluaciones puntuales o la combinación de ambas.

(1) Seguimiento continuo
El seguimiento continuo de control interno está construido dentro de las operaciones normales y recurrentes de la entidad. Incluye la administración y actividades de supervisión y otras acciones que el personal ejecuta al cumplir con sus obligaciones.

Las actividades de seguimiento continuo cubren cada uno de los componentes de control interno e involucran acciones contra los sistemas de control interno irregulares, antiéticos, antieconómicos, ineficientes e ineficaces.

(2) Evaluaciones puntuales
El rango y frecuencia de las evaluaciones puntuales dependerá en primer lugar de la valoración de riesgos y de la efectividad de los procedimientos permanentes de seguimiento.

Las evaluaciones puntuales cubren la evaluación de la efectividad del sistema de control interno y aseguran que el control interno logre los resultados deseados basándose en métodos predefinidos y procedimientos. Las deficiencias de control interno deben ser reportadas al nivel adecuado de la gerencia.

El seguimiento debe asegurar que los hallazgos de auditoría y las recomendaciones sean adecuados y oportunamente resueltos.

El seguimiento del control interno busca asegurar que los controles operen como se requiere y que sean modificados apropiadamente de acuerdo a los cambios en las condiciones. El seguimiento también debería valorar si, en cumplimiento de la misión de la entidad, se alcanzan los objetivos generales expuesto en la definición de control interno. Esto se puede lograr a través de las actividades de seguimiento continuo, evaluaciones puntuales, o una combinación de ambas, para poder ayudar a asegurar que el control interno siga siendo aplicable a todos los niveles y a través de toda la entidad, y que el control interno logre los resultados deseados. El seguimiento de las actividades de control interno como tal, debe distinguirse claramente de la revisión de las operaciones de la organización, misma que es una actividad de control interno como se describió previamente en la sección 2.3.

El seguimiento continuo de control interno ocurre en el curso normal de las operaciones recurrentes de una organización. Se ejecuta continuamente y sobre la base del tiempo real, reacciona dinámicamente al cambio de condiciones y forma parte del engranaje de las operaciones de una entidad. Como resultado, es más efectivo que las evaluaciones puntuales y las acciones correctivas son potencialmente menos costosas. Dado que las evaluaciones puntuales toman lugar después de los hechos, muchas veces los problemas son más fácilmente identificables a través de las rutinas del seguimiento continuo.

El rango y la frecuencia de las evaluaciones puntuales dependen en primer lugar de la evaluación del riesgo y de la efectividad de las actividades del seguimiento continuo. Al tomar esta determinación, la organización debe considerar la naturaleza y el grado de los cambios, tanto desde hechos internos, como desde hechos externos y los riesgos asociados, la competencia y experiencia del personal que implanta las respuestas al riesgo, los controles relacionados, y los resultados del seguimiento continuo. Las evaluaciones puntuales de control también pueden ser útiles para enfocar directamente la efectividad de los controles en un tiempo específico. Las evaluaciones puntuales pueden tomar la forma de autoevaluación al igual que de una revisión del diseño de control de pruebas sobre el control interno. Las evaluaciones puntuales también pueden ser ejecutadas por las instituciones fiscalizadoras superiores o los auditores externos o internos.

Usualmente, alguna combinación del seguimiento permanente y de las evaluaciones puntuales ayudará a asegurar que el control interno mantenga su efectividad a través del tiempo.

Todas las deficiencias encontradas durante el seguimiento continuo o a través de evaluaciones puntuales deben ser comunicadas a aquellas personas que puedan tomar las acciones necesarias. El término "deficiencia" se refiere a la condición que afecta la habilidad de la entidad para lograr sus objetivos generales. Una deficiencia, por lo tanto, puede representar un defecto percibido, potencial o real, o una oportunidad para fortalecer el control interno con la idea de aumentar las probabilidades de que la entidad logre sus objetivos generales.

Proveer la información necesaria sobre las deficiencias de control interno a la parte responsable es difícil. Deben establecerse por ello requerimientos para identificar qué información es necesaria en un nivel particular para tomar decisiones de modo efectivo. Estos requerimientos reflejan la regla general que una gerencia debe recibir la información que afecta las acciones o conductas del personal bajo su responsabilidad, al igual que la información necesaria para lograr objetivos específicos.

La información generada en el curso de las operaciones es usualmente reportada a través de canales normales, lo que significa al individuo responsable por el funcionamiento y también al último nivel de la gerencia que esté sobre dicho individuo. De cualquier modo, los canales alternativos de comunicación deben existir para reportar información delicada como ser actos ilegales o incorrectos.

El seguimiento del control interno debe incluir políticas y procedimientos que buscan asegurar que los hallazgos de auditoría y otras revisiones sean adecuados y oportunamente resueltos. Los gerentes deben (1) evaluar oportunamente los hallazgos de auditoría y otras revisiones, incluyendo aquellos que muestren deficiencias y recomendaciones reportadas por los auditores y otros que evalúen las operaciones de los departamentos, (2) determinar las acciones correctivas en respuesta a los hallazgos y recomendaciones de las auditorías y revisiones, y (3) completar, dentro de los marcos establecidos, todas las acciones que corrijan o resuelvan de cualquier otra manera los asuntos que han llamado su atención.

El proceso de resolución empieza cuando los resultados de la auditoría o de otra revisión son reportados a la gerencia y se termina sólo cuando se toma una acción que (1) corrija las deficiencias identificadas, (2) produzca mejoras, o (3) demuestre que los hallazgos y las recomendaciones no garanticen la acción gerencial.

Ejemplos

El lector puede referirse a los anexos para ejemplos integrados de cada uno de los objetivos y componentes.

3 Roles y Responsabilidades

Todos en una organización tienen responsabilidad por el control interno:

Gerentes	Son los responsables directos por todas las actividades de una organización, incluyendo el diseño, la implantación, la supervisión del funcionamiento correcto, el mantenimiento y la documentación del sistema de control interno. Sus responsabilidades varían de acuerdo a su función en la organización y las características de la organización.
Auditores Internos	Examinan y contribuyen a la continua efectividad del sistema de control interno a través de sus evaluaciones y recomendaciones y por lo tanto desempeñan un papel importante en un control interno efectivo . Sin embargo, no tienen una responsabilidad general primaria sobre el diseño, puesta en marcha, mantenimiento y documentación del control interno.
Miembros del personal:	También contribuyen al control interno. El control interno es parte implícita y explícita de las funciones de cada uno. Todos los miembros del personal juegan un rol al efectuar el control y deben ser responsables por reportar problemas de operaciones, de no cumplimiento al código de conducta o de violaciones a la política.

