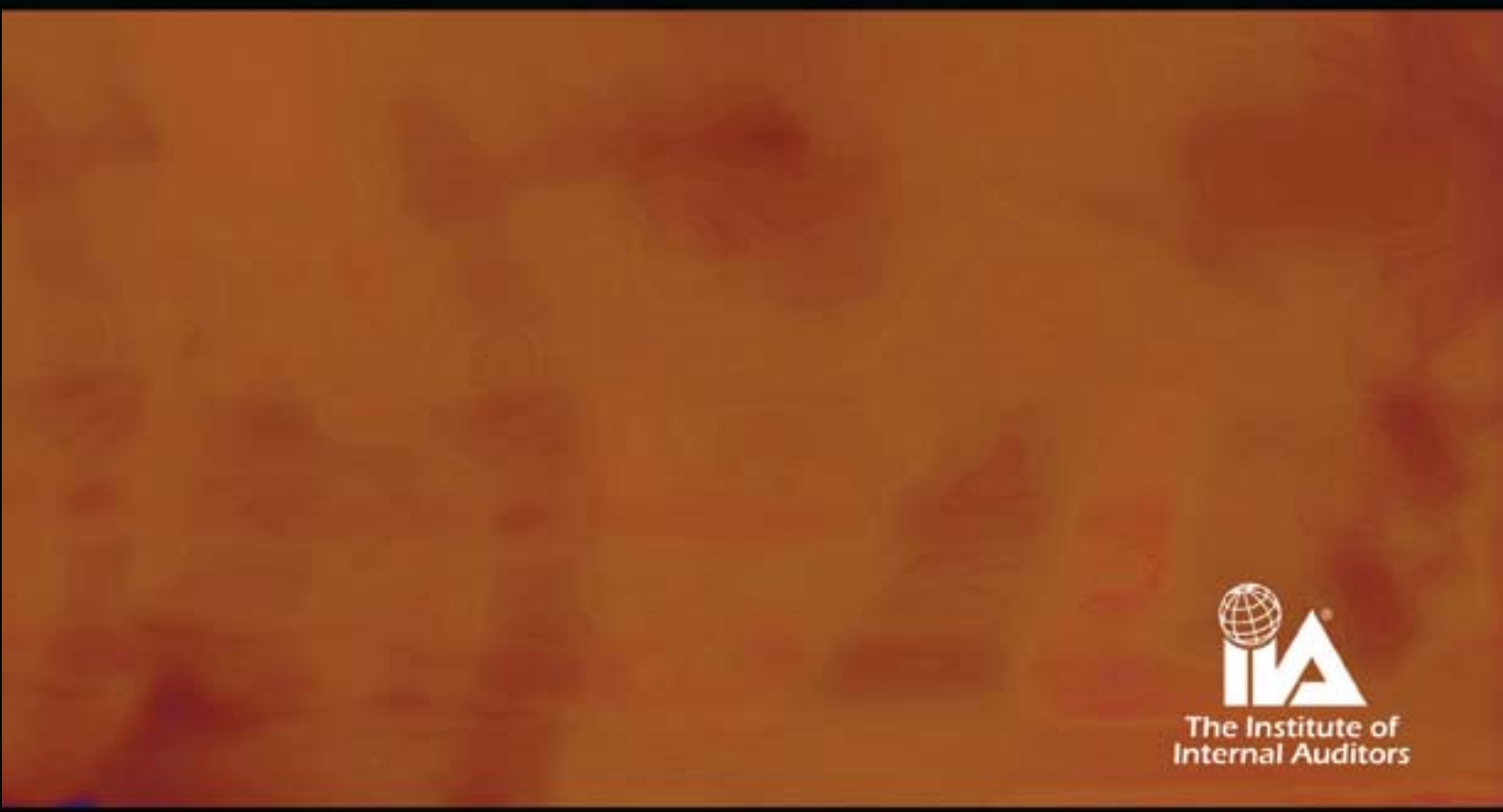
GTAG®

GUÍA DE AUDITORÍA DE TECNOLOGÍA GLOBAL

Auditar controles de aplicacións



The Institute of Internal Auditors

Auditar controles de aplicación

Autores

Christine Bellino, Jefferson Wells

Steve Hunt, Enterprise Controls Consulting LP

Julio 2007

GTAG – Índice

Durante los últimos años, las organizaciones de todo el mundo han gastado miles de millones de dólares en la actualización o instalación de nuevos sistemas de aplicaciones de negocios por distintos motivos, desde objetivos tácticos, como la compatibilidad con el año 2000, hasta actividades estratégicas, como el uso de tecnología para posibilitar la diferenciación de la compañía en el mercado. Una aplicación o sistema de aplicación es un tipo de software que les permite a los usuarios realizar tareas mediante el empleo directo de las capacidades de una computadora. Según la *GTAG 4: Gestión de la auditoría de TI* del Instituto de Auditores Internos (IIA), estos tipos de sistemas se pueden clasificar en aplicaciones transaccionales o aplicaciones de soporte.

Las aplicaciones transaccionales procesan datos en toda la organización:

- Registrando el valor de las transacciones comerciales en términos de débitos y créditos.
- Actuando como repositorios de datos financieros, operativos y reglamentarios.
- Admitiendo varias formas de generación de informes financieros y de gestión, incluido el procesamiento de órdenes de venta, facturas de clientes, facturas de proveedores y asientos en el libro diario.

Entre ellos, algunos ejemplos de sistemas de procesamiento transaccional son SAP R/3, PeopleSoft y Oracle Financials, que muchas veces se conocen como sistemas de planificación de recursos empresariales (ERP, en inglés), así como también muchísimos otros ejemplos de sistemas que no son del tipo ERP. Estos sistemas procesan transacciones según una lógica programada y, en muchos casos, agregan tablas configurables que almacenan reglas comerciales y de procesamiento exclusivas de la empresa.

Por otro lado, las aplicaciones de soporte son programas de software especializados que facilitan las actividades comerciales. Entre ellos, algunos ejemplos son los programas de correo electrónico, software de fax, software de creación de imágenes de documentos y software de diseño. No obstante, estas aplicaciones generalmente no procesan transacciones.[1]

Como sucede con cualquier tecnología que se utiliza para respaldar los procesos de negocio, las aplicaciones transaccionales y de soporte pueden presentar riesgos para la organización, que radican en la naturaleza de la tecnología y en la forma en que los empleados configuran, administran y utilizan el sistema. Con respecto a los sistemas de procesamiento transaccional, si los riesgos no se mitigan correctamente, pueden tener un impacto negativo en la integridad, unidad, puntualidad y disponibilidad de los datos financieros u operativos. Además, los procesos de negocio siempre tienen algún elemento de riesgo inherente, independientemente de la aplicación utilizada para respaldarlos. Como consecuencia de esos riesgos en cuanto a tecnología de aplicaciones y procesos de negocio, muchas organizaciones utilizan una combinación de controles automatizados y manuales para gestionar dichos riesgos en las aplicaciones transaccionales y de soporte. No obstante, el grado de éxito de la gestión de riesgos depende directamente de:

- El grado de aceptación de riesgo de la organización o tolerancia.
- La exhaustividad de la evaluación de riesgos relacionada con la aplicación.
- Los procesos de negocio afectados.
- La eficacia de los controles generales de tecnología de la información (TI).
- El diseño y el alcance continuo de la eficacia operativa de las actividades de control.

Uno de los enfoques más eficientes y más eficaz en relación con su costo que utilizan las organizaciones para gestionar estos riesgos es mediante el uso de controles que son inherentes o están incorporados tanto a las aplicaciones transaccionales y de soporte (por ejemplo, una coincidencia de tres vías respecto de las facturas de cuentas a pagar) como a los controles que se pueden configurar (por ejemplo, las tolerancias de facturas de cuentas a pagar). Por lo general, estos tipos de controles se conocen como controles de aplicación, es decir, controles que pertenecen al alcance de los procesos de negocio o sistemas de aplicaciones individuales, que incluyen las ediciones de datos, la separación de funciones de negocio, el balanceo de totales de procesamiento, el registro de transacciones y la generación de informes de errores.[2]

También es importante que los directores ejecutivos de auditoría (DEA) y su personal comprendan la diferencia entre los controles de aplicación y los controles generales de tecnología de la información (ITGC, en inglés). Los ITGC se aplican a los componentes, procesos y datos de sistemas de toda la organización3 mientras que los controles de aplicación son específicos de un programa o sistema que respalda un proceso de negocio en particular. En este capítulo, la sección "Controles de aplicación versus controles generales de TI" describirá detalladamente estos dos tipos de controles.

Debido a la importancia de los controles de aplicación para las estrategias de gestión de riesgos, los DEA y sus equipos necesitan desarrollar y ejecutar auditorías de controles de aplicación periódicamente para determinar si están diseñados correctamente y funcionan con eficacia. Por lo tanto, el objetivo de esta GTAG es brindarles a los DEA información acerca de:

1. Qué controles de aplicación existen y sus beneficios.
2. El rol de los auditores internos.
3. Cómo realizar una evaluación de riesgos.
4. La determinación del alcance de la revisión del control de aplicación.
5. Los enfoques de revisión de aplicaciones y otras consideraciones.

Para brindarles más ayuda a los DEA y a otras personas que utilizan esta guía, también hemos incluido una lista de los controles de aplicación más comunes y un ejemplo de plan de auditoría.

1 *GTAG 4: Gestión de la auditoría de TI*, pág. 5.

2 *GTAG 1: Controles de tecnología de la información*, pág. 3.

3 *GTAG 1: Controles de tecnología de la información*, pág. 3.

Definir controles de aplicación

Los controles de aplicación son aquellos controles que corresponden al alcance de los procesos de negocio o sistemas de aplicaciones individuales, incluidos las ediciones de datos, la separación de funciones de negocio, el balanceo de totales de procesamiento, el registro de transacciones y la generación de informes de errores. Por lo tanto, el objetivo de los controles de aplicación es asegurar que:

- Los datos de ingreso sean precisos, completos, autorizados y correctos.
- Los datos se procesen según lo planeado en un período de tiempo aceptable.
- Los datos almacenados sean precisos y completos.
- Las salidas sean precisas y completas.
- Se mantenga un registro para realizar el seguimiento del proceso de datos desde el ingreso hasta el almacenamiento y la eventual salida.[4]

Existen varios tipos de controles de aplicación. Estos incluyen:

- **Controles de ingreso de datos:** Estos controles se utilizan principalmente para verificar la integridad de los datos ingresados en una aplicación comercial, ya sea que los datos hayan sido ingresados directamente por el personal, remotamente por un socio comercial o a través de una aplicación o interfaz basada en la Web. El ingreso de datos es verificado para asegurar que se mantenga dentro de los parámetros especificados.
- **Controles de procesamiento:** Estos controles proporcionan un medio automatizado para garantizar que el procesamiento sea completo, preciso y autorizado.
- **Controles de salida:** Estos controles se ocupan de lo que se ha hecho con los datos y deben comparar los resultados de salida con el resultado planeado, cotejando la salida contra el ingreso.
- **Controles de integridad:** Estos controles supervisan los datos que están en proceso y en almacenamiento para garantizar que sigan siendo coherentes y correctos.
- **Pistas para la dirección:** Los controles de historial de procesamiento, muchas veces denominados pista de auditoría, le permiten a la dirección identificar las transacciones y los eventos que registran mediante un seguimiento de las transacciones desde la fuente hasta la salida y mediante un seguimiento inverso. Estos controles también supervisan la eficacia de otros controles e identifican errores tan cerca como sea posible de sus fuentes.[5]

Los componentes adicionales de controles de aplicación incluyen si son preventivos o de detección. Si bien ambos tipos de controles se deben desarrollar dentro de una aplicación basada en una lógica de sistema programada o configurable, los controles preventivos se realizan, tal como su nombre lo indica, para prevenir que se produzca un error dentro de aplicación. Un ejemplo de control preventivo es una rutina de validación de datos de ingreso. La rutina realiza una verificación para garantizar que los datos ingresados sean coherentes con la lógica del programa asociado y sólo permite que se guarden datos correctos. De lo contrario, los datos incorrectos o no válidos se rechazan al ser ingresados.

Los controles de detección también realizan, como su nombre lo indica, una detección de errores según una lógica de programa predefinida. Un ejemplo de control de detección es aquel que descubre una variación favorable o desfavorable entre un precio de factura de proveedor y el precio de la orden de compra.

Los controles de aplicación, especialmente aquellos que son de detección por naturaleza, también se utilizan para respaldar los controles manuales utilizados en el entorno. En particular, los datos o resultados de un control de detección se pueden utilizar para respaldar un control de supervisión. Por ejemplo, el control de detección que se describió en el párrafo anterior puede advertir variaciones de precios de compra utilizando un programa para enumerar esas excepciones en un informe. La revisión de estas excepciones por parte de la dirección se puede considerar un control de supervisión.

Controles de aplicación versus controles generales de TI

Es importante que los DEA y su personal comprendan la relación y la diferencia entre los controles de aplicación y los Controles generales de tecnología de la información (ITGC). De lo contrario, es posible que el alcance de una revisión del control de aplicación no se determine correctamente; lo que impactaría en la calidad de la auditoría y su cobertura.

Los ITGC se aplican a todos los componentes, procesos y datos de sistemas presentes en una organización o al entorno de sistemas.[6] El objetivo de estos controles es garantizar el desarrollo y la implementación adecuados de las aplicaciones, así como también la integridad de los archivos de datos y programas y de las operaciones informáticas.[7] Los ITGC más comunes son:

- Controles de acceso lógico sobre la infraestructura, las aplicaciones y los datos.
- Controles de ciclo de vida del desarrollo del sistema.
- Controles de gestión de cambio de programa.
- Controles de seguridad física sobre el centro de datos.
- Controles de respaldo y recuperación de datos y sistema.
- Controles de operaciones informáticas.

