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

COMPONENTE TRES:
ACTIVIDADES DE CONTROL

COMPONENTE TRES: ACTIVIDADES DE CONTROL

En el diseño organizacional deben establecerse las políticas y procedimientos que ayuden a que las normas de la organización se ejecuten con una seguridad razonable para enfrentar de forma eficaz los riesgos. Las actividades de control se definen como las acciones establecidas a través de las políticas y procedimientos que contribuyan a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos con impacto potencial en los objetivos.

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
Actividades de Control	**10.** La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.	Se integra con la evaluación de riesgos. Las actividades de control ayudan a asegurar que las respuestas a los riesgos que direccionan y mitigan los riesgos son llevadas a cabo.
		Considera factores específicos de la entidad. La administración considera cómo el ambiente, complejidad, naturaleza y alcance de sus operaciones, así como las características específicas de la organización, afectan la selección y desarrollo de las actividades de control.
		Determina la importancia de los procesos del negocio. La administración determina cual importancia de los procesos del negocio requiere las actividades de control.
		Evalúa una mezcla de tipos de actividades de control. Las actividades de control incluyen un rango y una variedad de controles que y pueden incluir un equilibrio de enfoques para mitigar los riesgos teniendo en cuenta controles manuales y automatizados, y controles preventivos y de detección.

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
		Considera en qué nivel las actividades son aplicadas. La administración considera las actividades de control en varios niveles de la entidad.
		Direcciona la segregación de funciones. La administración segrega funciones incompatibles, y donde dicha segregación no es práctica, la administración selecciona y desarrolla actividades de control alternativas.
	11. La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.	Determina la dependencia entre el uso de la tecnología en los procesos del negocio y los controles generales de Tecnología: La dirección entiende y determina la dependencia y la vinculación entre los procesos de negocios, las actividades de control automatizadas y los Controles Generales de tecnología.
		Establece actividades de control para la infraestructura tecnológica relevante: La Dirección selecciona y desarrolla actividades de control diseñadas e implementadas para ayudar a asegurar la completitud, precisión y disponibilidad de la tecnología.

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
		Establece las actividades de control para la administración de procesos relevantes de seguridad: La dirección selecciona y desarrolla actividades de control diseñadas e implementadas para restringir los derechos de acceso, con el fin de proteger los activos de la organización de amenazas externas.
		Establece actividades de control relevantes para los procesos de adquisición, desarrollo y mantenimiento de la tecnología: La dirección selecciona y desarrolla actividades de control sobre la adquisición, desarrollo y mantenimiento de la tecnología y su infraestructura.
	12. La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos que llevan dichas políticas.	Establece políticas y procedimientos para apoyar el despliegue de las directivas de la administración: La administración establece actividades de control que están construidas dentro de los procesos del negocio y las actividades del día a día de los empleados a través de políticas estableciendo lo que se espera y los procedimientos relevantes especificando acciones.

COMPONENTE	PRINCIPIOS	PUNTOS DE ENFOQUE - ATRIBUTOS
		Establece responsabilidad y rendición de cuentas para ejecutar las políticas y procedimientos: La administración establece la responsabilidad y rendición de cuentas para las actividades de control con la administración (u otro personal asignado) de la unidad de negocios o función en el cual los riesgos relevantes residen.
		Funciona oportunamente: El personal responsable desarrolla las actividades de control oportunamente como es definido en las políticas y procedimientos.
		Toma acciones correctivas: El personal responsable investiga y actúa sobre temas identificados como resultado de la ejecución de actividades de control.
		Trabaja con personal competente: Personal competente con la suficiente autoridad desarrolla actividades de control con diligencia y continúa atención.
		Reevalúa políticas y procedimientos: La administración revisa periódicamente las actividades de control para determinar su continua relevancia, y las actualiza cuando es necesario.

