Normaria

Boletín de la Comisión de Normas y Asuntos Profesionales del Instituto de Auditores Internos de Argentina – Nº 15 – Junio de 2004

CONTENIDO

La Comisión de Normas y Asuntos Profesionales del Instituto de Auditores Internos de Argentina tiene como Misión promover el conocimiento y uso de las Normas para el Ejercicio Profesional de la Auditoría Interna por parte de los socios del Instituto y de las auditorías internas, proporcionar consejos oportunos a los socios sobre conceptos, metodologías y técnicas incluidas en el marco para la práctica profesional, y hacer comentarios o elaborar opiniones sobre otros asuntos que directa o indirectamente influyan sobre la profesión de auditoría interna. Los miembros de la Comisión son: Enrique Gonzalvo, CIA, CISA; Gustavo Rios (Superintendencia de Administradoras de Fondos de Jubilaciones y Pensiones); Guillermo Bilick, CIA (Organismo Nacional de Administración de Bienes); Adriana Fernández Menta, CIA. Puede contactarse con nosotros o hacernos llegar sus comentarios a la dirección de correo electrónico:

Consejos para la Práctica

Tercerización de Actividades de Sistemas de Información en otras Organizaciones

Por Juan de Dios Bel, CISA, CISM, CFE

Habíamos comenzado a considerar los temas de Tecnología Informática relacionados con la norma **2100 – Naturaleza del Trabajo** en la que se estipula que en el transcurso de la auditoría, el auditor interno debe obtener evidencia suficiente, confiable, pertinente y útil a fin de que se alcancen los objetivos de auditoría con eficacia. Los hallazgos y las conclusiones de la auditoría deben ser sustentados mediante el análisis y la interpretación adecuados de dicha evidencia. Por lo tanto, el propósito de este Consejo para la Práctica será describir las prácticas recomendadas para realizar una revisión de las actividades de sistema de información cuando han sido tercerizadas en otra organización.

En este tipo de revisiones, el Gerente de Auditoría Interna (Chief Audit Executive) debe determinar si auditoria interna posee, o tiene acceso a, los recursos (de manera independiente y competente) para realizar una revisión de las actividades y evaluar las exposiciones a riesgo asociadas.

1. ¿Porqué auditar actividades de Sistemas de Información tercerizadas?

Actualmente, es común encontrar que una organización (el usuario del servicio) puede delegar parcial o totalmente algunas o todas sus actividades de Sistemas de Información a un prestador externo de tales servicios (el prestador del servicio). Las actividades de Sistemas de Información que pueden tercerizarse comprenden funciones de Sistemas de Información como operaciones de centros de datos, seguridad y desarrollo y mantenimiento de sistemas de aplicación.

En estos casos la responsabilidad de verificar el cumplimiento de los contratos, acuerdos, leyes y reglamentaciones queda a cargo del usuario del servicio y, frecuentemente, los derechos de auditoría y la responsabilidad de auditar el cumplimiento no están bien clarificados. ¿De qué modo la función de Auditoría Interna debe cumplir con las Normas en esta situación?

2. Impacto sobre el Estatuto de auditoría (Audit Charter)

Cuando algún aspecto de la función de Sistemas de Información se terceriza en un prestador de servicios, éste debe incluirse en el alcance del estatuto de auditoría.

En el estatuto de auditoría debe constar claramente el derecho de Auditoría Interna a:

- Revisar el acuerdo entre el usuario y el prestador del servicio (antes o después de su puesta en vigencia)
- Llevar a cabo las tareas de auditoría que se consideren necesarias con relación a la función tercerizada
- Comunicar los hallazgos, las conclusiones y las recomendaciones a la gerencia del usuario del servicio

3. Consideraciones del planeamiento

Auditoría Interna debe comprender la naturaleza, oportunidad y alcance de los servicios tercerizados.

El Auditor debe establecer qué controles implementó el usuario del servicio para abordar

direccion@iaia.org.ar.

el requerimiento de negocio “de garantizar que las funciones y responsabilidades de terceros estén claramente definidas, se cumplan y continúen satisfaciendo los requerimientos pertinentes” (Objetivo de Control de Alto Nivel de COBIT[1] ES2). También, deben identificarse y evaluarse los riesgos relacionados con los servicios tercerizados.

El Auditor debe evaluar hasta qué punto los controles del usuario del servicio garantizan razonablemente que se alcanzarán los objetivos de negocio y que se evitarán o detectarán y corregirán los eventos no deseados. Otro aspecto a tener en cuenta por el Auditor es determinar hasta qué punto el acuerdo de tercerización contempla la realización de auditorías del prestador del servicio, y considerar si esta disposición es adecuada. Esto comprende la evaluación de la confianza potencial en cualquiera de las tareas de auditoría que lleven a cabo los auditores internos del prestador del servicio o un tercero independiente contratado por el prestador.