Dado que los controles de aplicación se relacionan con las transacciones y los datos que pertenecen a cada sistema de aplicación basado en computadora, son específicos de cada aplicación individual. El objetivo de los controles de aplicación es garantizar la integridad y precisión de los registros y la validez de las entradas realizadas en cada registro, como el resultado del procesamiento de programas.[8]

4, 5 *GTAG 1: Controles de tecnología de la información*, pág 8.

6 *GTAG 1: Controles de tecnología de la información*, pág 3.

7,8 ISACA, Pautas de auditoría de sistemas de información – Revisión de sistemas de aplicación, Documento G14, pág 3.

En otras palabras, los controles de aplicación son específicos de una determinada aplicación mientras que los ITGC no lo son. Las actividades de control de aplicación más comunes incluyen:

- Determinar si las órdenes de ventas se procesan dentro de los parámetros de límites de créditos de clientes.
- Asegurar que las mercaderías y servicios sólo se compren mediante una orden de compra aprobada.
- Supervisar la separación de responsabilidades basada en las responsabilidades definidas del puesto de trabajo.
- Identificar que las mercaderías recibidas se acumulen en la recepción.
- Garantizar que la depreciación de activos fijos se registre correctamente en el período contable adecuado.
- Determinar si existe una coincidencia de tres vías entre la orden de compra, el receptor y la factura de proveedor.

Además, es importante que los DEA adviertan hasta qué grado la dirección puede confiar en los controles de aplicación para la gestión de riesgos. Esta confianza depende directamente de la eficacia operativa y del diseño de los ITGC. En otras palabras, si estos controles no se implementan correctamente ni funcionan con eficacia, la organización no podrá confiar en sus controles de aplicación para gestionar riesgos. Por ejemplo, si los ITGC que supervisan cambios del programa no son eficaces, entonces en el entorno de producción se pueden introducir cambios no autorizados, no aprobados y no probados comprometiendo la integridad total de los controles de aplicación.

Entornos de TI complejos versus no complejos

La sofisticación o complejidad del entorno de TI de una organización tiene un efecto director sobre el perfil de riesgo general y las estrategias de gestión relacionadas que se encuentran disponibles. Las organizaciones que tienen una infraestructura de TI más compleja se caracterizan por lo siguiente:

- Cambios en aplicaciones, bases de datos y sistemas existentes.
- La creación de un código fuente para software fundamental desarrollado en la empresa.
- Software personalizado preempaquetado que se adapta a las necesidades de procesamiento de la organización.
- Desarrollo de aplicaciones preempaquetadas, cambios y código en producción.[9]

Por otro lado, las organizaciones que tienen un entorno de TI menos complejo se caracterizan por lo siguiente:

- Menos cambios en el entorno de TI existente.
- Implementación de una aplicación financiera preempaquetada sin modificaciones significativas que se completa en el año actual.
- Opciones configurables por el usuario que no alteran significativamente el funcionamiento de la aplicación.
- Falta de proyectos de desarrollo de TI.[10]

Como estas diferencias lo señalan, existe una correlación directa entre la complejidad de las aplicaciones transaccionales y de soporte, y la disponibilidad, uso y confianza en los controles de aplicación inherentes y configurables. En otras palabras, una infraestructura de TI menos compleja no puede ofrecer tantos controles de aplicación inherentes o configurables para la gestión de riesgos. Por lo tanto, el grado de complejidad de la aplicación transaccional y de soporte determinará el alcance, la implementación, el nivel de esfuerzo y el conocimiento requerido para ejecutar una revisión del control de aplicación, así como también el grado hasta donde los auditores internos pueden ayudar en su función de consultoría.

Los beneficios de confiar en los controles de aplicación

Confiar en los controles de aplicación puede generar varios beneficios. A continuación se presenta una descripción de los beneficios clave.

Confiabilidad

Los controles de aplicación son más confiables que los controles manuales a la hora de evaluar la posibilidad de errores de control generados por la intervención humana. Una vez establecido un control de aplicación, y si hay pocos cambios en la aplicación, base de datos o tecnología de soporte, la organización puede confiar en el control de aplicación hasta que se produzca un cambio.

Además, un control de aplicación seguirá funcionando de manera eficaz si los ITGC que tienen impacto directo sobre la naturaleza programática también funcionan de manera eficaz. Esto resulta especialmente cierto para los controles relacionados con cambios de programa y separación de responsabilidades de administradores de TI. Como resultado, el auditor podrá probar el control una sola vez y no varias veces durante el período de prueba.

Benchmarking

El apéndice B de la Norma de Auditoría N.º 5 del Consejo de Supervisión Contable de Sociedades Públicas (PCAOB, en inglés) de EE.UU., "Una auditoría de control interno sobre informes financieros realizada en conjunto con una auditoría de estados contables", establece que se puede utilizar benchmarking en los controles de aplicación ya que, por lo general, estos controles no están sujetos a problemas generados por una falla humana. Si los controles generales que se utilizan para supervisar los cambios de programas, el acceso a programas y las operaciones informáticas son eficaces y se prueban en forma habitual, el auditor puede llegar a la conclusión que el control de aplicación es eficaz sin tener que repetir la prueba de control del año anterior. Esto es especialmente cierto si el auditor verifica que el control de aplicación no se ha modificado desde la última vez que lo probó.[11]

9 *Control interno sobre los informes financieros: guía para empresas públicas más pequeñas* del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO), vol. III, pág. 61.

10 *Control interno sobre los informes financieros: guía para empresas públicas más pequeñas* del COSO, vol. III, pág. 56.

11 Norma de Auditoría N.º 5 del PCAOB, "Una auditoría de control interno sobre informes financieros realizada en conjunto con una auditoría de estados contables", párrafo B29.

Además, la naturaleza y el alcance de la evidencia que el auditor debe obtener para verificar que el control no se haya modificado pueden variar según algunas circunstancias como la eficacia de los controles de cambios de programas de la organización.[12] Como resultado, al utilizar una estrategia de para un control determinado, el auditor debe considerar el efecto de los archivos, tablas, datos y parámetros relacionados sobre la funcionalidad del control de aplicación. Por ejemplo, una aplicación que calcula el ingreso por intereses podría depender de la integridad continua de la tabla de tasas que se utiliza para el cálculo automatizado.[13]

Para evaluar el uso adecuado del de un control automatizado, el auditor debe considerar la frecuencia con que la aplicación se modifica. Así, a medida que aumenta la frecuencia de cambio de código, disminuye la oportunidad de confiar en una estrategia de del control de aplicación. Además, el auditor debe evaluar la confiabilidad de la información respecto de los cambios realizados en el sistema. Entonces, si prácticamente no hay información verificable ni informes disponibles para los cambios realizados en la aplicación, base de datos o tecnología de soporte, es poco probable que el control de aplicación pueda utilizarse para el benchmarking.

No obstante, el benchmarking es particularmente eficaz cuando las compañías utilizan software preempaquetado que no permite ningún desarrollo ni modificación del código fuente. En estos casos, la organización debe considerar más aspectos que sólo el cambio de código. Un control de aplicación dentro de una aplicación compleja, como SAP u Oracle Financials, se puede cambiar, inhabilitar o habilitar fácilmente sin ningún cambio de código.

Finalmente, los cambios de parámetro y configuración tienen un impacto significativo en la mayoría de los controles de aplicación. Por ejemplo, los niveles de tolerancia se pueden manipular fácilmente para inhabilitar controles de nivel de tolerancia y los controles de aprobación de compra se pueden manipular cuando se modifica su estrategia de liberación, una vez más, sin requerir ningún cambio de código.

Las organizaciones necesitan evaluar cada control de aplicación para determinar el tiempo durante el cual el benchmarking puede ser efectivo. Una vez que el benchmark ya no sea efectivo, es importante restablecer la referencia. Para ello, se debe volver a probar el control de aplicación. Los auditores deben plantear las siguientes preguntas a la hora de identificar si el control de aplicación sigue funcionando eficazmente y tal como cuando se estableció originalmente como punto de referencia:

- ¿Se han producido cambios en el nivel de riesgo asociado con el proceso de negocio y el control de aplicación desde el momento en que se estableció originalmente como punto de referencia? (es decir, ¿el proceso de negocio implica un riesgo sustancialmente mayor para el cumplimiento financiero, operativo o de regulaciones que lo que implicaba cuando el control de aplicación se estableció originalmente como punto de referencia?)
- ¿Los ITGC funcionan eficazmente, incluidos los controles de acceso lógico, de gestión de cambios, de desarrollo de sistemas, de adquisición y de operaciones informáticas?
- ¿El auditor puede obtener una amplia comprensión de los efectos de los cambios, si existe alguno, sobre las aplicaciones, bases de datos o tecnología de soporte que contienen los controles de aplicación?
- ¿Se implementaron cambios en el proceso de negocio confiando en el control de aplicación que pudieron impactar en el diseño de control o en su eficacia?

Ahorros de costo y tiempo

Por lo general, probar los controles de aplicación lleva menos tiempo que probar los controles manuales. Esto se debe a que los tamaños de la muestra para los controles manuales están vinculados a la frecuencia con que se ejecutan (por ejemplo, diariamente, semanalmente, mensualmente, trimestralmente o anualmente), mientras que el tamaño de la muestra de los controles de aplicación no depende de la frecuencia de ejecución del control (es decir, los controles de aplicación funcionan eficazmente o no). Además, los controles de aplicación normalmente se prueban una sola vez en la medida que los ITGC estén vigentes. Como resultado, todos estos factores potencialmente pueden implicar un ahorro significativo en la cantidad de horas requeridas para probar un control de aplicación versus un control manual.

El rol de los auditores internos

Conocimiento

Hoy, las organizaciones están confiando más que antes en los controles de aplicación para gestionar riesgos debido a su inherente naturaleza eficaz, a su eficacia en relación con el costo y a su confiabilidad. Tradicionalmente, toda clase de control relacionado con la tecnología era probado por un auditor de TI experimentado, mientras que los controles financieros, operativos y reglamentarios debían ser probados por un auditor que no fuera un auditor de TI. Si bien la demanda de auditores de TI ha crecido sustancialmente en los últimos años y no muestra ningún signo de disminución, es necesario que todos los auditores internos puedan evaluar todos los controles de procesos de negocio de principio a fin.

Además, según las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (Normas)*, específicamente las Normas 1220 y 1210.A3, los auditores internos deben aplicar el cuidado y la pericia de un auditor razonablemente prudente y competente[14], y tener el conocimiento necesario de los riesgos, controles y técnicas de auditoría de TI clave para realizar el trabajo asignado, aunque no se espera que todos los auditores internos tengan la competencia de un auditor cuya responsabilidad principal es la auditoría de TI.[15] En otras

12 Norma de Auditoría N.º 5 del PCAOB, Una auditoría de control interno sobre informes financieros realizada en conjunto con una auditoría de estados contables, párrafo B29.

13 Norma de Auditoría N.º 5 del PCAOB, Una auditoría de control interno sobre informes financieros realizada en conjunto con una auditoría de estados contables, párrafos B29-30.

14 Norma 1220 del IIA: Cuidado profesional.

15 Norma 1210.A3 del IIA.

palabras, todos los auditores internos deben conocer los riesgos y controles de TI y deben ser lo suficientemente competentes como para determinar si los controles de aplicación implementados están diseñados correctamente y funcionan con eficacia para gestionar riesgos financieros, operativos o de cumplimiento.

Consultoría o aseguramiento

Además de los tradicionales servicios de aseguramiento, una de las grandes oportunidades para que la actividad de auditoría interna agregue valor a una organización es a través de los trabajos de consultoría, que se pueden realizar de distintas formas y pueden abarcar cualquier área o función de negocio. Un ejemplo de un trabajo de consultoría es ayudar al personal de la organización con el diseño de los controles durante la implementación o actualización de aplicaciones transaccionales o de soporte.

Lamentablemente, muchos auditores internos no ayudan a la dirección a comprender cómo cambiarán los riesgos cuando la organización implemente una nueva aplicación transaccional o de soporte o realice una actualización importante. En prácticamente todos los casos, esta falta de participación no se debe a una falta de deseo o enfoque, sino al hecho de que los auditores internos no conocen ninguna actividad de desarrollo de sistemas o al hecho de que la dirección no quiere que los auditores se involucren.

Independientemente de la razón, es responsabilidad del DEA garantizar que los auditores internos conozcan dichas actividades y posicionar adecuadamente el valor, el conocimiento y la competencia de los auditores internos para brindar servicios de gestión de riesgos. Además, es importante que los auditores internos participen de esta clase de actividades de desarrollo de sistemas para ayudar a gestionar el riesgo que presenta la aplicación y garantizar que los controles inherentes y configurables estén funcionando con eficacia antes de la etapa de lanzamiento de la aplicación. De lo contrario, será mucho más costoso realizar una revisión después de los hechos, encontrar debilidades y reconstruir controles. A continuación se presentan ejemplos de cómo los auditores internos pueden agregar valor durante los esfuerzos de desarrollo de sistemas con un enfoque sobre los controles de aplicación desde una perspectiva de consultoría.

