GTAG®

GUÍA DE AUDITORÍA DE TECNOLOGÍA GLOBAL

Tercerización de tecnología de la información

The Institute of Internal Auditors

Guía de Auditoría de Tecnología Global (GTAG) 7: Tercerización de tecnología de la información

Autores

Mayurakshi Ray

Parthasarathy Ramaswamy

Consejero

Jaideep Ganguli

Marzo 2007

GTAG – Índice

La tercerización de tecnología de información (TI) es cada vez más reconocida como una solución eficiente, experta y eficaz en relación con su costo, diseñada para satisfacer las demandas de implementación, mantenimiento, seguridad y operaciones de los sistemas. El acceso a personal capacitado, infraestructuras de tecnología avanzada, flexibilidad y ahorro en los costos son los componentes que impulsan la tercerización de TI.

Los beneficios de la tercerización de TI van acompañados de la necesidad de gestionar complejidades, riesgos y desafíos inherentes. Por lo tanto, los auditores internos pueden colaborar con las organizaciones aportando una revisión integral de sus operaciones de tercerización, identificando riesgos, ofreciendo recomendaciones para gestionar los riesgos en forma más adecuada e incluyendo una evaluación sobre el cumplimiento de la actividad de tercerización relativa a las leyes y regulaciones aplicables. Esta guía no fue concebida para representar todas las consideraciones que pueden resultar necesarias sino para presentar un conjunto de puntos que se recomienda abordar. Todas las decisiones sobre tercerización de TI deben ser evaluadas en forma exhaustiva por cada organización.

Un ejemplo de preguntas clave que, entre otras, deben hacerse durante las auditorías de las actividades de tercerización de TI son:

- ¿Los auditores internos tienen una participación adecuada en las etapas clave del ciclo de vida de tercerización?
- ¿Los auditores internos tienen suficiente conocimiento y experiencia sobre tercerización para hacer aportes apropiados?
- ¿Los auditores internos comprenden los roles y las expectativas de las partes interesadas en el contexto de la iniciativa de tercerización de la organización?
- Si los planes de auditoría de TI están tercerizados, ¿los planes se crearon en base a un alcance de trabajo completo, descendente y basado en los riesgos?
- ¿Los auditores internos son capaces de presentar recomendaciones de tercerización comprensibles para los gerentes a fin de facilitar su implementación?
- ¿Los auditores internos son capaces de comunicar los hallazgos de auditoría de TI tercerizada de modo que el consejo de administración de la organización los comprenda y tome con seriedad?

Esta guía refleja las consideraciones clave de la función de auditoría interna en un contexto de tercerización de TI. También ofrece información sobre los tipos de actividades de tercerización de TI que se pueden aplicar, el ciclo de vida de tercerización de TI y la forma en la que se deben gestionar las actividades de tercerización implementando planes bien definidos y respaldados por un enfoque de riesgo, control, cumplimiento y gobierno de toda la compañía.

Las cuestiones clave incluyen:

- ¿Cómo elegir el proveedor correcto de tercerización de TI? La selección del proveedor repercutirá directamente en el éxito del acuerdo de tercerización. Esta guía ofrece consideraciones clave para la selección del proveedor.
- ¿Cuáles son las mejores formas de elaborar el borrador y gestionar los contratos de tercerización? El concepto de tercerización de TI está bastante desarrollado, lo que da lugar a prácticas de contratación bien establecidas. En esta guía, se analizan la estructura y los componentes clave de los contratos.
- ¿Qué prácticas se deben aplicar para garantizar que las operaciones internas tengan la mejor transición posible hacia la parte que toma la tercerización? La gestión de la transición puede ser un proceso difícil y requiere una planificación y una ejecución precisas para tener éxito. Esta guía ofrece información sobre el proceso de transición para ayudar a que las organizaciones logren una migración sin inconvenientes.
- ¿De qué forma las organizaciones pueden mitigar los riesgos de tercerización? La tercerización de TI puede tener un impacto notable en la organización. Las funciones de negocio críticas que se tercerizan pueden tener un impacto significativo en los controles internos de la organización. En esta guía se analizan los principales riesgos de tercerización y las recomendaciones relacionadas.
- ¿Cuál es el enfoque más eficaz para establecer controles de tercerización? Cuando se tercerizan las funciones de TI, determinados controles críticos se trasladan a la organización proveedora, tanto en el aspecto operativo como físico. Sin embargo, la responsabilidad final de alcanzar los objetivos de control recae en el cliente. En esta guía se analizan los enfoques disponibles para ayudar a que las organizaciones diseñen controles internos para gestionar en forma más eficaz las actividades de tercerización.

Necesidad de una guía de tercerización de TI para los auditores internos

Si bien la tercerización de TI es una práctica establecida y varias organizaciones grandes ya están experimentando la gran cantidad de beneficios que ofrece, todavía es una actividad en evolución. Sin embargo, antes de contratar a un proveedor de servicios de TI, la dirección se enfrenta con varias preguntas críticas que debe responder si desea alcanzar sus objetivos de negocio. En esta guía se detallan algunas de las ventajas y desventajas de la tercerización de TI, lo que a su vez, permitirá a las organizaciones tomar mejores decisiones de tercerización.

Es importante que los auditores internos conozcan las expectativas de tercerización que tienen las partes interesadas en cuanto a la actividad tercerizada y alineen sus objetivos de auditoría con los de la organización. En el contexto de las operaciones de TI tercerizadas, la evaluación de la eficacia del enfoque de control y riesgo interno y del proveedor de servicios elegido por parte de la organización es crítica para mitigar los riesgos de control interno en la etapa previa a la transición y durante todo el acuerdo de tercerización.

Otro aspecto clave es el rol del auditor interno destinado a garantizar la adhesión a diversas normas de seguridad y cumplimiento, y a definir hasta qué punto se puede depender del trabajo realizado por los auditores y otros especialistas independientes. Esencialmente, esta guía proporciona un mapa de ruta para conducirse a través del complejo entramado de la tercerización de TI y destaca diversas tendencias emergentes en el área.

Tenga en cuenta que los términos proveedor, proveedor de servicios, organización de servicios y tercero se utilizan indistintamente en esta guía.

Definición de tercerización de TI

En los últimos 15 años, la tercerización; concebida inicialmente como un intento creativo, innovador y de alto riesgo destinado a la reducción de costos; ha pasado a ser una colaboración estratégica probada que ayuda a las organizaciones a obtener valor de negocio. Un factor importante en este cambio fue el éxito de la tercerización de TI. Sin embargo, uno de los desafíos clave para las organizaciones es su capacidad para mantener los beneficios obtenidos con la tercerización (como la reducción en los costos operativos), sin perder un nivel de grado de aceptación del riesgo saludable.

La tercerización de TI se suele definir como el uso de proveedores o proveedores de servicios para crear, mantener o rediseñar los sistemas y la arquitectura de TI de una compañía. Si bien esta definición es aparentemente simple, comprende una gran cantidad de actividades de tercerización.

Con los años, la tercerización de TI ha evolucionado significativamente en términos de formato y objetivos. La tercerización de TI ha atravesado un proceso de evolución desde la tercerización de las actividades más económicas, secundarias y con mucha mano de obra para reducir los costos hasta la realización fuera del territorio de funciones tales como:

- Gestión de infraestructura de TI y redes.
- Desarrollo y mantenimiento de aplicaciones.
- Gestión de centro de datos.
- Integración de sistemas.
- Investigación y desarrollo.
- Desarrollo de producto.
- Gestión de seguridad.

Otros servicios tercerizados son alojamiento, desarrollo y mantenimiento de sitios Web, además de servicios de monitoreo y seguridad de Internet.

Dos de los principales factores que permitieron el éxito de la tercerización de TI fueron el uso de habilidades especiales en TI a nivel mundial y mejoras en el sector tecnológico que se tradujeron en la creación de sistemas y servicios más rápidos, más económicos y más eficaces. Países como India, China y Filipinas han sido testigos del surgimiento de proveedores especializados y de gran alcance, que han invertido infinidad de recursos en el desarrollo de procesos e infraestructuras de TI de nivel internacional. Estos proveedores han evolucionado para ofrecer productos de nivel mundial, de próxima generación y de extremo a extremo con costos más bajos y tiempos más rápidos.

Un impulsor fundamental de la tercerización de TI ha sido la heterogeneidad de los servicios, plataformas y programas de TI que hoy en día usan muchas compañías grandes. En muchas de estas compañías, los directores de TI (CIO, en inglés) ya no están a cargo de la función de servicios de TI. En cambio, se les pide que realicen funciones más estratégicas, como mejorar los niveles de servicio y eficacia, reducir los costos y agregar valor de negocio significativo. Por eso, la tercerización de TI se utiliza para:

- Reducir la carga de trabajo interno de TI. Esto les permite a las compañías concentrarse en actividades críticas, como el desarrollo de estrategias de TI y la alineación de los objetivos de TI con las estrategias de negocio.
- Lograr mejoras significativas en los niveles de eficacia de los procesos. Por definición, la tercerización incluye la reingeniería de procesos, lo que genera una función de TI más eficaz y proactiva.
- Ofrecer diversas habilidades en TI que de otra forma no se podrían mantener fácilmente en la organización. Como resultado, el proveedor suministra una variedad de competencias y habilidades en TI que se pueden aprovechar como el eje de la función de TI.

El cautivante caso de negocio de la tercerización de TI como un proceso de colaboración estratégica capaz de brindar importantes beneficios y reducir los costos a largo plazo la convierte en una práctica de negocio frecuente. Lamentablemente, el ahorro en los costos previstos a veces hace que los contratos de tercerización se generen por motivos equivocados o con una planificación inadecuada. La tercerización requiere establecer y mantener una relación en la cual el proveedor es parte del equipo del director de TI y de la organización. Esas relaciones generan confianza a largo plazo, se centran en los objetivos de la compañía y crean situaciones convenientes para todos que son necesarias para que las relaciones de trabajo sean más productivas.

Los riesgos y los impactos pueden tener un efecto considerable en la organización. Que los procesos de las áreas clave se hayan tercerizado no significa que la organización no siga siendo vulnerable a los riesgos de TI. Por eso, los auditores internos pueden ayudar a que la dirección comprenda y maneje mejor esos riesgos de tercerización. La Tabla 1, en la siguiente página, contiene una lista de los riesgos de tercerización habituales y los posibles impactos durante todo el ciclo de vida de tercerización.

Para establecer las bases que permitan el éxito de la tercerización de TI en términos de optimización de desempeño y gastos de TI, las funciones de dirección, control interno y operaciones deben estar coordinadas. Componentes como gobierno de TI, gestión de carteras de inversión de TI y gestión de contratos se abordan mejor desde la casa central global. Otros componentes, como gestión cultural y de comunicaciones, selección de proveedores locales de TI, supervisión de desempeño de proveedores y cuestiones impositivas y reglamentarias locales, se gestionan mejor en el sitio desde las oficinas locales. Más allá de dónde se gestione cada función, todos estos elementos deben estar presentes y coordinados en forma correcta para garantizar el éxito del proyecto.

Esencialmente, la tercerización estratégica de funciones de negocio secundarias asistidas por TI, puede permitirle a las organizaciones centrarse menos en la gestión de tecnología diaria y más en sus actividades y competencias principales. No obstante, una tercerización de TI eficaz requiere una colaboración con el proveedor de servicios de TI gestionada de manera eficiente. Esto es esencial para ayudar a que la organización logre ciertos beneficios, como por ejemplo:

- Menores costos.
- Más productividad.
- Mejores relaciones cliente/proveedor.
- Uso más adecuado de la tecnología.
- Más controles.
- Continuidad del negocio apropiada.
- Ventaja competitiva.
- Enfoque renovado en innovación y excelencia.

Los auditores internos pueden asistir a la dirección en el control de las actividades de tercerización mediante un rol proactivo en la supervisión del desempeño y el cumplimiento, la identificación de áreas que deban ser mejoradas y la propuesta de recomendaciones que ayuden a los proveedores a gestionar las actividades de tercerización de TI.

Cuadro 1: Ejemplos de impacto y riesgos de tercerización

Riesgos	Impacto
Estrategia: la estrategia de tercerización no está alineada con los objetivos corporativos.	• La decisión de tercerizar no es la adecuada. • El contrato no se establece y gestiona de acuerdo con los objetivos corporativos.
Factibilidad: las suposiciones (por ejemplo, período de recuperación de la inversión, impactos en la cadena de suministro y cliente, y ahorro de costos) son equivocadas debido a la diligencia debida inadecuada de los proveedores y a que la organización no pudo evaluar los riesgos pertinentes.	• La potencialidad de la tercerización no se analiza en detalle, lo que hace que los beneficios no se obtengan por completo. • El contrato se le adjudica a un proveedor inadecuado. • Los problemas con el proveedor no se gestionan de manera eficaz y eficiente ya que no se anticiparon correctamente.
Transacción: no se cumplen las políticas de adquisición; no se implementan los correspondientes acuerdos de nivel de servicio; no se consideran las implicancias operativas, de recursos humanos y reglamentarias; y no se planifican acuerdos de contingencia.	• Ausencia de un acuerdo bien elaborado para lidiar con una situación en la que el cliente no pueda recurrir a un documento legalmente obligatorio para garantizar que el proveedor cumpla los términos contractuales previstos. • Existen posibles violaciones del cumplimiento de regulaciones que generan sanciones financieras y repercusiones negativas en la marca de la compañía.
Transición: falta una planificación de transición formal, no existe un plan para la retención de las habilidades apropiadas, y el escalamiento y la resolución de problemas operativos de TI son ineficaces.	• Hay una pérdida de recursos clave durante el período de transición. • Existen dificultades operativas. • Hay una pérdida de confianza de los clientes en el servicio de tercerización.
Optimización y transformación: el contrato de tercerización no se gestiona con eficacia. Por lo tanto, los beneficios y las eficiencias de la tercerización no se concretan.	• El retorno de la inversión no es el esperado o es mínimo en comparación con los costos de tercerización. • La organización brinda servicios que se encuentran por debajo de los niveles esperados. • Existe un aumento en los costos no planificados.
Rescisión y renegociación: se produce una rescisión inadecuada de los procesos de tercerización.	• La compañía no puede hacerse cargo de la actividad tercerizada en una fecha posterior o rescindir o renegociar el contrato.

La tercerización de TI ha cambiado con los años. Desde servicios con tercerización tradicional (como desarrollo de aplicaciones y actividades de mesa de ayuda de TI) hasta servicios sofisticados (como desarrollo de productos, investigación y desarrollo especializado y soporte informático distribuido), las compañías continuaron tercerizando servicios de TI mientras el mercado de la tecnología seguía madurando. En la actualidad, los servicios de TI que se tercerizan con mayor frecuencia son:

- Gestión de aplicaciones.
- Gestión de infraestructura.
- Servicios de mesa de ayuda.
- Servicios de validación y prueba independientes.
- Gestión de centro de datos.
- Integración de sistemas.
- Servicios de investigación y desarrollo.
- Servicios de seguridad gestionados.

Tenga en cuenta que los proveedores de servicios y los clientes pueden utilizar distintos nombres para los tipos de actividades de tercerización mencionados arriba. Los clientes también pueden tercerizar uno o más de los servicios nombrados a uno o más proveedores de servicios.

GESTIÓN DE APLICACIONES

La gestión de aplicaciones puede realizarse mediante el desarrollo de aplicaciones, el desarrollo de software a medida, el mantenimiento de software y el soporte de la producción.

Desarrollo de aplicaciones

El desarrollo de aplicaciones de software o de módulos o funcionalidades específicas de una aplicación se debe tercerizar a firmas de desarrollo de software independientes que cuenten con el conocimiento y la experiencia técnicos que se necesitan para desarrollar aplicaciones de acuerdo con las especificaciones del cliente. Normalmente, esos servicios comienzan con una solicitud que hace el cliente de una especificación técnica o funcional (por ejemplo, solicitudes de mayor funcionalidad del sistema, módulos nuevos, actividades de estructura o de flujo de trabajo, o funcionamiento de la capacidad del sistema), especificaciones de requerimientos del sistema (SRS, en inglés) y especificaciones de requerimientos funcionales (FRS, en inglés). Sin embargo, es probable que en algunos casos el proveedor de servicios necesite realizar un estudio de los procesos de negocio y de los requerimientos del usuario, preparar las FRS y validar los requerimientos con el cliente.

La codificación se debe realizar después de crear la metodología del ciclo de vida de desarrollo de software (SDLC, en inglés) como parte del proceso de calidad del proveedor de servicios. En determinados acuerdos, el cliente puede especificar, supervisar y gestionar directamente los pasos del SDLC. El contrato o declaración de trabajo se debe definir claramente desde el comienzo, así como las etapas finales de la fase de desarrollo, que son responsabilidad del proveedor de servicios.