Las partes externas también juegan un rol importante en el proceso de control interno. Pueden contribuir a que la organización alcance sus objetivos, o pueden proveer información útil para efectuar el control interno. De cualquier modo, no son responsables del diseño, puesta en marcha, funcionamiento adecuado, mantenimiento o documentación del sistema de control interno.

Entidades Fiscalizadoras Superiores (EFSs)	Fortalecen y apoyan la implantación de control interno efectivo en el gobierno. La evaluación del control interno es esencial para el cumplimiento de las EFSs, las auditorías financieras y operativas, mismas que comunican sus hallazgos y recomendaciones a los interesados.

Auditores Externos:	Auditan algunas organizaciones gubernamentales en algunos países. Ellos y sus cuerpos de profesionales deben asesorar y dar recomendaciones de control interno.
Legisladores y reguladores:	Establecen las reglas y directivas relacionadas con el control interno. Deben contribuir a la comprensión común del control interno.
Otras partes	Interactúan con la organización (beneficiarios, proveedores, etc.) y proveen información relacionada con el logro de los objetivos.

El control interno está primeramente efectuado por los interesados internos de la entidad, incluyendo la gerencia, auditores internos y otros miembros del personal. De todas maneras, las acciones de interesados externos también tienen impacto en el sistema de control interno.

Ejecutivos

Todo el personal de una organización juega roles importantes en la ejecución del control interno. De cualquier manera, la gerencia tiene la responsabilidad global del diseño, implantación, supervisión del funcionamiento correcto, mantenimiento y documentación del sistema de control interno. La estructura gerencial de la organización puede incluir directorios y comités de auditoría, mismos que tienen roles diferentes y composiciones diferentes, y son sujetos a diferentes legislaciones en cada país.

Auditores Internos

La gerencia muchas veces establece unidades de auditoría interna como parte del sistema de control interno y las utiliza para ayudar a monitorear la efectividad del sistema de control interno. Los auditores internos proporcionan información regular sobre el funcionamiento del control interno, poniendo especial atención en la evaluación del diseño y operación del control interno. Estos facilitan información sobre los puntos fuertes y los puntos débiles así como recomendaciones para mejorar el control interno. Sin embargo, debería estar garantizada la independencia y la objetividad.

Por lo tanto, el control interno debería ser una actividad independiente, de garantía objetiva y carácter consultivo que añada valor y mejore el funcionamiento de la organización. Ayuda a la organización a cumplir sus objetivos mediante un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y administración.

Pese a que los auditores internos pueden ser una fuente valiosa de capacitación y consejo sobre el control interno, los mismos no deben sustituir a un sólido sistema de control interno.

Para que la función de auditoría interna sea efectiva, es esencial que el personal de auditoría interna sea independiente de la gerencia, trabaje de modo imparcial, correcto y honesto y que reporte directamente al más alto nivel de autoridad dentro de la organización. Esto permite que los auditores internos presenten opiniones imparciales en su valoración sobre el control interno y presenten propuestas objetivas de control interno que busquen corregir los obstáculos revelados. Para las directrices profesionales, los auditores internos pueden utilizar el Marco de Prácticas Profesionales (PPF) del Instituto de Auditores Internos (IIA) que comprende la Definición, el Código Ético, las Normas y los Consejos Prácticos. Adicionalmente los auditores deberían seguir el código de ética de INTOSAI .

Además de cumplir su rol de monitorear el control interno, personal adecuado de auditoría interna puede contribuir a la eficiencia de los esfuerzos de auditoría externa dando asistencia al auditor externo. La naturaleza, rango o límites de tiempo de los procedimientos del auditor pueden ser modificados si el auditor externo confía en el trabajo del auditor interno.

Miembros del personal

Los miembros dependientes y todo el resto del personal también tienen un efecto en el control interno. Muchas veces son los individuos de primera línea los que aplican los controles, revisan los controles, corrigen los controles mal aplicados e identifican qué aspectos pueden ser atacados a través de los controles al conducir sus actividades diarias.

Agentes externos

El segundo más importante grupo de interesados en el control interno son agentes externos tales como auditores externos (incluyendo las entidades fiscalizadoras superiores (EFSs) legisladores, reguladores y otras partes. Pueden contribuir a la consecución de objetivos de la entidad, o pueden proveer información útil para efectuar el control interno. De cualquier manera, no son responsables por la implantación ni operación del sistema de control interno de la entidad.

Las tareas de las partes externas, en particular auditoría externa e instituciones fiscalizadoras superiores incluyen la evaluación del funcionamiento del sistema de control interno y la información a la gerencia sobre sus hallazgos. Sin embargo, la consideración del sistema de control interno como parte externa está determinada por su mandato.

La evaluación del auditor del control interno implica:

- Determinar la importancia y el grado de sensibilidad del riesgo al que los controles están siendo dirigidos;
- Valorar la susceptibilidad del mal uso de recursos, las fallas relacionadas con los objetivos de ética, economía, eficiencia o eficacia o los errores al cumplir con las obligaciones de contabilidad, y el no cumplimiento de las leyes y regulaciones;
- Identificar y comprender los controles relevantes;
- Determinar lo que ya se conoce sobre la efectividad del control;
- Evaluar si el diseño de control es adecuado;
- Determinar, a través de pruebas, si los controles son efectivos;
- Reportar sobre la evaluación del control interno y discutir las acciones correctivas necesarias.

La Entidad Fiscalizadora Superior también tiene interés en asegurar que existan sólidas unidades de auditoría interna donde se las necesite. Estas unidades de auditoría constituyen un elemento importante de control interno al proveer métodos continuos para mejorar las operaciones de una organización. En algunos países, de cualquier manera, las unidades de auditoría interna pueden no tener independencia, ser débiles, o no existir. En esos casos, la Entidad Fiscalizadora Superior debe, siempre que sea posible, ofrecer asistencia y directrices para establecer y desarrollar esas capacidades y para asegurar la independencia de las actividades del auditor interno. Esta asistencia puede incluir asesoramiento o préstamo de personal, dar conferencias, compartir material de capacitación y

desarrollar metodologías y programas de trabajo. Esto debería hacerse sin amenazar la independencia de la EFS o del auditor externo.

La Entidad Fiscalizadora Superior también necesita desarrollar una buena relación de trabajo con las unidades de auditoría interna para que la experiencia y el conocimiento puedan ser compartidos y el trabajo mutuo pueda ser suplementado y complementado. Incluir las observaciones de auditoría interna y reconocer sus contribuciones en el informe de auditoría externa cuando sea posible, puede también fortalecer esta relación. La Entidad Fiscalizadora Superior también debe desarrollar procedimientos de evaluación del trabajo de la unidad de auditoría interna para determinar hasta que grado de confiabilidad una sólida unidad de auditoría interna podría reducir el trabajo de auditoría de la Entidad Fiscalizadora Superior y evitar la no necesaria duplicación de trabajo. La Entidad Fiscalizadora Superior puede tener acceso a los informes de auditoría interna, los papeles de trabajo relacionados y la información del dictamen de auditoría.