Evaluación de riesgos independiente

Cada vez que se implemente una aplicación transaccional o de soporte nueva o una actualización significativa, pueden suceder dos cosas. En primer lugar, muchos controles automatizados o manuales que se implementaron para gestionar el riesgo dentro del entorno heredado deberán ser reemplazados por controles nuevos. En segundo lugar, el perfil de riesgo de la aplicación podría cambiar. En otras palabras, la aplicación nueva dará lugar a nuevos riesgos inherentes (es decir, en la forma en que se configura la aplicación) y a riesgos que no se podrán mitigar dentro de la aplicación y se requerirá el uso de controles manuales. Como resultado, los auditores internos pueden ayudar, por no decir liderar, los esfuerzos de la organización para comprender cómo los riesgos actuales cambiarán con la incorporación de la nueva aplicación. Esto se debe a que los auditores internos están capacitados para brindar este nivel de servicio y tienen una posición única para hacerlo debido a su independencia respecto de la dirección.

Para que los auditores internos presten este servicio, además de los otros enumerados a continuación, deben tener conocimiento suficiente de la aplicación bajo desarrollo. La cantidad y el tipo de auditores que necesitan dicho conocimiento dependen de la aplicación bajo desarrollo, el alcance de la implementación en términos de procesos de negocio afectados, el tamaño de la organización y la cantidad de entidades o áreas auditables una vez que la aplicación se haya implementado por completo en la organización. Los DEA pueden tomar distintos caminos para garantizar que se obtenga el conocimiento suficiente, por ejemplo, el uso de manuales, cursos en línea, capacitación en aulas y consultores externos.

Diseño de controles

Otro servicio valioso que los auditores internos pueden proporcionar durante la implementación de un nuevo sistema o una actualización significativa, es una extensión de la evaluación de riesgos independiente. Más específicamente, los auditores pueden ayudar a la dirección con el diseño de los controles para mitigar los riesgos identificados durante la evaluación de riesgos. Los auditores internos asignados a esta actividad deben ser parte del equipo de implementación y no auxiliares. Por lo tanto, las tareas, el tiempo y la cantidad de recursos de auditoría interna requeridos para el diseño de controles de aplicación se deben incorporar en el plan general del proyecto.

Es importante que los DEA asignen la cantidad adecuada de auditores, así como también que tengan las habilidades y la experiencia necesarias para realizar la tarea. En muchos casos, los auditores deben trabajar en el proyecto a tiempo completo. Si es así, los DEA deben asignar las responsabilidades actuales del personal seleccionado para trabajar en el proyecto a otros auditores internos del departamento para que los auditores asignados al proyecto puedan concentrarse en la tarea. Además, los auditores internos que trabajan en el proyecto deben informar al gerente de proyecto durante el ciclo de vida de la implementación del sistema.

En caso de que los auditores sean asignados para ayudar a la dirección en el diseño de los controles de aplicación, los DEA deben tener en cuenta que la independencia y la objetividad pueden ser afectadas si se brindan servicios de aseguramiento un año después de haber realizado un trabajo formal de consultoría. Además, para minimizar los efectos de la restricción se deben llevar a cabo los siguientes pasos: asignar distintos auditores para realizar cada uno de los servicios, establecer una dirección y una supervisión independientes de los auditores, definir una responsabilidad separada para los resultados del proyecto y revelar la supuesta restricción del auditor. Por último, la dirección debe ser responsable de la aceptación e implementación de las recomendaciones.[16] En otras palabras, si un auditor interno participa en el diseño de controles relacionados con una aplicación transaccional o de

16 Norma 1130.C1 del IIA

soporte, no debe participar en la evaluación de la eficacia operativa de los controles durante los primeros 12 meses posteriores a la finalización del trabajo de consultoría.

Educación

El valor educativo que los auditores internos pueden agregar a la organización no se limita a los controles de aplicación. Otra oportunidad clave para que los auditores internos puedan agregar valor a la organización es a través de la educación de controles. Desde una perspectiva de control de de aplicación, los auditores internos pueden educar a la dirección en los siguientes temas:

- Cómo el perfil de riesgo cambiará una vez que se haya implementado la nueva aplicación.
- Debilidades de control inherentes conocidas en las aplicaciones bajo desarrollo.
- Soluciones futuras para mitigar las debilidades identificadas.
- Los diversos servicios que los auditores pueden brindar a la dirección como parte de los esfuerzos de desarrollo del sistema.

Pruebas de controles

Si el equipo de implementación ha diseñado e implementado controles basados en la evaluación de riesgos, o sin la ayuda de una evaluación, los auditores internos pueden agregar valor probando, de manera independiente, los controles de aplicación. Esta prueba debe determinar si los controles están diseñados correctamente y funcionarán con eficacia una vez implementada la aplicación. Si alguno de los controles no está diseñado correctamente ni funciona con eficacia, los auditores deben presentar esta información junto con las recomendaciones a la dirección para evitar la presencia de riesgos no gestionados cuando se implemente por completo la aplicación.

Revisiones de aplicaciones

Las aplicaciones transaccionales y de soporte requieren revisiones de controles de vez en cuando, según la importancia del entorno de control general. La frecuencia, el alcance y la exhaustividad de estas revisiones varían según el tipo de aplicación y su impacto en los informes financieros, en el cumplimiento de regulaciones o en los requisitos operativos y según la confianza de la organización en los controles dentro de la aplicación para la gestión de riesgos.

Evaluar riesgo

El auditor debe utilizar las técnicas de evaluación de riesgos para identificar los puntos vulnerables críticos relacionados con la generación de informes y los requisitos operativos y de cumplimiento de la organización al desarrollar el plan de revisión de evaluación de riesgo. Estas técnicas incluyen:

- La naturaleza, el tiempo y el alcance de la revisión.
- Las funciones de negocio críticas respaldadas por los controles de aplicación.
- El período y los recursos que se gastarán en la revisión.

Además, los auditores deben realizar cuatro preguntas clave al determinar el alcance adecuado de la revisión:

1. ¿Cuáles son los mayores riesgos de toda la organización y las principales preocupaciones del comité de auditoría que se deben evaluar y gestionar al considerar los puntos de vista de la dirección?
2. ¿Qué procesos de negocio se ven afectados por estos riesgos?
3. ¿Qué sistemas se utilizan para realizar estos procesos?
4. ¿Dónde se realizan los procesos?

Al identificar los riesgos, posiblemente les resulte útil a los auditores implementar una evaluación de riesgos descendente para determinar qué aplicaciones se deben incluir como parte de la revisión de controles y qué pruebas se deben realizar. Por ejemplo, la Figura 1 detalla una metodología eficaz para identificar riesgos de informes financieros y el alcance de la revisión. Tenga en cuenta que esta ilustración no representa la única manera de llevar a cabo todos los tipos de evaluación de riesgos.

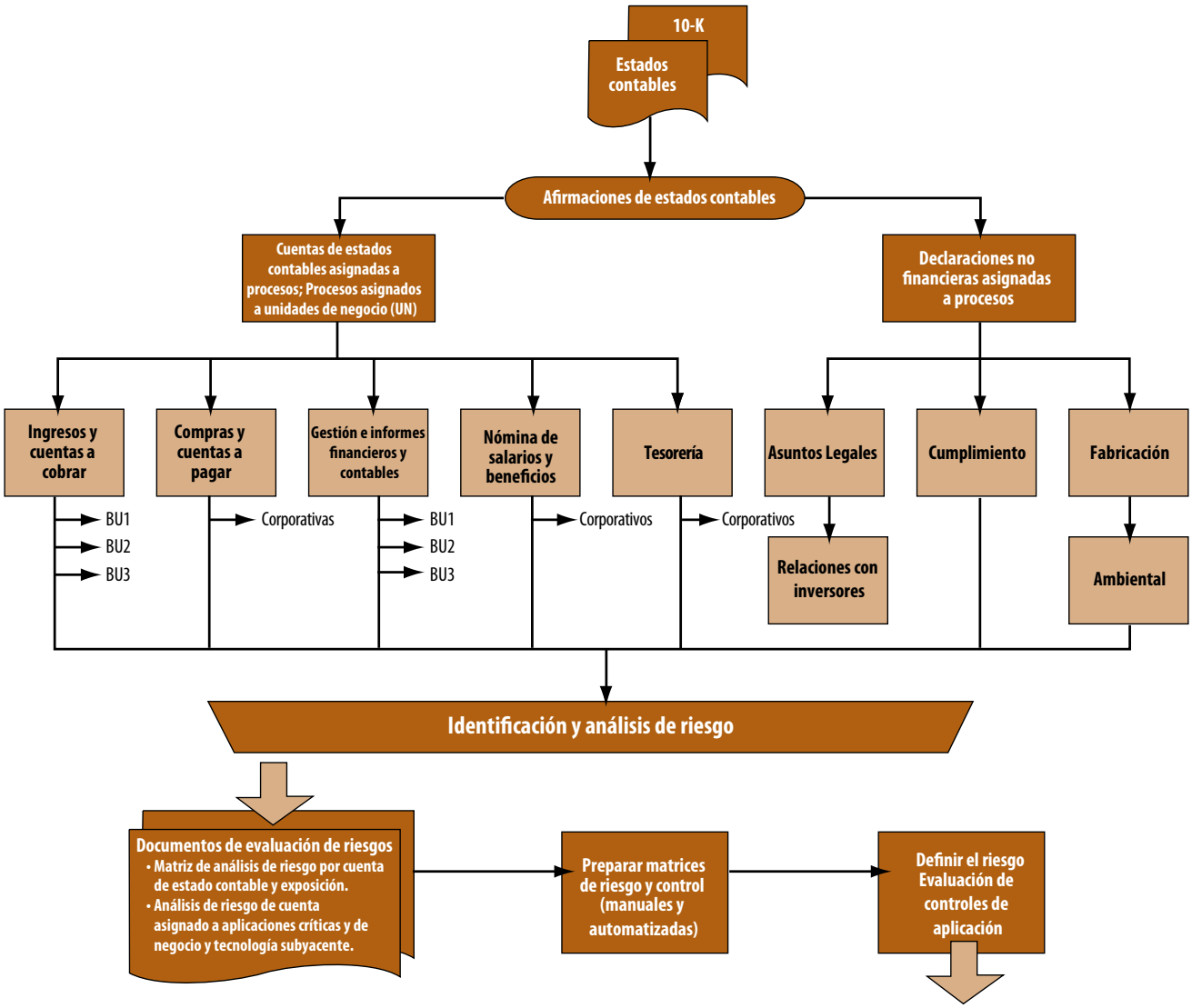


Figura 1. Enfoque de análisis de riesgo de estados contables.

Consulte el Enfoque de Evaluación de Riesgos en la siguiente sección.

Control de aplicación: Enfoque de evaluación de riesgos

Para agregar valor a las actividades de evaluación de riesgos de control de aplicación en toda la organización, los auditores internos deben:

- Definir el universo de aplicaciones, bases de datos y tecnología de soporte que utilizan controles de aplicación y resumir el riesgo y los controles utilizando las matrices de riesgo y control documentadas durante el proceso de evaluación de riesgos.
- Definir los factores de riesgo asociados con cada control de aplicación, incluidos:
  - Los controles de aplicación principales (es decir, clave).
  - La eficacia del diseño de los controles de aplicación.
  - Aplicaciones o bases de datos preempaquetadas o desarrolladas. Las aplicaciones preempaquetadas o desarrolladas no configuradas, a diferencia de las aplicaciones desarrolladas en la empresa o compradas pero altamente configuradas.
  - Si la aplicación admite más de un proceso de negocio crítico.
  - La clasificación de datos procesados por la aplicación (por ejemplo, financieros, privados o confidenciales).
  - La frecuencia de cambios realizados en las aplicaciones o bases de datos.
  - La complejidad de los cambios (por ejemplo, cambios de tabla versus cambios de código).
  - El impacto financiero de los controles de aplicación.
  - La eficacia de los ITGC que residen dentro de la aplicación (por ejemplo, gestión de cambios, seguridad lógica y controles operativos).
  - El historial de auditoría de controles.
- Sopesar todos los factores de riesgo para determinar qué riesgos deben ser ponderados con mayor eficacia..
- Determinar la escala correcta para clasificar cada riesgo de control de aplicación considerando las escalas cualitativas y cuantitativas como:
  - Riesgo de control bajo, medio o alto.
  - Escalas numéricas basadas en información cualitativa (por ejemplo, 1 = riesgo de bajo impacto, 5 = riesgo de alto impacto, 1 = control sólido y 5 = control inadecuado).
  - Escalas numéricas basadas en información cuantitativa (por ejemplo, 1 = < US$ 50.000 y 5 = > US$ 1.000.000).
- Realizar la evaluación de riesgos y clasificar todas las áreas de riesgo.
- Evaluar los resultados de la evaluación de riesgos.
- Crear un plan de revisión de riesgos que se base en la evaluación de riesgos y en las áreas de riesgo clasificadas.

La Figura 2 muestra un ejemplo de una evaluación de riesgo de control de aplicación que utiliza una escala de clasificación cualitativa (1 = bajo impacto o riesgo y 5 = alto impacto o riesgo). Los puntajes compuestos para cada aplicación se calculan multiplicando cada factor de riesgo y su importancia en la aplicación y sumando los totales. Por ejemplo, un puntaje compuesto de 375 en la primera línea se calcula multiplicando la calificación del factor de riesgo por la calificación de la aplicación específica [(20 x 5) + (10 x 1) + (10 x 5) +…]. Para este ejemplo, el auditor puede determinar que la revisión del control de aplicación incluirá todas las aplicaciones cuyo puntaje sea 200 o más.