Las actividades de control se ejecutan en todos los niveles de la entidad, en las diferentes etapas de los procesos de negocio y en el entorno tecnológico, y sirven como mecanismos para asegurar el cumplimiento de los objetivos. Según su naturaleza pueden ser preventivas o de detección y pueden abarcar una amplia gama de actividades manuales y automatizadas. Las actividades de control conforman una parte fundamental de los elementos de control interno, estas actividades están orientadas a minimizar los riesgos que dificulten la realización de los objetivos generales de la organización. Cada control que se realice debe estar de acuerdo con el riesgo que previene, teniendo en cuenta que demasiados controles son tan peligrosos como lo es tomar riesgos excesivos. Estos controles permiten:

- Prevenir la ocurrencia de riesgos innecesarios.
- Minimizar el impacto de las consecuencias de los mismos.
- Restablecer el sistema en el menor tiempo posible.

En todos los niveles de la organización existen responsabilidades en las actividades de control, debido a esto es necesario que todo el personal dentro de la organización conozca cuales son las tareas de control que debe ejecutar. Para esto se debe explicitar cuales son las funciones de control que le corresponde a cada individuo.

Principio 10: Selecciona y desarrolla actividades de control

La organización selecciona y desarrolla actividades de control que contribuyen a la mitigación de riesgos hasta niveles aceptables para la consecución de los objetivos. Las actividades de control apoyan todos los componentes del sistema de control interno, particularmente el componente de Evaluación de Riesgos. Durante la evaluación de los riesgos la administración identifica e implementa acciones necesarias para llevar a cabo las respuestas a los riesgos, y asegurar que dichas respuestas son apropiadas y oportunas.

Los factores específicos de cada entidad influyen en las actividades de control necesarias para apoyar el sistema de control interno. Algunos son:

- El ambiente y complejidad de la entidad, y naturaleza y alcance de sus operaciones.
- Alcance y naturaleza de las respuestas a los riesgos y actividades de control de entidades multinacionales.
- Sistemas de información más sofisticados.
- Estructuras de las entidades.

Tipos de actividades de control

Los controles se pueden agrupar en tres categorías dependiendo del objetivo de la entidad con las que se relacione: las operaciones, la confiabilidad de la información financiera, el cumplimiento de las leyes y reglamentos. Algunos controles se relacionan solamente con un área específica dentro de la organización, pero frecuentemente las tareas de control definidas para un objetivo específico pueden utilizarse para lograr el cumplimiento de otros

objetivos. Dentro de estas categorías se pueden distinguir otros tipos de control: preventivos, de detección y correctivos; manuales, automatizados o informatizados; gerenciales y operativos.

Los controles preventivos son diseñados para evitar eventos no deseados; y los controles de detección son diseñados para identificar y descubrir eventos no deseados después de que ya han ocurrido.

La dirección debe realizar un seguimiento de todos los procesos de la entidad para determinar en qué medida se están alcanzando los objetivos. Una correcta toma de decisiones viene dada por la obtención de la correcta información en el momento en que se necesita, para esto se debe verificar la confiabilidad de la información. Algunas herramientas útiles en esta actividad son: comparación de los datos con los históricos referidos a los mismos periodos, análisis de la información real contra la información pronosticada, cruzamiento de fuentes de información, seguimiento de campañas comerciales, programas de mejoramiento de productos, entre otras.

Algunos tipos de actividades de control son:

- ✓ **Autorizaciones y aprobaciones:** Las autorizaciones confirman que una transacción es válida, y se convierten en aprobaciones a nivel de la administración. las transacciones y tareas más relevantes para la organización solo deben ser autorizados y ejecutados por personal al que se le asignó la responsabilidad dentro de sus competencias. Esta es la forma más conocida para asegurar que solo se llevan a cabo tareas y transacciones que tienen el apoyo de la dirección de la organización. Las autorizaciones deben documentarse y comunicarse debidamente a las personas o áreas autorizadas, quienes deberán ejecutar las tareas asignadas que se les explícito dentro del ámbito de las competencias establecidas dentro de las organización.
- ✓ **Verificaciones:** Las verificaciones comprenden comparaciones de dos o más ítems, para constatar que se cumplan las políticas y regulaciones pertinentes.
- ✓ **Gestión directa de funciones por actividades:** Los responsables de las diversas funciones o actividades en la entidad deben revisar los informes sobre resultados alcanzados.
- ✓ **Proceso de información:** Se debe realizar una serie de controles para comprobar la exactitud, totalidad y autorización de las transacciones. Así mismo se debe controlar el desarrollo de nuevos sistemas y la modificación de los existentes, al igual que el acceso a los datos, archivos, y programas.
- ✓ **Controles físicos:** Los equipos, inversiones financieras, tesorería, y demás activos, son objeto de protección y supervisión constante para comparar los recuentos físicos con las cifran que aparezcan en los registros de control.
- ✓ **Controles sobre la información de inicio:** La información de inicio es usada para apoyar el proceso de transacciones dentro de los procesos del negocio. La organización lleva a cabo actividades de control sobre los procesos de ingreso de datos, actualización y mantenimiento de la precisión, totalidad y validez de los datos.

- ✓ **Indicadores de rendimiento:** El análisis de diferentes datos operativos o financieros junto con la puesta en marcha de acciones correctivas, constituyen actividades de control. Los métodos de medición de desempeño deben estar presentes en toda organización. El resultado de la evaluación de estos indicadores se utiliza para tomar medidas correctivas en las actividades y de esta manera mejorar el rendimiento. Este mecanismo contribuye al sustento de las decisiones, los indicadores de rendimiento no deben ser muy numerosos ni tampoco tan escasos. Esto se logra analizando el sistema de indicadores que se ajuste a las características de la entidad tales como el tamaño, producción, nivel de competencia de los empleados, y demás elementos que diferencien a la organización. El sistema debe tener indicadores cuantitativos para montos presupuestarios, y cualitativos para el nivel de satisfacción de los usuarios.
- ✓ **Segregación de funciones:** Es uno de los controles internos más importantes y efectivos. Todas las actividades de autorizar, ejecutar, registrar y comprobar una transacción deben ser claramente segregadas y diferenciadas. La segregación de responsabilidades es fundamental para mitigar el riesgo de fraude, debido a que lo reduce a niveles aceptables.
- ✓ **Documentación:** Todas las transacciones, hechos significativos y la estructura de control interno deben estar correctamente documentados y disponibles para su revisión. La información referente a control interno debe estar consignada en las políticas de la organización y en los manuales de procedimientos, incluyendo objetivos, estructura y procedimientos de control interno.
- ✓ **Registro oportuno y adecuado de las transacciones y hechos:** Se debe registrar y clasificar debidamente los hechos y transacciones que afectan a la organización. Este registro se debe realizar al momento de ocurrencia de los hechos para garantizar su relevancia y utilidad para la toma de decisiones. Asimismo se deben clasificar debidamente para ser presentados en informes y/o estados financieros contables a los directivos y gerentes.
- ✓ **Acceso restringido a los recursos, activos y registros:** Los accesos deben estar protegidos por mecanismos de seguridad y limitados a las personas autorizadas. Estas personas tienen la responsabilidad sobre los mismos accesos. Todo activo de valor para la organización debe asignarse a un responsable para su custodia y además debe contar con las protecciones adecuadas como seguros, almacenaje, sistemas de alarma, etc. Deben estar debidamente registrados y periódicamente se deben verificar las existencias físicas y registros contables para controlar su coincidencia. Estos mecanismos de protección cuestan tiempo y dinero, por lo que se debe analizar cuidadosamente los riesgos que puedan afectar los activos de la organización como robo, mal uso, destrucción, y realizar una comparativa con los costos del control que se quiera implementar.
- ✓ **Rotación del personal en las tareas claves:** La idea es que ningún empleado tenga la posibilidad de cometer algún tipo de irregularidad por un tiempo prolongado al realizar su tarea. Para esto los empleados deben rotar periódicamente con otros empleados dentro de la organización, mecanismo que muchas veces no se utiliza.