Las EFS también juega un papel de liderazgo para el resto del sector público mediante el establecimiento de su propio marco de control interno en la organización de una forma coherente y en base a los principios expuestos en esta guía.

No sólo las EFS sino también los auditores externos juegan un papel relevante en su contribución al logro de los objetivos de control interno, en particular " en el cumplimiento de sus obligaciones de respondabilidad" y de "salvaguarda de recursos". Esto se debe a que los controles externos de los informes financieros y de la información son una parte integral de la respondabilidad y de la buena administración. Todavía las auditorías externas son el mecanismo esencial que los participantes externos utilizan para analizar la gestión, junto con la información no financiera.

Legisladores y reguladores

La legislación puede proveer un entendimiento común sobre la definición de control interno para que los objetivos sean alcanzados. También puede prescribir las políticas que los interesados internos y externos deban seguir al ejecutar sus roles respectivos y responsabilidades para el control interno.

Anexo 1 Ejemplos

Ejemplo (1) de cumplimiento de las obligaciones de respondabilidad: Un departamento que es responsable por el manejo del transporte seguro por río y mar ha sido organizado por los diferentes departamentos de servicios responsables por pilotaje, flotación, inspección de la calidad del agua, promoción de utilización de medios acuáticos de transporte, inversión y mantenimiento de infraestructura (puentes, diques, canales y esclusas)

Entorno de control	Evaluación de riesgo	Actividades de control	Información y comunicación	Seguimiento
Para cada uno de los departamentos de servicio se designa un gerente operacional que reporte al gerente general del departamento. Los gerentes operacionales tienen que tener las habilidades necesarias y la autoridad para tomar algunas decisiones. Todos ellos también firman un código de conducta correcta.	Los posibles riesgos son choque de barcos, derrame de materia tóxica o combustible y explosión de diques. Si los problemas estuvieran relacionados con negligencia por parte del departamento de gobierno, éste podría sufrir una severa sanción.	Las actividades de control que pueden ser organizadas son el pilotaje de barcos por pilotos competentes, colocación de boyas, faros y marcas; inspección visual por aire, y toma de ejemplos de agua.	La información y comunicación relacionadas con esta situación pueden reportar colisiones para prevenir a otros barcos, informar a los barcos sobre condiciones climáticas, y publicar los nombres de sustancias contaminantes, las sanciones que tienen que enfrentar, y las acciones correctivas tomadas.	Un seguimiento de los números de coaliciones, violaciones al medio ambiente, resultados de muestras y una comparación con las de otros países, con sus datos históricos, pueden ayudar a monitorear la efectividad y la eficiencia del pilotaje de barcos, la colocación de faros y marcas, las inspecciones y las muestras de agua.

Ejemplo (2) de cumplimiento de las obligaciones de respondabilidad: El gerente del departamento de deportes estipuló el año pasado un objetivo según el cual la práctica de deportes debía aumentar en un 15% los años siguientes:

Entorno de control	Evaluación de riesgo	Actividades de control	Información y comunicación	Seguimiento
Dado el buen prestigio del gerente, el comité ejecutivo confió plenamente en él y no llevó a cabo las reuniones para revisar el progreso de su trabajo. (Esto no es un ejemplo de buenas prácticas)	Al no especificar los objetivos, el riesgo se da por no alcanzarlos. También existe peligro de que los reportes no se hagan a tiempo porque el gerente quiere esperar con el reporte hasta poder decir que ha cumplido el objetivo del 15% de crecimiento. Además, no se especificó cómo medir el 15%, o sea que el maestro puede decir que el número de gente que hace deporte se incrementó, o que el número de horas aumentó, o inclusive que el número de centros de deportes o clubes aumentó en un 15%. De esta manera la calidad de la información reportada decrece sustancialmente.	El riesgo puede disminuir instalando líneas apropiadas de reporte y un modelo de reporte que defina la información que tiene que transmitirse.	El reporte debe ser enviado a tiempo y de acuerdo al modelo específico. Tiene que especificar los objetivos del crecimiento, cómo son medidos y porqué se los mide de esa manera. Toda la información de respaldo tiene que ser accesible.	La verificación de si el reporte es o no satisfactorio, de cual es la información que se provee y cual es la información que falta, puede ser una forma de seguimiento.

Ejemplo del cumplimiento de leyes y regulaciones aplicables: el Ministerio de Defensa quiere comprar nuevos aviones de combate a través de un contrato público y publica todas las estipulaciones y procedimientos para esta licitación gubernamental. Todas las licitaciones que llegan se mantienen cerradas hasta que termine el plazo establecido. Cuando el plazo concluye todas las licitaciones son abiertas en presencia de los gerentes responsables y algunos oficiales. Sólo las licitaciones recibidas en este período serán investigadas y comparadas para decidir cual de todas es la mejor.

Entorno de control	Evaluación de riesgo	Actividades de control	Información y comunicación	Seguimiento
El equipo que ejecutará esta transacción está compuesto por gente competente que firmó un documento asegurando no tener relaciones financieras o de ninguna otra índole con ninguno de los licitantes. Los gerentes responsables y oficiales también firmaron el documento.	Uno de los riesgos relacionados con las licitaciones gubernamentales y contratos públicos son las relaciones internas. Uno de los licitantes puede tener conocimiento previo sobre la oferta de otros de los licitantes y puede formular una licitación utilizando esta información, que resulte ganadora, pero que no sea la mejor opción entre todas las demás licitaciones. Otro riesgo consiste en escoger la licitación errónea que puede resultar en un nuevo contrato público, si es que el otro no hubiera cumplido con las expectaciones. Además algunos otros licitadores que sintieran que no fueron tratados justamente, podrían hacer demandas.	Para mitigar los riesgos, los procedimientos deben ser desarrollados y aplicados en concordancia con todas las leyes y regulaciones relevantes concernientes a los contratos públicos.	En los procedimientos relacionados con la publicación de las estipulaciones para esta licitación pública, la valoración de las licitaciones recibidas y el anuncio de la licitación escogida deben estar documentados por escrito y se deben detallar todas las acciones tomadas. Al valorar las licitaciones, todas las razones por las que una licitación fue o no fue escogida deben estar documentadas.	La auditoría interna puede hacer revisiones de documentación y seguimiento de los juicios o demandas.

Ejemplo (1) de operaciones ordenadas, éticas, económicas, eficientes y efectivas: El departamento de cultura quiere aumentar las visitas que el público hace al museo. Para lograr este cometido, propone construir nuevos museos, darle a cada ciudadano un cheque cultural y disminuir el costo de las entradas. Para ser económica, eficiente y efectiva, la gerencia tiene que considerar y evaluar si los objetivos pueden lograrse tal y como han sido concebidos a través de las propuestas, y cuanto costará cada una de estas propuestas.