Importancia o peso de los factores de riesgos									
	20	10	10	10	10	10	15	15	
Aplicación	La aplicación contiene controles principales	Eficacia del diseño de los controles de aplicación	Preempaquetado o desarrollado	La aplicación admite más de un proceso de negocio crítico	Frecuencia del cambio	Complejidad del cambio	Impacto financiero	Eficacia de los ITGC	Puntaje compuesto
APLA	5	1	5	5	3	3	5	2	375
APLB	1	1	2	1	1	1	4	2	170
APLC	5	2	2	1	5	5	5	2	245
APLD	5	3	5	1	5	5	5	2	395
APLE	5	1	1	1	1	1	3	2	225

Figura 2. Ejemplo de una evaluación de riesgo de control de aplicación.

A continuación se presentan dos métodos para determinar el alcance de la revisión de los controles de aplicación. Los auditores internos deben tener en cuenta que el alcance, la exhaustividad, el enfoque y la frecuencia de la revisión dependen de los resultados de la evaluación de riesgos y de la disponibilidad de recursos de auditoría interna. Independientemente del método de determinación de alcance elegido, la revisión debe abarcar una evaluación de los controles de ingreso, procesamiento y salida de datos.

Método de proceso de negocio

El método de determinación de alcance de procesos de negocio es un enfoque de revisión descendente que se utiliza para evaluar los controles de aplicación presentes en todos los sistemas que respaldan un proceso de negocio en particular. Durante los últimos años, este método ha cobrado importancia como la metodología de determinación del alcance más común y ampliamente aceptada. Esto se debe, principalmente, a un incremento en el uso de aplicaciones transaccionales de ERP y a una reducción de aplicaciones independientes de mejor nivel en su campo.

Al utilizar el método de proceso de negocio en un mundo que no pertenece a una ERP, los auditores internos deben incluir, dentro del alcance de la revisión, todas las aplicaciones utilizadas por la compañía que estén involucradas en el proceso de negocio bajo revisión ya que, por lo general, corresponden a sistemas independientes. En otras palabras, el auditor debe incluir, dentro del alcance de la revisión, las aplicaciones independientes que integran los distintos componentes del ciclo de proceso de negocio. Luego, el auditor puede identificar las interfaces entrantes y salientes dentro de la aplicación bajo revisión y completar la actividad de determinación del alcance.

El uso del método de proceso de negocio para determinar el alcance de la revisión de controles de aplicación es distinto para las aplicaciones integradas, como un sistema de ERP, ya que los procesos de negocio atraviesan varios módulos. Por ejemplo, considere el proceso de negocio desde la compra hasta el pago. En un entorno de ERP, este proceso generalmente consiste en módulos o subaplicaciones de compras, gestión de inventario, libro mayor y cuentas a pagar incorporados al sistema. Por lo tanto, es importante lograr una comprensión general de los módulos que abarcan el proceso de negocio y de la forma en que los datos se gestionan y fluyen de un módulo a otro.

Método de aplicación única

El método de determinación de alcance de aplicación única se utiliza cuando el auditor desea revisar los controles de aplicación dentro de una única aplicación o en un único módulo, a diferencia de adoptar un enfoque de determinación de alcance de proceso de negocio. Como se analizó anteriormente, este es el método de determinación de alcance más eficaz en un entorno que no pertenece a una ERP o no está integrado ya que el auditor puede "encasillar" fácilmente la aplicación (es decir, incluir la aplicación dentro del alcance). En otras palabras, el auditor puede identificar las interfaces de ingresos y salidas de datos ya que estos y las reglas de procesamiento relacionadas se incluyen y se utilizan sólo para una aplicación.

No obstante, en un entorno de ERP o integrado, este método no es el más adecuado. Si bien puede parecer relativamente fácil encasillar el módulo de un sistema transaccional integrado o de ERP, la realidad es que esta actividad puede resultar bastante difícil. Esto se debe a que pueden existir varias transferencias de datos entrantes y salientes de un determinado módulo e intentar identificarlas podría resultar ser un ejercicio inútil. Por lo tanto, es probable que el uso del enfoque de módulos genere una revisión inadecuada. El uso del método de proceso de negocio es un método de determinación de alcance más eficaz en un entorno de ERP o integrado.

Controles de acceso

Independientemente del método elegido para determinar el alcance de la revisión de controles de aplicación, los controles de acceso lógico del módulo o de aplicación se deben revisar periódicamente. En la mayoría de los casos, los derechos de acceso administrativo y del usuario (por ejemplo, lectura, escritura y eliminación) se crean utilizando la plataforma de seguridad inherente y las herramientas de la aplicación. Las estrategias empleadas para determinar qué derechos de acceso lógico se asignarán a los usuarios varían desde la "necesidad de conocer" a la "necesidad de mantener". No obstante, los derechos de acceso se deben otorgar según la función laboral y las responsabilidades del usuario.

La forma en que se crean los derechos de acceso lógico varía según el paquete. En algunos casos, los derechos de acceso lógico se otorgan según un código de transacción o un nombre o número de pantalla, mientras que otros, como SAP R/3, utilizan protocolos de seguridad más complejos basados en objetos. Cuando se realiza una revisión de controles de acceso lógico de una aplicación, es importante garantizar que también se revisen los controles de seguridad generales de la aplicación, incluidos los siguientes:

- La longitud del nombre del usuario o identificación del usuario..
- La longitud de la contraseña.
- Las combinaciones de caracteres de la contraseña.
- La antigüedad de la contraseña (por ejemplo, los usuarios deben cambiar su contraseña cada 90 días).
- La rotación de las contraseñas (por ejemplo, los usuarios no pueden utilizar ninguna de sus últimas cinco contraseñas).
- El bloqueo de la cuenta del usuario luego de una cierta cantidad de intentos de inicio de sesión fallidos.
- El tiempo de espera de sesión (por ejemplo, la aplicación se bloquea automáticamente si el usuario no ha interactuado en ella durante 15 minutos).

La última generación de aplicaciones se crea con parámetros que pueden ser configurados por la dirección, como los anteriores. No obstante, en algunos casos, la dirección puede olvidarse de activar los parámetros o bien, la configuración utilizada para cada parámetro puede no ser representativa de las normas para las mejores prácticas. Por ejemplo, el parámetro de antigüedad de contraseña podría estar configurado para requerir un cambio cada 90 días. Además, los auditores deben revisar los derechos de acceso administrativo en el entorno de desarrollo y prueba periódicamente.

Una vez que se haya determinado el alcance adecuado de la revisión, la próxima tarea es determinar cómo se ejecutará la revisión. Además de la metodología de auditoría estándar elegida, a continuación se presentan algunas recomendaciones que pueden ayudar a los auditores a ejecutar una revisión de controles de aplicación cuyo alcance se ha determinado adecuadamente.

Planificación

Luego de completar la evaluación de riesgos y de determinar el alcance de la revisión, los auditores se deben concentrar en el desarrollo y en la comunicación del plan de revisión detallado. El primer paso en el desarrollo del plan de revisión detallado es crear un memorando de planificación que enumere los siguientes componentes de revisión del control de aplicación:

- Todos los procedimientos de revisión que se realizarán.
- Las herramientas y técnicas asistidas por computadora utilizadas y la forma en que se utilizan.
- Tamaño de las muestras, si corresponde.
- Elementos de revisión que se seleccionarán.
- Tiempo de la revisión.

Al preparar el memorando, todos los recursos de auditoría interna requeridos se deben incluir en el equipo de planificación. En este momento también se deben identificar los especialistas de TI que se deben incluir como parte del proceso de planificación.

Luego de completar el memorando de planificación, el auditor debe preparar un programa de revisión detallado. (Consulte el Apéndice B en la página 21 para obtener un ejemplo de un programa de auditoría). Al preparar el programa de revisión, se debe llevar a cabo una reunión con la dirección para debatir lo siguiente:

- Las preocupaciones de la dirección respecto de los riesgos.
- Los problemas informados anteriormente.
- La evaluación de riesgos y controles de la auditoría interna.
- Un resumen de la metodología de revisión.
- El alcance de la revisión.
- La forma en que se comunicarán las preocupaciones.
- Los directores que trabajarán en el equipo de revisión.
- La información preliminar necesaria (por ejemplo, informes).
- La duración de la revisión.

Además de completar un resumen de la fase de evaluación de riesgos, una parte importante de esta reunión es obtener el apoyo de la dirección. Si bien los debates se llevan a cabo al inicio de la fase de planificación de la revisión; los procesos de negocio, riesgos y controles clave se deben debatir durante la revisión para garantizar que la dirección esté de acuerdo con el alcance planificado.

Se deben informar a la dirección todas las preocupaciones conocidas, especialmente, los problemas identificados durante la fase de evaluación o planificación de riesgos, aun cuando estos problemas no se hayan corroborado. Se deben realizar debates para garantizar que la dirección esté de acuerdo con todos los riesgos y controles identificados. De esta manera, el equipo puede ejercer influencia sobre la dirección para que tome medidas correctivas inmediatamente e incentive un comportamiento adecuado, atento a los riesgos, en toda la compañía. Para esto, los auditores pueden enviar una carta a la dirección anunciando la revisión. Esta carta debe incluir:

- La fecha de inicio esperada de la revisión.
- El plazo de la revisión.
- Las áreas de negocio clave bajo revisión.

Necesidad de recursos de auditoría especializados

El auditor interno debe evaluar el alcance de la revisión y determinar si se requerirá un auditor de TI para realizar parte de la revisión. No obstante, agregar un auditor de TI al equipo de revisión no libera al auditor de su responsabilidad de evaluar la idoneidad de los controles de TI. El auditor de TI simplemente evaluará la confianza de la organización respecto de la TI para determinar la integridad de los datos y la precisión, integridad y autorización de las transacciones. Otro factor que podrían revisar los auditores de TI es la cantidad de transacciones procesadas por la aplicación. Posiblemente se requieran herramientas especiales para evaluar e informar la eficacia de los controles de aplicación. La información recolectada por los auditores de TI, junto con el conocimiento del auditor interno, ayudará a determinar si se requieren recursos especializados.

Un ejemplo de una situación en la que se requieren recursos especializados implica una revisión de separación de responsabilidades durante la instalación de una aplicación de Oracle eBusiness Suite para una compañía manufacturera grande. La complejidad y los roles y funciones incluidos en la aplicación y la base de datos requieren el uso de personal que tenga conocimiento de las capacidades de configuración de la aplicación Oracle. Posiblemente se necesite personal adicional que conozca cómo extraer datos de la aplicación y la base de datos Oracle para facilitar la revisión. Además, es posible que el equipo de revisión necesite un especialista que esté familiarizado con una determinada herramienta de auditoría asistida por computadora para facilitar la extracción y el análisis de datos.

Método de proceso de negocio

En el capítulo anterior, el método de proceso de negocio se identificó como el método más utilizado para la determinación del alcance de la revisión del control de aplicación. En la actualidad, muchas aplicaciones transaccionales están integradas en un sistema de ERP. Dado que las transacciones de negocio que fluyen a través de estos sistemas de ERP pueden afectar a diversos módulos durante su ciclo de vida, la mejor forma de realizar la revisión es utilizando un enfoque de proceso de negocio o ciclo (es decir, identificando las transacciones que crean, cambian o eliminan datos en un proceso de negocio y evaluando, al menos, los controles de aplicación de ingreso, procesamiento y salida asociados). La mejor forma de enfocar la revisión es mediante un desglose de los procesos de negocio con el modelo de cuatro niveles que se muestra en la Figura 3:

- Mega proceso (Nivel 1): Se refiere al proceso completo "punto a punto", por ejemplo, el de compras a pagar.

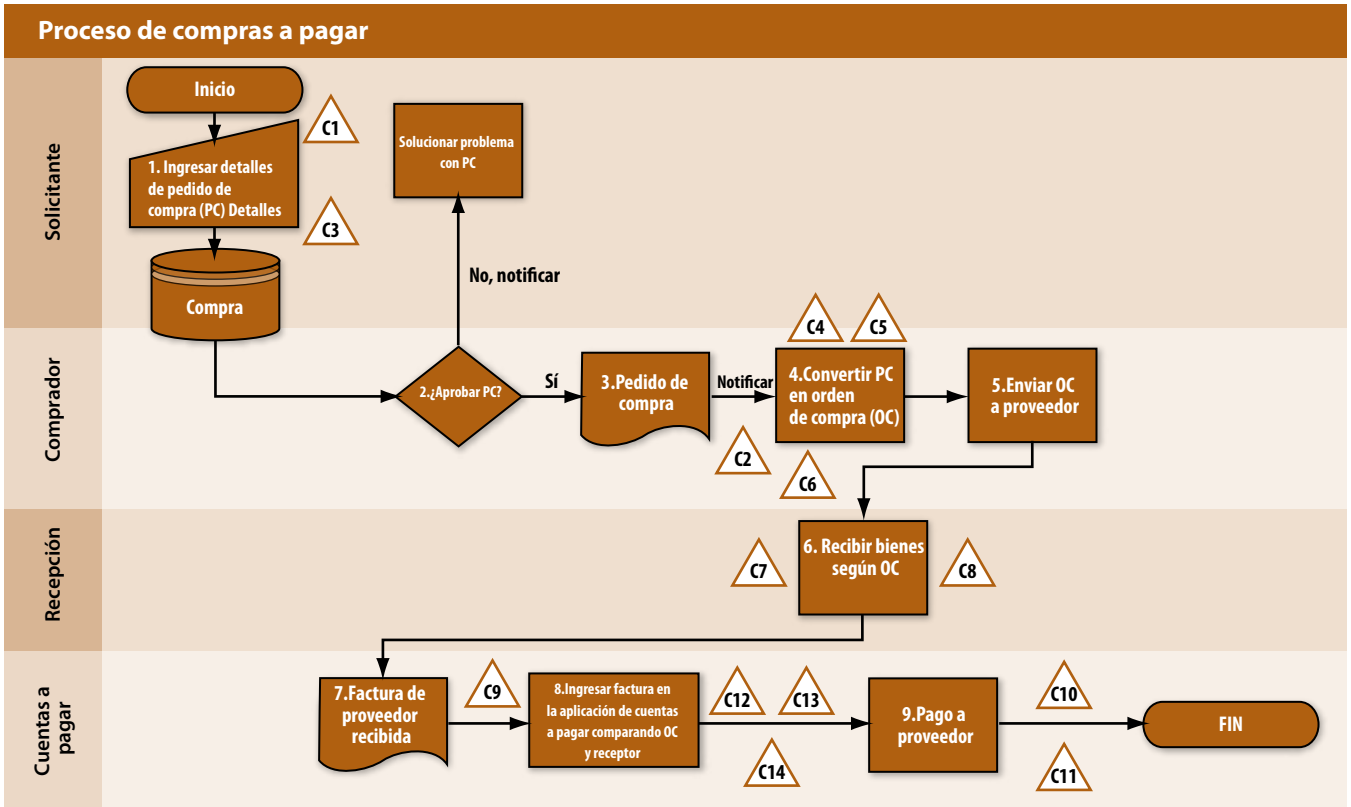
- Proceso principal (Nivel 2): Se refiere a los componentes principales del proceso "punto a punto", como compra, recepción y pago de bienes.
- Proceso menor o subproceso (Nivel 3): Este nivel enumera los componentes menores, o de subproceso, de cada proceso principal, como la generación del pedido y las órdenes de compra.
- Actividad (Nivel 4): Este último nivel enumera las transacciones del sistema que generan la creación, modificación o eliminación de datos para cada componente menor o de subproceso.