- **Función de auditoria interna independiente:** Esta función de auditoria interna debe depender de sus autoridades y las funciones y actividades que se realizan en dichas auditorias deben ser independientes de las operaciones que se analizan. Es una forma certera y efectiva para la gerencia de estar informada sobre el funcionamiento y confiabilidad de los sistemas de control interno que posee la organización. De esta manera al ser la auditoria interna independiente, puede realizar su cometido con total libertad realizando inspecciones, verificaciones y pruebas que considere necesarias, debido a que las actividades que realiza están desligadas de las operaciones que analiza.

  La auditoría interna hace las veces de un representante de la autoridad superior en cuanto a vigilar el adecuado funcionamiento del sistema informando de forma oportuna de las ocurrencias de cualquier situación indeseada.

- **Autoevaluación de controles basada en los modelos:** metodología desarrollada por la auditoria interna del banco de Canadá, también conocida como autoevaluación de control o evaluación dinámica de control (Dynamic control assesment). Se basa y está implícito en las teorías modernas de control interno. En la estructura de los modelos COSO y COCO, se definen los componentes que estructuran el marco integrado de control y están involucrados en sus tareas, el personal jerárquico de toda la organización, y todas las actividades del negocio, para evaluar los controles que apoyan el logro de los objetivos predefinidos. Si esta metodología se aplica correctamente produce una mejora sustancial, en el rendimiento y eficiencia de la organización proporcionando mayores resultados con menos recursos. Además permite establecer los mecanismos para el análisis de los controles formales e informales.

- **Evaluación de los controles informales:** En primera medida es necesario identificar los controles informales dentro del ambiente de control y los controles formales en los 4 componentes restantes del marco de control interno: evaluación de riesgo, actividades de control, información y comunicación, y supervisión. Para esto el personal de auditoria interna debe desarrollar talleres con el personal de actividades operativas, sin la participación del nivel gerencial de la organización. Tratando temas sobre unidades de trabajo o funciones específicas. La gerencia debe definir los objetivos de trabajo más importantes, así como los controles necesarios para apoyar a su realización. A partir del análisis desarrollado se determinan las fortalezas y debilidades de los procesos de trabajo y se comenta como afectan a la consecución de los objetivos propuestos por la empresa. En este proceso se utilizan plantillas para evaluación de riesgos de auditoria y fijación de prioridades, previstas en el modelo COSO. En los talleres se evalúan los controles formales, e informales, utilizando el mismo criterio en cada taller para facilitar la acumulación y comparaciones en el ámbito de toda la organización. Los participantes votan para definir la importancia de cada aspecto, y para evaluar la eficacia, este procedimiento se automatiza para proporcionar los resultados de los talleres, los cuales son posteriormente analizados.

- **Evaluación de controles formales:** Este método analiza las actividades de control que se relacionan con los objetivos específicos de los trabajos que se realizan en cada área de la organización. En una reunión se definen los controles específicos, y a la vez se identifican y agrupan en 4 componentes de control: evaluación de riesgos, actividades de control, información y comunicación, monitoreo o supervisión. Además se discute sobre la importancia de los controles propuestos a fin de que ayuden a concretar los objetivos. En los talleres la discusión se realiza en relación a las actividades de control dentro de los componentes, y la votación se realiza para definir la importancia y eficacia de dichas actividades.