En la mayoría de los casos, el proceso de SDLC termina cuando se completa con éxito la prueba de aceptación por parte del usuario (UAT, en inglés); no obstante, el proveedor de servicios sólo es responsable hasta que se completa la prueba de la unidad. Las fases de prueba del sistema, de la integración y por parte del usuario son elementos esenciales destinados a garantizar que el sistema cumpla con los requerimientos del cliente. Las pruebas las pueden realizar el equipo del cliente o el cliente y el proveedor de servicios en forma conjunta. En cualquier caso, los problemas o los inconvenientes que se detecten en la fase de prueba se deben remitir al proveedor de servicios para su corrección.

A continuación, se enumeran aspectos clave que se deben tener en cuenta durante las auditorías de las actividades del SDLC:

1. El cliente y el proveedor de servicios deben acordar todas las actividades, hitos y entregas del SDLC. Los controles del proveedor de servicios ayudan a garantizar que el desarrollo respete las pautas definidas por el cliente y el proveedor de servicios.
2. El cliente debe aprobar formalmente los documentos con las especificaciones técnicas y funcionales previo al desarrollo de la aplicación. O bien, los usuarios deben enviar los requerimientos de negocio en base a las especificaciones funcionales aprobadas por el proveedor de servicios y el gerente de proyecto del cliente.
3. La programación de software debe respetar una norma sobre codificación definida.
4. Es necesario diseñar las revisiones independientes en cada etapa del proceso de SDLC y documentar el proceso de revisión.
5. Los planes, casos y resultados de las pruebas se deben documentar y dar a conocer al cliente, tal como se especifica en el contrato.
6. Los registros deben documentar los problemas detectados durante la fase de prueba de integración o de la unidad, así como los inconvenientes notificados por el cliente con posterioridad a la fase de prueba del usuario. Los registros se pueden utilizar como evidencia al evaluar todos los defectos o errores de software.
7. Se deben mantener la separación y el control de acceso durante el desarrollo, las pruebas y la migración de códigos o programas tal como lo definen las normas sobre seguridad del cliente.
8. Se definen los derechos de propiedad intelectual.
9. Se especifica el acceso al código fuente en caso de insolvencia financiera del tercerizador.

Desarrollo de software a medida

El propósito del software a medida es desarrollar aplicaciones que cumplan con requerimientos específicos del usuario o proveer soluciones específicas para la industria. A menudo, los clientes desean una solución puntual que cubra una necesidad o un requerimiento específico. Puede ser desde una aplicación simple e independiente hasta un sistema empresarial integrado que procese transacciones de diversos ciclos de negocio en toda la organización y actualice la base de datos central. Si bien las auditorías de aplicaciones de software a medida son similares a las de los procesos de desarrollo estándar, se deben tener en cuenta las siguientes actividades al realizar auditorías internas del proceso del SDLC en las aplicaciones a medida:

1. Los clientes deben aprobar formalmente todos los documentos de especificaciones de requerimientos del negocio (BRS, en inglés), es decir los documentos que estipulan las especificaciones funcionales y

técnicas de la solución propuesta. De lo contrario, la aplicación no cubriría las necesidades del cliente. Por lo tanto, los usuarios deben estar conformes con el diseño propuesto y dar su aprobación formal.
2. Las evaluaciones de riesgos y los análisis de impacto deben evaluar la solución propuesta y su capacidad para cumplir con los requerimientos establecidos.

Mantenimiento de software

Las recomendaciones para el desarrollo de software a medida se deben implementar durante el mantenimiento de aplicaciones existentes y durante toda actualización de las aplicaciones, sean estas cambios menores (como la creación de nuevos campos o informes) o cambios importantes (como la creación de un nuevo módulo). Además de los factores enumerados anteriormente, los auditores internos deben analizar los siguientes puntos durante la fase de mantenimiento de software:

1. El tiempo de entrega (TAT, en inglés) establecido por el cliente para todas las actividades de mantenimiento.
2. El tiempo requerido para completar el mantenimiento del sistema según los registros y bajo la supervisión del cliente.
3. Que haya controles del proveedor de servicios y que se respeten los tiempos de entrega. Esta es una expectativa de nivel de servicio fundamental ya que el hecho de que el proveedor de servicios no aplique controles apropiados podría generar un problema de mantenimiento.
4. Que las pruebas de integración y regresión del nuevo módulo o funcionalidad se lleven a cabo con éxito, al mismo tiempo que se corrigen los problemas a fin de garantizar una integración sin sobresaltos de las aplicaciones existentes.

Soporte de la producción

Las actividades de soporte de la producción apuntan a eliminar errores e interrupciones de los sistemas en funcionamiento (es decir, aplicaciones, computadoras centrales y bases de datos) que se encuentran en producción. El proveedor de servicios debe investigar los motivos del error y la interrupción, y corregir el problema rápidamente. El tiempo de entrega debe ser menor que el tiempo de servicio de mantenimiento porque los sistemas afectados están en uso y requieren una recuperación rápida para que la organización pueda reanudar sus operaciones habituales.

Las consideraciones clave de auditoría incluyen identificar si:

1. El cliente ha definido en el contrato expectativas de nivel de servicio, como el tiempo de entrega y la calidad del servicio brindado. El tiempo de entrega debe guardar relación con una respuesta (por ejemplo, el tiempo necesario para responder al tique de un problema informado) y una solución (por ejemplo, el tiempo necesario para resolver el error o el problema informado después de su registro por parte del usuario o el tiempo necesario para enviar una respuesta al problema).
2. Se mantiene una pista de cada respuesta y resolución. Además, los auditores deben asegurarse de que exista el seguimiento y la supervisión adecuados del cumplimiento del acuerdo de nivel de servicio (SLA, en inglés) por parte del cliente. Puntualmente, los auditores internos deben controlar la eficacia del proceso de supervisión y verificar que se mida el desempeño del sistema.

GESTIÓN DE INFRAESTRUCTURA

Los servicios destinados a gestionar y mantener la infraestructura de TI se pueden clasificar como gestión de infraestructura. Estos servicios comprenden la gestión y mantenimiento de desempeño de infraestructura, la resolución de errores, el mantenimiento de bases de datos y el respaldo y reanudación de servicios. Otros servicios de valor agregado más recientes incluidos en esta categoría son la supervisión de actividades de infraestructura de TI, el análisis de tiempo improductivo y los informes de fallas de sistema críticos y sus implicancias de gestión.

Las consideraciones clave de auditoría incluyen determinar si:

1. Las solicitudes de los servicios tercerizados de mantenimiento, soporte de la producción y gestión de infraestructura se envían formalmente al proveedor de servicios. Si bien la forma más eficaz de enviar una solicitud de servicio es mediante un sistema basado en flujo de trabajo en el cual el cliente emite tiques de trabajo para el proveedor de servicios, el correo electrónico también puede funcionar como una alternativa. Las solicitudes verbales se deben considerar una debilidad en los procedimientos o controles.
2. La aprobación del cliente para la implementación está incluida en el mismo tique de trabajo o en forma separada a través de un mensaje escrito.
3. El cliente ha definido en el contrato las expectativas de nivel de servicio (es decir, los tiempos de entrega y la calidad de resolución esperada).
4. Los tiempos de entrega se miden y supervisan adecuadamente para garantizar que no se altere el eje de la infraestructura.

SERVICIOS DE MESA DE AYUDA

Todos los servicios de mantenimiento, como la resolución de problemas, el soporte de la producción y la gestión de infraestructura, se pueden categorizar como servicios de mesa de ayuda. De acuerdo con esta distribución, el personal del proveedor de servicios brinda soporte al cliente para diversos problemas de TI, ya sea en el sitio (es decir, en el establecimiento del cliente) o fuera del sitio (es decir, en el establecimiento del proveedor de servicios). Los tiempos de entrega (de respuestas y resoluciones) luego se definen para cada nivel de servicio.

El cumplimiento crítico de los niveles de servicio implica respetar los tiempos de entrega definidos y la calidad del servicio brindado. Además, el proceso de evaluación debe incluir una valoración de los procedimientos destinada a medir y comparar el desempeño logrado con los parámetros de nivel de servicio esperados. Finalmente, los resultados del desempeño se deben utilizar como uno de los criterios de mayor peso para la evaluación continua del proveedor. Las revisiones de auditoría deben determinar si se enviaron informes de estado periódicos al cliente y si se documentaron problemas y medidas para lograr mejoras.

VALIDACIÓN Y PRUEBAS INDEPENDIENTES

Muchas organizaciones tercerizan las pruebas y la validación de software desarrollado en forma interna o por un tercero. Las pruebas especializadas del sistema desarrollado son necesarias para supervisar el desempeño del sistema y para identificar y corregir errores o problemas de programación. Durante la fase de prueba y validación, los auditores internos deben controlar que:

1. El cliente haya definido los parámetros de prueba (es decir, el sistema o la aplicación que se debe probar; los parámetros de prueba en sí y la duración, el nivel y la ubicación de la prueba).
2. Las especificaciones de prueba desarrolladas por el proveedor de servicios estén basadas en los requerimientos del cliente y aprobadas formalmente por él.
3. Los parámetros de prueba incluyen:
    - Una validación del diseño del sistema para determinar si los requerimientos del usuario están estipulados en el documento de especificaciones funcionales del sistema.
    - Un diseño de sistema con una capacidad adecuada de equilibrio de carga (es decir, que el sistema pueda manejar la cantidad requerida de transacciones de usuario simultáneas).
    - La aceptación correcta de las entradas de usuario, el procesamiento completo de las transacciones y la obtención del resultado deseado.
    - La incorporación de parámetros de seguridad de aplicaciones para evitar puntos vulnerables habituales o conocidos, inherentes al producto o la plataforma.
4. El cliente valide los casos de prueba diseñados para evaluar los parámetros definidos en el punto (b) anterior. Esos casos también se deben conservar como evidencia y para futuras pruebas y referencia.
5. Se conserven los resultados de las pruebas.
6. Se identifiquen y notifiquen en el informe de las pruebas los errores, las interrupciones y los problemas técnicos (por ejemplo, salida incorrecta o actualizaciones incompletas).

GESTIÓN DE CENTRO DE DATOS

Con el ingreso en el mercado de más proveedores, proveedores de servicios y sectores de la industria de TI, se produjo un cambio en el modo de pensar la tercerización. El objetivo de la tercerización cambió de un simple ahorro en los costos al suministro de niveles más altos de eficacia operativa, productos especializados y crecimiento dinámico. Los proveedores comenzaron a ofrecer servicios especializados que se podían aprovechar para múltiples clientes, más allá del sector de la industria. Un ejemplo es el uso de operaciones de centros de datos.

La tercerización de operaciones de centros de datos se originó a partir de la necesidad de las organizaciones de reducir los costos de gestión de la información. Por eso, hoy en día los centros de datos suelen brindar los siguientes servicios:

- Planificación, especificación, compra, instalación, configuración, mantenimiento, actualización y gestión de hardware, software y sistema operativo.
- Supervisión continua del desempeño y el estado operativo del servidor.
- Gestión de la capacidad del servidor, incluidos planificación de la capacidad, equilibrio de carga, ajustes y reconfiguración.
- Instalación y actualizaciones del software de aplicación del servidor que cumplen con los procedimientos de versión acordados por el cliente y el proveedor de servicios.
- Instalación y gestión continuas de hardware y software.
- Administración de seguridad y respaldo de datos para garantizar la seguridad y la integridad de los sistemas y las aplicaciones.
- Recuperación de sistemas del servidor en el caso de producirse un desastre con posterioridad a los tiempos de entrega implementados.

Durante las revisiones de los servicios de datos tercerizados, los auditores deben determinar si:

1. El proveedor de servicios cuenta con la capacidad necesaria (es decir, capacidad financiera, técnica y de infraestructura) para dar cabida a los servicios tercerizados.
2. El proveedor de servicios ha separado físicamente los datos y los sistemas de cada cliente para garantizar su confidencialidad e integridad.
3. El proveedor de servicios cuenta con una capacidad de respaldo adecuada para garantizar la disponibilidad de la red y la infraestructura del cliente.

INTEGRACIÓN DE SISTEMAS

En un entorno descentralizado, diversas funciones están organizadas en sistemas y aplicaciones dispares sin comunicación entre sí. Los riesgos de tener un entorno descentralizado incluyen la ausencia de actualizaciones de sistemas y aplicaciones perfectamente integradas, la existencia de saldos de cuentas sin conciliar, e informes o gestión de sistemas de información incorrectos.

Los servicios de integración de sistemas implican el desarrollo de secuencias de comandos, módulos, herramientas o programas destinados a integrar múltiples aplicaciones y sistemas. Esto permite que las aplicaciones existentes se comuniquen perfectamente entre sí, obteniendo como resultado un sistema consolidado. Una limitación clave para la integración de sistemas es su dependencia de la precisión de los datos existentes.

Al revisar los servicios de integración de sistemas, los auditores deben determinar si:

1. Las evaluaciones internas del cliente certifican que el sistema propuesto cumple con los requerimientos de escalabilidad, interoperabilidad, seguridad y confiabilidad. Los parámetros de evaluación deben tener en cuenta la interdependencia, la capacidad de equilibrio de carga de la infraestructura, la planificación de la capacidad para infraestructura agregada y el diseño funcional del sistema.
2. Las herramientas utilizadas para la integración se prueban en forma separada para controlar su aplicabilidad y eficacia.
3. Las revisiones de salida generadas por el sistema integrado guardan relación con los resultados deseados y validan la unidad y la precisión de la integración.

4. Las revisiones de los resultados de las pruebas validan la unidad y la precisión de la integración.
5. Los procedimientos y las condiciones para regresar al estado anterior están bien definidos en lo que atañe a las fallas de integración y del sistema.

SERVICIOS DE INVESTIGACIÓN Y DESARROLLO

Para estar al día con las necesidades de mercado existentes y al mismo tiempo continuar generando y manteniendo sus directorios y las bases de datos, muchas compañías tercerizan la investigación y desarrollo de distintas tecnologías, soluciones, procesos y sistemas. El trabajo de investigación tercerizado también incluye el uso de proveedores independientes para realizar análisis de mercado destinados a identificar las tendencias y la respuesta de sectores clave de la industria a determinados productos.

Las auditorías de las actividades de investigación y desarrollo deben determinar si:

1. Las actividades tercerizadas de investigación y desarrollo están clasificadas según sus soluciones necesarias, tecnologías o áreas de trabajo específicas.
2. Se creó un plan de tareas que identifique las fuentes, las estrategias y los tipos de investigaciones que se realizarán.
3. Se mantiene una base de datos o un repositorio de datos que almacene información recabada de diversas fuentes por categoría o por tipo de tarea identificada. También es necesario reunir la información y cargarla adecuadamente en la base de datos o en el repositorio de datos.

SERVICIOS DE SEGURIDAD GESTIONADOS

Recientemente, muchas organizaciones comenzaron a tercerizar sus servicios de seguridad. Esta área de tercerización también se conoce como servicios de seguridad gestionados (MSS, en inglés), haciendo referencia a la gestión de los requerimientos de seguridad externa de una organización. Otros términos utilizados para identificar esta función son: servicios de seguridad de Internet, tercerización de seguridad, servicios de inteligencia, servicios de consultoría en seguridad, servicios de seguridad de redes, servicios de gestión de seguridad, servicios de evaluación de seguridad, consultoría en seguridad y servicios de seguridad de TI.

Los MSS se definen como los servicios con los cuales se supervisa la seguridad de una organización aplicada a toda la infraestructura de TI, a los activos de datos y a las actividades de gestión del usuario. Según las necesidades del cliente, los términos del contrato pueden incluir el uso de diseño y soporte de arquitectura de seguridad punto a punto (por ejemplo, consultas de diseño, implementación, administración de seguridad y soporte técnico) o bien incluir la gestión de funciones de seguridad específicas de un sistema particular (por ejemplo, supervisión de filtros de seguridad, transmisión de datos, filtrado de contenido, protección contra virus, detección y respuesta a intrusiones, y evaluaciones de vulnerabilidad de red).

Debido al incremento en los requerimientos de seguridad de la información en regulaciones como la Ley de Responsabilidad y Portabilidad de Seguros Médicos (HIPAA, en inglés) de 1996 de Estados Unidos, la Ley Gramm-Leach-Bliley (GLBA, en inglés) de 1999 de Estados Unidos, la Directiva sobre protección de datos de 1995 de la Unión Europea (UE) y la Ley Sarbanes-Oxley de 2002 de Estados Unidos, cada vez más organizaciones de todo el mundo están considerando a la seguridad como una prioridad absoluta del negocio.