Al momento de preparar su planificación el Auditor debe:

- tener en cuenta la posibilidad de obtener adecuado asesoramiento jurídico de profesionales expertos.
- evaluar los informes de auditoría que se hayan preparado anteriormente para el prestador del servicio y planificar las tareas de auditoría interna de sistemas de información a fin de abordar los objetivos de auditoría relacionados con el ambiente del prestador del servicio, teniendo en cuenta la información obtenida durante la planificación.
- acordar los objetivos de auditoría con la gerencia del usuario del servicio antes de ser comunicados al prestador. Los cambios solicitados por el prestador deben ser acordados con la gerencia del usuario.
- planificar las tareas de auditoría interna de sistemas de información a fin de cumplir con las normas aplicables de auditoría profesional, como si la auditoría se llevara a cabo en el ambiente del usuario del servicio.

4. Realización del trabajo de auditoría

4.1 Requisito de Evidencia de Auditoría

La auditoría debe llevarse a cabo como si el servicio fuera provisto en el ambiente de Sistemas de Información del usuario del servicio.

4.2. Revisión del acuerdo con el prestador del servicio

El Auditor debe verificar si:

- existe un acuerdo formal entre el prestador y el usuario del servicio
- el acuerdo de tercerización incluye una cláusula que establece claramente que el prestador del servicio está obligado a satisfacer todos los requisitos legales que se aplican a sus actividades y a cumplir con las leyes y normas relativas a las funciones que debe desempeñar en nombre del usuario del servicio.
- el acuerdo de tercerización estipula que las actividades realizadas por el prestador del servicio están sujetas a controles y auditorías como si fueran realizadas por el usuario del servicio.
- los derechos de acceso de la auditoría están contemplados en el acuerdo con el prestador del servicio.
- se implementan los Acuerdos de Nivel de Servicio (ANS) y se aplican procedimientos de monitoreo del desempeño**.**
- se cumplen las políticas de seguridad del usuario del servicio.
- los acuerdos de seguros de fidelidad del prestador del servicio son adecuados.
- las políticas y los procedimientos del personal del prestador del servicio son adecuados.

4.3 Revisión de la gestión de los servicios tercerizados

[1] COBIT (por su siglas en ingles): Objetivos de Control para la Información y su Tecnología relacionada publicado por el IT Governance Institute e ISACA.

El Auditor debe verificar si:

- se controlan adecuadamente los procesos de Negocio que producen la información que se utiliza para monitorear el cumplimiento de los ANS
- de no haberse cumplido los ANS, el usuario del servicio ha buscado una solución y se ha considerado la posibilidad de tomar medidas correctivas para alcanzar el nivel de servicio acordado
- el usuario del servicio tiene la capacidad y la competencia para realizar el seguimiento y la revisión de los servicios prestados

4.4 Limitaciones al alcance

En los casos en que el prestador del servicio no se muestra dispuesto a cooperar con el Auditor Interno, éste debe comunicar el problema a la gerencia del usuario del servicio.

5. Informes

5.1 Emisión y aceptación del Informe

Al finalizar las tareas de auditoría, el Auditor debe proporcionar un informe –con una estructura apropiada– a los usuarios previstos del servicio.

El Auditor debe considerar la posibilidad de discutir el informe con el prestador del servicio antes de su emisión; no obstante, el Auditor no debería ser responsable de entregar el informe definitivo al prestador del servicio. Si éste ha de recibir una copia, la misma debería ser remitida por la gerencia del usuario del servicio.

El informe debe especificar cualquier restricción a la distribución que desee imponer el Auditor o la gerencia del usuario del servicio. Por ejemplo, no se debe permitir que el prestador del servicio distribuya copias del informe entre otros usuarios de su servicio sin obtener permiso de la organización del Auditor y, cuando corresponda, del usuario. Asimismo, el Auditor debe considerar la inclusión de un apartado que excluya responsabilidad hacia terceros.

5.2 Limitaciones al Alcance

El informe de auditoría debe identificar claramente una limitación al alcance cuando se nieguen los derechos de acceso de la auditoría y debe explicar el efecto de esta limitación con respecto a la misma.

6. Actividades de seguimiento

Como en el caso de las auditorías realizadas en el ambiente del usuario del servicio, el Auditor debe solicitar información adecuada, tanto al usuario como al prestador del servicio, sobre hallazgos, conclusiones y recomendaciones pertinentes de auditorías anteriores. El Auditor debe determinar si el prestador del servicio implementó medidas correctivas adecuadas en forma oportuna.