- **Informe de resultados:** Los reportes sobre las calificaciones y evaluaciones realizadas, basándose en los resultados de los talleres, constituyen la base para el análisis que realiza la gerencia junto con el departamento de auditoria interna cuyo resultado incluye las áreas o acciones a tomar que consideren necesarias para mejorar la gestión. Las gerencias de cada departamento reciben un informe detallado de la autoevaluación de control, el cual brinda una visión general de los controles formales e informales, y también reciben un reporte del perfil de confianza, el cual contrasta la evaluación de los controles de cada componente, con el nivel general de la totalidad de toda la organización. Este proceso permite obtener información valiosa sobre los controles potenciales a implementar. La auditoría adquiere un conocimiento integral de las operaciones de la organización y para efectos de revisiones posteriores ayuda a identificar las prioridades en el proceso de planeación, de las actividades que se requieran.

- **Controles de aplicación:** Estos controles están diseñados para controlar el funcionamiento de las aplicaciones. Permiten asegurar la totalidad y exactitud en el proceso de transacciones, su autorización y su validez. Diseñados principalmente para evitar que se ingresen en el sistema datos erróneos, es decir que son controles preventivos. También pueden ser eficaces para detectar y corregir errores que fueron ingresados al sistema con anterioridad, están dirigidos a: registro de transacciones, actualización de datos aceptados y seguimiento de los rechazados, actualización de archivos, controles de acceso a los registros, documentación técnica y del usuario actualizado, resguardo de los archivos, administración del sistema, e interfaces con otros sistemas. Estos controles de aplicación tienen en cuenta:

  - Totalidad: Todas las transacciones son registradas.
  - Exactitud y precisión: Las transacciones son registradas con las cantidades correctas y en las cuentas adecuadas en cada fase del proceso.
  - Validez: Implementación de actividades de control que incluyan la autorización de transacciones de acuerdo a las políticas y procedimientos de la organización.

Principio 11: Selecciona y desarrolla controles generales sobre tecnología

La organización selecciona y desarrolla actividades de control general sobre la tecnología para apoyar el cumplimiento de los objetivos. Las actividades de control y la tecnología se relacionan de dos formas:

- La tecnología apoya los procesos del negocio: Cuando la tecnología está integrada en los procesos del negocio, se necesitan actividades de control para mitigar el riesgo de un funcionamiento adecuado.
- La tecnología se utiliza para automatizar las actividades de control: Muchas actividades de control de una organización están parcial o completamente automatizadas.

- ✓ **Control del sistema de información**: Para asegurar el correcto funcionamiento y la confiabilidad del procesamiento de transacciones el sistema de información debe ser controlado debidamente. Los sistemas de información deben contar son mecanismos de seguridad que alcancen a las entradas, procesos, almacenamiento y salidas. Con una flexibilidad que permita cambios o modificaciones cuando sea necesario. El sistema debe dar apoyo y controlar todas las actividades de la organización como registrar y supervisar las actividades y eventos que ocurran, además de mantener registros financieros.

Las actividades de control en los sistemas de información pueden agruparse en dos categorías 1) Controles Generales y 2) Controles de Aplicación explicados anteriormente:

- ✓ Controles generales: Incluyen las actividades de control sobre la infraestructura tecnológica, seguridad de la administración y adquisición, desarrollo y mantenimiento de los sistemas de información y herramientas tecnológicas. Estas actividades se aplican en todos los aspectos relacionados con la tecnología: sobre las operaciones del centro de proceso de datos, la adquisición y mantenimiento de software, el control de acceso y el desarrollo y mantenimiento de aplicaciones. Incluyen las medidas y procedimientos manuales que permiten garantizar el funcionamiento continuo y correcto del sistema de información.

  La tecnología requiere de una infraestructura para operar, establecer redes de comunicación, desarrollo de aplicaciones, y demás elementos que puede ser complejos dependiendo las características de la organización. Esta puede ser compartida por las unidades de la entidad, o contratada a proveedores de servicios externos. Dichas características pueden generar riesgos que deben ser entendidos y manejados por la entidad.

Los procesos de seguridad de la administración incluyen las actividades de control para controlar el acceso a la infraestructura tecnológica de la organización, previniendo así accesos y usos no autorizados o inapropiados. Además tienen en cuenta las amenazas tanto internas como externas que pueden afectar a la infraestructura tecnológica.

