Davis A. Porras Rodríguez, CISA, CISM, es un docente de la Facultad de Ingeniería de la Universidad Americana (Managua, Nicaragua) y el oficial de riesgos y seguridad de la información de Accedo Technologies, una empresa de externalización de servicios BPO/ITO en Nicaragua. En los últimos cinco años, fue el auditor de SI de una empresa privada del sector financiero de Nicaragua.

Auditorías Integradas—Un Modelo Práctico

Una auditoría integrada es el proceso en el cual se combinan las disciplinas de auditoría (operaciones, financiera, legal, TI, otros) para evaluar los riesgos y controles claves de un proceso de negocio, producto o servicio organizacional. Este concepto de auditoría integrada emerge y cambia radicalmente la forma en que son consideradas las auditorías internas por las diferentes partes interesadas. Aunque pueden existir otras definiciones de auditoría integrada, lo más importante es garantizar que el enfoque integrado se concentre en el riesgo, abarcando de esta manera riesgos operacionales, tecnológicos, financieros, regulatorios, cumplimiento, de imagen/reputación, fraude, entre otros. El presente artículo describe un modelo de auditoría integrada basado en mejores prácticas y normas como la ISO/IEC 27005:2008 y COSO.

UN MODELO PRÁCTICO

De acuerdo con la guía práctica del IIA, se presenta un modelo práctico de auditoria integrada que incluye las actividades descritas en la **figura 1**. Algunas actividades se pueden incluir en modelos aislados para conducir auditorías tradicionales (operativa, cumplimiento, TI, otros), por ejemplo, la evaluación del diagnóstico de control interno y gestión de riesgos basados en los dominios de COSO. Otras actividades como el análisis de estrategias y evaluación de riesgos contra los criterios de impacto y aceptación, posiblemente no apliquen por el contexto y madurez de la organización. Sin embargo, el modelo representa un conjunto de pasos razonables para conducir una auditoria integrada a los procesos de negocio, servicios o productos de una organización.

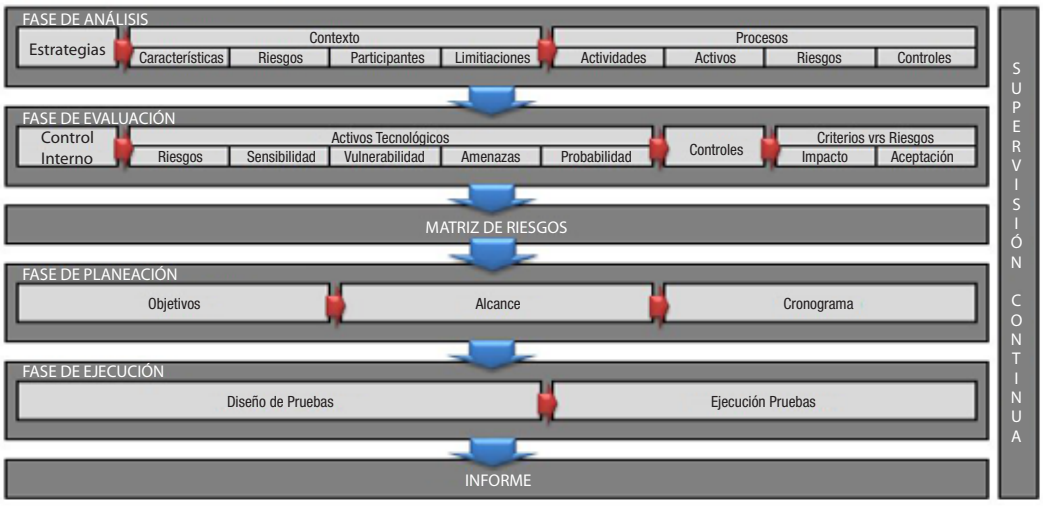
FASE DE ANÁLISIS

El equipo de auditores comienza analizando el entorno de la organización y se enfoca en conocer las estrategias, contexto y proceso del servicio, producto o proceso de negocio que se está auditando.