Entorno de control	Evaluación de riesgo	Actividades de control	Información y comunicación	Seguimiento
El departamento de cultura necesita asegurarse de que la estructura de la organización sea adecuada para la supervisión, diseño y construcción de las obras propuestas, así como para la planificación y operaciones de los nuevos museos.	El hecho de que las visitas al museo no aumenten es un posible riesgo. También existe el riesgo de que algunas de las propuestas excedan su presupuesto. Por ejemplo, si rebajar el precio de las entradas no aumenta las visitas al museo, entonces bajan los ingresos del gobierno. Además construir nuevos museos sin la planificación necesaria y considera-ción de requerimientos como ser iluminación, temperatura y seguridad, puede resultar en ajustes muy caros durante o después de la construcción.	Las actividades de control relacionadas a los riesgos anteriormente mencionados pueden ser un control presupuestario que compare el presupuesto actual, observaciones del progreso de la construcción, y solicitud de justificaciones si el presupuesto se extralimita.	La información y comunicación relacionadas con este ejemplo pueden consistir en la documentación de las reuniones con arquitectos, bomberos (para regulaciones de seguridad), artistas y otros. También puede contener diferentes informes relacionados al seguimiento del presupuesto y de los progresos en el trabajo de construcción.	El análisis de las justificaciones de las extralimitaciones en el presupuesto y los costos de intereses relacionados debido a atrasos en el trabajo o en los pagos son parte del seguimiento.

Ejemplo (2) de operaciones ordenadas, éticas, económicas, eficientes y efectivas: El gobierno quiere desarrollar la agricultura y mejorar la calidad de vida en el campo. Proveerán fondos para subsidiar la construcción de pozos de irrigación y drenaje.

Entorno de control	Evaluación de riesgo	Actividades de control	Información y comunicación	Seguimiento
El gobierno debe estar seguro de tener un departamento apropiado para implantar y conducir una operación de subsidio, y crear los mecanismos apropiados para terminar el proyecto puntual y eficientemente.	Los riesgos son que asociaciones inescrupulosas califiquen para obtener el préstamo pero no usen ese dinero para lo que fue destinado.	Las actividades de control pueden ser: Revisar las característi-cas de las asociaciones que aplican para el préstamo. Revisar *in situ* el progreso y los informes sobre el progreso de los trabajos de construcción. Revisar los gastos de las asociaciones a través de sus facturas, y posponer el pago (o parte de él) y los subsidios hasta que la revisión esté terminada.	Reportes del progreso detallando los costos y el número de pozos que fueron drenados y el número de acres que fueron irrigados. (copia de) facturas requeridas como justificativos de los gastos subsidiados.	El seguimiento puede consistir en el seguimiento del drenaje de los pozos y la construcción del sistema de irrigación, y una comparación con otros proyectos similares. También un seguimiento de los trámites de la tierra irrigada puede ser considerado.

Ejemplo (1) de salvaguarda de recursos: El Ministerio de Defensa ha construido depósitos, tiendas militares y estaciones de combustible. El comando militar tiene la política de que estos suministros sean sólo para el uso profesional de los militares, y no así para su uso personal.

Entorno de control	Evaluación de riesgo	Actividades de control	Información y comunicación	Seguimiento
Políticas adecuadas sobre el capital humano serían efectivas para reclutar y mantener el personal adecuado para dirigir y operar los depósitos.	Los riesgos que existen son que la gente quiera tratar de robar armas para usarlas inapropiadamente o venderlas. Además los otros implementos como el combustible pueden ser vulnerables al robo.	Las actividades de control que tienen que ver con estos riesgos son poner vallas y paredes alrededor de los depósitos y estaciones, o poner guardias armados con perros en las puertas. Revisar regularmente los inventarios con el material y un procedimiento que establezca que los implementos sólo pueden ser entregados con la aprobación de un oficial superior también ayudará a salvaguardar los bienes.	Reportes sobre vallas dañadas y diferencias encontradas en la entrega de los implementos. Aprobaciones para las entregas y procedimientos también dan información y comunicación relacionadas con este tema.	El seguimiento puede ser una inspección a las vallas, entregas no anunciadas de material, seguimiento de los movimientos de los bienes o inclusive una prueba secreta de seguridad.

Ejemplo (2) de salvaguarda de recursos: Grandes cantidades de información sensible son almacenadas en los sistemas de computación en una agencia del Ministerio de Justicia. De cualquier modo, la importancia de los controles IT es reducida por negligencia y por ello estos controles tienen numerosas deficiencias.

Entorno de control	Evaluación de riesgo	Actividades de control	Información y comunicación	Seguimiento
La gerencia debe comprometerse a la competencia y buen comportamiento relacionado con el IT, y a dar buena capacitación en esta área. Las políticas de capital humano también juegan un papel importante al establecer un entorno de control positivo para los temas del IT. (Esto no es un ejemplo de buenas prácticas)	A nivel de los controles generales la agencia no ha: limitado el acceso del usuario a sólo aquello que se necesita para cumplir con sus actividades; desarrollado un sistema adecuado de software para proteger los programas y la información sensible; Documentado los cambios en el software; Segregando las actividades incompatibles; Dirigiendo la continuidad del servicio; Protegiendo la red del tráfico no autorizado. Al nivel de aplicación de controles, la agencia no ha mantenido las autorizaciones de acceso	La agencia puede: Implementar accesos lógicos (ejemplo: Password) y controles de acceso físico (ejemplo: seguros, tarjetas de identificación, alarmas). Negar a algunos usuarios la habilidad de ingresar al sistema operativo. Limitar el acceso del ambiente de producción al personal del desarrollo de la aplicación. Utilizar claves de auditoría para registrar todos los accesos (intentos de acceso) y comandos para detectar violaciones a la seguridad. Tener un plan de contingencia y de recuperación de algún desastre para asegurar accesibilidad a recursos críticos y facilitar la continuidad de las operaciones. Tener protección y monitorear la actividad del servidor de la página web para asegurar el tráfico por la red.	Los procedimientos sobre el control IT deben ser accesibles y los cambios al software deben estar documentados antes de que el software empiece a operar. Las políticas y las descripciones de los puestos de trabajo que apoyen la segregación de obligaciones deben ser promovidas. Las claves de acceso (intentos), y los comandos (no autorizados) deben ser periódicamente reportados y revisados.	Ejecutar una auditoría IT, hacer un simulacro de desastre, y monitorear la actividad del sitio web, pueden ser parte del medio IT de seguimiento.