Para ayudar a que las organizaciones gestionen mejor sus MSS, los auditores deben examinar los siguientes puntos:

1. Evaluaciones de los requerimientos de seguridad en toda la compañía. Estos requerimientos deben estar basados en el tipo de trabajo, el país donde opera, las regulaciones de seguridad aplicables, la distribución de la infraestructura y los requerimientos del usuario (por ejemplo, el nivel de acceso al sistema o la disponibilidad del sistema) de la organización. Son evaluaciones que se deben llevar a cabo al menos una vez por año calendario para validar la aplicabilidad y la idoneidad de los requerimientos de seguridad establecidos.
2. La función tercerizada. Los MSS tercerizados deben guardar relación con las evaluaciones anteriores.
3. El diseño prototipo. Este diseño debe estar validado antes de la implementación y debe basarse en requerimientos de seguridad identificados.
4. Informes posteriores a la implementación y de supervisión de los MSS. Estos informes se deben presentar al equipo de gestión del usuario e incluyen informes sobre evaluaciones de vulnerabilidad, registros de detección de intrusiones y alertas de virus.
5. Análisis de la causa raíz relativos a los puntos vulnerables o incidentes informados.
6. Procedimientos de mitigación diseñados. Estos procedimientos no se deben poner en riesgo en ningún punto y garantizan la seguridad, confidencialidad y disponibilidad de los activos de datos y sistemas.

De acuerdo con los tipos de actividades que se describieron arriba, las revisiones de auditoría también deben determinar si:

- El cliente respeta un proceso definido destinado a establecer los derechos de acceso requeridos por el proveedor de servicios en los sistemas del cliente.
- El acceso otorgado al equipo del proveedor de servicios guarda relación con el tipo de servicio prestado.
- El acceso se otorga y se revoca de manera oportuna y está determinado por la adición o remoción de personal del proveedor de servicios, o por el vencimiento de servicios basados en el tiempo.
- Se aplican revisiones periódicas de los derechos de acceso a fin de garantizar que los derechos establecidos sean válidos de acuerdo con los requerimientos del usuario del sistema y que lleven a la remoción de derechos de acceso redundantes.
- El equipo de tercerización tiene habilidades y experiencia adecuadas para determinar la causa de errores y elaborar planes para corregirlos.

Una iniciativa de tercerización exitosa requiere un análisis minucioso de diversos aspectos antes de establecer la relación y durante todo su ciclo de vida. Toda iniciativa exitosa comienza con un análisis minucioso del caso de negocio, en el que se especifican el cronograma de inversión y los beneficios de negocio esperados en términos de reducción de costos y máximo aprovechamiento de la eficacia de trabajo a lo largo de un período de tres a cinco años. Por lo tanto, el caso de negocio ayuda a establecer el período de recuperación de la inversión esperado. Un caso de negocio correctamente elaborado también indica cómo alcanzar los beneficios identificados por medio de una cuidadosa alineación de la selección de proveedores, un enfoque de mejora de procesos y de transición establecido, y el uso de soluciones de riesgo y seguridad.

La figura a continuación muestra una cadena de valor de tercerización típica. Algunos de sus componentes se analizan en detalle en los siguientes párrafos.

1. Enfoque de gobierno en la tercerización

Al emprender una iniciativa de tercerización de TI, el gobierno posiblemente sea un área que las organizaciones subestiman con más frecuencia en términos de tiempo e inversión, y arquitectura estructural necesaria para gestionar la responsabilidad. Las compañías que se comprometen en una relación de tercerización de TI sin una capacidad de gobierno sólida no cuentan con los medios necesarios para gestionar correctamente la actividad tercerizada.

Un enfoque de gobierno sólido exige habilidades y experiencia de modo que la organización pueda ofrecer guías estratégicas, operativas y de gestión de proyectos necesarias para que la actividad de tercerización sea eficaz. Como la actividad de tercerización involucra a dos organizaciones distintas, es fundamental contar con una estructura de gobierno clara al especificar los procesos, roles, responsabilidades e incentivos que constituirán el acuerdo de tercerización. Como resultado, la estructura de gobierno debe ayudar a que la organización alcance los siguientes objetivos:

- Alinear cada contrato de tercerización de TI con los objetivos de negocio clave de la organización y las necesidades de las partes interesadas más importantes.
- Crear un mecanismo de supervisión para garantizar que los servicios de TI tercerizados se presten de acuerdo con las especificaciones del cliente.
- Gestionar cambios en servicios y proyectos de TI para carteras complejas.
- Establecer responsabilidades directas y visibles para el desempeño de TI.
- Definir la propiedad específica de términos clave del contrato.
- Definir procesos de gestión de TI bien integrados para el cliente y el proveedor de servicios.

Las auditorías de eficacia de gobierno deben evaluar los riesgos en la organización cliente en relación con los objetivos que se describieron arriba. Los auditores deben hacerse preguntas clave, entre las que se incluyen:

- ¿Qué grado de transparencia tiene el proceso de gobierno?

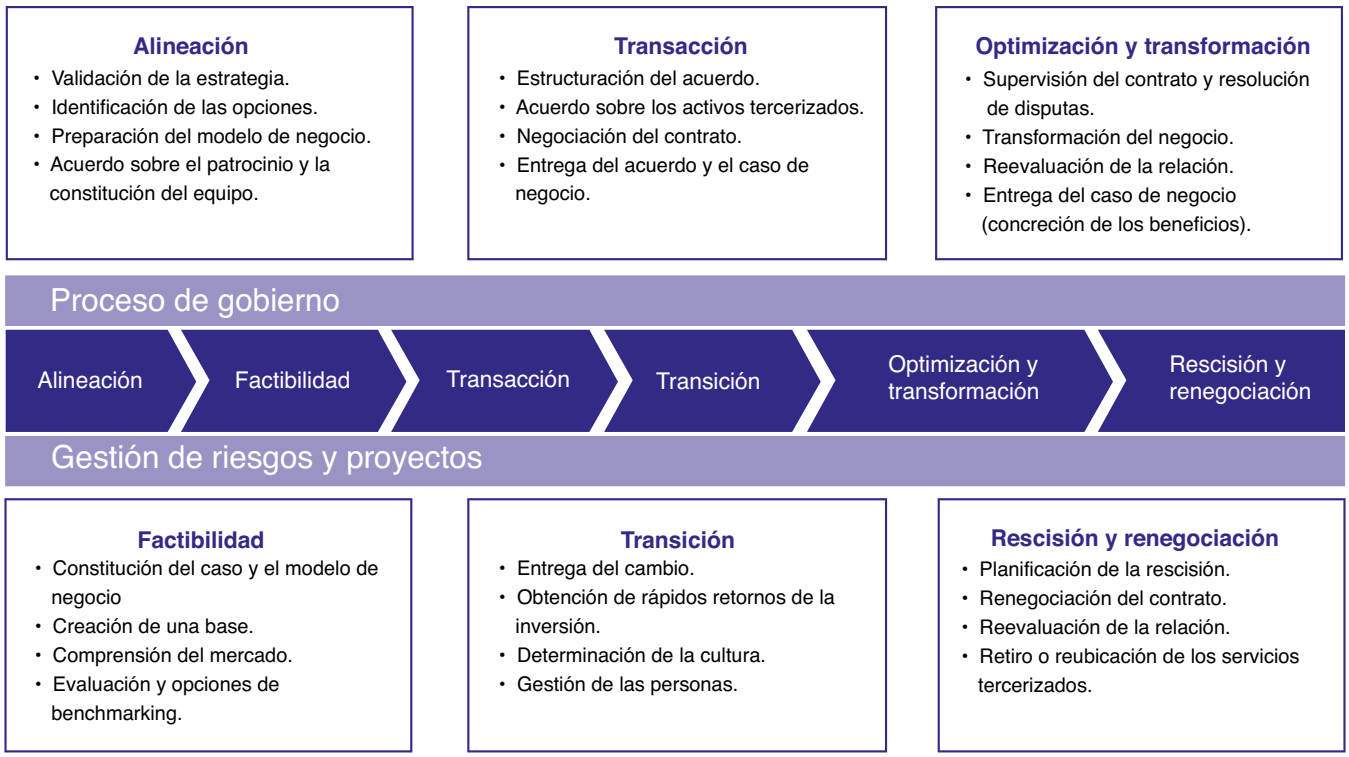

Figura 1: Cadena de valor de tercerización típica.

- ¿Los procesos de gestión de relaciones formales abordan conflictos de tercerización y generan relaciones de trabajo eficaces entre las partes involucradas en el contrato?
- ¿Están claramente definidos los roles, las responsabilidades y las actividades de delegación de autoridad entre las partes involucradas en el contrato?
- ¿Están establecidos con claridad los canales de comunicación?

2. Alineación y factibilidad

La fase de alineación y factibilidad se encarga de la formalización de la estrategia de tercerización de TI. En esta fase, el cliente debe preparar un caso de negocio basado en los diversos modelos de tercerización de TI y una evaluación de las opciones de tercerización basada en investigaciones y benchmarking. La estrategia de tercerización elegida debe detallar la cartera de servicios que se asignará a un proveedor de servicios, o a diversos proveedores de servicios, y la ubicación de esos servicios (es decir, en el sitio o fuera del sitio). Los distintos modelos de tercerización suelen incluir actividades de construcción, operación, transferencia; inversiones conjuntas con los proveedores de servicios; o una combinación de ambas. Las consideraciones clave de auditoría incluyen:

- ¿La estrategia de tercerización de TI del cliente está alineada con la estrategia de negocio general de la compañía?
- ¿El cliente analizó de manera adecuada todas las consideraciones financieras, operativas y legales antes de embarcarse en la relación de tercerización de TI?
- ¿Las suposiciones de tercerización están respaldadas por investigaciones o datos?

3. Transacción

Selección de proveedores – La selección de proveedores exige una evaluación integral de las competencias y las limitaciones técnicas del proveedor de servicios y está basada en las necesidades de servicios de tercerización de la organización. Si bien no existen enfoques correctos o incorrectos, las organizaciones deben seguir los pasos que se detallan a continuación como parte de todo programa de selección de proveedores.

Paso 1: Planificar y preparar

- Establecer un proceso de gestión de proyectos formal que deje en claro los roles y las responsabilidades de todo el personal interno involucrado en la relación de tercerización. El proceso además debe basarse en el tipo de servicio tercerizado y debe definir cómo se delegará la autoridad.
- Crear un equipo principal que evalúe a los proveedores y participe en las negociaciones. De acuerdo con las mejores prácticas de la industria, los miembros del equipo deben representar a distintos segmentos de la compañía, incluidos TI, finanzas, legal y recursos humanos, así como a la dirección de las unidades de negocio afectadas. Normalmente, el director de TI lidera este equipo.
- Identificar los roles y las responsabilidades de los miembros del equipo durante todo el ciclo de vida de la iniciativa de tercerización de TI.
- Detallar el alcance del trabajo (es decir, aplicación, infraestructura y tipo de servicio) que se espera tercerizar. Esto incluye la creación de un plan basado en hitos que analice cómo y cuándo la organización debe aumentar o ampliar el alcance del trabajo tercerizado.
- Crear una lista de parámetros que se deberá tomar en cuenta para la selección del proveedor y que concuerde con los requerimientos de tercerización clave de la organización. Las consideraciones para los parámetros pueden incluir el uso de centros de entrega globales, habilidades lingüísticas necesarias y un nivel mínimo de experiencia en tercerización de TI en tipos de entornos específicos. Los atributos de la lista pueden provenir de múltiples fuentes formales o informales tales como referencias, conocimiento del mercado, percepción de la competencia y recomendaciones de consultores independientes.
- Comprender los requerimientos legales de la tercerización, incluido el cumplimiento de regulaciones específicas de cada país, como restricciones de mercado abierto y licitación abierta.

Paso 2: Recabar datos específicos del proveedor

Después de poner en marcha los planes y las preparaciones, el equipo debe evaluar la capacidad y las operaciones del proveedor. Según la importancia, el valor, la oportunidad y el alcance del contrato,la evaluación podrá realizarse por medio de un proceso formal de solicitud de propuestas (RFP, en inglés) o a través de discusiones informales con los proveedores identificados. Las medidas clave que se deben tomar al recabar información específica del proveedor incluyen:

- Recabar detalles específicos, como tamaño, estabilidad, experiencia, ubicación, infraestructura, nivel de calidad de procesos y habilidades del proveedor.
- Incorporar requerimientos de especificaciones claros en un documento llamado "declaración de requerimientos" que destaque el alcance de los servicios que se tercerizarán, la duración del contrato, los requerimientos de control y cumplimiento esperados, los requerimientos de nivel de servicio para todos los procesos y servicios clave, y los requerimientos de capacidad del cliente. La declaración de requerimientos debe formar parte del proceso de RFP.
- Elaborar una lista exhaustiva de requerimientos de información del proveedor con valores para cada parámetro, que se puede utilizar durante la ronda final de selección. Se pueden utilizar parámetros relativos al proveedor, incluidos:
  - Sus antecedentes y grado de experiencia.
  - Información de empleados de gestión de proyectos y de la dirección. Este punto es particularmente relevante para organizaciones que prestan especial atención a las habilidades técnicas del proveedor.
  - Enfoques de gestión de riesgos y operación, incluidas certificaciones relevantes, metodologías y medidas de continuidad del negocio; acatamiento de los derechos de propiedad intelectual; medidas

de seguridad de subcontratación y de los datos; y actividades de cumplimiento de leyes y regulaciones.
- Enfoque y metodología específicos del proyecto, incluida la asignación de recursos.
- Referencias del cliente, incluida información sobre transiciones exitosas.

La capacidad del proveedor de servicios de gestionar la transición de los servicios del cliente es un aspecto fundamental que se debe evaluar durante la etapa de selección de proveedores. Los parámetros de transición abarcan evaluaciones críticas de la solidez de la metodología del proveedor para llevar a cabo la transición mediante puntos que incluyen:

- Todas las fases de la etapa de transición y la incorporación de mejores prácticas, como los principios de Six Sigma.
- Detalles de la transición relativos a hitos específicos, documentación, análisis de tecnología, planificación de la capacidad y costos.
- Soporte disponible para mitigar riesgos y gestionar la productividad durante el período de transición.
- Redundancia, reorganización y recapacitación en el sitio.
- Éxitos en transiciones previas, incluida cantidad de transiciones y si se realizaron puntualmente y dentro del presupuesto.
- Solidez de planes de soporte, como planes de continuidad del negocio, de contingencia y de riesgos.
- Calidad del equipo encargado de la transición, incluido el perfil y la experiencia.

Paso 3: Aplicar diligencia debida

Luego de recibir respuestas a las RFP, el equipo del proyecto debe comenzar a analizar la información presentada comparándola con el enfoque predefinido para la evaluación. Las medidas que se deben tomar incluyen:

- Controles de las referencias del cliente durante la etapa de diligencia debida final. El equipo del proyecto debe evaluar la competencia de la gestión de proyectos, el índice de éxito, la calidad y el nivel de trabajo, el cumplimiento de términos del contrato y el proceso de comunicación del proveedor.
- Análisis de información y riesgos específicos del país, incluida la disponibilidad de habilidades, costos, entorno y estabilidad políticos, compatibilidad cultural y posibilidad de acceso.
- Visitas al sitio para evaluar las capacidades, las operaciones, la infraestructura y la cultura local del proveedor de servicios.

Según la respuesta de cada proveedor, los controles de las referencias del cliente y las visitas al sitio, las negociaciones finales suelen darse con un grupo de dos o tres proveedores de servicios.

Paso 4: Negociar y cerrar el acuerdo

La negociación y el cierre del acuerdo son los últimos pasos del proceso de selección de proveedores. Cómo realizar este paso depende en gran medida de la diligencia debida aplicada en los pasos previos. A continuación se ofrece una descripción de las medidas que pueden tomar las organizaciones.

- Negociar al menos con dos proveedores en forma simultánea. Esto le permite a la compañía comparar precios y términos legales del acuerdo. Los grandes contratos de tercerización pueden involucrar negociaciones con tres o cuatro proveedores.
- Involucrar al personal del área legal y de la alta dirección para analizar los términos y condiciones del contrato. En general, los proveedores de servicios presentan contratos estándar con los términos y condiciones de la relación. La mayoría de las organizaciones analizan el contrato con sus asesores legales antes de hacerlo con el proveedor de servicios.
- Firmar el contrato. La mayoría de los proveedores de servicios están dispuestos a modificar el contrato como sea necesario antes de firmarlo.