Estrategias

Es necesario que los auditores conozcan en que estrategias organizacionales se enfoca el negocio y qué tipo de acciones se consideran para desarrollarlas. Esta información permite al equipo de auditores valorar si la administración del proceso, servicio o producto está alineada a las estrategias del negocio. Por ejemplo, hay organizaciones que tienen como estrategia crecer continuamente, por lo que, el equipo de auditores

Figura 1—Modelo Práctico de Auditoría Integrada



tiene que identificar cuáles son los planes que desarrollan los responsables del proceso, servicio o producto para contribuir con esta estrategia.

Contexto

El equipo de auditores tiene que investigar todas las características del proceso, servicio o producto sujeto a evaluación, esto incluye pero no se limita a los siguientes aspectos: una descripción sobre el diseño y operación del proceso, servicio o producto, área responsable, importancia (crítico, sensible, vital—tomando de referencia el tiempo de recuperación [RTO por sus siglas en inglés] definido), canales que se utilizan para ofrecer los servicios o productos de una organización, por ejemplo, banca electrónica, cajeros automáticos, comercios afiliados, centros de atención al cliente, sucursales físicas, segmento de mercado, volúmenes de venta, leyes, regulaciones, reglamentos, políticas y áreas que intervienen en el proceso, servicio o producto.

Es importante que el equipo de auditores conozca los eventos de riesgos que han ocurrido y afectado el proceso, servicio o producto sujeto a evaluación. Una descripción breve del evento de riesgo se necesita documentar, al igual que la cantidad de eventos ocurridos en los últimos dos años, la causa que originó el evento y el impacto (financiero, regulatorio, de reputación, otros) del evento de riesgo. Dependiendo del tipo de evento de riesgo, el auditor analiza las acciones realizadas por la administración y determina si el riesgo fue mitigado o administrado. Los eventos de riesgo materializados se pueden encontrar en bitácoras de incidentes, registro de quejas y/o sugerencias, solicitudes de cambio a los sistemas o por medio de entrevistas con los involucrados en el proceso, servicio o producto para los casos en que los eventos ocurridos no se encuentran documentados.

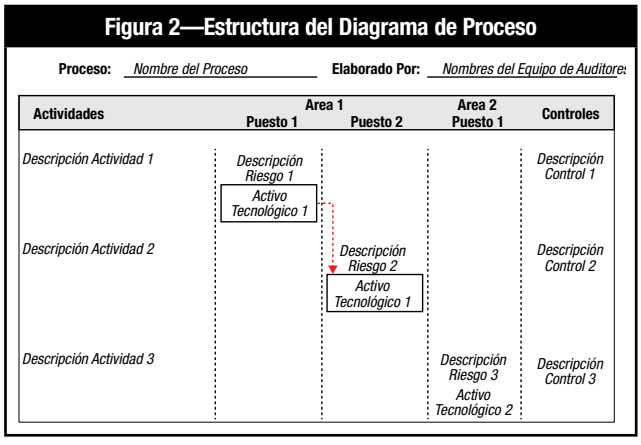
De las áreas que intervienen en el proceso, servicio o producto auditado, el equipo de auditores tiene que entender su misión y visión, su organigrama detallado para identificar los empleados claves y las estrategias que desarrollan. En esta parte, el equipo de auditores realiza un cruce entre las acciones estratégicas de las áreas con las definidas por la alta gerencia y evalúa el alineamiento entre las mismas, por ejemplo, si una organización prioriza entre sus estrategias la reducción de costos operativos, el auditor analiza la existencia de planes de acción en donde el proceso, producto o servicio que se está auditando apoya la estrategia organizacional.

Por último, para llegar a establecer el contexto del proceso, servicio o producto, es necesario que el equipo de auditores conozca las restricciones que limitan la operación del proceso, servicio o producto, por lo que, realizan un inventario de las leyes y normas regulatorias, lineamientos y políticas internas/externas aplicables al proceso, servicio o producto. En este inventario se puede incluir una clasificación del tipo de limitación (política interna, ley, norma regulatoria, otras), a qué tipo de sanción estaría expuesta la organización y cuál será el impacto por un incumplimiento.

Diagrama de Proceso

Para analizar riesgos, es necesario conocer las actividades del proceso sujeto a evaluación, por lo que, el equipo de auditores tiene la tarea de documentarlo. Existen diferentes maneras para documentar un proceso, sin embargo, se recomienda la estructura que se muestra en la **figura 2**.