Adoptar una visión de negocio centralizada en los controles de aplicación es fundamental para garantizar que la revisión sea completa y resulte útil para la organización. De aquí en adelante, la revisión se puede ejecutar como un trabajo único o como parte de una revisión integrada.

Mega proceso (Nivel 1): Compras a pagar

Proceso mayor (Nivel 2)	Subproceso (Nivel 3)	Actividad (Nivel 4)
Compras	Procesamiento de pedido	Crear, cambiar y eliminar
	Procesamiento de orden de compra	Crear, cambiar, eliminar, aprobar y liberar
Recepción	Procesamiento de recepción de bienes	Crear, cambiar y eliminar
	Procesamiento de devolución de bienes	Crear, cambiar y eliminar
Cuentas a pagar	Gestión del proveedor	Crear, cambiar y eliminar
	Procesamiento de factura	Crear, cambiar y eliminar
	Procesamiento de nota de crédito	Crear, cambiar y eliminar
	Procesar pagos	Crear, cambiar y eliminar
	Anular pagos	Crear, cambiar y eliminar

Figura 3. Desglose de un proceso de negocio.



Los triángulos representan cada control del proceso. El número de cada control está vinculado a la actividad representada en la matriz de riesgo y control.

Figura 4. Diagrama de flujo de un proceso de compras a pagar.

Técnicas de documentación

Además de las normas de documentación utilizadas por los auditores internos, se sugieren los siguientes enfoques para documentar cada control de aplicación.

Diagramas de flujo

Dado que los diagramas de flujo ilustran los flujos de transacciones, estos constituyen una de las técnicas más eficaces utilizadas para capturar el flujo de transacciones y sus controles manuales y de aplicación asociados, que se emplean en un proceso de negocio "punto a punto". La Figura 4 muestra un ejemplo de un diagrama de flujo correspondiente a un proceso de compras a pagar. Debido a la dificultad de incorporar las descripciones de controles existentes en el diagrama de flujo, es conveniente enumerar los controles en el diagrama de flujo y agregar un documento, como una matriz de riesgo y control (consulte la Figura 6, páginas 14-17), que contenga las descripciones de los controles y la información relacionada. No obstante, los diagramas de flujo pueden no ser prácticos para todos los casos y algunas veces es más adecuado utilizar notas descriptivas de proceso. Por lo general, esto sucede cuando un auditor está documentando las áreas o el trabajo realizado dentro del entorno de TI. En muchos casos, el trabajo realizado por TI y los controles de aplicación relacionados no fluyen de una manera lineal como lo hacen los procesos de negocio, por ejemplo, el de compras a pagar.

Notas de proceso

Las notas de proceso constituyen otra técnica disponible para documentar los flujos de transacciones de procesos de negocio con sus aplicaciones asociadas, como se muestra en la Figura 5. Estas notas se utilizan mejor como una herramienta de documentación para procesos de negocio y entornos de TI que no son relativamente complejos. Esto se debe a que cuanto más complejo es el proceso de negocio, más difícil es crear una nota de proceso que refleje, de manera adecuada y precisa, la verdadera naturaleza del proceso. Por lo tanto, cuando se documentan procesos de negocio relativamente complejos, los auditores deben crear un diagrama de flujo con su correspondiente nota de proceso que enumere los controles. Los auditores también deben crear otro documento, como una matriz de riesgo y control.

Notas	Compras a pagar
Contactos principales	
Componentes clave	C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13, and C14.

Figura 5. Matriz de riesgo y control.

A continuación se presenta un ejemplo de nota de proceso que cubre el proceso de compras a pagar.

1) Compra

a) Pedido
   i) Cuando los empleados necesiten comprar bienes o servicios, generarán un pedido de compra en la aplicación de compras **(Control C1)**. Una vez creado el pedido, el comprador revisará el pedido de compra para verificar que sea adecuado, esté completo y sea preciso. Los componentes del pedido de compra que se revisan, incluyen, entre otros, el proveedor, artículo, cantidad y codificación de cuenta. Si la revisión no revela ningún error, el comprador aprobará el pedido de compra. Si el comprador rechaza el pedido de compra por alguna razón, se le notificará al solicitante. Por último, si se solucionan los problemas del pedido original como corresponde, el comprador aprobará el pedido.
   ii) Todos los pedidos de compra se revisan mensualmente para detectar los pedidos no autorizados y, también, los realizados por cantidades excesivas **(Controles C2 y C3)**.

b) Procesamiento de orden de compra
   i) Una vez que el comprador haya aprobado el pedido de compra, creará una orden de compra que haga referencia al pedido en la aplicación de compras **(Control C4)**. Luego, el comprador reenviará una copia de la orden de compra al proveedor.
   ii) Todas las órdenes de compra se revisan mensualmente para detectar las órdenes de compra no autorizadas y, también, las realizadas por cantidades excesivas **(Controles C5 y C6)**.

2) Recepción

a) Todos los bienes se reciben en la playa de despacho y recepción. Un empleado del almacén revisará el recibo de empaque, tomará nota del número de orden de compra y contará los artículos que se reciben físicamente. Luego, el empleado del almacén inicia una sesión en la aplicación de compras e ingresa la cantidad de artículos recibidos en el número de partida correspondiente en la orden de compra.
b) El miembro adecuado del departamento contable revisa y concilia la cuenta del libro general de inventario mensualmente para determinar los bienes que se han recibido pero no han sido facturados por el proveedor **(Control C7)**.
c) El comprador adecuado del departamento de compras revisa mensualmente todos los informes de órdenes de compra que no coinciden **(Control C8)**.

3) Cuentas a pagar

a) El departamento de cuentas a pagar recibe diariamente facturas de distintos proveedores. Estas facturas se ordenan y se asignan a cada empleado de cuentas a pagar, en función del nombre del proveedor. Cada empleado debe marcar cada factura con la fecha en que el departamento de cuentas a pagar la recibió. Luego, cada empleado de cuentas a pagar compara las cantidades y precios de la factura con la orden de compra y el receptor e ingresa la factura en la aplicación de cuentas a pagar **(Controles C9 y C14)**.
b) La aplicación de cuentas a pagar genera automáticamente las solicitudes de pago en función de las condiciones de pago del proveedor y todos los miércoles

se procesa una ejecución de verificación de cuentas a pagar **(Controles C10, C12 y C13)**.

c) A fin de mes, el director de cuentas a pagar compara el total del libro auxiliar del sistema de cuentas a pagar con el total de control del libro mayor. Luego se corrigen las diferencias detectadas **(Control C11)**.

Las matrices de riesgo y control deben capturar toda la información relevante asociada con un proceso de negocio determinado. Además, cada actividad de control debe estar numerada y ese número se debe volver a vincular con los diagramas de flujo o las notas de proceso. La información importante de actividades de control que se debe capturar en la matriz incluye:

- Riesgos identificados.
- Objetivos de control.
- Actividades de control.
- Atributos de control, como tipo de control (por ejemplo, automatizado o manual) y frecuencia (por ejemplo, diariamente, semanalmente, mensualmente, trimestralmente, anualmente, etc.).
- Información de pruebas.

Pruebas

El auditor debe evaluar si los controles de aplicación funcionan o si están siendo evadidos por actos de usuarios creativos o de la dirección. Es necesario realizar pruebas sustantivas sobre la eficacia de los controles en lugar de una revisión de la configuración de controles. Los auditores también deben identificar la eficacia de los ITGC y considerar, si es necesario, que el equipo de auditoría revise los registros de control de cambios, los registros de seguridad y los registros de administración generados por la aplicación.

El auditor puede probar los controles de aplicación utilizando varios métodos basados en el tipo de control. Según la naturaleza, el tiempo y el alcance de la prueba, un control o informe específico se podría probar mediante:

- La inspección de las configuraciones del sistema.
- La inspección de las pruebas de aceptación del usuario, si se realizó alguna durante el año actual.
- La inspección o reejecución de conciliaciones con detalles de respaldo.
- La reejecución de la actividad de control utilizando datos del sistema.
- La inspección de los listados de acceso de usuarios.
- La reejecución de la actividad de control en un entorno de prueba (utilizando los mismos procedimientos programados que la producción) con sólidas secuencias de comandos de prueba.

Un ejemplo de una prueba de configuración del sistema incluye la revisión de los parámetros de coincidencia de tres vías del sistema probado mediante el seguimiento de una transacción. Otro ejemplo de una revisión de configuración del sistema es consultar el código de programación subyacente del proceso de generación de informes de la aplicación para determinar la lógica adecuada. Además, el auditor debe observar una reejecución de la consulta para comparar el informe con aquel que generó la dirección.

El auditor podría probar las verificaciones de ediciones de campos clave, que se pueden realizar estratificando o clasificando las transacciones en los valores de campos. Además, utilizando el software de auditoría, sería fácil volver a calcular y verificar los cálculos realizados por el sistema. Por ejemplo, si el sistema utiliza los campos de cantidad y precio unitario para calcular el costo total, el auditor podría utilizar el software de auditoría para realizar el mismo cálculo e identificar las transacciones en las que los valores calculados no coinciden con los valores de la aplicación.

Por último, los auditores pueden realizar verificaciones de razonabilidad para examinar los rangos de datos de valores posibles para los campos clave. Por ejemplo, mediante el cálculo de la edad actual en función del campo de fecha de nacimiento, los auditores pueden identificar edades, incluidos los valores negativos y los superiores a 100 que se excluyen de los rangos esperados.

Técnicas de auditoría asistidas por computadora

Las técnicas de auditoría asistidas por computadora (CAAT, en inglés) utilizan aplicaciones informáticas, como ACL, IDEA, VIRSA, SAS, SQL, Excel, Crystal Reports, Business Objects, Access y Word, para automatizar y facilitar el proceso de auditoría. El uso de CAAT ayuda a garantizar que se proporcione la cobertura adecuada para una revisión del control de aplicación, en especial cuando existen cientos, o tal vez millones, de transacciones que se generan durante un período de prueba. En estas situaciones, sería imposible obtener información adecuada en un formato que se pudiera revisar sin el uso de una herramienta automatizada. Dado que las CAAT brindan la posibilidad de analizar grandes volúmenes de datos, una prueba de auditoría bien diseñada y respaldada por una CAAT puede realizar una revisión completa de todas las transacciones y anormalidades no descubiertas (por ejemplo, transacciones o proveedores duplicados) o un conjunto de problemas predeterminados (por ejemplo, conflictos de separación de funciones).