Consideraciones legales y contractuales en la contratación de proveedores de servicios – Los acuerdos de tercerización de TI involucran distintos niveles de complejidad, riesgo y diversos aspectos legales y contractuales. Hay inquietudes especiales relacionadas con la dificultad de rescindir acuerdos a largo plazo y de definir responsabilidades en organizaciones que trabajan juntas por primera vez, especialmente en entornos afectados por condiciones de negocio cambiantes.

Muchos miembros de la alta dirección consideran que parte de la base de una iniciativa exitosa depende de la diligencia debida legal y contractual que se aplique antes de formalizar el acuerdo de tercerización. Por eso, salvo que los controles de tercerización de gestión estén respaldados por un contrato bien redactado, se corre el riesgo de que las actividades operativas y de gestión no reciban una supervisión suficiente. Esto aumenta la probabilidad de que los procesos clave, las especificaciones de calidad, los tiempos de entrega de servicios y los resultados estén controlados por el proveedor o dependan de él.

Los aspectos legales y contractuales que se deben abordar al elaborar un contrato correctamente redactado incluyen:

1) Niveles de servicio e incentivos. La organización debe definir el nivel mínimo de benchmark, normas y mediciones de desempeño más acordes al objetivo de tercerización, como medidas directamente vinculadas con indicadores operativos (es decir, calidad de servicio, disponibilidad del sistema y tiempos de respuesta). De ser posible, es importante evitar cláusulas de exclusividad o de proveedor preferido para mantener una presión competitiva sobre el proveedor.

2) Personal del proveedor. Las personas son los factores condicionantes del desempeño. El cliente debe poder aprobar la selección de personal clave del proveedor y definir los criterios utilizados para analizar el personal de reemplazo. Como la pérdida de personal clave puede afectar la capacidad del proveedor para cumplir con las obligaciones contraídas, algunos clientes hacen hincapié en disponer de derechos de aprobación sobre las estrategias de retención y compensación del proveedor. De esta forma, lo más probable es que el personal crítico para la entrega de la solución y la transferencia de conocimientos continúe trabajando para el proveedor mientras dure el contrato.

3) Protección de datos, privacidad y propiedad intelectual. Siempre existen riesgos cuando entidades independientes tienen acceso a información confidencial del cliente, detalles de operaciones de negocio privilegiadas o propiedad intelectual vulnerable a su divulgación al público o a la competencia. Las cuestiones clave pueden abarcar desde exigir al proveedor que mantenga los niveles de seguridad especificados capacitando a sus empleados al efecto, hasta obligaciones contractuales, como la firma de un acuerdo de confidencialidad por parte del personal encargado de prestar el servicio y la indemnización a la compañía en caso de existir un incumplimiento.

4) Protección de precios. Establecer cambios de precios es una de las áreas más importantes del contrato en la tercerización de TI ya que pequeñas diferencias en los precios pueden afectar las opciones, alternativas y objetivos de negocio del tercerizador. Los contratos deben cubrir cuestiones relativas a los precios como cambios en el alcance del servicio, parámetros de precios acordados, mantenimiento de precios preferentes o de "cliente más favorecido" y procedimientos para acelerar la resolución de desacuerdos en los precios.

5) Asignaciones a terceros. En situaciones en las cuales el proveedor contrata a un tercero para prestar el servicio (es decir, una subcontratación), el cliente debe incluir en el contrato la forma en que se gestionará la calidad del servicio y cualquier riesgo que pueda acarrear su desempeño.

6) Propiedad de los activos utilizados o creados por la relación de tercerización de TI. En ocasiones, los proveedores de tercerización de TI requieren el uso de recursos o activos de la organización para cumplir con obligaciones contractuales. Debe haber reglas y procedimientos que definan y generen derechos de propiedad cuando se crea valor nuevo a partir de una actividad de tercerización. Los términos del contrato deben especificar los procedimientos necesarios para limitar al mínimo la confusión y los desacuerdos que pueden surgir cuando se comparten sistemas, recursos y activos.

7) Conflictos entre distintos sistemas legales. Los contratos se deben basar en leyes nacionales y locales aplicables. Los contratos de tercerización, en especial los parámetros que definen las iniciativas realizadas fuera del territorio, se pueden tornar muy complejos si no se tienen en cuenta los distintos sistemas de justicia y las controversias que requieren una resolución legal desde el comienzo de la iniciativa. Las cuestiones clave en esta área incluyen el uso de terminología que aclare posibles ambigüedades en la interpretación del contrato y la solución de controversias, así como terminología que defina claramente los procedimientos y procesos para la identificación, discusión, escalamiento, resolución y gestión de problemas (por ejemplo, resolución de controversias, mediación y arbitraje).

8) Gestión de contingencia y planificación de cambios. Uno de los objetivos más importantes del contrato es proteger la posibilidad del cliente de reformar el contrato de tercerización, la relación o el enfoque de operación de modo que el cliente se pueda adaptar a los cambios en el entorno de negocio. Un elemento crítico en cualquier relación de tercerización es la flexibilidad para adaptarse a cambios no previstos en el negocio, como crecimiento, eventos extraordinarios, fusiones, adquisiciones o ventas. Es necesario definir esta flexibilidad en el contrato.

9) Aviso de impactos adversos importantes. Un contrato bien redactado debe garantizar el derecho del cliente de ser informado de todo evento que pudiera afectar la capacidad del proveedor para cumplir con sus obligaciones. Un aviso oportuno sobre eventos inminentes permite a la organización no aumentar los costos de planificación de contingencias y al mismo tiempo mantener un alto retorno de la inversión (ROI, en inglés) cuando en efecto ocurren eventos imprevistos.

10) Derecho a efectuar una auditoría. Los contratos deben incluir cláusulas que estipulen derechos claramente definidos para el cliente de auditar procesos, controles y resultados asociados con la actividad tercerizada. Entre ellas, se incluye el uso de informes de las Declaraciones sobre Normas de Auditoría N.º 70 (SAS 70) o un tipo de revisión similar, así como la auditoría de diversos aspectos relativos al cumplimiento de regulaciones, como por ejemplo, las asociadas con la Ley Sarbanes-Oxley de 2002 de Estados Unidos.

11) Rescisión. Incluso los contratos de tercerización de TI elaborados en base a una relación o colaboración auspiciosa deben estipular las condiciones que implican la rescisión. Estas condiciones abarcan desde la rescisión por un motivo específico hasta la rescisión por una cuestión de conveniencia. El lenguaje del contrato debe definir los derechos del cliente, así como los procedimientos que se deben aplicar para la rescisión y las opciones para comprar o autorizar el uso de activos.

Las consideraciones clave de auditoría interna que se deben revisar en esta etapa incluyen:

- Determinar si el proceso de selección de proveedores se realizó en forma justa.
- Examinar la descripción del contrato relativa a los aspectos a los que el cliente quedará expuesto una vez iniciada la relación de tercerización.
- Identificar si existe una lista de verificación de los factores legales y contractuales acordados por el cliente y el proveedor de servicios que contribuya a determinar el cumplimiento de cada uno de esos factores por parte del proveedor.

4. Gestión de la transición

La transición o migración implica la transferencia de conocimiento, y su propiedad, a una entidad sin experiencia previa en un sistema, proceso, cultura corporativa o industria determinada. Si bien los planes de transición son responsabilidad del

cliente, se suelen delegar a los proveedores. Las actividades de migración habitualmente incluyen dos etapas: planificación y transferencia de conocimiento.

Planificación

La fase de planificación involucra el desarrollo de una estrategia de migración. Durante la fase de planificación, la organización debe incluir los costos y las líneas cronológicas para cada hito significativo del plan de migración. Como parte de la estrategia de transición, el cliente y el proveedor de servicios identifican en forma conjunta el modo de migración ideal (por ejemplo, una transferencia completa de todas las actividades o una implementación gradual de funciones basada en un esquema de prioridades). La estrategia también debe asignar recursos y presupuestos específicos para cada paso de la fase de migración.

Transferencia de conocimiento

Aplicar un plan de transferencia de conocimiento eficaz es fundamental para el éxito a largo plazo de la relación de tercerización. Esto requiere que el cliente y el proveedor de servicios identifiquen y documenten toda la información necesaria (por ejemplo, información técnica, de negocio, de procesos y de base) de modo que el proceso de transferencia genere el menor impacto posible sobre la calidad del servicio de la actividad tercerizada.

Un proveedor de servicios de alta calidad debe contar con un proceso bien establecido de gestión de conocimiento continuo que no altere la calidad de servicio del cliente. Debe haber documentación completa y detallada a disposición, de modo que la compañía pueda regresar la actividad a la organización o trasladarla a otro proveedor de servicios, si fuera necesario. Esto le permite al cliente una influencia mayor para asegurarse de que los servicios se brinden tal como se estipularon en el contrato. Además, el cliente debe tener acceso a la información relevante documentada en esta fase. En consecuencia, la compañía debe realizar auditorías periódicas del proceso de transferencia de conocimiento.

Por último, esta etapa puede implicar visitas al sitio por parte de gerentes de proyecto de rango superior del proveedor de servicios. Algunas organizaciones también desean que su personal visite al proveedor de servicios para establecer el proceso de tercerización. El personal clave puede incluir gerentes de rango superior o directores de producto para organizar la actividad de tercerización e ingenieros de rango superior para capacitar al equipo del proveedor de servicios. La frecuencia y la duración de las visitas deben disminuir a medida que las operaciones van madurando y haciéndose más estables.

5. Gestión del cambio

El proyecto de tercerización puede interrumpir las operaciones de la organización durante diversas etapas de la iniciativa de tercerización. Las organizaciones deben identificar, prever y gestionar estas interrupciones de la mejor manera posible para alcanzar el resultado deseado.

La transición es una etapa en la cual el cliente y el proveedor de servicios pueden estar sometidos a muchos cambios. Durante esta etapa, el proveedor de servicios debe asegurarse de contar con la experiencia necesaria para abordar estas interrupciones causadas por el proceso de transición. El cliente y el proveedor de servicios pueden gestionar los cambios que suceden en esta fase de transición de las siguientes formas:

- Definiendo requerimientos de control y procesos clave. Estos procesos y controles deben abarcar las actividades de seguridad, planificación de la continuidad del negocio, recuperación de desastres, cumplimiento y protección de datos.
- Identificando elementos de planificación y sus correspondientes líneas cronológicas.
- Describiendo las responsabilidades del cliente y del proveedor de servicios durante la fase de transición.
- Estableciendo requerimientos de nivel de servicio para todos los procesos y servicios clave, incluidos los niveles de servicio en las diversas etapas del proceso de transición.
- Especificando las diferentes adaptaciones de tecnología y conectividad necesarias durante el período de transición.
- Describiendo procedimientos, políticas y herramientas de comunicación sólidas para manejar las interfaces durante y después de la transición de formatos de informes (es decir, informes de estado, informes de indicadores clave de desempeño [KPI, en inglés], informes de jerarquía e informes de frecuencia) y escalando mecanismos para utilizar durante la fase de transición.

Estabilización y supervisión

La última etapa del proceso de gestión del cambio es la estabilización de las operaciones. Esto se refiere al desempeño en concreto de los procesos tercerizados bajo los controles del proveedor de servicios. Durante la fase de transición, ciertas actividades tercerizadas pueden reanudar sus operaciones normales dentro de un plazo definido. Las demoras se deben supervisar de cerca ya que pueden repercutir negativamente en la obtención de beneficios de tercerización. Esto también sirve para que la organización reaccione y responda a cualquier problema en forma proactiva.

Durante la fase de supervisión, las organizaciones deben asegurarse de que exista comunicación entre el equipo en el sitio y el proveedor de servicios. Esto es imprescindible para el éxito de la relación. La comunicación debe abordar los siguientes puntos:

- Informes sobre KPI y otras medidas de desempeño.
- Análisis de desempeño y tendencias de KPI.
- Documentación sobre desviaciones de desempeño y su análisis.
- Planes que identifiquen cuestiones relativas a la resolución, incluido el plazo para cada resolución.
- Comunicaciones por medio de los canales apropiados. Entre ellos, se incluyen llamadas telefónicas, reuniones por Internet o Webex, sesiones de chat, mensajes de correo electrónico y videoconferencias, o bien canales más formales, como reuniones o actualizaciones semanales o mensuales.
- La responsabilidad del proveedor de cargar información de desarrollo de productos de software, documentación relacionada con el proyecto e informes de trabajo en curso en el sitio de intranet apropiado, de modo que los clientes puedan obtener la información necesaria sobre el estado del proyecto.

Consideraciones de auditoría interna

Las preguntas clave que los auditores internos deben evaluar en esta etapa incluyen:

- ¿Existe una estrategia formal de gestión de la transición?
- ¿Cuán eficaz es la estrategia de transferencia de conocimiento en términos de su diseño y eficacia operativa?
- ¿El desgaste repercutió en la fase de transferencia o en la operación de las actividades tercerizadas?
- ¿Cuán eficaz es el proceso de comunicación y revisión?
- ¿Cuán eficaz es el proceso de gestión del cambio en términos de su diseño y eficacia operativa?
- ¿Se ha implementado un proceso para garantizar que el proveedor de servicios aplique sólo los cambios aprobados?
- ¿Están bien documentadas las muestras de revisión a fin de demostrar que se respetaron todas las etapas del proceso de gestión del cambio?
- ¿Existe un proceso de gestión formal? Si lo hay, ¿sirvió para supervisar el progreso del proyecto y sus beneficios en las líneas cronológicas especificadas?

6. Transformación y optimización

Un contrato bien definido pero a la vez flexible suele ser la clave de una relación de tercerización de TI exitosa. Se trata de un contrato que define los límites, los derechos, la responsabilidad y las expectativas del cliente y del proveedor de tercerización y a menudo es el único mecanismo para regular la relación de tercerización. Los contratos de tercerización de TI deben elaborarse de modo que ofrezcan a los clientes herramientas destinadas a:

- Mantener la influencia y gestionar el cambio.
- Gestionar servicios nuevos y dentro del alcance.
- Supervisar y gestionar la calidad del servicio.
- Permitir los ahorros en costos prometidos.
- Brindar protección de precios competitivos.
- Gestionar la responsabilidad y los riesgos potenciales sin afectar el precio del proyecto.

Uno de los elementos más críticos del contrato de tercerización es definir los objetivos de nivel de servicio, que se deben alcanzar como parte de la entrega de servicios tercerizados. Para el cliente es importante tener un proceso implementado que se centre en cómo modificar los parámetros de nivel de servicio, de qué manera las revisiones formales deben abordar el cumplimiento de los parámetros acordados y cómo evaluar las desviaciones.

El SLA debe describir:

- Los objetivos y el alcance del servicio.
- Las mediciones del desempeño y los niveles de servicio correspondientes para cada medición, incluidos:
  - Volumen (es decir, cantidad de solicitudes de mantenimiento por mes y líneas de código).
  - Disponibilidad (es decir, disponibilidad de servicios provistos por período determinado).
  - Calidad (es decir, cantidad de fallas de producción por mes, cantidad de plazos no cumplidos y cantidad de entregas rechazadas).
  - Respuesta (es decir, tiempo necesario para implementar una mejora o resolver problemas de producción).
  - Eficacia (es decir, cantidad de programas respaldados por persona, índice de reprocesos y encuestas de satisfacción del cliente).
- Las definiciones de frecuencia para medir el desempeño (por ejemplo, mensual, trimestral, etc.) y otras revisiones informales de desempeño del contrato por medio de informes y reuniones para informar el progreso en forma regular.
- Los pagos basados en el desempeño del SLA.
- La definición de cláusulas que estipulen la disponibilidad de renegociación del contrato por incumplimiento de acuerdos de nivel de servicio.

Como la gestión de contratos es cada vez más compleja, es posible que surja el rol de gerente de contratos, en especial en organizaciones con una gran cantidad de contratos de tercerización. El gerente de contratos puede ser un empleado contratado o de la organización, que debe trabajar junto con el departamento legal interno del cliente para cumplir con las formalidades de los contratos. Un gerente de contratos con experiencia y de tiempo completo debe hacer un seguimiento de las comunicaciones, además de revisar y mantener procedimientos manuales y relativos a las operaciones de supervisión para constatar el cumplimiento de los términos del contrato.