Anexo 2 Glosario

Este glosario está realizado con la intención de proveer un entendimiento común de los términos más importantes utilizados en esta guía respecto de las definiciones y prácticas del control interno. Además de algunas definiciones que introdujimos en este documento, también utilizamos definiciones existentes, tomadas de diversas fuentes citadas.

- Código de ética y Normas de Auditoría, INTOSAI, 2001. (Normas de Auditoría INTOSAI).
- Control Interno. Marco integrado, COSO 1992 (COSO 1992).
- Glosario, Oficina para las publicaciones oficiales de las comunidades europeas, P. Everard y D. Wolter, 1989 (glosario).
- Servicios de auditoría y seguros, un acercamiento integral, A.A. Arens, R.J. Elder and M.S. Beasley, Edición Internacional Prentice Hall, novena edición, 2003. (Arens, Elder & Beasley).
- Borrador de exposición COSO "Marco del riesgo gerencial de una empresa", COSO, 2003. (COSO ERM).
- Manual de auditoría internacional, seguros y pronunciamientos sobre ética, IFAC, 203. (IFAC).
- Libro fuente de Transparencia Internacional 2000 (Transparencia Internacional).
- INCOSAI XVI, Montevideo, Uruguay, 1998, Informe Principal 1 A (Prevención y detección de fraude y corrupción), febrero 1997, (XVI INCOSAI, Uruguay, 1998).

A

Acceso físico
En el control de acceso, tener acceso hacia áreas físicas o entidades (ver acceso lógico).

Acceso lógico
El acto de ganar acceso hacia la información de la computadora. El acceso puede estar limitado a "sólo leer", pero derechos de acceso más extensivos incluyen la habilidad de arreglar los datos, crear nuevos archivos, y borrar archivos existentes. (ver acceso físico).

Actividad de control
Las actividades de control son políticas y procedimientos establecidos para enfrentar los riesgos y lograr los objetivos de la entidad. Los procedimientos que una organización ejecuta para tratar el riesgo se llaman actividades de control interno. Las actividades de control interno son una respuesta al riesgo en tanto que son diseñadas para contener la parte poco certera del resultado que ha sido identificado.

Aplicación
Un programa de computación diseñado para ayudar a la gente a realizar cierto tipo de trabajo, incluyendo funciones especiales, tales como roles de pago,

control de inventario, contabilidad y misión de apoyo. Dependiendo de la tarea para la que haya sido diseñada, la aplicación puede manipular texto, números, gráficas o una combinación de estos elementos.

Auditoría
Revisión de las actividades de una organización y de las operaciones para asegurar que éstas están siendo ejecutadas o están funcionando de acuerdo con los objetivos, el presupuesto, las reglas y normas. El objetivo de esta revisión es identificar, en intervalos regulares, desviaciones que pudieran necesitar una acción correctiva. (glosario).

Auditoría interna
• Los medios funcionales a través de los cuales los gerentes de una entidad reciben de fuentes internas la seguridad de que todos los procesos contables están operando de manera en la que puedan minimizar la probabilidad de la ocurrencia de un fraude, error o prácticas ineficientes o antieconómicas. Tiene muchas de las características de la auditoría externa, pero puede llevar a cabo las directivas provenientes de la gerencia a la que reporta. (Normas de auditoría INTOSAI).
• Una actividad independiente y objectiva que da a una organización una seguridad sobre el grado de dominio de sus operaciones, que da sus consejos para mejorarlas y que contribuye a crear valor añadido. Ayuda esta organización a alcanzar sus objectivos, evaluando, con un enfoque sistemático y metódico, sus procedimientos de gestión de riesgos, de control y de dirección de empresa, y haciendo propuestas fara reforzar su eficacia. (IIA, IFACI)
• La auditoría interna es una actividad de avalúo establecida dentro de una entidad como servicio para la misma. Sus funciones incluyen, entre otras cosas, examinar, evaluar y monitorear cuan adecuada y efectiva es la contabilidad de los sistemas de control interno (IFAC).

Auditores internos
Examinan la efectividad del sistema de control interno y recomiendan mejorías, pero no tienen responsabilidad primaria por implantarlo o mantenerlo.

Auditoría externa
Una auditoría llevada a cabo por un cuerpo que es externo e independiente del auditado, siendo el propósito dar una opinión o un informe sobre las cuentas de los estados financieros, la regularidad y legalidad de las operaciones, y/o el manejo financiero (glosario).

C

Ciclo de valoración del riesgo

Es un proceso continuo e interactivo para identificar y analizar cambios en las condiciones, oportunidades y riesgos y realizar las acciones necesarias al respecto,

en particular, modificar el control interno para dar respuesta a un riesgo cambiante. Los perfiles de riesgo y los controles asociados a este tienen que ser revisados y reconsiderados con regularidad cara a garantizar que el perfil de riesgo continua siendo válido, que las respuestas al riesgo continúan ofreciéndose de una manera adecuada y proporcionada, y que los controles para mitigarlo continúan siendo efectivos en la medida en que los riesgos cambian con el tiempo.

Colusión
Un esfuerzo corporativo entre los empleados para defraudar efectivo, inventarios u otros bienes (Arens, Elder & Beasley).

Comité de auditoría
Es un comité de la mesa directiva cuyo rol típico se centra en aspectos de información financiera y en los procesos gerenciales de la entidad para administrar el riesgo del negocio y el riesgo financiero, y para cumplir con todos los requerimientos significativos ya sea de orden legal, ético o regulatorio. El comité normalmente asiste al directorio con una mirada global sobre: (a) la integridad de los estados financieros de la entidad, (b) el cumplimiento de la entidad con requerimientos legales y regulatorios, (c) las calificaciones e independencia de los auditores, (d) el funcionamiento del auditor interno de la entidad y el de los auditores independientes, y (e) las remuneraciones de los ejecutivos de la entidad.

Componente de control interno
Uno de los cinco elementos del control interno. Los componentes del control interno de una entidad son: entorno de control, evaluación de riesgo, actividades de control, información y comunicación, y seguimiento. (COSO 1992).

Control
• 1. Un sustantivo, utilizado como sujeto, ejemplo: existencia de un control, una política o procedimiento que sea parte del control interno. Un control puede existir dentro de estos cinco componentes 2. Un sustantivo, utilizado como objeto, ejemplo efectuar control- el resultado de políticas y procedimientos diseñados para controlar; este resultado puede o puede no ser un control interno efectivo. 3. Un verbo, ejemplo: controlar, regular, establecer o implantar una política que afecte el control (COSO 1992).
• Cualquier acción tomada por la gerencia, el consejo y otras partes para gestionar el riesgo y aumentar las posibilidades de que los objetivos y metas se alcancen. La gerencia planifica, organiza y dirige la gestión con suficientes acciones para proporcionar una garantía razonable de que los objetivos y metas se alcanzan (IIA)

Control interno
El control interno es un proceso integrado que afecta a la gerencia y al personal de la entidad y está diseñado para dar seguridad razonable de que en la búsqueda de su misión, los siguientes objetivos generales serán conseguidos:

ejecutar las operaciones de forma ordenada, ética, económica, eficiente y efectiva, cumpliendo con las obligaciones de contabilidad y todas las leyes aplicables, así como las regulaciones y la salvaguarda de los recursos contra la pérdida.