La adquisición, desarrollo y mantenimiento de tecnologías son soportados por los controles generales de tecnología. Estos supervisan los cambios, autorizaciones, uso de licencias, aprobaciones, con el fin de asegurar un adecuado uso de las tecnologías y sistemas de información. Algunos controles generales son:

- ✓ Controles sobre las operaciones del centro de procesamiento de datos: Este control está relacionado con la estructura del centro de procesamiento de datos, determinando responsable del sector, separación de funciones, niveles de autorización. Las normas COBIT complementarias de las COSO, aconsejan la existencia de un comité de sistemas y controles gerenciales sobre el área de procesamiento de datos.
- ✓ El área de sistemas debe estar definida como un sector autónomo que no supervisa ni es supervisado por ninguna de las áreas usuarias.
- ✓ Normativas y procedimientos: Pautas o instrucciones básicas que refieren a las buenas prácticas que son deseables dentro del ambiente de sistemas, estas normas y procedimientos se refieren al desarrollo y mantenimiento de programas, pruebas de programas, pasajes de programas a producción y documentación de sistemas.
- ✓ Normas sobre continuidad del procesamiento: Estar normas preservan a la organización ante un posible colapso de los sistemas de información. Controles que están dirigidos al análisis de criticidad de los procesos, biblioteca de operaciones, back up de archivos, plan de contingencias, creación y mantenimiento, capacitación y entrenamiento, y pruebas.
- ✓ Proveedores externos: Se deben implementar en la organización los mecanismos necesarios para el control de las aplicaciones que puedan llegar a adquirirse a proveedores externos. Para esto se debe tener en cuenta: contrataciones formales, disposición de programas fuentes, documentación de desarrollo del sistema, acceso irrestricto a sistemas, datos y documentación.
- ✓ Controles sobre la seguridad física: Se deben establecer restricciones a la utilización del sistema apersonas no autorizadas. Así como la creación y mantenimiento de condiciones ambientales adecuadas que ayuden al funcionamiento de los medios en que se procesa la información. Para esto se debe tener en cuenta: acceso restringido al área de procesamiento de datos central, instalaciones adecuadas, energía interrumpible, medios de detección y extinción de incendios, y aire acondicionado.

- ✓ Controles sobre la seguridad lógica: Controles relacionados con las redes de telecomunicaciones, para proteger al sistema contra el acceso y uso no autorizados, incluso para prevenir la piratería informática. Actividades de control aplicables son: identificación o login, autenticación, autorización, registración. La autenticación o identificación se sustentan en algo conocido, contraseña, algo poseído, tarjeta, clave, algo personal, reconocimiento, firma, huellas dactilares.

Principio 12: Se implementa a través de políticas y procedimientos

La organización despliega actividades de control a través de políticas que establecen lo que es esperado y los procedimientos que ponen las políticas en acción. Las políticas reflejan las afirmaciones de la administración sobre lo que debe hacerse para llevar a cabo los controles. Estas afirmaciones deben documentadas, y expresados tanto explícitamente como implícitamente, a través de comunicaciones y acciones y decisiones. Los procedimientos son las acciones para implementar las políticas establecidas.

Las políticas y procedimientos deben cumplir con:

- ✓ Oportunidad: Los procedimientos deben incluir el tiempo en el que se llevara a cabo una actividad de control, o acciones correctivas o de supervisión.
- ✓ Acciones correctivas: Se Deben tomar acciones correctivas cuando sea apropiado.
- ✓ Competencia: Las actividades de control deben ser implementadas por personal competente con la suficiente autoridad para desarrollarla. Esta competencia dependerá de la actividad de control y su complejidad.
- ✓ Reevaluación periódica: Las políticas y procedimientos deben ser evaluados constantemente para determinar su relevancia y efectividad, debido a los cambios en las personas, procesos y tecnología que pueden reducir la efectividad o hacer algunas actividades redundantes.