Figura 2—Estructura del Diagrama de Proceso



En el recorrido del proceso se conocen los puestos de trabajo, riesgos, controles y activos tecnológicos involucrados. Algunos beneficios de documentar el proceso conforme la estructura de la **figura 2**, es que permite a los auditores:

- Reconocer puestos claves e identificar concentración de funciones y riesgos.
- Identificar alta dependencia de los activos tecnológicos.
- Conocer los controles de los riesgos identificados.
- Conocer el flujo que siguen los datos y/o activos tecnológicos.

Los entregables de la fase de análisis son pero no se limitan a un listado de las acciones que se llevan a cabo para contribuir a las metas estratégicas (riesgos estratégicos), las restricciones legales, regulatorias o internas (riesgos legales y de cumplimiento),

las actividades del proceso (riesgos operacionales), los riesgos materializados, los activos tecnológicos que soportan las actividades del proceso y los "riesgos y controles" que el equipo de auditores detecta en la operatividad.

FASE DE EVALUACIÓN

En esta fase se realiza una evaluación del control interno y gestión de riesgos, activos tecnológicos, controles y criterios (de impacto y aceptación) vs. riesgos identificados.

Diagnóstico de Control Interno y Gestión de Riesgos

El diagnóstico sobre el control interno y la gestión de riesgos se basa en los ocho componentes de COSO ERM. Se recomienda que este diagnóstico sea aplicable obligatoriamente al menos a la unidad funcional encargada del proceso, servicio o producto auditado. En la **figura 3**, se aprecia un ejemplo breve de cómo evaluar el componente "Establecimiento de Objetivos".

Activos Tecnológicos

El auditor de TI es quien determina los riesgos a los que está expuesto el activo tecnológico que soporta las diferentes actividades del proceso y los evalúa tomando en consideración su sensibilidad, vulnerabilidad, amenazas y probabilidad de ocurrencia del evento descrito en la amenaza. En la **figura 4** se muestra una estructura de evaluación práctica para los activos tecnológicos.

La evaluación de la sensibilidad puede llevarse a cabo de la siguiente manera:

- Valor=1: El riesgo puede resultar en poca o nula pérdida o daño.

Figura 3—Ejemplo de Evaluación del Componente COSO "Establecimiento de Objetivos"

Insumos Para la Evaluación	Aspectos Claves Para la Evaluación	Sí	No	Observaciones
• Balanced scorecard • Plan estratégico de la unidad	Objetivos generales de la unidad claramente definidos y alineados con los objetivos estratégicos de la organización	✔		Los objetivos son comunicados a cierto nivel; lo conocen solo el gerente y los jefes de área; coordinadores, supervisores y operadores no lo conocen. A lo interno, no hay un seguimiento periódico sobre el cumplimiento de los objetivos, solo se hace al momento de la evaluación al desempeño.
	Objetivos especificos de los procesos claramente definidos y alineados con los objetivos generales	✔		
	Objetivos comunicados a todo el personal		X	
	Plan estratégico de la unidad apoya a los objetivos de la organización	✔		
	Se evalúan los objetivos periódicamente		X	

Figura 4—Estructura de Evaluación Activos Tecnológicos

	Amenazas		Sensibilidad			Vulnerabilidad		Amenazas		
Vunerabilidades	Agente	Evento	Confidencialidad	Integridad	Disponibilidad	Severidad	Exposición	Capacidad	Motivación	Probabilidad
Descripción de la debilidad **Ej: Almacenamiento Desprotegido**	*?Quién se aprovecha de la debilidad?* **Ej: Empleado y Visitanes**	*Descripción de lo que cause daño* **Ej: Robo**	2	2	4	2	1	2	1	2

- **Valor=2:** El riesgo puede resultar en pérdida o daño menor.
- **Valor=3:** El riesgo puede resultar en pérdida o daño serio y los procesos del negocio pueden verse afectados negativamente.
- **Valor=4:** El riesgo puede resultar en una pérdida o daño serio y los procesos de negocio pueden fallar o interrumpirse.
- **Valor=5:** El riesgo puede resultar en altas perdidas de dinero o en un daño critico a un individuo o el bienestar, reputación, privacidad y o competitividad de la empresa. Los procesos del negocio fallaran.