Matriz de riesgo y control: Compras a pagar

	PROCESO DE NEGOCIO Y OBJETIVOS DE CONTROL	RIESGOS		ACTIVIDADES DE CONTROL	COMPONENTES DE COSO					ATRIBUTOS DE CONTROL				CLASIFICACIÓN DE CONTROL						PRUEBA		
Número	Objetivos de control	Riesgos	Impacto/ Probabilidad	Actividades de control	EC	ER	AC	I/C	S	C(SI/No)	Man/Auto	Pre/Det	Frecuencia	Verdadero	Registrado	Valorado	Oportuno	Clasificado	Asentado	Resultados de la prueba	Eficacia operativa (Si/No)	Notas
	Principal: Compra																					
	Sub: Procesamiento de pedido de compra																					
	Actividad: Crear																					
C1	Los controles proporcionan aseguramiento razonable respecto de que los pedidos de compra sean creados por personal autorizado de manera completa y precisa.	Debido a la falta de una separación de responsabilidades adecuada, el usuario puede crear, aprobar (liberar), asignar y convertir un pedido de compra, lo que genera retribuciones incorrectas a los proveedores, sobrepagos y niveles de inventario excesivos.	H	Gracias a los controles, se otorga acceso sólo a aquellas personas que tengan un fin comercial para crear pedidos de compra.			X				A	P	Siempre	X	X	X		X	X			
C2	Los controles proporcionan aseguramiento razonable respecto de que los pedidos sean creados por personal autorizado de manera completa y precisa.	Debido a la falta de una separación de responsabilidades adecuada, el usuario puede crear, aprobar (liberar), asignar y convertir un pedido de compra; lo que genera retribuciones incorrectas al proveedor, sobrepagos y niveles de inventario excesivos.	H	Los pedidos de compra se revisan mensualmente para detectar pedidos no autorizados.			X	X	X		M	D	Mensualmente	X	X	X		X	X			
C1	Los controles proporcionan aseguramiento razonable respecto de que los pedidos de compra sean creados por personal autorizado de manera completa y precisa.	Debido a la falta de una separación de responsabilidades adecuada, el usuario puede crear, aprobar (liberar), asignar y convertir un pedido de compra; lo que genera retribuciones incorrectas al proveedor, sobrepagos y niveles de inventario excesivos.	M	Gracias a los controles, se otorga acceso sólo a aquellas personas que tengan un fin comercial para crear pedidos de compra.			X				A	P	Siempre	X	X	X		X	X			
C3	Los controles proporcionan aseguramiento razonable respecto de que los pedidos de compra sean creados por personal autorizado de manera completa y precisa.	Debido a la falta de una separación de responsabilidades adecuada, el usuario puede crear, aprobar (liberar), asignar y convertir un pedido de compra; lo que genera retribuciones incorrectas al proveedor, sobrepagos y niveles de inventario excesivos.	M	Gracias a los controles, se otorga acceso sólo a aquellas personas que tengan un fin comercial para crear pedidos de compra.			X	X	X		M	D	Mensualmente	X	X	X			X			

Lista de siglas utilizadas en el gráfico:

Componentes de COSO

1. EC: entorno de control
2. ER: evaluación de riesgos
3. AC: actividades de control
4. I/C: información y comunicación
5. S: supervisión

Atributos de control

6. C: control clave
7. Man/Aut: manual o automático
8. Pre/Det: prevenir o detectar

Figura 6. Matriz de riesgo y control para un proceso de compras a pagar.

Matriz de riesgo y control: Compras a pagar

	PROCESO DE NEGOCIO Y OBJETIVOS DE CONTROL	RIESGOS		ACTIVIDADES DE CONTROL	COMPONENTES DE COSO					ATRIBUTOS DE CONTROL				CLASIFICACIÓN DE CONTROL						PRUEBA		
Número	Objetivos de control	Riesgos	Impacto/ Probabilidad	Actividades de control	EC	ER	AC	I/C	S	C(SI/No)	Man/Auto	Pre/Det	Frecuencia	Verdadero	Registrado	Valorado	Oportuno	Clasificado	Asentado	Resultados de la prueba	Eficacia operativa (Si/No)	Notas
	Principal: Compra																					
	Sub: Procesamiento de orden de compra																					
	Actividad: Crear																					
C4	Los controles proporcionan aseguramiento razonable respecto de que las órdenes de compra sean procesadas por personal autorizado de manera completa, precisa y oportuna.	Debido a la falta de una separación de responsabilidades adecuada, el usuario puede crear, aprobar (liberar), asignar y convertir un pedido de compra, lo que genera retribuciones incorrectas a los proveedores, sobrepagos y niveles de inventario excesivos.	H	Gracias a los controles, se otorga acceso sólo a aquellas personas que tengan un fin comercial para crear órdenes de compra.			X				A	P	Siempre	X	X	X		X	X			
C5	Los controles proporcionan aseguramiento razonable respecto de que las órdenes de compra sean creadas por personal autorizado de manera completa y precisa.	Debido a la falta de una separación de responsabilidades adecuada, el usuario puede crear, aprobar (liberar), asignar y convertir un pedido de compra, lo que genera retribuciones incorrectas a los proveedores, sobrepagos y niveles de inventario excesivos.	H	Las órdenes de compra se revisan mensualmente para detectar órdenes no autorizadas.			X	X	X		M	D	Mensualmente	X	X	X		X	X			
C6	Los controles proporcionan aseguramiento razonable respecto de que las órdenes de compra sean creadas por personal autorizado de manera completa y precisa.	Las cantidades de las órdenes de compra no autorizadas o excesivas podrían generar precios desfavorables, inventario excesivo y devoluciones de productos innecesarios.	M	Las órdenes de compra se revisan mensualmente para detectar cantidades de órdenes excesivas.			X	X	X		M	D	Mensualmente	X	X	X		X	X			

Lista de siglas utilizadas en el gráfico:
Componentes de COSO
1. EC: entorno de control
2. ER: evaluación de riesgos
3. AC: actividades de control
4. I/C: información y comunicación
5. S: supervisión

Atributos de control
6. C: control clave
7. Man/Aut: manual o automático
8. Pre/Det: prevenir o detectar

Figura 6 (continuación).

Matriz de riesgo y control: Compras a pagar

	PROCESO DE NEGOCIO Y OBJETIVOS DE CONTROL	RIESGOS		ACTIVIDADES DE CONTROL	COMPONENTES DE COSO					ATRIBUTOS DE CONTROL				CLASIFICACIÓN DE CONTROL						PRUEBA		
Número	Objetivos de control	Riesgos	Impacto/ Probabilidad	Actividades de control	EC	ER	AC	I/C	S	C(Sí/No)	Man/Auto	Pre/Det	Frecuencia	Verdadero	Registrado	Valorado	Oportuno	Clasificado	Asentado	Resultados de la prueba	Eficacia operativa (Sí/No)	Notas
	Principal: Recepción																					
	Sub: Procesamiento de recepción de bienes																					
	Actividad: Crear																					
C7	Los controles proporcionan aseguramiento razonable respecto de que las recepciones de bienes sean procesadas por personal autorizado de manera completa, precisa y oportuna.	Asociar una recepción de bienes con una orden de compra incorrecta o una partida incorrecta podría generar una valorización inadecuada del inventario y de la cuenta de mercaderías recibidas - no facturadas causando demoras en el proceso de facturación y pago.	H	La cuenta de mercaderías recibidas - no facturadas se concilia mensualmente.			X	X	X		M	D	Mensualmente	X	X	X		X	X			
C8	Los controles proporcionan aseguramiento razonable respecto de que las recepciones de bienes sean procesadas por personal autorizado de manera completa, precisa y oportuna.	Las recepciones de bienes no se registran correctamente.	M	Los informes de órdenes de compra no coincidentes se revisan mensualmente.			X	X	X		M	D	Mensualmente	X	X		X	X				
	Principal: Cuentas a pagar																					
	Sub: Procesamiento de factura																					
	Actividad: Crear																					
C9	Los controles proporcionan aseguramiento razonable respecto de que las facturas de proveedores sean creadas por personal autorizado de manera completa, precisa y oportuna.	Una factura, que se debería pagar por su correspondencia con la orden de compra, se paga sin una referencia a la orden de compra; lo que podría generar un pago aceptable de materiales o servicios (es decir, variaciones de precio inaceptables y desfavorables).	M	Gracias a la seguridad de aplicaciones, el acceso a transacciones de ingreso de facturas sin órdenes de compra está restringido todo lo posible.			X				A	P	Siempre	X	X	X		X	X			
C10	Los controles proporcionan aseguramiento razonable respecto de que las facturas de proveedores sean creadas por personal autorizado de manera completa, precisa y oportuna.	Se ingresan montos de factura incorrectos; lo que genera pagos incorrectos a proveedores.	H	Las verificaciones se comparan con los documentos de respaldo (factura, cheque, solicitudes o reembolsos de gastos) en función de un umbral monetario.			X	X			M	P	Según se requiera	X	X	X			X			
C11	Los controles proporcionan aseguramiento razonable respecto de que las facturas de proveedores sean creadas por personal autorizado de manera completa, precisa y oportuna.	Los asientos del libro auxiliar de facturas de cuentas a pagar no se pasan al libro mayor.	L	El total del libro auxiliar de cuentas a pagar se compara con el saldo de libro mayor a fin de mes mediante un informe de antigüedad. Se corrigen las diferencias			X	X	X		M	D	Mensualmente	X	X	X			X			

Lista de siglas utilizadas en el gráfico:
Componentes de COSO
1. EC: entorno de control
2. ER: evaluación de riesgos
3. AC: actividades de control
4. I/C: información y comunicación
5. S: supervisión

Atributos de control
6. C: control clave
7. Man/Aut: manual o automático
8. Pre/Det: prevenir o detectar

Figura 6 (continuación).

Matriz de riesgo y control: Compras a pagar

	PROCESO DE NEGOCIO Y OBJETIVOS DE CONTROL	RIESGOS		ACTIVIDADES DE CONTROL	COMPONENTES DE COSO					ATRIBUTOS DE CONTROL				CLASIFICACIÓN DE CONTROL						PRUEBA		
Número	Objetivos de control	Riesgos	Impacto/ Probabilidad	Actividades de control	EC	ER	AC	I/C	S	C(Sí/No)	Man/Auto	Pre/Det	Frecuencia	Verdadero	Registrado	Valorado	Oportuno	Clasificado	Asentado	Resultados de la prueba	Eficacia operativa (Sí/No)	Notas
	Principal: Cuentas a pagar																					
	Sub: Procesar pagos																					
	Actividad: Crear																					
C12	Los controles proporcionan aseguramiento razonable respecto de que los pagos a proveedores sean procesados por personal autorizado de manera completa, precisa y oportuna.	Los desembolsos registrados difieren de los montos pagados.	L	La aplicación de cuentas a pagar genera automáticamente cheques o pagos electrónicos basados en el valor de las facturas aprobadas de acuerdo a las condiciones del sistema y de pagos a proveedores.			X				A	P	Siempre	X	X	X	X	X	X			
C13	Los controles proporcionan aseguramiento razonable respecto de que los pagos a proveedores sean procesados por personal autorizado de manera completa, precisa y oportuna.	Los desembolsos realizados no se registran.	H	El acceso está restringido al personal autorizado a emitir cheques.			X				A	P	Siempre	X	X	X			X			
C14	Los controles proporcionan aseguramiento razonable respecto de que los pagos a proveedores sean procesados por personal autorizado de manera completa, precisa y oportuna.	Se registran desembolsos ficticios.	M	La aplicación de cuentas a pagar realiza una coincidencia de tres vías entre la partida de la orden de compra, el receptor y la factura al procesar las facturas de cuentas a pagar.			X	X			A	P	Siempre		X			X	X			

Lista de siglas utilizadas en el gráfico:
Componentes de COSO
1. EC: entorno de control
2. ER: evaluación de riesgos
3. AC: actividades de control
4. I/C: información y comunicación
5. S: supervisión

Atributos de control
6. C: control clave
7. Man/Aut: manual o automático
8. Pre/Det: prevenir o detectar

Figura 6 (continuación).

Apéndice A: Controles de aplicación comunes y pruebas sugeridas

A continuación se describen los controles de aplicación más comunes y las pruebas sugeridas para cada control. La tabla fue suministrada por el Grupo AXA.[17]

Controles de ingreso de datos

Estos controles están diseñados para proporcionar aseguramiento razonable respecto de que los datos recibidos para el procesamiento por computadora estén adecuadamente autorizados y convertidos a un formato aceptable y que los datos no se hayan perdido, suprimido, agregado, duplicado ni modificado inadecuadamente. Los controles de ingreso de datos computarizados incluyen verificaciones de datos y procedimientos de validación, como dígitos verificadores, recuentos de registros, totales de control y totales financieros de lotes, mientras que las rutinas de edición computarizadas, que están diseñadas para detectar errores de datos, incluyen pruebas de caracteres válidos, pruebas de datos faltantes, pruebas de secuencias y pruebas de límites o razonabilidad. En la siguiente tabla se identifican los controles de ingreso de datos y las pruebas sugeridas.

Controles de ingreso de datos y acceso

Estos controles garantizan que todos los datos de transacción de ingreso sean precisos, completos y autorizados.

Dominio	Control	Pruebas posibles
Verificaciones y validación de datos	• Verificaciones de razonabilidad y límites en los valores financieros. • Verificaciones de formato y de campos obligatorios; pantallas de ingreso de datos estandarizada. • Verificaciones de secuencias (por ejemplo, artículos faltantes), verificaciones de rangos y dígitos verificadores. • Verificaciones cruzadas (por ejemplo, ciertas políticas sólo son válidas con ciertos códigos de tablas superiores). • Validaciones (por ejemplo, la tabla almacenada y el menú desplegable de artículos válidos).	• Realizar una prueba de muestra de cada situación. • Observar los intentos de ingreso de datos incorrectos. • Determinar quién puede eludir controles. • Si se rige por una tabla, determinar quién puede cambiar las ediciones y los niveles de tolerancia.
Autorización, aprobación y capacidad de eludir automatizadas	• Los derechos de autorización y aprobación (por ejemplo, de gastos o pagos o crédito de reclamos sobre un umbral determinado) son asignados a usuarios en función de sus roles y su necesidad de utilizar la aplicación. • La capacidad de eludir (por ejemplo, eludir la aprobación de reclamos extraordinariamente grandes) está restringida según el rol del usuario y la necesidad de la dirección de utilizar la aplicación.	• Realizar pruebas basadas en los derechos de acceso de los usuarios. • Probar los privilegios de acceso para cada función o transacción confidencial. • Revisar los derechos de acceso que definen y enmiendan límites de autorización y aprobación configurables.
Separación de responsabilidades automatizada y derechos de acceso	• Las personas que configuran proveedores aprobados no pueden iniciar transacciones de compra. • Las personas que tienen acceso al procesamiento de reclamos no pueden configurar ni enmendar una política.	• Realizar pruebas basadas en los derechos de acceso de los usuarios. • Revisar los derechos de acceso que definen y enmiendan roles y estructuras de menú configurables.
Artículos pendientes	• Los informes de antigüedad que muestran nuevos elementos de política con un procesamiento incompleto son revisados por los supervisores diariamente o semanalmente. • Los archivos pendientes en los que no hay información suficiente disponible para procesar transacciones.	• Revisar los resultados de antigüedad y la evidencia de los procedimientos de revisión del supervisor. • Revisar una muestra de artículos del informe de antigüedad o de un archivo pendiente.