Una garantía independiente y objetiva y una actividad consultora diseñada para proporcionar valor añadido y mejorar la operativa de la organización. Ayuda a la organización a cumplir sus objetivos mediante el uso de un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia en los procesos de gestión del riesgo, control y administración (IIA).

Control de acceso
En tecnología de la información los controles diseñados para proteger los recursos de modificaciones no autorizadas, pérdida o exposición.

Control de detección
Un control diseñado para descubrir un hecho o un resultado no intencionado (en contraste con el control preventivo) (COSO 1992).

Control preventivo
Un control diseñado para evitar hechos o resultados no intencionados (contrastar con control de detección) (COSO 1992).

Control continuo de servicio
Este tipo de control involucra asegurar que cuando ocurran eventos inesperados, las operaciones críticas continúen sin interrupción o sean rápidamente reasumidas y la información crítica y sensible sea protegida.

Control presupuestario
Es el control por el que una autoridad puede asegurar que el presupuesto ha sido bien diseñado e implementado de acuerdo a sus estimados, autorizaciones y regulaciones. (glosario)

Controles generales
• Los controles generales son la estructura, políticas y procedimientos que aplican a todos o a un gran segmento de los sistemas de información de una entidad y ayudan a asegurar su correcta operación. Crean el entorno en el que operan los sistemas de aplicación y controles.
• Políticas y procedimientos que ayudan a asegurar la continuidad y operación apropiada de los sistemas de información. Incluyen controles sobre el manejo de la información tecnológica, la infraestructura de la tecnología de la información, seguridad gerencial, adquisición de software, desarrollo y mantenimiento. Los controles generales apoyan el funcionamiento de los controles de aplicación programados. Otros términos que se utilizan a veces para describir los controles generales son: controles generales de computación y controles de tecnología de la información (COSO ERM).

Controles de aplicación
• La estructura, políticas y procedimientos que se aplican a los sistemas separados o individuales de aplicaciones y que están diseñados para cubrir el procesamiento de datos dentro de aplicaciones específicas del software.
• Procedimientos programados en la aplicación del software, y un manual de procedimientos relacionados, diseñados para ayudar a asegurar la integridad y exactitud de la información que se procesa. Los ejemplos incluyen revisiones computarizados de entradas a los datos, secuencia numérica de revisiones y procedimientos manuales para dar seguimiento a los ítems listados en informes de excepción. (COSO 1992).

Controles manuales
Son los controles que se ejecutan manualmente, no a través de la computadora (contrastar con controles computacionales) (COSO 1992).

Controles computarizados
1. Los controles ejecutados por computadora, ejemplo: los controles programados en el software de la computadora (en oposición a los controles manuales).
2. Los controles que se ejecutan al procesar la información y que son controles generales o controles de aplicación (tanto programados como manuales) (COSO 1992).

Controles del sistema de software
Los controles sobre los programas de computadoras y rutinas relacionadas diseñadas para operar y controlar las actividades de procesamiento del equipo de la computadora.

Corrupción
• Cualquier forma de utilización no ética de la autoridad pública para ventaja personal o privada (INTOSAI XVI, Uruguay, 1998).
• El mal uso del poder que se tiene, para el beneficio privado (Transparencia Internacional).

COSO
Comité de organizaciones patrocinadas, un grupo de varias organizaciones de contabilidad. En 1992 publicó un estudio significativo sobre el control interno llamado Control Interno- un marco integrado. El informe es muchas veces llamado Informe COSO.

Cumplimiento
• Todo lo que tenga que ver con estar conforme con las leyes y regulaciones aplicables a la entidad. (COSO 1992).
• Conformidad con y adhesión a las orientaciones, los planes, los procedimientos, las leyes, las regulaciones, los contratos o otras exigencias. (IIA)

D

Datos
Hechos e información que pueden ser comunicados o manipulados.

Deficiencia
Una falla percibida, potencial o real de control interno, o una oportunidad para fortalecer el control interno para dar una mayor probabilidad de que los objetivos de la entidad son alcanzados. (COSO 1992).

Diagrama de flujo
Una representación gráfica de los documentos y archivos del cliente, y la secuencia con la que son procesados. (Arens, Elder & Beasley).

Diagramación de flujo
Ilustra un flujo de procedimientos, información y documentos. La técnica hace posible que se dé una descripción sintética de circuitos complejos o procedimientos. (glosario).

Diseño
1.Intención. Como se lo utiliza en la definición, el control interno está creado para dar seguridad razonable en términos de logros y objetivos; cuando la intención se hace realidad, el sistema puede ser considerado efectivo. 2. Plan. la manera en la que un sistema debería trabajar, en contraste con la manera en la que lo hace (COSO 1992).

Documentación
La documentación de la estructura de control interno es la prueba material y escrita de los componentes del proceso de control interno que incluye la identificación de la estructura de una organización, las políticas y las categorías operacionales, los objetivos relacionados y las actividades de control. Esta debe aparecer en documentos como ser las directivas gerenciales, políticas administrativas, manuales de procedimiento y manuales de contabilidad.

El examen del auditor de los documentos del cliente y los archivos para substanciar la información que está o debe estar incluida en los estados financieros, (Arens, Elder& Beasley).

E

Economía
• Minimizar el costo de los recursos utilizados para una actividad, poniendo cuidado en la calidad apropiada. (Normas de auditoría INTOSAI).

• Adquisición en el momento correcto al costo financiero, humano y material más bajo de los recursos que sean más apropiados en términos de calidad y cantidad (glosario).

Económico
Que no implique desperdicio ni extravagancia. Significa tener la cantidad correcta de recursos, de la calidad correcta, entregados al momento correcto, al lugar correcto, al precio más bajo.

Efectivo
Se refiere al cumplimiento de los objetivos o al grado al que los resultados de una actividad cumplen con los objetivos o con los efectos para los que se realizó una actividad.

Efectividad
• El grado al que los objetivos son logrados, y la relación entre el impacto deseado y el impacto verdadero que recibe la entidad. (Normas de auditoría INTOSAI).
• El grado en el que los objetivos establecidos han sido logrados bajo la óptica de costo-efectividad. (glosario).

Eficiente
Se refiere a los recursos utilizados para lograr los objetivos. Significa que el mínimo de recursos como entradas deben ser utilizados para obtener una determinada cantidad y calidad de salidas, o el máximo producto con una cantidad y calidad determinadas utilizadas como entradas.