La vulnerabilidad se evalúa en base a su severidad y exposición, podría valorarse así:

- **Severidad Menor, Valor=1:** Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad tiene poco potencial de pérdida o daño en el activo.
- **Severidad Moderada, Valor=2:** Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo, o se requiere pocos recursos para explotar la vulnerabilidad y tiene un potencial moderado de pérdida o daño en el activo.
- **Severidad Alta, Valor=3:** Se requiere pocos recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo.
- **Exposición Menor, Valor=1:** Los efectos de la vulnerabilidad son mínimos. No incrementa la probabilidad de que vulnerabilidades adicionales sean explotadas.
- **Exposición Moderada, Valor=2:** La vulnerabilidad puede afectar a más que un elemento o componente del sistema. La explotación de la vulnerabilidad aumenta la probabilidad de explotar vulnerabilidades adicionales.
- **Exposición Alta, Valor=3:** La vulnerabilidad afecta a la mayoría de los componentes del sistema. La explotación de la vulnerabilidad aumenta significativamente la probabilidad de explotar vulnerabilidades adicionales.

La capacidad y motivación en la amenaza puede valorarse de la siguiente manera:

- **Capacidad Menor, Valor=1:** Poca o nula de realizar el ataque.
- **Capacidad moderada, Valor=2:** Se tiene el conocimiento y habilidades para realizar el ataque, pero pocos recursos o tiene suficientes recursos pero conocimiento y habilidades limitadas.
- **Capacidad Alta, Valor=3:** Se tiene los conocimientos, habilidades y recursos necesarios para realizar el ataque.
- **Motivación Menor, Valor=1:** Poca o nula motivación. No se está inclinando a actuar.
- **Motivación Moderada, Valor=2:** Se actuará si se le pide o provoca.
- **Motivación Alta, Valor=3:** Casi seguro que intentará el ataque.

La evaluación de la probabilidad puede ser:

- **Baja, Valor=1:** No hay historial y es raro que el escenario de amenaza ocurra.
- **Media, Valor=2:** Se han presentado casos y puede ocurrir el escenario de amenaza.
- **Alta, Valor=3:** Se han presentado suficientes casos y el escenario de amenaza seguramente ocurrirá.

Cada unidad de auditoría establece los criterios necesarios para decidir cuáles de los riesgos presentes en los activos tecnológicos requieren ser evaluados.

Evaluación de Controles

El equipo de auditores evalúa si las características de los controles en su diseño son suficientes para mitigar el riesgo asociado, identifican las brechas y las presentan al responsable de gestionar el riesgo. No es necesario ejecutar pruebas a

los controles con deficiencia en diseño si existe un consenso entre el dueño del riesgo y el equipo de auditores. En la **figura 5**, se muestra un ejemplo de cómo evaluar el diseño de los controles, la cual forma parte integral de la matriz de riesgo para tener todos los elementos interrelacionados.

Criterios (de impacto y aceptación) Vs. Riesgos

Es necesario determinar si algunos riesgos identificados se encuentran dentro del apetito de riesgo definido por los directores de la organización, darle una valoración cuantitativa o cualitativa basándose en escenarios posibles que afecten a la organización tomando en cuenta los criterios de impacto y aceptación establecidos por la organización. En la **figura 6** se muestra un ejemplo de la evaluación de riesgo contra los criterios de impacto alto, éstos fueron supuestos por el autor, sin embargo en la práctica son definidos por la alta dirección de las compañías (ej: un comité de auditoría), en ningún momento, el auditor puede definir estos criterios ya que de hacerlo estaría utilizando criterios erróneos para la valoración del impacto de los riesgos.

Los entregables de la fase de análisis son pero no se limitan a una conclusión sobre la efectividad del sistema de control interno y de gestión de riesgo según los componentes de COSO, un listado de los riesgos y controles tecnológicos, de las brechas existentes en el diseño de los controles y los riesgos que están dentro y fuera del apetito de riesgo del negocio.