Controles de transmisión de datos y archivos

Estos controles garantizan que los archivos y las transacciones internos y externos transmitidos electrónicamente se reciban desde una fuente identificada y se procesen de manera completa y precisa.

Dominio	Control	Pruebas posibles
Controles de transmisión de archivos	• Verificaciones de la integridad y validez del contenido, incluidos la hora y la fecha, el tamaño de los datos, el volumen de los registros y la autenticación de la fuente.	• Observar informes de transmisiones e informes de errores. • Observar la validez e integridad de los parámetros y configuraciones. • Revisar el acceso para definir y enmendar parámetros configurables en transferencias de archivos.
Controles de transmisión de datos	• Solicitud de controles de ingreso de datos seleccionados para validar los datos recibidos (por ejemplo, campos clave, razonabilidad, etc.).	• Probar muestras de cada situación. • Observar los intentos de ingreso de datos incorrectos. • Determinar quién puede eludir controles. • Si se rige por una tabla, determinar quién puede cambiar las ediciones y los niveles de tolerancia.

17 Extraído de *Common Application Controls and Suggested Testing* del Grupo AXA.

Controles de procesamiento

Estos controles están diseñados para proporcionar aseguramiento razonable respecto de que el procesamiento de datos se haya realizado de la forma prevista sin ninguna omisión ni recuento duplicado. Muchos controles de procesamiento son iguales a los controles de ingreso de datos, en especial para los sistemas de procesamiento en línea o en tiempo real, pero se utilizan durante las fases de procesamiento. Estos controles incluyen totales de pasada en pasada, informes de totales de control y controles de archivos y operadores, como etiquetas externas e internas, registros de operaciones informáticas del sistema y pruebas de límites o razonabilidad.

Controles de procesamiento
Estos controles garantizan que los datos de ingreso válidos se hayan procesado de manera completa y precisa.

Dominio	Control	Pruebas posibles
Identificación y validación de archivos automatizadas	• Los archivos para procesamiento están disponibles y completos.	• Revisar el proceso de validación y ejecución de pruebas.
Funcionalidad y cálculos automatizados	• Los cálculos específicos realizados en uno o más ingresos de datos y elementos de datos almacenados generan más elementos de datos. • Uso de tablas de datos existentes (por ejemplo, archivos maestro o datos de posición como tablas de calificaciones).	• Comparar valores de ingreso y de salida para todas las situaciones mediante una revisión y una reejecución. • Revisar los controles de mantenimiento de tablas y determinar quién puede cambiar las ediciones y los niveles de tolerancia.
Pistas de auditoría y elusiones	• Rastreo automatizado de cambios de los datos, asociando el cambio con un usuario específico. • Rastreo y resaltado automatizados de elusiones a procesos normales.	• Revisar los informes y la evidencia de las revisiones. • Revisar el acceso para eludir procesos normales.
Extracción de datos, filtrado y generación de informes	• Las salidas de rutinas de extracción se evalúan para verificar su razonabilidad e integridad. • Asignación de transacciones automatizada (por ejemplo, con fines de reaseguramiento, procesos actuariales adicionales o asignación de fondos). • Evaluación de datos utilizados para realizar estimaciones con el fin de generar informes financieros.	• Revisar el diseño de la rutina de extracción respecto de los archivos de datos utilizados. • Revisar la evaluación de supervisión de la salida desde la rutina de extracción para obtener evidencia de la revisión y los desafíos normales. • Revisar la muestra de asignaciones para verificar su idoneidad. • Revisar el proceso de evaluación de datos extraídos para verificar su integridad y validez.
Balanceo de interfaz	• Verificación automatizada de los datos recibidos desde los sistemas alimentadores (por ejemplo, nómina de salarios, datos de reclamos, etc.) en los almacenes de datos o sistemas de libro mayor. • Verificación automatizada respecto de la coincidencia de los saldos en ambos sistemas. Si no coinciden, se debe generar y utilizar un informe de excepción.	• Inspeccionar los informes de errores de interfaz. • Inspeccionar la validez e integridad de los parámetros y configuraciones. • Revisar el acceso para definir y enmendar parámetros configurables en las interfaces. • Inspeccionar la evidencia de informes, verificaciones y procesamiento de archivos de errores coincidentes.
Funcionalidad y antigüedad automatizadas	• Extracciones de archivos del listado de deudores para proporcionarle a la dirección los datos sobre transacciones vencidas.	• Probar una muestra de las transacciones enumeradas para validar la idoneidad del procesamiento de antigüedad.
Verificaciones duplicadas	• Comparación de transacciones individuales con transacciones previamente registradas para cotejar campos. • Comparación de archivos individuales con fechas, horas, tamaños esperados, etc.	• Revisar el acceso para definir y enmendar parámetros configurables en transferencias o archivos duplicados. • Revisar el proceso para el manejo de archivos o transacciones rechazados.

Controles de salida

Estos controles están diseñados para proporcionar aseguramiento razonable respecto de que los resultados de procesamiento sean precisos y distribuidos únicamente al personal autorizado. Los totales de control generados como salida durante el procesamiento se deben comparar y conciliar con los totales de control de ingreso de datos y de pasada en pasada, generados durante el procesamiento. Los informes de cambios generados por el sistema para los archivos maestro se deben comparar con los documentos fuente para garantizar que la información sea correcta.

Controles de salida

Estos controles garantizan que la salida sea completa y precisa y se distribuya correctamente.

Dominio	Control	Pruebas posibles
Pases al libro mayor	• Todas las transacciones individuales y resumidas asentadas en el libro mayor.	• Muestra de resumen de transacciones del libro auxiliar y de ingreso rastreadas en el libro mayor.
Pases al libro auxiliar	• Todas las transacciones exitosas asentadas en el libro auxiliar.	• Muestra de transacciones de ingreso rastreadas en el libro auxiliar.

Controles de datos de posición y archivos maestro

Estos controles garantizan la integridad y la idoneidad de los archivos maestro y los datos de posición.

Dominio	Control	Pruebas posibles
Autorización de actualización	• Acceder para actualizar los derechos asignados a usuarios de rango superior en función de sus roles y de la necesidad de utilizar la aplicación.	• Revisar el acceso para definir y enmendar archivos maestro y datos de posición.

Apéndice B: Ejemplo de un programa de auditoría

Los auditores internos deben desarrollar y registrar un plan para cada trabajo de auditoría, incluidos los objetivos, el alcance, las consideraciones de recursos y el plan de trabajo de auditoría. Los objetivos le permiten al auditor determinar si los controles de aplicación están diseñados correctamente y funcionan con eficacia para gestionar riesgos financieros, operativos y de cumplimiento de regulaciones. Los objetivos de los controles de aplicación incluyen lo siguiente, tal como se describió en la página 2 de esta guía:

- Los datos de ingreso son precisos, completos, autorizados y correctos.
- Los datos se procesan según lo planeado en un período aceptable.
- Los datos almacenados son precisos y completos.
- Las salidas son precisas y completas.
- Se mantiene un registro que rastrea el proceso de ingreso, almacenamiento y salida de datos.

A continuación se enumeran los pasos necesarios para lograr los objetivos mencionados:

- Paso 1. Realizar una evaluación de riesgos (consulte la página 7 de esta guía).
- Paso 2. Determinar el alcance de la revisión (consulte la página 9 de esta guía).
- Paso 3. Desarrollar y comunicar el plan de revisión detallado (consulte la página 10 de esta guía).
- Paso 4. Determinar la necesidad de recursos especializados (consulte la página 10 de esta guía).
- Paso 5. Determinar si se requerirán técnicas de auditoría asistidas por computadora (consulte la página 13 de esta guía).
- Paso 6. Realizar la auditoría (consulte el siguiente ejemplo de un programa de auditoría). Tenga en cuenta que este ejemplo de programa no pretende abarcar todas las pruebas aplicables a su organización.

Ejemplo de un programa de auditoría

Una revisión de los datos específicos de la compañía y del alcance de la auditoría determinará los pasos de prueba detallados relacionados con las siguientes actividades de revisión.

Objetivo del control	Controles	Actividades de revisión
Objetivo 1: Los datos de ingreso son precisos, completos, autorizados y correctos.		
	Los controles de ingreso de datos están diseñados y funcionan con eficacia para garantizar que todas las transacciones se hayan autorizado y aprobado antes de la entrada de datos.	Obtener los procedimientos de ingreso de datos, comprender el proceso de autorización y aprobación y determinar si existe un proceso de revisión y aprobación y si se ha comunicado a los usuarios responsables de obtener las aprobaciones correspondientes. Verificar que el responsable de la aplicación o del proceso garantice que todos los datos están autorizados antes del ingreso. Esto puede hacerse mediante el otorgamiento de roles y responsabilidades en función de los puestos de trabajo. Obtener una copia de los niveles de aprobación y determinar si se ha asignado la responsabilidad de verificar que las aprobaciones adecuadas se apliquen coherentemente.

Ejemplo de un programa auditoría

Objetivo del control	Controles	Actividades de revisión
	Los controles de ingreso de datos están diseñados y funcionan correctamente para garantizar que todas las transacciones ingresadas se procesarán de manera correcta y completa.	Obtener los procedimientos de ingreso de datos y verificar que las personas responsables de ingresar los datos se hayan capacitado en la preparación, entrada y control de ingreso de datos. Determinar si las rutinas de edición están incorporadas en la aplicación que verifica y rechaza posteriormente la información de ingreso que no coincide con ciertos criterios, incluidos, entre otros, fechas incorrectas, caracteres incorrectos, longitud de campo no válida, datos faltantes y entradas y números de transacción duplicados. Verificar la existencia y el funcionamiento de controles de ingreso de datos manuales para evitar la entrada de registros duplicados. Los controles de ingreso de datos manuales pueden incluir la numeración previa de documentos originales y la marcación de registros como "ingreso" luego de la entrada. Verificar que los datos agregados provengan de una fuente aceptable y se concilien con la fuente utilizando totales de control, recuentos de registros y otras técnicas, incluido el uso de informes de fuentes independientes. Determinar si existe una separación de responsabilidades adecuada para evitar que los usuarios ingresen y autoricen transacciones. Verificar que exista una separación de responsabilidades entre el personal de ingreso de datos y aquellos responsables de conciliar y verificar que la salida sea precisa y completa. Verificar que existan controles para evitar cambios no autorizados en los programas del sistema, como cálculos y tablas.
	Los controles de ingreso de datos están diseñados y funcionan correctamente para garantizar que todas las transacciones rechazadas se hayan identificado y reprocesado de manera correcta y completa.	Obtener los procedimientos de ingreso de datos para el manejo de transacciones rechazadas y corrección de errores subsiguiente, y determinar si el personal responsable de la corrección de errores y del reingreso de datos se ha capacitado adecuadamente. Verificar que exista un mecanismo para notificar al responsable del proceso cuando se han rechazado transacciones o se han corregido errores. Verificar que los elementos rechazados se reprocesen adecuadamente de manera oportuna y conforme a los procedimientos, y que los errores se corrijan antes del reingreso en el sistema.

Ejemplo de un programa de auditoría

Objetivo del control	Controles	Actividades de revisión
	Los controles están diseñados y funcionan correctamente para garantizar que los datos asentados automáticamente desde otro sistema se procesen de manera precisa y completa.	Obtener los procedimientos y verificar que se incluya información detallada sobre cómo se autorizan las interfaces automatizadas y qué activa el evento de procesamiento automatizado. Verificar que se documenten los programas de procesamiento y que se identifiquen y corrijan los problemas de manera oportuna. Determinar si los recuentos de registros de sistema a sistema y los valores monetarios totales se verifican sistemáticamente para las interfaces automatizadas y si los elementos rechazados no se pueden asentar y se marcan para seguimiento y reejecución. Verificar que los archivos y los datos que se crearon para ser utilizados por otras aplicaciones o que se transfirieron de otras aplicaciones estén protegidos contra modificaciones no autorizadas durante todo el proceso de transferencia.
	Los controles están diseñados y funcionan correctamente para garantizar que se utilicen archivos de datos y bases de datos correctos en el procesamiento.	Validar que los datos y programas de prueba estén separados de la producción.
Objetivo 2: Los datos se procesan según lo planeado en un período aceptable.		
	Los controles de procesamiento están diseñados y funcionan correctamente para garantizar que todas las transacciones se procesen de manera oportuna y dentro del período contable correcto.	Verificar que la salida se revise o se concilie con los documentos originales para comprobar la integridad e idoneidad, incluyendo una verificación de los totales de control. Determinar si las rutinas están incorporadas en la aplicación para garantizar que todas las transacciones ingresadas correctamente se procesen y se asienten según lo planeado en el período contable correcto.
	Los controles de procesamiento están diseñados y funcionan correctamente para garantizar que todas las transacciones rechazadas se hayan identificado y reprocesado de manera oportuna.	Obtener los procedimientos para el manejo de transacciones rechazadas y corrección de errores subsiguiente, y determinar si el personal responsable de la corrección de errores y del reingreso de datos se ha capacitado adecuadamente. Verificar que exista un mecanismo para notificar al responsable del proceso cuando se han rechazado transacciones o se han corregido errores. Verificar que los elementos rechazados se procesen adecuadamente de manera oportuna y conforme a los procedimientos, y que los errores se corrijan antes del reingreso en el sistema.