Eficiencia
• La relación entre la salida, en términos de bienes, servicios y otros resultados y los recursos utilizados para producirlos. (Normas de auditoría INTOSAI).
• Utilización de los recursos financieros, humanos y materiales de manera que se puedan maximizar las salidas por un determinado número de recursos, o minimizar los recursos invertidos para determinada cantidad y calidad de salidas (glosario).

Ente
Una organización de cualquier tamaño establecida con un propósito particular. Una entidad, por ejemplo, puede ser una empresa de negocios, una organización sin fines de lucro, una organización gubernamental o institución académica. Otros términos usados como sinónimos son organización o departamento. (COSO 1992).

Entorno de control
El entorno de control establece el tono de una organización, influyendo en la conciencia de control de su personal. Es el fundamento para todos los componentes del control interno, el que da disciplina y estructura.

Entrada
Cualquier información introducida a una computadora o el proceso de ingresar datos a la computadora.

Ético
Relacionado con principios morales.

Evaluación de riesgo
La evaluación de riesgo es el proceso de identificación y análisis de los riesgos relevantes al alcanzar los objetivos de la entidad y determinar una respuesta apropiada.

F

Fraude
Interacción fuera de la ley entre dos entidades, donde una de las partes intencionalmente defrauda a la otra a través de representaciones falsas para ganar ventajas ilícitas o injustas. Involucra actos de engaño, conciliación falsa, utilizados para ganar alguna ventaja injusta o deshonesta. (INCOSAI XVI, Uruguay 1998).

G

Gerencia
Comprende a los gerentes y otros que realizan funciones superiores de la gerencia. La gerencia incluye directores y al comité de auditoría sólo en los casos en los que éstos cumplen tales funciones. (IFAC).

I

Incertidumbre
La falta de habilidad para saber de antemano la exacta probabilidad o impacto de eventos futuros. (COSO ERM)

Independencia
• La libertad que se le da a un cuerpo de auditoría y a sus auditores para actuar en concordancia con los poderes de auditoría conferidos a ellos, sin ninguna interferencia externa (glosario).
• La libertad que tiene una Institución Suprema de Auditoría en temas de auditoría, para actuar de acuerdo a sus mandatos sin dirección externa o interferencia de cualquier clase. (Normas de auditoría INTOSAI).
• La libertad no condicionada que amenaza la objetividad o la apariencia de objetividad. Tales amenazas a la objetividad deben ser gestionadas a nivel de auditor individual, de compromiso, funcional y organizativo (IIA).

• La habilidad de un auditor para mantener un punto de vista imparcial en el cumplimiento de servicios profesionales (independencia de hecho). (Arens, Elder & Beasley).
• La habilidad de un auditor para mantener un punto de vista imparcial ante los ojos de los demás (independencia en apariencia). (Arens, Elder & Beasley).

Institución de auditoría
Organización que, sea cual fuere su designación, composición u organización lleva a cabo obligaciones de auditoría externa en concordancia con la ley (glosario).

Intervención gerencial
Las acciones de la gerencia sobre la reglamentación de las políticas prescritas o los propósitos legítimos; la intervención gerencial generalmente es necesaria para tratar con transacciones no recurrentes o que no hayan sido normadas o eventos que de otra manera serían manejados por el sistema en forma no apropiada (contrastar este término con el de regulación gerencial) (COSO 1992).

Instituto de auditores internos (IAI)
Esta es una organización que establece normas éticas y de práctica, provee capacitación y fortalece el profesionalismo entre sus miembros.

Entidad Fiscalizadora Superior (EFS)
La organización pública de un Estado que, sin importar su diseño, constitución u organización, ejerce por ley, la más alta función pública de auditoría de ese Estado. (Normas de auditoría INTOSAI & IFAC).

Integridad
La calidad o el estado de un importante principio moral; rectitud, honestidad y sinceridad; el deseo de hacer las cosas correctamente, profesar y vivir de acuerdo con ciertos valores y expectaciones. (COSO 1992).

L

Legislatura
La autoridad que hace las leyes en un país, por ejemplo el Parlamento. (Normas de auditoría INTOSAI)

Limitaciones inherentes
Las limitaciones de todos los sistemas de control interno. Las limitaciones se relacionan a los límites del juicio humano; problemas de los recursos y la necesidad de considerar el costo de los controles en relación con los beneficios que se esperan. Puede ocurrir una caída del sistema, y la posibilidad de que la gerencia exagere sus controles o incurra en colusiones. (COSO 1992).

M

Mapa de riesgo
Una mirada conjunta o matriz de los riesgos clave que enfrenta una entidad o una unidad que incluye el nivel de impacto (ejemplo: alto, medio, bajo) junto con la probabilidad de que el evento ocurra.

Marco central
Una computadora de alto nivel diseñada para las tareas computacionales más intensivas. Las computadoras de marco central son compartidas muchas veces por múltiples usuarios conectados a la computadora por terminales.

Seguimiento
El seguimiento es un componente del control interno y es el proceso que valora la calidad del sistema de control interno a través del tiempo.

O

Objetividad

Es una actitud mental que permite que los auditores externos e internos de las EFS realcen su actividad de tal manera que crean de honesta en su trabajo y que tengan compromisos con otros en detrimento de la calidad del mismo. La objetividad requiere que los auditores no subordinen su juicio sobre temas de auditoría a la de otros.

Operaciones
• La palabra usada con "objetivos" o "controles" tiene que ver con la efectividad o la eficiencia de las actividades de una entidad, incluyendo la actuación y beneficio de los objetivos, y salvo guardando los recursos. (COSO 1992).
• Las funciones, procesos, y actividades con los que los objetivos de una entidad son alcanzados.

Ordenadamente
Significa en forma ordenada, metódicamente.

Organización Internacional de Instituciones fiscalizadoras superiores (INTOSAI)
INTOSAI es la organización profesional de las instituciones fiscalizadoras superiores (EFS's) en los países que pertenecen a las Naciones Unidas o a sus agencias especializadas. Las EFS's juegan un rol central en la auditoría de cuentas gubernamentales y operaciones, y en la promoción de gerencias financieras sólidas y respondabilidad en los gobiernos. INTOSAI se fundó en 1953 y ha crecido de los 34 países que eran miembros al inicio, a tener más de 1870 miembros en el presente.

P

Partes en juego
Las partes que son afectadas por la entidad, tales como los involucrados, las comunidades en las que la entidad opera, empleados, clientes y proveedores. (COSO ERM).

Política
Instrucción gerencial sobre lo que se debe hacer para efectuar un control. Una política sirve de base para la implantación de los procedimientos. (COSO 1992).