MATRIZ DE RIESGO

La matriz de riesgo que se obtiene después de analizar y evaluar los diferentes componentes señalados en fases anteriores contiene las actividades, riesgos, controles, brechas de controles, impacto y nivel de riesgo. La **figura 7** proporciona una estructura sencilla para crear la matriz.

En base a esta matriz de riesgo, el equipo de auditores junto con el líder/supervisor del equipo seleccionan las áreas con mayor riesgo y que desean abarcar en la auditoría, se enfocan en los riesgos altos y medios del proceso, servicio o producto sujeto a evaluación, de esta manera la auditoría es más efectiva ya que le asegura al negocio que los controles claves fueron sometidos a evaluación y que la gestión de riesgos se encuentra o no en niveles apropiados.

Como entregable a partir de la matriz de riesgo, el equipo de auditores debe presentar los riesgos que cubrirán en la auditoría basándose en el análisis y evaluación de las fases anteriores.

FASE DE PLANEACIÓN

Una vez que se seleccionan las áreas de mayor riesgo y los controles claves a evaluar a partir de la matriz de riesgo, el

Figura 5—Ejemplo de Evaluación del Diseño de los Controles

Riesgo	Nivel de Riesgo	Controles Identificados	Brecha en los Controles
Pérdida de integridad de la información	Alto	Se revisa un reporte diario sobre los cambios a los parámetros críticos del afiliado, ej: Los cambios en la tasa de interés se ven reflejados en el reporte y se hace un cruce con las solicitudes de cambio de tasa.	Los cambios en los parámetros que son restablecido a su valor inicial en el mismo día no se incluyen en el reporte. Ej: Si a un afiliado se le cobra un 3.5% de interes de su facturación, se podría establecer en 0% y antes de concluir el día, restablecer a 3.5% para que el cambio no se vea reflejado en el reporte.

Figura 6—Ejemplo de Evaluación de Riesgo Contra Criterio de Impacto Alto

Proceso, Servicio ó Producto: ***Nombre del Procesa, Servicio ó Producto***			
		1	
Detalle de Riesgo		Pérdida de corfidencialidad de información el exponer datos de tarjetas en ciertos módulos del sistema principal de tarjetas	
Criterio de Impacto		**Seleccionar**	**Justificar**
Alto	La materialización del riesgo ocasiona pérdidas financieras igulaes o mayores a US $50,000		Incumplimiento con lo establecido en el estándar PCI DSS. Las marcos (Visa, MC, AMEX, otras) pueden multar a la organización por no salvaguardar la confidencialidad de la información de tarjetas. Con los datos expuestos, un usuario mal intencionado prodría realizar transacciones fraudulentas.
	Incumplimiento regulatorio con consecuencias graves tales como multas o sanciones superiores a los US $50,000	✔	
	Afecta la imagen o reputación de la compañia y puede ocasionar una sanción escrita o una exposición pública	✔	
	Inadecuado uso de recursos con repercusiones graves		

Figura 7—Estructura de Matriz de Riesgo

Fuente	**Ref. Doc.**	**Tipo de Riesgo**	**Riesgo**	**Nivel de Riesgo**	**Ref. Criterios**	**Controles Identificados**	**Brecha en los Controles**	**Criterio de Evalución**
Estrategias Eventos de Reisgo Limitaciones Proceso Eval. Control Interno Activos Tecnológicos	*Hacer referencia al formulario utilizado para documentar la fuente*	*Operacional Tecnológico Regulatorio Fraude Reputación Otros*	*Descripción del Riesgo identificado*	*Alto Medio Bajo*	*Hacer referencia al formulario utilizado para el cruce de riesgos versus criterios de impacto/ aceptación*	*Descripción del control identificado*	*Descripción de la brecha identificada en los controles*	*Descripción de la decisión tomada por el equipo de auditores, si realizan o no prueba al control.*

equipo de auditores define con mayor exactitud cuáles son los objetivos y el alcance de la auditoría.

Al conocer el alcance de la auditoría en una forma más exacta, el líder del equipo confecciona un cronograma de actividades para la ejecución del trabajo con el cual mide los tiempos establecidos para el equipo de auditores y evalúa la efectividad del mismo.