Consideraciones de auditoría interna

Un aspecto clave que los auditores internos deben evaluar durante esta etapa es la observancia del SLA. Además, los auditores deben evaluar la solidez del proceso de revisión del cliente. Las preguntas clave para hacer incluyen:

- ¿Las áreas clave definidas en el SLA están alineadas con los beneficios o los parámetros de mejora de procesos identificados en el caso de negocio?
- ¿Los informes periódicos del proveedor de servicios están basados en las áreas clave acordadas en el SLA?
- ¿Los informes del proveedor de servicios tienen una validación independiente con respecto a su precisión e integridad?
- ¿Es eficaz la revisión de los informes del proveedor de servicios? ¿Se tomaron medidas adecuadas cuando se produjeron desviaciones?
- ¿Están aprobados correctamente los cambios en los términos del SLA?

7. Gestión de riesgos y proyectos

Dado el panorama de regulaciones actual, la gestión de riesgos de cumplimiento está surgiendo como una prioridad principal para muchas organizaciones, en especial para las que pertenecen a las industrias de los servicios financieros y la atención de la salud. Para establecer un proceso de gestión de riesgos de cumplimiento eficaz, los clientes y los proveedores de servicios deben:

- Determinar los tipos de riesgos de cumplimiento a los cuales está expuesta la organización cliente de acuerdo con el tipo de servicio tercerizado.

- Identificar los procesos que pueden tener un impacto considerable sobre el riesgo de cumplimiento.
- Establecer controles de procesos manuales y automatizados para garantizar que se mitiguen todos los riesgos.
- Definir acuerdos de nivel de servicio relativos a potenciales exposiciones a riesgos de cumplimiento, qué procesos se revisarán, responsabilidades y frecuencia de las auditorías y pasos correctivos.
- Implementar y supervisar un modelo de gobierno sólido para controlar el cumplimiento de regulaciones.

Los riesgos de tercerización abarcan una selección de proveedores incorrecta, una gestión de contratos deficiente, problemas en la transición, riesgos de reacciones adversas en la organización y puntos vulnerables en la seguridad. A medida que las actividades de tercerización maduran, las organizaciones toman más conciencia sobre estos riesgos y están más alerta a ellos. El desafío, entonces, es identificar los riesgos ocultos y definir las estrategias apropiadas que se necesitan para minimizar sus impactos. Por ejemplo, podría surgir un riesgo de control posible luego de que el proveedor de servicios fuera considerado responsable por el éxito o el fracaso de la actividad tercerizada. Como consecuencia, la organización cliente debe interactuar codo a codo con los equipos tercerizados para realizar el seguimiento, guiar y planificar las operaciones tercerizadas de acuerdo con los objetivos y las expectativas de la organización.

El seguimiento de proyectos se basa en mediciones predefinidas, como calidad, líneas cronológicas y planificación de recursos, permite la integración sin inconvenientes de los equipos, las culturas y el conocimiento del cliente y del proveedor de servicios. Esto se puede realizar por medio de los siguientes puntos:

- Reuniones e informes de estado. Muchas organizaciones mantienen registros de riesgos conjuntos. Esto permite asegurar mayor transparencia y visibilidad de problemas y planes de acción, facilitando así la toma de decisiones proactivas.
- Informes de hitos del proyecto.
- Comunicación diaria entre miembros del equipo relativa a problemas operativos por medio de llamadas telefónicas, sesiones de chat, videoconferencias o correo electrónico.
- Entrega de muestras provisorias, como diseños de programa, códigos, documentación y planes de prueba.
- Portales del proyecto donde se almacenan todos los documentos relacionados con el proyecto. Los portales del proyecto deben brindar acceso sólo a los miembros del equipo asignado al proyecto.
- Viajes al sitio por parte del personal de servicio o visitas al proveedor por parte de los miembros del equipo de desarrollo de las organizaciones cliente para hacer revisiones.

Conservar y mejorar la calidad del desarrollo de software es uno de los principales objetivos de las organizaciones que tercerizan operaciones de TI. Para eso, los procesos de tercerización deben estar planificados, gestionados y supervisados correctamente. Las organizaciones también deben formar un equipo especial de aseguramiento de calidad (QA, en inglés) para garantizar la buena calidad de los procesos, en especial en organizaciones involucradas con procesos especializados como el desarrollo de software.

Además, los contratos se pueden utilizar para establecer expectativas de gestión de riesgos. Si bien un contrato es una declaración útil de las responsabilidades de las partes, no debe sustituir un modelo de gobierno sólido destinado a supervisar, comunicar y resolver controversias con los proveedores. Las relaciones cliente-proveedor son mutuamente beneficiosas cuando los términos del contrato son claros y las partes disponen de un mecanismo sólido para gestionar las actividades diarias y de un procedimiento para la resolución de controversias.

Consideraciones de auditoría interna

Durante sus evaluaciones, los auditores internos deben determinar si el proveedor de servicios cumple con el acuerdo de tercerización y si las actividades son sólidas, transparentes e imparciales. Para eso, los auditores internos deben identificar:

- La presencia de un caso de negocio bien estructurado que describa claramente los resultados de negocio esperados.
- Una declaración de requerimientos correctamente documentada.
- Una lista final, una evaluación y un proceso de selección de proveedores planeados, estructurados y transparentes con criterios predefinidos y puntajes objetivos.
- Una estrategia de migración y un proceso de transferencia de conocimiento formales.
- Mecanismos para la estabilización y la supervisión del acuerdo por medio de KPI definidos y canales de comunicación y supervisión de estado preacordados.
- Contratos flexibles integrales y acuerdos de nivel de servicio bien definidos.
- Procesos establecidos para la gestión de cambios y riesgos, así como el aseguramiento de calidad de procesos.
- Enfoques correctamente documentados para gestionar procesos de continuidad del negocio, así como la seguridad física, de la información, de las redes y del personal.

Para que el auditor interno determine que la actividad tercerizada se ejecuta en un entorno controlado y planificado en forma adecuada, se deben satisfacer por completo cada uno de los puntos antes mencionados en términos de documentación apropiada y evidencia de operaciones.

Como parte de la operación de tercerización de TI, algunos de los controles del cliente pueden transferirse al proveedor de servicios en forma total o parcial. En esos casos, el alcance de la auditoría va más allá de las operaciones del cliente. Esta sección analiza consideraciones clave de control que deben evaluarse para determinar la eficacia de los controles internos del proveedor de servicios.

1. Entorno de control

Una importante consideración de control es la evaluación del entorno de control de TI del proveedor de servicios. El entorno de control determina el estilo de la organización, influye en el comportamiento del usuario y es la base de otros componentes de control interno. Por ejemplo, determinados aspectos de un entorno de control del proveedor de servicios pueden afectar los servicios prestados al cliente. Los requisitos previos del entorno de control incluyen el uso de pautas, procedimientos y políticas debidamente documentados, así como también una clara definición de los roles y responsabilidades del personal de sistemas de información.

Otro objetivo de esta evaluación es lograr un grado de seguridad razonable respecto de la fuerza que tiene la estructura de gobierno de TI del proveedor de servicios. Por lo tanto, esta evaluación debe analizar los siguientes puntos respecto del proveedor de servicios:

- Estructura y composición del equipo (es decir, ¿el equipo cuenta con las habilidades, las competencias y la experiencia que requieren los servicios prestados?).
- Prestación de servicios conforme a los SLA establecidos.
- Controles de seguridad para toda la información de los clientes.
- Seguridad extrema para todas las redes, extranets e intranets, además de controles de seguridad para todas las actividades y los servicios de Internet, los proveedores de servicios de Internet y las actividades de sitios Web que están vinculados directamente con los centros de datos.
- Retroalimentación de los clientes.
- Copias de seguridad de los datos del cliente.
- Planes de recuperación de desastres y continuidad del negocio.
- Desempeño y tiempo productivo del sistema.

Las organizaciones de servicios también deben llevar a cabo evaluaciones de riesgos periódicas que tengan en cuenta los distintos factores que afectan a los servicios prestados al cliente. Las evaluaciones de riesgos periódicas y estructuradas de las aplicaciones, los sistemas y la infraestructura de TI son un buen indicador de la actitud que adopta el proveedor de servicios frente al entorno de TI, desde una perspectiva de control. Los factores que se deben tener en cuenta al llevar a cabo estas evaluaciones de riesgos incluyen:

- Cambios en el entorno operativo.
- Sistemas de información nuevos o remodelados.
- Crecimiento que incluye, entre otros, el crecimiento organizacional y el crecimiento en los servicios prestados a los clientes.
- Tecnología nueva.
- Actividades, productos o modelos de negocio nuevos.
- Declaraciones contables nuevas.
- Personal nuevo.

Políticas y procedimientos de seguridad de la información

Los proveedores de servicios generalmente cuentan con políticas y procedimientos documentados en relación con varias funciones de seguridad de la información, como por ejemplo:

- Administración de TI. Es decir, gestión de TI, gestión de registros, gestión de documentos, convenciones para las denominaciones de dispositivos, normas de implementación de protocolo de control de transmisión/protocolo de Internet, normas de infraestructura de red, políticas de uso de computadoras e Internet y políticas de correo electrónico.
- Gestión de activos de TI. Es decir, normas de activos de TI, selección de proveedores de TI, evaluación de activos, satisfacción de la instalación de activos y procedimientos de almacenamiento de medios.
- Apoyo y capacitación de TI. Es decir, administración de sistema, centro de asistencia de TI, soporte de red y servidor de TI, resolución de problemas de TI y planes de capacitación para personal y usuarios de TI.

Las organizaciones pueden contar con un equipo de seguridad de la información separado que tenga una estructura organizacional claramente definida y funciones y responsabilidades documentados. El equipo de seguridad de la información establece políticas y procedimientos de seguridad detallados sobre actividades de recuperación de desastres y seguridad de TI, tales como:

- Evaluación de riesgos y amenazas de TI.
- Planificación de seguridad de TI.
- Almacenamiento de medios.
- Recuperación de desastres de TI.
- Presencia de software maligno en la computadora.
- Control de accesos de usuarios.
- Seguridad del correo electrónico.
- Controles de acceso remoto.
- Gestión de seguridad de la red.
- Políticas de contraseñas.
- Pautas de clasificación de datos.
- Auditorías de seguridad de TI.
- Manejo de incidentes de TI.

Las organizaciones de servicios deben garantizar que se formulen, desarrollen y documenten políticas y procedimientos para todas las actividades clave de TI. Las políticas y los procedimientos desarrollados deben comunicarse con claridad a los correspondientes propietarios del proceso y equipos de negocio. Es necesario que haya un proceso para revisar las políticas y los procedimientos en forma periódica y se deben realizar las modificaciones necesarias en función de las condiciones actuales del negocio.

También es vital que haya un proceso de cumplimiento de las políticas y los procedimientos. Una vez formalizados los procedimientos de tercerización, se los debe revisar en forma periódica para garantizar el cumplimiento de las políticas establecidas. También es necesario implementar un proceso concreto para abordar la falta de cumplimiento de políticas y procedimientos, y solucionar los problemas identificados.

2. Consideraciones de seguridad

Para obtener el ROI deseado, los riesgos de seguridad se deben controlar con eficacia. Los tipos de riesgo de seguridad más

importantes que se deben abordar en cualquier contexto de tercerización de TI incluyen:

- Protección de la información.
- Seguridad de la red.
- Seguridad física.
- Seguridad del personal.
- Controles de acceso lógico a las aplicaciones.

Riesgos de protección de datos

Los datos son un componente esencial del negocio y deben tratarse como un activo corporativo importante. La información no se limita a papeles y documentos; incluye los datos que residen en servicios y software de aplicación, información de empleados, registros de investigación, listas de precios y contratos. Para proteger los activos de datos, las compañías deben:

- Identificar qué riesgos de seguridad pueden afectar a la organización.
- Establecer políticas y procedimientos que se ocupen de áreas clave, como uso aceptable, clasificación de la información, acceso de terceros, transmisión de datos y acceso remoto a los datos, y políticas de acceso de usuarios y contraseñas.
- Respaldar las políticas con las pautas, las plantillas y los procedimientos necesarios.
- Lograr que la alta dirección se comprometa con la iniciativa de seguridad de la información. Esto demuestra la presencia de un sólido equipo operativo que comprende las amenazas que implican los problemas de seguridad. Demuestra además la capacidad que tiene la organización de supervisar y tratar estos puntos vulnerables y problemas de seguridad.

Seguridad de la red

Las organizaciones pueden tomar diversas medidas para proteger sus redes, el lugar donde se almacena y transmite la información. Para garantizar la seguridad de sus redes, se deben incluir los siguientes elementos de seguridad como parte de los esfuerzos de protección de datos de la organización:

- Documentación, diseño e implementación adecuados de la red.
- Configuración de los filtros de seguridad para denegar el acceso al tráfico no autorizado.
- Separación física y lógica de la red de cliente y la red de área local del proveedor de servicios.
- Instalación de software antivirus en todos los servidores y sistemas.
- Uso de actualizaciones regulares de firma de antivirus.
- Medidas para impedir el acceso no autorizado a la red o los datos de la compañía.
- Conexión segura y encriptación.
- Seguridad de sistemas operativos y software de red.
- Políticas para control de accesos y autenticación.
- Protección del puerto de diagnóstico remoto.
- Control de la conexión de red.
- Control de enrutamiento de la red.
- Sistemas de detección de intrusiones.

Controles de seguridad física y entorno

La seguridad física hace referencia a los medios utilizados para proteger un objeto o un lugar, como por ejemplo, el edificio de la compañía, las áreas de trabajo, los sistemas y dispositivos utilizados y los documentos. Según el tipo de actividad tercerizada, las organizaciones cliente deben garantizar que los documentos, los sistemas y la infraestructura del proveedor de servicios estén correctamente protegidos.

Muchas organizaciones están exigiendo niveles de seguridad más altos en las instalaciones de tercerización, especialmente cuando la actividad que se terceriza es fundamental para el éxito de las operaciones de la organización. Las medidas clave de seguridad incluyen:

- Presencia, las 24 horas, de guardias de seguridad capacitados provenientes de agencias de seguridad profesionales y controles físicos de ingreso, como:
  - Autorización de acceso y mecanismos de identificación (por ejemplo, tarjetas de identificación y tarjetas magnéticas).
  - Restricción de acceso, en función de las necesidades, a las áreas destinadas al procesamiento de clientes y a la entrega de servicios. Estas áreas deben contar con sus propias estaciones de trabajo especializadas, su red informática y su infraestructura (por ejemplo, líneas telefónicas, servidores de impresión y archivo, e impresoras).
  - Un sistema de seguimiento de entrada y salida para garantizar que los visitantes cuenten con las identificaciones correspondientes y que se verifiquen sus pertenencias.
  - Acceso restringido adicional a las salas de servidores y a los centros de datos.
  - Una planta especializada supervisada por televisión de circuito cerrado, las 24 horas del día, los siete días de la semana para impedir y controlar cualquier tipo de actividad sospechosa en lugares críticos (por ejemplo, el centro de datos, la sala de la red, la entrada del edificio y las áreas de fabricación).
  - Traslado restringido de medios (por ejemplo, discos compactos, disquetes y unidades de memoria flash) y papeles, controlados mediante inspección física y autorización en los pases de entrada.
- Uso de trituradoras de papel ubicadas en diferentes lugares para desechar datos y documentos. Esto ayuda a garantizar que los datos y los documentos confidenciales no se almacenen o trasladen fuera del edificio.
- Almacenamiento de los medios de respaldo que contienen datos críticos en gabinetes a prueba de fuego, dentro y fuera de la organización.
- Uso de sistemas contra incendio, como detectores de humo.

Seguridad del personal

La seguridad del personal hace referencia a los procedimientos implementados en la compañía para garantizar que todo el personal que tiene acceso a información confidencial o a un determinado lugar cuente con la autoridad y los poderes requeridos. La evaluación de la seguridad del personal debe incluir los siguientes puntos:

- Comprobaciones detalladas de antecedentes de empleados potenciales para identificar verificaciones de referencias de empleadores anteriores, verificaciones de antecedentes penales y calificaciones escolares. Las comprobaciones de antecedentes también podrían verificar otros aspectos, como por ejemplo, el entorno social de la persona. A pesar de que la mayoría de las organizaciones prefieren realizar internamente las verificaciones de las referencias del empleado, esta tarea se puede tercerizar a una agencia local especializada.
- Acuerdos de confidencialidad obligatorios para todos los empleados. La mayoría de los socios de tercerización cuentan con un acuerdo de confidencialidad estándar que determina las penas por su incumplimiento, como por ejemplo, la rescisión de los servicios.
- Uso de impresoras y fotocopiadoras en base a las necesidades. Muchos proveedores de servicios protegen sus fotocopiadoras con personal y realizan un seguimiento de los empleados, la cantidad de páginas y la información impresa o fotocopiada.
- Registros de trabajo y acceso de cada empleado.
- Controles de acceso a Internet. Algunos proveedores de servicios cuentan con cibercafés fuera del área de procesamiento de clientes para uso de los empleados.
- Herramientas que escanean todos los mensajes de correo electrónico internos, prohíben el acceso a mensajes de correo electrónico externos y escanean los mensajes de correo electrónico en busca de palabras críticas y límites de tamaño.
- Gestión de contraseñas, como por ejemplo, confidencialidad, programas de cambios regulares e inicio de sesión único donde se requieren accesos múltiples.
- Identificación de terminal automático, procedimientos de inicio de sesión de terminal, e identificación y autenticación de usuarios.