Apéndice – Glosario

Tercerización: un acuerdo formal con un tercero para desempeñar una función de Sistemas de Información de una organización.

Acuerdo de Nivel de Servicio (ANS): definición de medidas de rendimiento mínimo por las cuales, o por encima de las cuales, el servicio prestado se considera aceptable.

Prestador del Servicio: – la organización que presta el servicio tercerizado.

Usuario del Servicio: – la organización que utiliza el servicio tercerizado.

Para más información contactar a:

Juan de Dios Bel, CISA, CISM, CFE
Comisión de Tecnología Avanzada

jbel@iaia.org.ar

Sitios de interés:
www.isaca.org/standards
www.itaudit.org
www.adacsi.org.ar

[1] COBIT (por sus siglas en inglés): Objetivos de Control para la Información y su Tecnología relacionada publicado por el IT Governance Institute e ISACA.

[volver]

Normas

La Exigencia de Conocer la Tecnología Informática

Por Gustavo Rios

Las nuevas normas de implementación establecen para los auditores internos como requisito, con relación a la pericia y debido cuidado profesional, el de contar con conocimientos sobre los riesgos y los controles claves en tecnología informática. También requieren conocimientos de técnicas de auditoría, basadas en herramientas tecnológicas que nos permitan desempeñar eficientemente el trabajo asignado. Asimismo, las normas hacen la salvedad de que no se espera que todos los auditores internos tengan la experiencia de aquel auditor interno cuya responsabilidad principal sea la de auditar tecnología informática.

Cuando hablamos de riesgos y controles claves de tecnología informática, nos referimos a todos aquellos generados en los procesos del auditado, en los cuales la utilización de dicha tecnología es importante. Para estos casos, como el auditor interno debe identificar y evaluar tales riesgos y controles de esos procesos, se considera necesario el conocimiento de técnicas de auditoría basadas en esas tecnologías. La norma no pretende con esto que todos los auditores internos tengan el un mayor conocimiento y experiencia que los auditores de sistemas.

Por último, las normas mencionan que los auditores internos deben considerar, a los efectos de ejercer el debido cuidado profesional, la utilización de software de auditoría u otras técnicas de análisis de datos disponibles.

NORMAS SOBRE TECNOLOGÍA INFORMÁTICA

Pericia

1210.A3 Los auditores internos deben tener conocimiento de los riesgos y controles clave en tecnología informática y de las técnicas de auditoría disponibles basadas en tecnología que le permitan desempeñar el trabajo asignado. Sin embargo, no se espera que todos los auditores internos tengan la experiencia de aquel auditor interno cuya responsabilidad fundamental es la auditoría de tecnología informática.

Debido Cuidado Profesional

1220.A2 Al ejercer el debido cuidado profesional el auditor interno debe considerar la utilización de herramientas de auditoría asistida por computador y otras técnicas de análisis de datos.

[volver]

Novedades

Nuevos Consejos para la Práctica

El pasado 25 de mayo el IIA publicó un nuevo Practice Advisory (Consejo para la Práctica):

- **Practice Advisory 1312-2 External Assessment - Self Assessment with Independent Validation** (Evaluaciones Externas – Auto Evaluación con Validación Independiente)

Además, se publicaron versiones revisadas de otros seis Consejos para la Práctica:

- **Practice Advisory 1300-1 Quality Assurance and Improvement Program** (Programa de Mejora y Aseguramiento de Calidad)
- **Practice Advisory 1310-1 Quality Program Assessments** (Evaluaciones de Programas de Calidad)
- **Practice Advisory 1311-1 Internal Assessments** (Evaluaciones Internas)
- **Practice Advisory 1312-1 External Assessments** (Evaluaciones Externas)
- **Practice Advisory 1320-1 Reporting on the Quality Program** (Reporte sobre el Programa de Calidad)
- **Practice Advisory 1330-1 Use of Conducted in Accordance with the Standards** (Uso de "Realizado de Acuerdo con las Normas)

El texto de estos documentos, en idioma ingles, se puede encontrar en la página del IIA en Internet, en la dirección http://www.theiia.org/ecm/guidance.cfm?doc_id=73 , siendo necesario autenticarse con número de miembro del IIA y contraseña[1] para tener acceso.

A diferencia de las Normas para el Ejercicio Profesional de la Auditoría Interna, cuya observancia es obligatoria para los socios del IIA y para los CIA, los Consejos para la Práctica son de cumplimiento optativo.

(1) Aquellos socios del IAIA que no conozcan su número de miembro del IIA y su contraseña podrán solicitarlos en la administración del IAIA

[volver]

Federación Latinoamericana de Auditores Internos

Instituto de Auditores Internos de Argentina

The Institute of Internal Auditors