El modelo propone invertir menos tiempo en la planificación y ejecución de la auditoria y más tiempo en la fase de pre auditoría (análisis y evaluación) a como comúnmente se le conoce, ya que los esfuerzos del equipo de auditores es en primer instancia conocer, entender, analizar y evaluar los diferentes componentes del proceso, producto o servicio sujeto a evaluar para luego definir objetivos y alcances precisos. Es labor del líder del equipo de auditores explicar durante la reunión de inicio con los auditados el método a seguir en la auditoría, de tal manera que los auditados conozcan y se comprometan con el proceso a seguir.

Como entregables en esta fase de planeación, el equipo de auditores debe proporcionar un perfil del proyecto junto al cronograma de ejecución de las actividades restantes.

FASE DE EJECUCIÓN

En esta fase, basados en las áreas de mayor riesgo seleccionadas, objetivos y alcances definidos, los auditores especializados diseñan y ejecutan las pruebas a los controles. Se recomienda que exista de una forma sencilla un enlace entre la pruebas, controles, riesgos, fuente de riesgo (proceso, activo tecnológico, restricciones, otros), por lo que, el diseño de pruebas puede quedar en la misma matriz de riesgos y tener así un mejor control sobre la documentación del trabajo de auditoría.

Durante la ejecución de pruebas, el presente modelo recomienda al equipo de auditores documentar cada uno de los resultados de las pruebas y comunicar los hallazgos en la medida que éstos se identifican. Los beneficios de comunicar los hallazgos en la medida que se identifican son:

- Mayor agilidad a la hora de presentar el informe final
- Brindar tiempo para que la administración atienda los hallazgos del equipo de auditores durante el transcurso de la auditoría
- Desarrollar planes de mitigación más reales
- El Comité de Auditoría y los Directores miembros de la junta directiva y del Comité de Auditoría valoran las medidas de control adoptadas por la administración para mitigar el riesgo presentado en los hallazgos.
- Comunicación más fluida entre el equipo de auditores y la administración
- Una gestión de riesgos más efectiva

Los entregables en esta fase de ejecución son un detalle de las pruebas a realizar y la documentación pertinente para sustentar la ejecución de las mismas.

INFORME

El formato de informe de auditoría lo establece cada unidad de auditoría interna, resume todo el esfuerzo del equipo de auditores y es dirigido al nivel más alto de la organización. El modelo no pretende establecer un formato para el informe, sin embargo, a continuación se detallan algunos aspectos claves que el autor considera se deben incluir en un informe de auditoría interna: fecha de informe, nombre de auditoría, período de revisión, a quien va dirigido, a quien se copia, objetivos, alcance, limitaciones, exclusiones, conclusión, nivel de exposición de riesgo, estrategias afectadas, evaluación general u opinión del auditor y hallazgos.

SUPERVISIÓN CONTINÚA

El presente modelo recomienda establecer una supervisión continúa en cada una de las actividades de las fases propuestas aunque pueda ser ejercida por fase y no por actividad. La idea de establecer la supervisión del trabajo con base en cada una de las actividades se fundamenta en que a la medida que el trabajo avance en sus actividades, un error de enfoque o entendimiento ocasionaría reproceso, investigaciones adicionales, ajustes de las demás actividades, ocasionando un impacto significativo en el tiempo a invertir en la auditoría integrada.

CONCLUSIONES

Una auditoría integrada exitosa depende de un modelo práctico y fiable a seguir por el equipo de auditores. En este artículo se describe un modelo práctico y fiable como herramienta para las unidades de auditoría interna al momento de ejecutar auditorias integradas, enfocándose en eliminar la duplicidad de esfuerzo, abarcar los riesgos y controles claves, entre otros.

RECURSOS ADICIONALES

The Institute of Internal Auditors (IIA), Guía Práctica: Auditoría Integrada, 2012

Garsoux, Monique; “Integrated Audit Approach: An Overview”, Qualified Audit Partners, 2005

International Organization for Standardization, ISO/IEC 27005 Information Security Risk Management, 2008

Helpert, Anita; John Lazarine; “Making Integrated Audits Reality”, Internal Auditor, The Institute of Internal Auditors (IIA), 2009

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

www.isaca.org