Presupuesto
Cuantitativamente, es la expresión financiera de un programa de medidas planificadas para un determinado período. El presupuesto se diseña con una visión de planificar operaciones futuras y de hacer revisiones ex post sobre los resultados obtenidos. (glosario)

Procedimiento
En tecnología de la información, la ejecución de las instrucciones de un programa por la unidad central de procesamiento de la computadora.

Proceso gerencial
La serie de acciones tomadas por la gerencia para manejar una entidad. El control interno es parte de un proceso integrado con la gerencia (COSO 1992).

Programa de seguridad
Un programa de toda una organización para la seguridad de planificación y gerencia que forma el fundamento de la estructura de control de seguridad de una organización y refleja la entrega de la gerencia superior a la atención de los riesgos de seguridad. El programa debería establecer un marco y un ciclo de continuidad de la valoración de riesgo, desarrollando e implementando procedimientos efectivos de seguridad, y realizando el seguimiento de la efectividad de esos procedimientos.

R

Red
En tecnología de la información, un grupo de computadoras y los accesorios necesarios comunicados por equipos de información. Una red puede involucrar conexiones permanentes, tales como cables, o conexiones temporales hechas a través del teléfono o de otros vínculos comunicacionales. Una red puede ser tan pequeña como una red local que consista en unas cuantas computadoras, impresoras u otros accesorios, o puede consistir en muchas

computadoras grandes y pequeñas distribuidas en una vasta área geográfica.

Respondabilidad
• El proceso en el que las organizaciones de servicio público y los individuos que las conforman son responsables por sus decisiones y acciones, incluyendo su salvaguarda de fondos públicos y su desempeño.
• Obligación impuesta a una persona o entidad auditadas de presentar que ha administrado o controlado los fondos que le fueron confiados conforme a los términos en los que le fueron entregados.

Responsabilidad pública
Las obligaciones de personas y entidades, incluyendo a empresas públicas y corporaciones, a las que se les confían los recursos públicos para que éstos respondan a las responsabilidades fiscales, gerenciales y programadas que les hayan sido conferidas, y para reportar ante quienes les han conferido estas responsabilidades. (Normas de Auditoría INTOSAI).

Revisiones editadas (información por excepción)
Controles programados concebidos en las primeras fases del proceso de las entradas para identificar campos erróneos de información. Por ejemplo, los caracteres alfanuméricos que son introducidos hacia los campos numéricos, pueden ser rechazados por este control. Los controles editados programados también pueden ser aplicados, por ejemplo, cuando la información de las transacciones ingresa a un ciclo de proceso desde otra aplicación

Riesgo
La posibilidad de que ocurra un evento adverso que afecte el logro de los objetivos. (COSO ERM)

Riesgo inherente
El riesgo que tiene una entidad de que en la ausencia de acciones gerenciales pueda mitigar la probabilidad del riesgo o su impacto. (COSO ERM)

Riesgo aceptable
La cantidad de riesgo a la que una entidad está preparada para exponerse antes de que una acción se juzgue necesaria.

Una base amplia de riesgo que una compañía o entidad está dispuesta a aceptar en la búsqueda de su misión o su visión. (COSO. ERM).

Riesgo residual

El riesgo que permanece después de que la gerencia dé respuesta al riesgo.

S

Salidas
En tecnología de la información, los datos/información producidos por el procesador de una computadora, tal como un gráfico en una terminal, o una copia impresa.

Sector público
El término "sector público" se refiere a los gobiernos nacionales, regionales (por ejemplo: estatal, provincial, territorial), a los gobiernos locales (por ejemplo: ciudad, pueblo) y entidades gubernamentales relacionadas (por ejemplo: agencias, directorios, comisiones y empresas). (IFAC).

Seguridad razonable
• Es igual a un nivel satisfactorio de confianza bajo consideraciones dadas de costos, beneficios y riesgos.
• El concepto de que el control interno, sin importar su buen diseño y operación, no puede garantizar que los objetivos de la entidad sean alcanzados. Esto se debe a limitaciones inherentes de todos los sistemas de control interno (COSO 1992).

Sistema de control interno (o proceso, o arquitectura)
Un sinónimo de control interno, aplicado en una entidad. (COSO 1992).

Sistemas computarizados de información
Un ambiente de sistemas de información por computadora existe cuando una computadora de cualquier tipo o tamaño está involucrada en el procesamiento de información financiera que tenga significado para la auditoría, sea esta computadora operada por la entidad o por una tercera parte. (IFAC).

Segregación (o separación) de funciones
Para reducir el riesgo de error, desperdicios, acciones equivocadas y el riesgo que conlleva no detectar estos problemas, un solo individuo o equipo no deben controlar todas las fases clave (autorización, procesamiento, archivo y revisión) de una transacción o evento.

Sistema de software
Es el software que primeramente está relacionado con el control del hardware y las fuentes de comunicación, acceso a carpetas y archivos y el control y programación de aplicaciones.

Sobre-regulación gerencial
La sobre-regulación gerencial de políticas prescritas o procedimientos para propósitos ilegítimos con la intención de obtener ganancias personales o permitir la presentación errónea de la condición financiera de una entidad (contrastar este término con el de intervención gerencial) (COSO 1992).

T

Tolerancia al riesgo
Es la variación relativa aceptable en la consecución de los objetivos. (COSO: ERM).

U

Últimos operadores
Se refiere a la utilización de procesamientos de información no centralizados (ejemplo: que no sean del departamento IT) que utiliza procedimientos automatizados desarrollados por los últimos usuarios, generalmente con la ayuda de paquetes de software (ejemplo: bases de datos). Los procesos de los últimos operadores pueden ser sofisticados y convertirse en una fuente extremadamente importante de la información de la gerencia. Si están adecuadamente probados y documentados puede ser un hecho a cuestionar.

Unidad de control interno
• Departamento (o actividad) dentro de una entidad, a la que se le confía revisiones y valoraciones de los sistemas de la entidad y procedimientos para minimizar la probabilidad de un fraude, errores y prácticas ineficientes. La auditoría interna debe ser independiente dentro de una organización y reportar directo a la gerencia (glosario).
• Un departamento, división o equipo de consultores u otros profesionales que proporciona una garantía independiente y objetiva así como servicios de consultoría diseñados para añadir valor y mejorar la operativa de la organización. El Control Interno ayuda a la organización a cumplir sus objetivos mediante el uso de un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia en los procesos de gestión del riesgo, control y administración (IIA).

V

Valores éticos
Los valores éticos son los que permiten que quien toma una decisión determine un curso apropiado de conducta, estos valores deben estar basados en lo que es "correcto", que puede ir más allá de lo que es legalmente requerido. (COSO 1992).

Valor por dinero
Ver economía, efectividad y eficiencia.

Valoración de riesgo
Significa estimar el significado de un riesgo y valorar la probabilidad de la ocurrencia de éste.