Ejemplo de un programa de auditoría

Objetivo del control	Controles	Actividades de revisión
Objetivo 3: Los datos almacenados son precisos y completos.		
	Los controles de acceso lógico están diseñados y funcionan correctamente para evitar el acceso, la modificación o la divulgación no autorizados de los datos del sistema.	Obtener las políticas de configuración y uso de contraseñas y determinar si están presentes los requisitos para contraseñas sólidas, restablecimiento de contraseñas, bloqueo de cuentas y reutilización de contraseñas. Verificar que la política anterior se haya aplicado en las aplicaciones bajo revisión. Verificar que los controles de acceso remoto estén diseñados y funcionen correctamente. Verificar que los usuarios estén restringidos a funciones específicas según las responsabilidades laborales (acceso basado en roles). Verificar que las ID de usuario estén asignadas a todos los usuarios, incluidos los usuarios privilegiados y que las cuentas administrativas y de usuario no se compartan. Verificar que se obtenga una aprobación adecuada de la creación y modificación de cuentas de usuario antes de otorgar o cambiar el acceso. (Los usuarios son, por ejemplo, los usuarios privilegiados, los empleados, los contratistas, los proveedores y el personal temporal). Verificar que el acceso se elimine inmediatamente al finalizar. Verificar que la persona a cargo de la aplicación sea responsable de garantizar que se realice una revisión semestral de las cuentas de usuario y del sistema con el fin de garantizar que el acceso a datos financieros, aplicaciones y sistemas operativos críticos sea correcto y esté actualizado.
	Los controles están diseñados y funcionan correctamente para garantizar que las copias de seguridad de datos sean precisas y completas y se realicen de manera oportuna.	Verificar que se obtenga una aprobación adecuada de la creación y modificación de cuentas de usuario antes de otorgar o cambiar el acceso. (Los usuarios son, por ejemplo, los usuarios privilegiados, los empleados, los contratistas, los proveedores y el personal temporal). Verificar que el acceso se elimine inmediatamente al finalizar. Verificar que la persona a cargo de la aplicación sea responsable de garantizar que se realice una revisión semestral de las cuentas de usuario y del sistema con el fin de garantizar que el acceso a datos financieros, aplicaciones y sistemas operativos críticos sea correcto y esté actualizado.
	Los controles están diseñados y funcionan correctamente para garantizar que los datos se almacenen físicamente en una ubicación externa segura y con control ambiental.	Verificar que se hayan implementado mecanismos para almacenar datos en una ubicación externa, segura y con control ambiental.

Ejemplo de un programa de auditoría

Objetivo del control	Controles	Actividades de revisión
Objetivo 4: Las salidas son precisas y completas.		
	Los controles de salida están diseñados y funcionan correctamente para garantizar que todas las salidas de transacciones sean completas y precisas.	Obtener los procedimientos de salida de datos, comprender el proceso de revisión y verificar que las personas responsables de la entrada de datos se hayan capacitado en la revisión y verificación de salida de datos. Verificar que la salida se revise o se concilie con los documentos originales para comprobar la integridad e idoneidad, incluyendo una verificación de los totales de control.
	Los controles de salida están diseñados y funcionan correctamente para garantizar que todas las salidas de transacciones se hayan distribuido al personal correspondiente y que la información sensible y confidencial esté protegida durante la distribución.	Revisar los procedimientos de salida de datos existentes y determinar si documentan qué personal recibe la salida de datos y cómo se protegerán durante la distribución.
	Los controles de salida están diseñados y funcionan correctamente para garantizar que un informe de salida se genere en el momento designado y abarque el período designado.	Verificar que se haya creado un informe de salida e identificar que la fecha y hora del informe correspondan a la fecha y hora designadas. Identificar que el informe abarque el período designado a través de una conciliación con los documentos originales de ese período.
Objetivo 5: Se mantiene un registro que rastrea el proceso de ingreso, almacenamiento y salida de datos.		
	Los controles están diseñados y funcionan correctamente para garantizar que se genere y mantenga una pista de auditoría para todos los datos transaccionales.	Verificar que existan registros y pistas de auditoría de procesamiento que garanticen que todos los registros se hayan procesado y que permitan un seguimiento de la transacción desde el ingreso hasta el almacenamiento y la salida. Verificar que existan informes de auditoría que rastreen la identificación y el reprocesamiento de transacciones rechazadas. Los informes deben contener una descripción clara de la transacción rechazada y la fecha y hora identificadas.

Glosario

Controles de aplicación: Los controles de aplicación son específicos de cada aplicación y se relacionan con las transacciones y los datos asociados a cada sistema de aplicación basado en computadora. El objetivo de los controles de aplicación es garantizar la integridad e idoneidad de los registros y la validez de las entradas realizadas como resultado de las actividades de procesamiento programadas. Algunos ejemplos de controles de aplicación son la validación de ingreso de datos, el acuerdo de totales de lotes y la encriptación de datos transmitidos.

Controles de ingreso de datos: Los controles de ingreso de datos garantizan la idoneidad, integridad y oportunidad de los datos en su conversión luego de haber ingresado a una computadora o aplicación. Los datos se pueden ingresar en una aplicación informática a través de un ingreso en línea manual o un procesamiento por lotes automatizado.

Controles de salida de datos: Los controles de salida de datos se utilizan para garantizar la integridad de la información de salida y la distribución correcta y oportuna de las salidas generadas. Las salidas se pueden generar en un formato de copia impresa, como los archivos utilizados para ser ingresados en otros sistemas, o pueden estar disponibles para ser visualizadas en línea.

Controles de procesamiento de datos: Los controles de procesamiento de datos se utilizan para garantizar la idoneidad, integridad y oportunidad de los datos durante un procesamiento por lotes o en tiempo real de la aplicación.

Planificación de recursos empresariales (ERP, en inglés): La ERP hace referencia a la planificación y gestión de recursos en una empresa y al uso de un sistema de software para gestionar todos los procesos de negocio e integrar las compras, los inventarios, el personal, las actividades de servicio al cliente, los envíos, la gestión financiera y otros aspectos del negocio. Por lo general, un sistema de ERP se basa en una base de datos común, módulos de aplicación de procesos de negocio integrados y herramientas de análisis de negocio.[18]

Controles generales de TI (ITGC, en inglés): Estos controles se aplican a todos los componentes, procesos y datos de sistemas para una organización o entorno de TI determinado. El objetivo de los ITGC es garantizar el desarrollo y la implementación adecuados de las aplicaciones y la integridad del programa, los archivos de datos y las operaciones informáticas.

A continuación se enumeran los ITGC más comunes:

- Controles de acceso lógico sobre la infraestructura, las aplicaciones y los datos.
- Controles de ciclo de vida del desarrollo del sistema.
- Controles de gestión de cambio de programa.
- Controles de seguridad física del centro de datos.
- Controles de respaldo y recuperación de datos y sistema.
- Controles de operaciones informáticas.

Riesgo: Posibilidad de que suceda un evento que tendrá un impacto en el logro de los objetivos. El riesgo se mide en términos de impacto y probabilidad.[19]

Separación de funciones: Controles que evitan errores e irregularidades mediante la asignación de responsabilidades a distintas personas para iniciar transacciones, registrar transacciones y supervisar activos. La separación de responsabilidades se utiliza comúnmente en organizaciones que tienen una gran cantidad de empleados para que nadie pueda cometer fraude sin ser detectado.

18 Extraído del Glosario para el Auditor de Sistemas Informáticos Certificado, emitido por ISACA.

19 Extraído del Marco Internacional para la Práctica Profesional del IIA.

Referencias

- GTAG 4: *Gestión de la auditoría de TI*.
- GTAG 1: *Controles de tecnología de la información*.
- ISACA, Guía de auditoría de sistemas de información — Revisión de sistemas de aplicación, Documento G14.
- *Control interno sobre los informes financieros—Guía para empresas públicas más pequeñas* de COSO.
- Norma de Auditoría N.º 5 del PCAOB, "Una auditoría de control interno sobre informes financieros realizada en conjunto con una auditoría de estados contables", párrafos B29-30.
- Norma 1220 del IIA: Cuidado profesional.
- Norma 1210.A3 del IIA.
- Norma 1130.C1 del IIA
- *Common Application Controls and Suggested Testing* del Grupo AXA.
- Glosario del Auditor de Sistemas Informáticos Certificado, emitido por ISACA.
- Marco para la Práctica Profesional del IIA.

Christine Bellino, CPA, CITP
Christine Bellino es director de gestión de riesgos de tecnología para la práctica de Denver de Jefferson Wells y es miembro de la Comisión de Tecnología de Avanzada del IIA. Bellino es miembro del equipo principal de Guía para la Evaluación del Alcance de los Controles Generales de TI en función del riesgo (GAIT, en inglés) de la organización. Sus responsabilidades actuales incluyen la gestión de varios procesos de negocio y las revisiones de los ITGC para organizaciones pequeñas, medianas y grandes.

Bellino tiene más de 25 años de experiencia en gestión de riesgos financieros, de operaciones y de tecnología y fue uno de los presidentes del Equipo de Trabajo de COSO responsable de la reciente publicación *Control interno sobre los informes financieros — Guía para empresas públicas más pequeñas*.

Steve Hunt, CIA, CISA, CBM
Steve Hunt es director de soluciones empresariales para Enterprise Controls Consulting (ECC) y es miembro de la Comisión de Tecnología de Avanzada del IIA, ISACA y la Association of Professionals in Business Management. En ECC, Hunt trabaja con compañías medianas y pequeñas de Fortune 1.000 en distintas industrias, dirigiendo la entrega de trabajos de gestión de riesgos financieros, operativos y de TI.

Hunt tiene más de 20 años de experiencia en diversos sectores e industrias, como por ejemplo, contabilidad, auditoría interna y consultoría de gestión. Más específicamente, ha realizado auditorías detalladas de cumplimiento de la Ley Sarbanes-Oxley y otras auditorías internas y externas y ha participado en proyectos de reingeniería de procesos de negocio e iniciativas de desarrollo de negocios. Además, tiene varios años de experiencia en la configuración de aplicaciones SAP R/3 y controles de procesos de negocio y seguridad de aplicaciones y ha brindado destacadas conferencias en varias universidades y organizaciones de Estados Unidos.

Revisores
El IIA agradece a las siguientes personas y organizaciones que brindaron valiosos comentarios y agregaron gran valor a esta guía:

- Grupo de especialización en auditoría de IT, IAI – Noruega.
- Comités técnicos del IAI–Reino Unido e Irlanda.
- Helge Aam, Deloitte – Noruega.
- Ken Askelson, JCPenney Co. Inc. – Estados Unidos.
- Rune Berggren, IBM – Noruega.
- Shirley Bernal, AXA Equitable Life Insurance Co. – Estados Unidos.
- Lily Bi, The IIA.
- Claude Cargou, AXA – Francia.
- Maria Castellanos, AXA Equitable Life Insurance Co. – Estados Unidos.
- Nelson Gibbs, Deloitte & Touche, LLP.
- Steven Markus, AXA Equitable Life Insurance Co. – Estados Unidos.
- Peter B. Millar, ACL Services Ltd. – Canadá.
- Stig J. Sunde, OAG – Noruega.
- Jay R. Taylor, General Motors Corp. – Estados Unidos.
- Karine Wegrzynowicz, Lafarge North America.
- Hajime Yoshitake, Nihon Unisys, Ltd. – Japón.
- Jim Zemaites, AXA Equitable Life Insurance Co. – Estados Unidos.
- Joe Zhou, GM Audit Services – China.

GTAG®

Auditar controles de aplicación

Los controles de aplicación son aquellos controles que corresponden al alcance de los procesos de negocio o sistemas de aplicaciones individuales, como las ediciones de datos, la separación de funciones de negocio, el balanceo o equilibrio de los totales de procesamiento, el registro de transacciones y la generación de informes de errores. Los controles de aplicación eficaces ayudarán a su organización a garantizar la unidad, idoneidad, confidencialidad e integridad de los datos y sistemas. Esta guía les proporciona a los directores ejecutivos de auditoría (DEA) información sobre el control de aplicación, su relación con los controles generales, la determinación del alcance de una revisión del control de aplicación basada en riesgos, los pasos para realizar una revisión del control de aplicación, una lista de los controles de aplicación clave y un ejemplo de plan de auditoría.

Visite www.theiia.org/guidance/technology/gtag/gtag8 para calificar esta GTAG o enviar comentarios.

¿Qué es GTAG?

Las Guías de Auditoría de Tecnología Global (GTAG) preparadas por el IIA están escrita en un lenguaje directo de negocio para abordar en forma oportuna problemas relacionados con la gestión, el control y la seguridad de la tecnología de la información. La colección GTAG es un recurso disponible para los DEA sobre los distintos riesgos asociados a la tecnología y las prácticas recomendadas.

Guía 1: *Controles de tecnología de la información*

Guía 2: *Controles de gestión de parches y cambios: críticos para el éxito de la organización*

Guía 3: *Auditoría continua: Implicancias para el aseguramiento, la supervisión y la evaluación de riesgos*

Guía 4: *Gestión de auditoría de tecnología de información*

Guía 5: *Gestión y auditoría de riesgos de privacidad*

Guía 6: *Gestión y auditoría de puntos vulnerables de tecnología de la información*

Guía 7: *Tercerización de la tecnología de la información*

Visite la sección de tecnología del sitio Web del IIA en www.theia.org/technology para descargar toda la colección.

ISBN 978-0-89413-613-9

The Institute of Internal Auditors

www.theiia.org