Acceso lógico

El acceso restringido y los controles de aplicación con contraseña son fundamentales para evitar el acceso no autorizado a lugares donde se almacena o procesa la información confidencial. Esto puede requerir que se restrinja el acceso a elementos de datos específicos de acuerdo con el rol y las responsabilidades de una persona, que se impida el acceso a otra información confidencial o que se restrinjan determinadas transacciones a determinados usuarios.

Entre las consideraciones clave del acceso lógico, se encuentran:

- Verificar que se implementen los requerimientos de seguridad especificados en el contrato, como por ejemplo, las especificaciones reglamentarias.
- Preparar regularmente informes sobre las violaciones de seguridad, como por ejemplo, intentos de acceso no válidos.
- Utilizar pruebas independientes para verificar que no se puedan violar los niveles de seguridad, como por ejemplo, realizar pruebas de penetrabilidad de las redes de TI y los sitios Web.
- Restringir el acceso a datos confidenciales o a determinadas transacciones para el personal clave.
- Auditar la tecnología y los procesos utilizados para impedir el acceso no autorizado a los registros del cliente en los casos en los que el proveedor brinde servicios de operaciones de TI a varios clientes. Esto puede requerir la asistencia de especialistas.

Además, es necesario prestar especial atención a los controles de acceso lógico de aplicaciones, bases de datos y sistemas operativos críticos, como por ejemplo:

- Un proceso formal para la gestión de cuentas, es decir, controles administrativos y de usuarios para sistemas críticos como los sistemas operativos, los sistemas de aplicación y las bases de datos.
- Pistas de auditoría para realizar un seguimiento de la creación de cuentas de usuario y la autorización de acceso para dichas cuentas.
- Un proceso de revisión formal de las cuentas de usuarios regulares en los sistemas operativos, las bases de datos y las aplicaciones que respaldan una función crítica, para garantizar que se brinde acceso lógico únicamente a los usuarios autorizados.

Por último, al utilizar servicios Web, se deben tener en cuenta los siguientes requerimientos de seguridad:

- Protección de filtro de seguridad con reglas y restricciones de acceso a la red interna y a las aplicaciones a las que se accede a través de un navegador de Internet.
- Software anti-spam para evitar direcciones de correo electrónico no autorizadas o descargas de software en la red.
- Instalación de software de protección antivirus para detectar y proteger contra virus los mensajes de correo electrónico o las descargas de Internet.
- Actualizaciones regulares de software antivirus para garantizar que se detecten virus nuevos.
- Controles de autenticación para las aplicaciones que residen fuera de la red (por ejemplo, uso de tarjetas inteligentes y certificados digitales).

Continuidad del negocio

La gestión de continuidad del negocio (BCM, en inglés) es un enfoque empresarial basado en riesgos para desarrollar medidas proactivas que garanticen la disponibilidad continua de los sistemas de respaldo del negocio y mitigar los riesgos de interrupciones. Tal como se indica en la figura 2, la BCM ayuda a las organizaciones a maximizar la disponibilidad, la confiabilidad y la capacidad de recuperación de los sistemas de negocio a través de la gestión eficaz de las personas, los procesos y la tecnología. Además, mejora la capacidad que tiene la organización para recuperarse de un desastre, minimizar las pérdidas y de contar con el mejor nivel de preparación para manejar interrupciones en el negocio y restaurar las operaciones. Ante la ausencia de un plan de este tipo, la organización podría sufrir pérdidas de ingresos a largo plazo y perder la confianza de los clientes.

Las pautas y políticas de continuidad del negocio son un componente crítico del contrato de tercerización y deben detallarse claramente en los SLA que se ocupan de:

- Mecanismos de la BCM.
- Tiempos de respuesta basados en el tipo de proceso tercerizado.
- Tipos de auditorías requeridos, así como también la ubicación de la auditoría, la frecuencia, el costo, la persona a cargo de la auditoría y la información que compartirán las partes.

- Sanciones al proveedor de servicios por su incapacidad para restablecer las operaciones de negocio durante y después de un desastre, según lo definido en el SLA.

El alcance y los aspectos operativos de la BCM generalmente difieren en función del grado de aceptación de riesgo de la organización, el nivel de importancia de la actividad y los proyectos tercerizados, y la dependencia general de las operaciones en la TI. Los planes de continuidad del negocio deben identificar:

- Fuentes potenciales de interrupción.
- Aplicaciones y procesos críticos y niveles aceptables de tiempo improductivo a través de un análisis de impacto en el negocio.
- Tiempos de recuperación y respuesta aceptables.
- Mecanismos de la BCM, como por ejemplo:
  - Ubicaciones y mecanismos de almacenamiento (por ejemplo, cintas, servidores fuera de la organización y series redundantes de discos independientes).
  - Frecuencia de las copias de seguridad de datos.
  - Creación de sitios alternativos.
  - Disponibilidad de infraestructura de equipos y redes.
  - Puntos de acceso a varias empresas de telecomunicaciones.
- Responsabilidades del personal en función del alcance de la interrupción y la naturaleza del proceso afectado.
- Las personas responsables del proceso de continuidad del negocio.
- Pruebas y actividades de mantenimiento del plan de continuidad del negocio.

Por lo tanto, los siguientes aspectos son críticos durante el proceso de BCM:

- Revisiones de la BCM del proveedor de servicios y planes de recuperación de desastres para garantizar que las interrupciones que se presenten en sus instalaciones, en su personal o en sus sistemas no perjudiquen los sistemas del cliente.
- Revisiones de la BCM del proveedor de servicios y planes de prueba de recuperación de desastres, e informes de las pruebas.
- Comprender la función que cumplen la BCM y las pruebas de recuperación de desastres al garantizar que los planes del proveedor de servicios son eficaces para los sistemas del cliente.

3. Controles del SDLC

Los controles del SDLC deben aplicarse a todas las aplicaciones nuevas desarrolladas o adquiridas por el proveedor de servicios, o bien durante mejoras importantes o actividades de mantenimiento realizadas a las aplicaciones existentes. Para reducir los riesgos de adquisición e implementación, las organizaciones pueden utilizar un desarrollo de sistema específico o un proceso o metodología de aseguramiento de calidad que sea compatible con componentes de arquitectura de TI y herramientas de software estándar. Este proceso brinda una estructura para identificar:

- Soluciones automatizadas.
- Actividades de implementación y diseño de sistemas.
- Requerimientos de documentación.

Gestión de continuidad del negocio			
Aspectos abordados	Disponibilidad	Confiabilidad	Capacidad de recuperación
Solución	Alta disponibilidad empresarial	Gestión de nivel de servicio	Alta disponibilidad empresarial
Objetivos	Alcanzar y mantener el nivel elegido de disponibilidad de infraestructura de TI de la empresa.	Gestionar y controlar con eficacia la infraestructura de TI para mejorar la confiabilidad operativa general.	Proporcionar un plan eficaz para minimizar el tiempo improductivo de los procesos clave ante una interrupción importante.
Énfasis	Tecnología	Procesos	Personas
Foco	Proactivo y preventivo		Respuesta y recuperación

Figura 2: Descripción del proceso de BCM.

- Pruebas, aprobaciones, gestión de proyectos y requerimientos de supervisión.
- Evaluaciones de riesgos de proyectos.

Lo ideal sería que las organizaciones de servicios conserven evidencias que demuestren que los siguientes procedimientos se siguen para todas las adquisiciones y los desarrollos nuevos, debido a que pueden tener un impacto directo en la prestación de servicios al cliente. Los componentes clave de la metodología incluyen:

- Definición del proyecto de TI y gestión de proyecto.
- Análisis de sistemas.
- Diseño de software, programación, documentación, pruebas, versiones y actualizaciones.
- Planificación de la infraestructura.
- Cambios de diseño durante el desarrollo.
- Procedimientos de protección de seguridad de la información.
- Revisiones de código.
- Procedimientos de migración de datos.
- Capacitación de usuarios finales.

4. Consideraciones de los controles de gestión del cambio

El mantenimiento de las aplicaciones se ocupa tanto de las actividades permanentes de gestión del cambio como de las nuevas versiones de software. Es necesario contar con controles de sistema adecuados para garantizar que todos los cambios se realicen correctamente. Los controles pueden incluir el uso de autorizaciones de solicitudes de cambio, revisiones, aprobaciones, documentación y prueba, así como también evaluaciones de cambios en otros componentes de TI y protocolos de implementación.

El proceso de gestión del cambio, además, debe estar integrado con otros procesos de TI, como por ejemplo, gestión de incidentes, gestión de problemas, gestión de disponibilidad y control de cambio de la infraestructura. Desde el punto de vista de una auditoría, el proveedor de servicios debe ser capaz de suministrar evidencia de que los cambios se basan únicamente en las solicitudes autorizadas.

5. Políticas y procedimientos de recursos humanos

El éxito de la tercerización depende de la tecnología y de las personas. Por lo tanto, para que los controles diseñados se implementen con éxito y funcionen con eficacia, es importante la evaluación de las políticas y los procedimientos de recursos humanos. Las consideraciones de revisión clave en esta área son:

- La aceptación y promoción de la cultura de gestión de integridad de la compañía, que incluye la ética de la organización, las prácticas de negocio y las evaluaciones de recursos humanos.
- Revisiones de los incentivos de los empleados para garantizar que no se vean forzados a implementar prácticas injustas o no éticas para cumplir con metas de desempeño poco realistas, especialmente para resultados a corto plazo.
- Uso de prácticas de contratación adecuadas, como especificación de los requerimientos de trabajo, procedimientos de publicación de trabajos, manejo de las solicitudes de empleo, entrevistas, comprobaciones de antecedentes, ofertas de trabajo y orientaciones para empleados nuevos.
- Captación, análisis y revisión de patrones de rotación de empleados en busca de fraude potencial o connivencia.

6. Consideraciones de auditoría interna

Al principio, muchas organizaciones no estaban muy dispuestas a tercerizar sus servicios ya que temían perder control. Por ello es importante contar con un sólido entorno de control de tercerización, especialmente en el lado del proveedor de servicios. Es necesario comprender y evaluar los aspectos de control que se analizan en este capítulo en todos los procesos de terceros, en función del tipo de servicios que se tercerizan y de su complejidad.

El auditor interno desempeña una función crítica en la evaluación del entorno de control del proveedor de servicios. Por consiguiente, los auditores deben evaluar la solidez de las actividades y el enfoque de control que afectan a los procesos tercerizados, además de informar la gestión sobre la eficacia de las operaciones de tercerización desde el punto de vista del cumplimiento y de las operaciones. Para ello, los auditores deben evaluar y probar las políticas, los procedimientos, las pautas, las evaluaciones de riesgos y las actividades de supervisión del control del SDLC del proveedor de servicios, además de obtener información independiente a través de los canales de comunicación establecidos. Los auditores también pueden confiar en las normas internacionales adoptadas por el proveedor de servicios para el cumplimiento, como por ejemplo, del uso de los informes SAS 70 y evaluar la documentación del proveedor de servicios para identificar si los controles se personalizaron para adaptarse al entorno exclusivo del cliente.

Al tercerizar una solución de TI, las compañías se enfrentan al riesgo de que la información confidencial de los clientes termine bajo custodia del proveedor de servicios. La pérdida de la integridad o la confidencialidad de los datos, así como también el uso no autorizado y la alteración de los datos del cliente, podrían resultar en multas o pérdida de la reputación. Las vulneraciones de los datos también podrían resultar en violaciones a la seguridad y la privacidad, tal como lo indican regulaciones como la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (HIPAA, en inglés), la Ley Gramm-Leach-Bliley (GLBA, en inglés) y la Ley de Protección de Datos de la UE, según el tipo de trabajo de la compañía y el país donde realice sus operaciones.

A pesar de que se pueden adoptar diferentes enfoques para supervisar la eficacia de las actividades tercerizadas, el contrato es el enfoque más importante en la revisión del trabajo y el cumplimiento de un proveedor de servicios. A continuación, se describen las principales regulaciones que tanto los proveedores de servicios como las organizaciones deben tener en cuenta o cumplir durante el período que dure la relación de tercerización.

Normas de cumplimiento

a) HIPAA

La HIPAA se aplica a las organizaciones estadounidenses que trabajan en la industria de los servicios de salud. Es obligatorio el cumplimiento de la HIPAA para todas las transacciones electrónicas relacionadas con la salud, como reclamos, formularios de inscripción, pagos y coordinación de beneficios. La norma se ocupa además de la seguridad y la privacidad de los datos y los sistemas de información electrónicos de salud. Incluye políticas y procedimientos para:

- Proteger la privacidad de la información electrónica.
- Impedir el acceso no autorizado a la información de servicios de salud y su divulgación.
- Mantener pistas de auditoría en sistemas de registro computarizados.

Los proveedores de servicios que brindan servicios de TI a las organizaciones de la industria de los servicios de salud deben cumplir con la HIPAA. Para cumplir con la regulación, el proveedor de servicios debe garantizar que:

- Se incorporen los requerimientos clave de cumplimiento en el contenido de la capacitación estándar. En muchos casos, el contenido de la capacitación lo provee directamente el cliente.
- Los empleados de servicio que trabajan en la cuenta reciban capacitación sobre las secciones pertinentes de la norma.
- El área de trabajo y la red que se utilizan para procesar la información de servicios de salud se encuentren en un lugar separado para evitar el acceso no autorizado a los datos del cliente.
- Se implementen controles y seguridad de red para proteger las transmisiones de datos, incluso el uso de redes separadas en túnel, filtros de seguridad y configuración del servidor proxy que:
  - Definan las reglas de acceso y tráfico.
  - Admitan la encriptación.
  - Controlen el acceso en función de reglas definidas.
  - Mantengan registros, revisiones y procedimientos de gestión de incidentes para las violaciones informadas.

b) GLBA

Esta ley se aplica a las instituciones financieras que brindan productos y servicios financieros a clientes, como por ejemplo:

- Préstamos, corretaje o cualquier tipo de empréstito al consumidor.
- Transferencia o protección de dinero.
- Preparación de declaraciones juradas de impuestos individuales.
- Asesoramiento financiero y asesoría crediticia.
- Servicios de liquidación de bienes raíces.
- Cobranza de deudas de consumidores.

En cualquier servicio de TI que sea tercerizado por una institución financiera, el proveedor de servicios debe cumplir con los requerimientos de la ley. Además de obtener la capacitación y educación adecuada sobre los requerimientos de la ley, el proveedor de servicios debe garantizar que:

- El área de trabajo y la red que se utilizan para procesar la información financiera se encuentren en un lugar separado para evitar el acceso no autorizado.
- Se implementen medidas de seguridad en el almacenamiento y el procesamiento de datos. Esto incluye restringir el uso de los dispositivos móviles (por ejemplo, teléfonos móviles, cámaras y asistentes personales digitales), los dispositivos de almacenamiento externo (por ejemplo, discos compactos y unidades de memoria flash) y los dispositivos de salida (por ejemplo, impresoras y máquinas de fax) para impedir la transmisión no autorizada de datos y registros.
- Se implementen controles y seguridad de red para proteger las transmisiones de datos, incluso el uso de redes separadas en túnel, filtros de seguridad y configuración del servidor proxy que:
  - Definan las reglas de acceso y tráfico.
  - Admitan la encriptación.
  - Controlen el acceso en función de reglas definidas.
  - Mantengan registros, revisiones y procedimientos de gestión de incidentes para las violaciones informadas.

c) Regulaciones adicionales

Para garantizar la protección de los datos, las normas más aceptadas son la Ley de Protección de Datos del Reino Unido de 1998 y la Directiva sobre protección de datos (95/46/EC) de la UE. La Ley de Protección de Datos del Reino Unido impone disposiciones que tratan la manera de procesar información personal identificable, como su obtención, conservación, uso o divulgación. Los requerimientos de seguridad que debe poner en práctica el proveedor de servicios para el cumplimiento son los mismos que los descritos anteriormente para la HIPAA y la GLBA.

