AUDITOOL
Red de Conocimientos en Auditoría y Control Interno

Buenas Prácticas para el Diseño de Controles

Los ejemplos aquí enunciados no pretenden abarcar todas las situaciones. Es necesario que se realice un análisis y se determine la mejor práctica de acuerdo a la naturaleza del negocio y al tipo de control que se espera diseñar.

Práctica	SI	NO	N/A
La organización ha realizado el proceso para la identificación y evaluación de riesgos, partiendo de los objetivos establecidos.			
Se han definido los riesgos que deben ser mitigados con controles			
El control se considera de obligatorio cumplimiento.			
Los controles parten de la definición de políticas y procedimientos de la organización.			
Los controles se documentan dentro del diagrama de flujo o narrativa del proceso.			
Los controles son diseñados para prevenir, detectar y corregir errores.			
El control preventivo tiene como objetivo anticiparse a los eventos no deseados, actuando sobre las causas del riesgo, así como evitando la generación de errores o eventos fraudulentos.			

Práctica	SI	NO	N/A
El control detectivo, identifica todos aquellos eventos en el momento en que ocurren, así como advierte sobre la presencia de riesgos.			
El control correctivo, se orienta a la implementación de las acciones correctivas una vez se ha identificado un evento no deseado. Su implementación se realiza cuando los controles preventivos y detectivos no han funcionado, lo cual representa que su implementación sea más costosa, pues actúan cuando ya se han materializado eventos de pérdida para la organización.			
La organización considera la siguiente clasificación de controles para su establecimiento: - Automático: lo realiza de principio a fin un sistema de información. - Semiautomático: es ejecutado de manera parcial por una persona, pero con la colaboración de un sistema de información. - Manual: lo ejerce en su totalidad una persona, sin la colaboración de un sistema de información.			
La organización da prioridad al diseño e implementación de controles automáticos y no manuales.			
La organización en la definición de controles, no parte de tener muchos controles, sino de tener un control clave con el cual mitigue el mayor número de riesgos posibles.			

Práctica	SI	NO	N/A
Las personas designadas para ejecutar el control cuentan con la experiencia y el conocimiento requerido, es decir son competentes.			
El diseño de todo control incluye lo siguiente: -Quién lo ejecuta - Cómo se debe aplicar el control - Cuál es la frecuencia del control - Qué busca el control (prevenir, detectar) - El soporte de la ejecución del control (evidencia) - Cómo se identifican las excepciones y qué hacer con ellas. - El control corresponde a una política de la organización			
La organización considera en el diseño de controles, los siguientes tipos de control: - Autorización y/o aprobación - Comprobaciones - Revisiones físicas - Validación de datos - Reconciliaciones - Monitoreo / Reportes / Indicadores de desempeño - Segregación de funciones - Accesos			
El control de autorización y/o aprobación está orientado a que una transacción es validada por un nivel independiente al que realizó la transacción.			
Todas las transacciones están autorizadas por el nivel que corresponde.			

Práctica	SI	NO	N/A
La comprobación confronta si una actividad cumple con una política, o si es válida de acuerdo con su naturaleza.			
Las revisiones físicas se orientan a confirmar la existencia de los activos de acuerdo con los registros contables.			
La validación de datos confirma que los datos con los cuales se generan las operaciones, corresponde con los autorizados, actualizados y registrados.			
La reconciliación compara dos fuentes de información de un mismo elemento, orientando sus resultados a la investigación oportuna de las diferencias.			
El monitoreo se orienta a verificar a nivel gerencial la aplicación de controles establecidos en niveles inferiores, bien sea por los resultados de indicadores de desempeño, o análisis de variaciones, entre otros.			
La organización ha establecido los tiempos precisos en que cada control debe ser ejecutado *(cada vez que ocurre la transacción, diariamente, semanalmente, mensualmente, semestralmente, entre otros).*			
La organización asigna de acuerdo a las responsabilidades de cada cargo, los controles a ser ejecutados, partiendo de minimizar el riesgo de error o fraude *(segregación de funciones).*			

Práctica	SI	NO	N/A
La organización valida en los accesos otorgados a su plataforma de IT, sean asignados de acuerdo al principio de segregación de funciones y responsabilidades asignadas.			
La organización considera el desarrollo de controles de seguridad a su plataforma de IT			
Para los controles automáticos, se mantiene documentación de los cambios que puedan tener las aplicaciones y los controles.			
Los controles automáticos son primero probados en ambiente de pruebas, antes de ser utilizados en la aplicación real.			
La administración verifica periódicamente, que la parametrización de los controles automáticos funcione correctamente de acuerdo a su diseño.			
La administración verifica la efectividad del control diseñado, validando que el mismo es ejecutado de forma oportuna.			
La administración realiza pruebas de recorrido de los controles para validar su diseño y efectividad, una vez se ha puesto en marcha el control.			
La organización realiza periódicamente evaluaciones sobre el conocimiento de los controles, a los colaboradores responsables de su ejecución.			