Otros enfoques y pautas disponibles

Las organizaciones que tercerizan servicios a otras empresas

deben asegurarse de que el enfoque de control y la estructura de gobierno del proveedor de servicios puedan garantizar la confidencialidad, integridad y disponibilidad de sus datos y sistemas, a los que puede acceder el personal del proveedor de servicios. Una medida para verificar la eficiencia de los procesos utilizados es examinar si están certificados por una norma internacional reconocida, como la Organización Internacional de Normalización (ISO, en inglés), la Norma 2007 de la Comisión Electrotécnica Internacional (IEC, en inglés), Six Sigma, the Customer Operations Performance Center Inc., la Norma británica (BS, en inglés) 7799 y el Modelo de madurez de capacidad del Instituto de Ingeniería de Software (SEI, en inglés) de la Universidad de Carnegie Mellon.

Un equipo especializado de la compañía de tercerización (por ejemplo, un grupo de auditoría interna) puede encargarse de realizar revisiones periódicas y de supervisar el enfoque de control interno y las políticas y los procedimientos del proveedor de servicios. No obstante, debido al impacto de la Ley Sarbanes-Oxley y legislación similar, muchas organizaciones están comenzando a utilizar los servicios de los auditores externos y de otros terceros para realizar evaluaciones del trabajo y la eficiencia de los controles internos del proveedor de servicios. Estos revisores independientes también proporcionan evaluaciones independientes que pueden utilizar tanto el proveedor de servicios como su equipo de auditoría.

Cuando una organización utiliza una organización de servicios, las transacciones que afectan los estados contables del cliente están sujetas a controles que pueden separarse física y operativamente del cliente. La importancia de los controles que tiene el proveedor de servicios sobre estas transacciones del cliente depende de la naturaleza de los servicios tercerizados, la naturaleza y materialidad de las transacciones procesadas y el grado de interacción entre las actividades del cliente y las del proveedor de servicios. Deben evaluarse los controles aplicados en la operación por parte de la organización cliente y el proveedor de servicios para identificar posibles inexactitudes y para diseñar pruebas de control.

Al igual que sus clientes, muchos proveedores de servicios están obteniendo certificación en diferentes enfoques y están cumpliendo diversas normas para ganar aceptación en el área internacional. El cumplimiento demuestra un compromiso de brindar servicios de alta calidad, lo que además ayuda a distinguir a los proveedores de servicios durante el proceso de selección de los mismos. Debido a que la certificación se debe mantener una vez que se logra, las organizaciones certificadas demuestran su compromiso de mantener altos niveles de servicios que coincidan con los requerimientos de cumplimiento del enfoque. A continuación, presentamos algunos de los enfoques y pautas más aceptados que se encuentran disponibles para probar y evaluar la eficacia de los controles.

a) SAS 70

La SAS 70 es una norma de auditoría desarrollada por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA, en inglés). La norma permite que los proveedores de servicios obtengan aseguramiento independiente sobre sus objetivos y procesos de control. La SAS 70 generalmente es utilizada por los auditores que revisan los estados contables de una organización que obtiene servicios de otra organización.

La SAS 70 no incluye un conjunto predeterminado de objetivos de control o actividades que deben alcanzar las organizaciones de servicios; sino que las partes involucradas deben negociar los objetivos de control que se incluirán en el informe SAS 70. Tenga en cuenta que a medida que aumenta el tamaño del proveedor de servicios, se torna más difícil para la organización de servicios adaptar su informe SAS 70 existente para satisfacer las necesidades de la organización cliente.

Informes SAS 70

El informe SAS 70 es más conocido como el Informe del auditor de servicios. Lo emite un auditor independiente a la organización de servicios al finalizar con la SAS 70 y ofrece una descripción de los controles del proveedor de servicios. El Informe del auditor de servicios es además una de las maneras más eficaces que tiene una organización de servicios para comunicar información acerca de sus controles. Existen dos tipos de Informes del auditor de servicios: el Tipo I y el Tipo II.

El informe del Tipo I describe los controles del proveedor de servicios en un momento determinado (por ejemplo, el 30 de junio de 2006). Un informe del Tipo II describe los controles del proveedor de servicios e incluye información detallada de pruebas de los controles de terceros en un período mínimo de seis meses (por ejemplo, desde el 1 de julio de 2006 hasta el 31 de diciembre de 2006). Conforme a la Ley Sarbanes-Oxley, un informe del Tipo II se ha convertido en un requerimiento de facto debido a la necesidad de evaluar tanto el diseño como la eficacia operativa de los controles internos, conforme a la Norma de Auditoría N.º 2.

En 2006, el Instituto de Contadores Certificados de Inglaterra y Gales emitió los AAF 01/06: Informes de aseguramiento sobre controles internos de las organizaciones de servicios disponibles para terceros. El informe AAF 01/06 es similar al SAS 70 y sirve de guía para los contadores que están a cargo de brindar aseguramiento sobre los controles internos de una organización de servicios.

b) SysTrust®

El servicio de aseguramiento SysTrust® fue desarrollado por AICPA y el Instituto Canadiense de Contadores Certificados. Su enfoque se centra en aumentar la confianza de la dirección, los clientes y los socios de negocio respecto de los sistemas que respaldan una organización o una determinada actividad.

El servicio SysTrust® describe diferentes criterios que pueden ayudar a las organizaciones a brindar aseguramiento sobre la confiabilidad del servicio de sus sistemas. Estos criterios incluyen:

- Disponibilidad. Es decir, un sistema debe estar disponible para el funcionamiento y la utilización en los momentos establecidos en los acuerdos de nivel de servicio.
- Seguridad. Es decir, un sistema debe estar protegido contra acceso físico y lógico no autorizado.
- Integridad de procesamiento. Es decir, el procesamiento del sistema debe ser completo, preciso, oportuno y autorizado.
- Capacidad de mantenimiento. Es decir, los sistemas se pueden actualizar cuando sea necesario para poder continuar ofreciendo disponibilidad, seguridad e integridad.

Cada uno de los principios y sus criterios relacionados están organizados en cuatro áreas de revisión:

- Política. Es decir, la organización debe definir y documentar las políticas que sean pertinentes para el principio particular.
- Comunicaciones. Es decir, la organización debe comunicar las políticas definidas para los usuarios autorizados.
- Procedimientos. Es decir, la organización debe utilizar los procedimientos para lograr sus objetivos de acuerdo con sus políticas definidas.
- Supervisión. Es decir, la organización debe supervisar el sistema y tomar medidas para seguir cumpliendo con las políticas definidas.

El objetivo de SysTrust® es ayudar a que los auditores independientes evalúen la administración, que hace la dirección, de los controles relacionados con los servicios que brinda SysTrust®. La función del auditor es determinar si existen controles del sistema y llevar a cabo pruebas para determinar si estos controles están funcionando con eficacia durante el período cubierto por el informe.

c) BS 7799 and ISO/IEC 27001

La BS 7799 se emitió por primera vez en 1995 para brindar un conjunto integral de controles compuesto por mejores prácticas de seguridad de la información. Los objetivos de la norma son proteger la confidencialidad, la integridad y la disponibilidad de la información. Esto es, la esencia de la seguridad de la información.

Si bien es similar a la BS 7799, la ISO/IEC 17799: 2000 Gestión de Seguridad de la Información fue desarrollada por un grupo de profesionales de seguridad de la información de diferentes industrias. La norma indica mejores prácticas de seguridad de la información que todas las organizaciones, independientemente de su tamaño, deben tener en cuenta e implementar, cuando corresponda. La certificación de BS7799 se emite en dos partes:

- Parte 1: Código de práctica para la gestión de seguridad de la información.
- Parte 2: Especificación para los sistemas de gestión de seguridad de la información.

La BS 7799-1:1999, o Parte 1, ha sido aprobada como la norma de seguridad internacional utilizada en ISO/IEC 17799. Su enfoque se centra en la protección de la información de una organización y en los mecanismos para crear, editar, transmitir y almacenar información. La norma cuenta con dos objetivos establecidos:

- Proporcionar un medio objetivo para medir o comparar mejores prácticas en gestión de seguridad de la información.
- Fomentar la confianza en la comercialización electrónica entre compañías.

La BS 7799-2: 2002 Especificación para los sistemas de gestión de seguridad de la información, o Parte 2, se desarrolló más tarde para ayudar a las organizaciones a prepararse debidamente para la certificación acreditada según la BS 7799. Se considera que tanto la Parte 1 como la Parte 2 conforman una colección integral de mejores prácticas de seguridad de la información mediante la cual las organizaciones pueden evaluar sus entornos de controles y seguridad.

El organismo de certificación, conocido como el Servicio de Acreditación del Reino Unido (UKAS, en inglés), emitió una declaración de transición de la BS 7799-2: 2002 a la ISO/IEC 27001. Las organizaciones acreditadas deben considerar la transición a la ISO/IEC27001 antes de julio de 2007.

En el año 2005, la ISO y la IEC emitieron la Norma 27001: 2005, que reemplazó a la BS 7799-2: 2002. La norma nueva es una versión nueva ampliada y adaptada de la BS 7799-2 y especifica los requerimientos para la certificación del sistema de gestión de seguridad de la información. Entre sus características distintivas, la nueva norma introdujo un nuevo campo para la seguridad, conocido como gestión de incidentes para la seguridad de la información y un total de 17 controles nuevos.

d) Objetivos de Control de Información y Tecnologías Relacionadas (CobiT)®

El enfoque CobiT del Instituto de Gobierno de TI (ITGI, en inglés) fija un conjunto de objetivos de control para el gobierno eficaz de la TI. Los CobiT además ayudan a las organizaciones a implementar los requerimientos necesarios para garantizar la eficacia, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información. Los procesos de TI de los CobiT se definen en cuatro campos: planificación y organización, adquisición e implementación, entrega y asistencia, y supervisión.

Se definen procesos y objetivos de control para cada uno de los cuatro campos, que se pueden adoptar como mejores prácticas para diseñar un enfoque eficaz. Específicamente, los CobiT proporcionan modelos de madurez para controlar los procesos de TI de manera que la dirección pueda trazar un mapa de sus niveles de madurez de control actuales, dónde se encuentra con respecto a las mejores organizaciones de su tipo y dónde desea estar. Los modelos de madurez describen:

i. Factores de éxito críticos que definen importantes pautas de implementación orientadas a la gestión para lograr el control sobre los procesos de TI y dentro de ellos.
ii. Indicadores clave de objetivos, que definen las medidas mediante las cuales la dirección puede identificar si el proceso de TI ha alcanzado los requerimientos del negocio.
iii. Indicadores claves de desempeño (KPI, en inglés) que sirven como los principales indicadores para determinar en qué medida el proceso de TI está haciendo posible la concreción de las metas.

e) La Biblioteca de Infraestructura de TI (ITIL, en inglés) de la Oficina de Comercio de Gobierno (OGC, en inglés) del Reino Unido

ITIL es otro enfoque global sobre la gestión y el gobierno de TI. Se trata de un enfoque de mejores prácticas de operaciones y servicios de TI que ayuda a las organizaciones a alinear su negocio con sus actividades de TI. OGC creó la ITIL a mediados de la década de 1980 para las compañías que buscaban administrar sus entornos de TI con mayor eficacia. Uno de los principales motivos por los que muchas organizaciones utilizan la ITIL es su libertad. La ITIL no exige a las organizaciones que implementen todas las especificaciones de los enfoques.

El libro de Asistencia de servicio (Service Support, en inglés) de la ITIL ayuda a las organizaciones a definir sus principales funciones de servicio de TI. De acuerdo con el libro, la función de un servicio de TI es ofrecer servicios en forma ininterrumpida y de la mejor manera posible a los usuarios. El libro define además cinco procesos: gestión de incidentes, gestión de problemas, gestión de configuración, gestión del cambio y gestión de versión, que describen cómo gestionar con eficacia los servicios de software, hardware y recursos humanos y cómo garantizar actividades de negocio continuadas e ininterrumpidas.

Consideraciones de auditoría interna

A medida que la tercerización continúa evolucionando hacia un modelo de entrega de servicios más global, es importante que los auditores internos estén al tanto de los enfoques de control utilizados en todo el mundo. Esto permite que los auditores se mantengan informados sobre las decisiones de los enfoques que mejor satisfacen las necesidades de las organizaciones cliente, de acuerdo con el tipo de trabajo, las actividades que se tercerizan y los diferentes tipos y niveles de riesgos. Los auditores internos también cumplen una función clave en la recomendación y evaluación de diferentes enfoques de control de TI y las opciones disponibles para su implementación.

Por consiguiente, los auditores internos deben evaluar la eficiencia de los procesos de revisión de certificación de la organización y diseñar un programa de auditoría destinado al enfoque específico que se evalúa. Los resultados de la auditoría ayudarán a las organizaciones cliente a determinar en qué medida pueden confiar en las actividades del proveedor de servicios, de acuerdo con la certificación obtenida.

Los factores que se deben tener en cuenta al evaluar la eficacia del proceso de revisión y la certificación incluyen:

1. La reputación y competencia de la organización que llevó a cabo la revisión y otorgó la certificación.
2. El período de cobertura de la revisión (es decir, el período de revisión debe ser actual y estar dentro del período financiero del cliente).
3. El enfoque de control definido (es decir, el control, los objetivos y los procesos de control deben abarcar los procesos y las operaciones de TI que se tercerizan, además de incluir los controles que desea el cliente y que exigen los requisitos reglamentarios).
4. Resultados de la revisión (es decir, la eficiencia del diseño de control para cumplir con los objetivos y la eficacia operativa durante el período cubierto por la revisión). Los resultados de la revisión deben indicar las excepciones, el coeficiente de riesgo de las excepciones en base a su impacto, la respuesta de la dirección y el tiempo que destina la dirección para implementar las medidas correctivas. En el caso de las excepciones de alto riesgo, los informes de auditoría deben documentar las medidas correctivas implementadas para garantizar la eficacia del programa.

10 preguntas principales que debe formular el DEA

1. ¿Los servicios tercerizados son importantes para el cliente?
2. ¿El cliente cuenta con una estrategia de tercerización bien definida?
3. ¿Cuál es la estructura de gobierno relacionada con las operaciones tercerizadas? ¿Los roles y responsabilidad están definidos con claridad?
4. ¿Se llevó a cabo un análisis de riesgo detallado al momento de la tercerización y se continúa realizando regularmente?
5. ¿Existen contratos formales o SLA para las actividades tercerizadas?
6. ¿El SLA define claramente los KPI para supervisar el desempeño del proveedor?
7. ¿Cómo se supervisa el cumplimiento del contrato o SLA?
8. ¿Cuál es el mecanismo utilizado para tratar el incumplimiento del SLA?
9. ¿Las responsabilidades de propiedad del sistema de datos, del sistema de comunicación, del sistema operativo, del software utilitario y del software de aplicación se definieron claramente y se acordaron con el proveedor de servicios?
10. ¿Cuál es el proceso para obtener aseguramiento de la eficacia operativa de los controles internos del lado del proveedor de servicios?

A pesar de que la tercerización de TI es una práctica de gestión consolidada, los permanentes y rápidos cambios de la industria han determinado la presencia de tendencias. A continuación, se presentan algunas de las tendencias más notables en el terreno de la tercerización de TI.

- El desarrollo de aplicaciones sigue siendo una de las actividades de TI más tercerizadas. En segundo lugar, están el mantenimiento y la asistencia técnica de las aplicaciones. Se espera que esta tendencia continúe en un futuro cercano. Los proveedores de servicios continúan desarrollando sus habilidades y sus capacidades en esta área y tienen grandes expectativas de crecimiento en la categoría de servicios gestionados, especialmente en las áreas de gestión de bases de datos y gestión de redes.

- Los mega acuerdos de más de USA 1.000 millones representan una proporción importante del valor total de los contratos de tercerización, que tuvo un promedio de US$ 25.300 millones por año entre 2003 y 2005. No obstante, se espera que en un futuro cercano disminuya la cantidad de mega acuerdos y aumenten los acuerdos medianos y grandes que se encuentran dentro del rango de US$100 millones a US$999 millones1. Se espera que esta tendencia genere más competencia en el terreno de los proveedores de servicios, ya que tanto los actores grandes como los medianos comienzan competir entre sí.

- A pesar de que hubo un mayor énfasis en el modelo de relación de tercerización, los plazos de los contratos están disminuyendo. La investigación indica que la duración promedio de un contrato de tercerización de TI descendió de 6,2 años a 5,3 años entre 2003 y 2005. Esto se atribuye a experiencias negativas con los proveedores en los acuerdos de tercerización de primera generación que se implementaron de manera apresurada para obtener ahorros estratégicos. La tendencia es que las organizaciones tengan flexibilidad y no estén limitadas a un determinado servicio.

- Los ahorros continúan siendo el factor condicionante clave de la tercerización de TI. No obstante, aumenta rápidamente la importancia de contar con mejores habilidades técnicas para mejorar la calidad. Esto puede ser corroborado por el hecho de que cada vez son más los clientes que utilizan la tercerización como una manera de introducir innovaciones en sus organizaciones. Este cambio de importancia relativa puede atribuirse al mayor consenso que existe sobre los ahorros de costos estimados entre el 15% y el 25%. Los acuerdos de tercerización que se han concentrado exclusivamente en los ahorros de entrega no han cumplido con las expectativas de los clientes y los proveedores de servicios

- Europa continuará presenciando una importante actividad en la tercerización de TI y llegará a aproximarse a la participación en el mercado que tiene EE. UU. India continuará siendo el destino de mayor preferencia para la tercerización de TI, aunque se espera que China surja como un importante competidor en el futuro.

- Muchas compañías están confiando en los proyectos piloto para garantizar una buena adaptación entre la organización cliente y el proveedor. Los pilotos permiten que las compañías revisen el proceso de gestión de proyectos del proveedor para determinar la eficacia y eficiencia. Específicamente, el piloto observa si la ejecución del proyecto se completa dentro de las pautas establecidas, si las entregas son oportunas y si el proveedor ha cumplido con las normas de calidad definidas. Los proyectos piloto constituyen una excelente manera para que las organizaciones puedan comprobar hechos antes de tomar una decisión final sobre el proveedor. Además permiten que las compañías experimenten los beneficios de la tercerización antes de lanzarse a una relación a largo plazo. A menudo, las compañías llevarán a cabo una prueba de concepto con varios proveedores para comparar los resultados y elegir el mejor proveedor.

- La contratación múltiple será una de las tendencias más visibles. Por consiguiente, las organizaciones deberán desarrollar las competencias necesarias para gestionar un entorno de proveedores múltiples.

- Los proveedores de servicios de TI desarrollarán sus negocios en torno a diversos modelos, entre ellos:
  - The global champion model (El modelo del campeón mundial). Dentro de este modelo, el proveedor de servicios puede ofrecer varias líneas de servicios y soluciones para grandes organizaciones.
  - The IT specialist model (El modelo del especialista de TI). En este modelo, los proveedores de servicios se centran en tres o cuatro servicios principales de la industria de TI o servicios inter industria.
  - The ADM factory model (El modelo de fábrica de ADM). En este modelo, los proveedores de servicios se pueden posicionar como programadores de aplicaciones y servicios de mantenimiento de bajo costo.

Los proveedores de servicios deberán innovar sus modelos de negocio al centrarse en las nuevas líneas de servicios, como la tercerización de infraestructura. Además, deberán aumentar sus áreas de conocimiento y mejorar la calidad de los entornos de negocio, proporcionando mejores servicios con mejores soluciones tecnológicas.

[1]Gartner Research: *Market Trends– Outsourcing Contracts, Worldwide (2005)*

Acuerdo de nivel de servicio (SLA, en inglés): se trata de un concepto central de la gestión de servicios de TI. El SLA es un acuerdo formal por escrito entre dos partes: el proveedor de servicios y el beneficiario de los servicios. El SLA define las bases para llegar a un acuerdo entre las dos partes respecto de la prestación del servicio. El documento puede ser bastante complejo y, en ocasiones, es el sustento para un contrato formal. Si bien el contenido de los SLA varía de acuerdo con la naturaleza del servicio en sí, generalmente incluyen varios elementos centrales o cláusulas que definen un determinado nivel de servicio, opciones de respaldo, premios de incentivo para la superación de los niveles de servicio y multas para los servicios no prestados.

Biblioteca de Infraestructura de TI (ITIL, en inglés): un enfoque de mejores prácticas que facilita la prestación de servicios de TI de alta calidad. La ITIL describe un amplio conjunto de procedimientos de gestión destinados a ayudar a las organizaciones a obtener calidad y valor del dinero en las operaciones de TI. Estos procedimientos no dependen del proveedor y se desarrollan para proporcionar pautas para diferentes infraestructuras, desarrollos y operaciones de TI.

BS 7799: norma británica para la gestión de seguridad de la información, que proporciona un conjunto integral de controles compuesto por mejores prácticas de seguridad de la información.

Contratación múltiple: gestión y distribución de diferentes procesos de negocio entre varios proveedores. Uno de sus objetivos clave es mitigar riesgos, eliminando la necesidad de depender de un determinado proveedor.

Customer Operations Performance Center Inc. (COPC): autoridad líder en el mundo en lo que respecta a gestión de operaciones y mejora de desempeño para compradores y proveedores de centros de contacto de clientes y servicios de tercerización de procesos de negocio (BPO, en inglés). El Sistema de gestión de desempeño de COPC® incluye programas de certificación operativa, capacitación de gestión operativa, Six Sigma en centros de contacto, consultoría para la mejora del desempeño y servicios de gestión y contratación de proveedores.

Equivalente a tiempo completo (FTE, en inglés): método para medir la productividad o la participación de un empleado. Un FTE de 1,0 significa que el trabajo de un empleado es equivalente al de un empleado de tiempo completo, mientras que un FTE de 0,5 indica que las horas de trabajo o la producción proyectada de un empleado equivalen sólo a la mitad de las de un empleado de tiempo completo.

Ley Gramm-Leach-Bliley (GLBA, en inglés) de 1999 de Estados Unidos: esta legislación, que anuló la Ley Glass-Steagall de 1933 de Estados Unidos, abrió la competencia entre bancos, compañías de valores y compañías de seguro. Mientras la Ley Glass-Steagall no permitía que un banco ofrezca servicios de seguros, comerciales y de inversión, la ley GLBA permite que los bancos comerciales y de inversiones consoliden sus servicios. Por ejemplo, y como producto de esta ley, Citibank se fusionó con la firma Salomon Brothers de Wall Street y, finalmente, se convirtió en el conglomerado de capitales Citigroup.

Ley Sarbanes-Oxley de 2002 de Estados Unidos: ley federal aprobada en respuesta a diversos escándalos contables y corporativos de gran repercusión que involucraron a destacadas compañías de Estados Unidos. La legislación establece normas nuevas o mejoradas para todos los consejos y direcciones de compañías públicas y firmas de contadores públicos independientes de Estados Unidos. La ley, que contiene 11 títulos o secciones que abarcan desde responsabilidades del consejo corporativo hasta sanciones penales, exige que la Comisión del Mercado de Valores de Estados Unidos implemente normas sobre los requisitos para cumplir con la ley.

Modelo de madurez de capacidad (CMM, en inglés): el CMM, desarrollado por SEI de la Universidad de Carnegie Mellon a mediados de la década de 1980, es un conjunto de instrucciones que puede seguir una organización con el fin de obtener mayor control de sus procesos de desarrollo de software. El CMM clasifica a las organizaciones de desarrollo de software en una jerarquía de cinco niveles, cada uno con una capacidad progresivamente mayor de producir software de calidad. Cada nivel se describe como un nivel de madurez y tiene diferentes instrucciones a seguir.

Objetivos de Control de Información y Tecnologías Relacionadas (CobiT®): un conjunto de mejores prácticas para la gestión de TI creado por ITGI.

Organización Internacional de Normalización (ISO, en inglés): organismo que dicta normas internacionales y que está integrado por representantes de diferentes grupos de industrias. Esta organización se fundó el 23 de febrero de 1947 y produce normas industriales y comerciales para todo el mundo (las denominadas normas ISO).

Pedido de información (RFI, en inglés): un RFI proporciona la información necesaria para completar las evaluaciones de la primera ronda de proveedores. Las organizaciones generalmente utilizan el RFI para validar el interés del proveedor y para evaluar el clima de negocio en la industria de la organización. A diferencia de un pedido de propuesta formal y altamente específico, el RFI alienta a los proveedores a responder con libertad. Además detalla los requerimientos de negocio definidos por el equipo principal, de manera que el proveedor pueda comprender qué intenta lograr la compañía.

Procedimientos acordados (AUP, en inglés): en un AUP, se contrata una empresa de servicios profesionales para proporcionar un informe sobre una actividad específica. Los AUP difieren de las auditorías debido a que en una auditoría, los auditores emiten opiniones en función de sus hallazgos.

Protocolo de Control de Transmisión (TCP, en inglés)/Protocolo de Internet (IP, en inglés): conjunto de protocolos de comunicación que implementa la pila de protocolo en la que se ejecutan Internet y la mayoría de las redes comerciales. A veces, se lo denomina conjunto de protocolos TCP/IP.

Prueba de integración: algunas veces se denomina integración y prueba. Se trata de la fase de la prueba de software en la que los módulos individuales de software se combinan y prueban en forma conjunta. La prueba de integración toma los módulos unitarios evaluados y los agrupa en conjuntos más grandes, aplica las pruebas definidas en un plan de prueba de integración para esos conjuntos y entrega un sistema integrado que está listo para la prueba del sistema.

Prueba de regresión: cualquier tipo de prueba de software que intente descubrir errores de regresión, que se producen siempre que una función que antes funcionaba correctamente deja de funcionar o ya no funciona de la misma manera. Generalmente, los errores de regresión se producen como una consecuencia no deseada de cambios de programas. Los métodos comunes para realizar pruebas de regresión incluyen ejecutar pruebas utilizadas anteriormente y determinar si volvieron a surgir fallos que se habían reparado.

SAS 70: norma de auditoría reconocida a nivel internacional, desarrollada por la AICPA. Un examen SAS 70 significa que una firma de contabilidad y auditoría independiente evaluó las actividades y los objetivos de control de una organización de servicios.

Autores

Mayurakshi Ray es consultora principal de PricewaterhouseCoopers (PwC) India en la práctica de Gobierno, riesgo y cumplimiento (GRC, en inglés). Ray cuenta con más de nueve años de experiencia en áreas de gestión de riesgos de TI, controles y seguridad de la información, y revisiones de procesos de negocio. Como parte de la práctica de GRC, Ray dirigió numerosos trabajos relacionados con la SAS 70 y la ley Sarbanes-Oxley, que incluyen servicios de asesoramiento sobre disponibilidad y respaldo para la gestión de revisión y programas, para varias compañías de TI y BPO fuera del territorio.

Ray cuenta además con una vasta experiencia en áreas de riesgo y controles, donde proporcionó servicios de asesoramiento sobre enfoques de control interno y actividades de seguridad de la información. Entre estos servicios se encuentran la revisión de aplicaciones independientes, servicios empaquetados y soluciones de planificación de recursos empresariales (ERP, en inglés); la mejora de procesos de TI y gobierno corporativo; los enfoques de políticas de seguridad de la información; y las revisiones de seguridad de alta migración de datos, diligencia debida de TI y aseguramiento de terceros.

Ray forma parte del equipo principal de implementación y certificación de la BS 7799-2: 2002 en PwC Salt Lake Technology Center de Calcuta, India. Recibió capacitación sobre los aspectos funcionales de la ERP, los riesgos y controles de seguridad de la información y los requerimientos de la ley Sarbanes-Oxley. Cuenta con un título en economía y es contadora certificada y auditora líder calificada de BS 7799.

Parthasarathy Ramaswamy es consultor principal de PwC India en la práctica de GRC. Ramaswamy cuenta con más de 10 años de experiencia en las áreas de gestión de riesgo empresarial, mejora del desempeño, reducción de costos, costo basado en actividades y revisiones operativas. Ha gestionado proyectos de la ley Sarbanes-Oxley y proporcionó asesoramiento sobre disponibilidad a clientes. Sus servicios de asesoramiento se centraron en controles generales de computación de TI y controles automatizados de procesos de negocio.

Ramaswamy trabajó además como consultor funcional líder mientras gestionaba grandes implementaciones de ERP y proporcionaba asesoramiento fuera del territorio a importantes clientes con sede en Estados Unidos. Ramaswamy es contador certificado y especialista en costos, secretario de compañía con licencia, miembro del Instituto de Contadores Certificados del Reino Unido y tiene una maestría en economía.

El asesor **Jaideep Ganguli,** es miembro de PwC India y lidera las prácticas de GRC y Eficacia de las funciones financieras, donde asesora a los clientes sobre las iniciativas para la mejora del desempeño en el campo de finanzas y proporciona servicios de asesoramiento central en asuntos de gobierno, riesgo y cumplimiento. Jaideep cuenta con 15 años de experiencia en las áreas de soluciones de gestión financiera, aplicaciones empresariales, controles internos y transformación del negocio.

Dirigió una gran cantidad de trabajos de asesoramiento sobre disponibilidad de Sarbanes-Oxley y SAS 70 para muchas compañías de TI y BPO fuera del territorio. Su experiencia en el campo del riesgo y controles incluye trabajos de asesoramiento para enfoques de controles internos, gobierno corporativo, enfoques de gestión de riesgo empresarial, evaluaciones de riesgos y controles, y revisiones de aseguramiento de terceros.

Jaideep además es el líder de eficacia de TI en India y cuenta con una vasta experiencia en ERP. Ha dirigido algunos de los proyectos de implementación de ERP más grandes de India. Jaideep gestionó la implementación mundial de Oracle Financials de PwC desde el centro de tecnología de la firma en Tampa, Florida. Además desempeñó un rol clave en el desarrollo de la iniciativa de implementación de Oracle de la empresa. Fue el director del proyecto de implementación de la solución de facturación de PwC India.

Jaideep es contador certificado y ha colaborado con PwC desde 1991.

GTAG – Contribuyentes y revisores – 10

Contribuyentes

Madhu Arora, PricewaterhouseCoopers India
Deepa Seshadri, PricewaterhouseCoopers India

Revisores

Las siguientes organizaciones formaron parte del proceso de revisión:

- Comisión de Tecnología de Avanzada del IIA
- Organizaciones mundiales afiliadas al IIA
- AICPA
- Centro encargado de Seguridad en Internet
- SEI de la Universidad de Carnegie Mellon
- Asociación de Seguridad de Sistemas de Información
- Instituto de Proceso de TI
- Asociación Nacional de Directores Corporativos
- Instituto SANS

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

- Comité Ejecutivo de TI de AICPA
- Comité de Auditoría de TI en Bancos, IAI-Alemania
- Grupo de Especialización en Auditoría de TI, IAI-Noruega
- Comités técnicos del IAI–Reino Unido e Irlanda
- Frank Alvern, IAI Noruega y Nordea
- Ken Askelson, JCPenney, Estados Unidos
- Kjetil Berg, OAG, Noruega
- Lily Bi, IIA
- Anders Blix, EDB, Noruega
- Larry Brown, The Options Clearing Corp., Estados Unidos
- Claude Cargou, AXA, Francia
- Faisal R. Danka, Ernst & Young LLP, Londres, Reino Unido
- Reiner Eickenberg, WestLB AG, Duesseldorf, Alemania
- Lars Erik Fjortoft, KPMG, Noruega
- Terje Graesmo, Nordea, Noruega
- Christian Grill, DAB Bank AG, Munich, Alemania
- F.M. Hallinan, Chevron Phillips Chemical Co. LLP, Estados Unidos
- Alf Martin Hansen, Statsbygg, Noruega
- Rune Johannessen, OAG, Noruega
- Juergen Maerz, SEB AG, Frankfurt, Alemania
- Steve Mar, Microsoft Corp., Estados Unidos
- Otto Reimer, Sparkassen-u. Giroverband Hessen-Thueringen, Frankfurt, Alemania
- Paula M. Stockwell, IBM Corp., Estados Unidos
- Stig J. Sunde, OAG, Noruega
- Jay R. Taylor, General Motors Corp., Estados Unidos
- Hajime Yoshitake, Nihon Unisys, Ltd., Japón

GTAG®

Tercerización de tecnología de la información

Esta guía ofrece información sobre los tipos de actividades de tercerización de TI que debe tomar en cuenta la función de auditoría interna, el ciclo de vida de tercerización de TI y la forma en la que se deben gestionar las actividades de tercerización implementando planes bien definidos y respaldados por un enfoque de riesgo, control, cumplimiento y gobierno de toda la compañía.

¿Qué es la GTAG?

Las Guías de Auditoría de Tecnología Global (GTAG) preparadas por el IIA están escritas 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 se utiliza como un recurso disponible para los directores ejecutivos de auditoría 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 la auditoría de TI*

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

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

Consulte la sección de tecnología del sitio del Web del IIA technology en www.theiia.org/technology

The Institute of Internal Auditors

www.theiia.org