Gestion de riesgos y Auditoria del Outsourcing de TI

En el último post se reflejaban los posibles riesgos y los diferentes tipos y clases de estos que podrían aparecer al realizar servicios de Outsourcing. Es fundamental el hecho de que una empresa tenga la habilidad para reducir esos riesgos de tal manera que sean insignificantes para la empresa. Para ello, en un proceso de Outsourcing, se debería de tener en cuenta las siguientes consideraciones [1]:

1. Revisar y evaluar los procesos de la compañía para monitorear la calidad de las actividades del Outsourcing. Habrá que determinar cómo se van a monitorear los cumplimientos de los SLA y otros requisitos fundamentales del contrato. Es primordial definir en el contrato las expectativas y los objetivos a cumplir, ya que serían afectadas tanto la disponibilidad, eficiencia y eficacia de las operaciones contratadas como la seguridad de los sistemas y de los datos.

Para evitar todo esto, será necesario revisar el contrato, y establecer métricas, cuadros de mando, etc. para comparar los requisitos estipulados con los resultados en tiempo real. Todo esto se hablará dentro de la administración interna para determinar los procesos que se irán a monitorear.

En caso de no plasmar en el contrato los requisitos, se tendrá que acordar como se supervisara la calidad de los servicios y de que manera se va ha responsabilizar el proveedor en caso de insatisfacción o errores. Por eso, hay que asegurarse de plasmar los siguientes temas en el contrato:

- Disponibilidad y tiempo de actividad esperado.
- Rendimiento esperado del servicio.
- Tiempo de respuesta del proveedor.
- Tiempo de resolución de problemas.
- Requisitos tanto de cumplimientos de los servicios como de seguridad.
- Métricas e indicadores de rendimiento.

2. Asegura de que haya procesos adecuados de recuperación de desastres para garantizar la continuidad del negocio en caso de un desastre en su proveedor.

La misma empresa deberá tener también procedimientos documentados sobre la forma en que se recuperarán sus datos en caso de desastre, donde se incluirán procesos de notificación y escalamiento, cualquier transferencia necesaria entre la empresa y el proveedor durante la recuperación, y posibles soluciones. También deberá especificarse un plan de contingencia. Por ello, se solicitará la información al proveedor sobre donde ubica sus datos, y si tiene cualquier replica de la arquitectura.

3. Revisar y evaluar los planes de la compañía en caso de una terminación esperada o inesperada de la relación de subcontratación. Para que esto no ocurra, la empresa debería exigir al proveedor que le entregue una copia de los datos periódicamente. Los sistemas desarrollados seran flexibles y fáciles de implementar en diferentes entornos.

4. Revisar los procesos del proveedor para garantizar la calidad del personal y minimizar el impacto de la rotación.

En caso de que los empleados de la empresa proveedora no estén calificados para desempeñar su trabajo de forma correcta o la proveedora tiene un índice alto de rotación, la calidad de los

servicios desarrollados se ve afectada. Por ello, hay que revisar el contrato para asegurarse de que las descripciones tanto de los puestos de trabajo como las calificaciones necesarias para cada uno de ellos estén bien definidas y documentadas. En caso de que el proveedor realice cambios frecuentes en los puestos de trabajo, se deberá especificar y garantizar la continuidad de los servicios.

Relacionado con el tema de la auditoria de Outsourcing, cabe destacar que ISACA publico un programa de auditoria para optimizar las relaciones, selección de proveedores, la incorporación y los controles en los servicios de Outsourcing, el cual incluye [2]:

- Procesos de gobernabilidad y evaluación de riesgos.
- Análisis del costo-beneficio.
- Controles internos y requisitos para el proceso de selección de los proveedores.
- Los pasos apropiados para gestionar la transición de los proveedores internos de servicios a terceros.
- Monitoreo clave y los controles cuantitativos de la prestación de servicios del proveedor subcontratado.

La parte del proceso de selección del proveedor incluye pasos detallados como:

- Garantizar que el proveedor cumple con los requisitos reglamentarios de los clientes
- Que el proveedor es un líder de la industria en el espacio de Outsourcing
- El proveedor ha establecido un plan de continuidad comercial
- Los códigos de la conducta entre el cliente y el proveedor están alineada
- Que los términos del contrato son apropiados.

A continuación, reflejare un modelo de checklist elaborado para los procesos de Outsourcing de IT:

Checklist para Auditar operaciones y servicios de Outsourcing
1. Revisar los contratos aplicables para asegurar que identifiquen adecuadamente todos los productos entregables, requisitos y responsabilidades pertinentes al compromiso de su empresa.
2. Revisar y evaluar el proceso utilizado para seleccionar el proveedor de outsourcing.
3. Determine cómo sus datos se segregan de los datos de otros clientes.
4. Revisar y evaluar el uso de la encriptación para proteger los datos almacenados de la compañía
5. Determinar cómo los empleados y los proveedores acceden a sus sistemas y cómo se controlan los datos.
6. Revisar y evaluar los procesos para controlar el acceso lógico de los no empleados a su red y sistemas internos.
7. Asegúrese de que los datos almacenados en las ubicaciones del proveedor estén protegidos de acuerdo con sus políticas internas.
8. Revisar y evaluar los controles para prevenir, detectar y reaccionar ante los ataques.
9. Determinar cómo se realiza la gestión de la identidad para los hosts basados en Cloud Computing.
10. Determinar cómo el cumplimiento de las leyes de privacidad aplicables y otras regulaciones es asegurado.
11. Revisar y evaluar los procesos para asegurar que la empresa cumple con licencias de software aplicables para cualquier software.

12. Garantizar que las prácticas de retención y destrucción para los datos almacenados fuera del sitio cumplen con la política interna.
13. Revisar y evaluar la seguridad física del proveedor.
14. Revisar y evaluar los procesos de su empresa para monitorear la calidad de operaciones externalizadas. Determinar cómo se monitorea el cumplimiento de los SLAs.
15. Asegurar que existan procesos adecuados de recuperación ante desastres.
16. Determinar si los procesos de gobernanza apropiados están en marcha
17. Revisar y evaluar los planes de su empresa en caso de espera o inesperada terminación de la relación de outsourcing.
18. Si los servicios de TI se han obtenido mediante Outsourcing, revise los procesos del proveedor de servicios para garantizar la calidad del personal y minimizar el impacto del volumen de negocios.
19. Revisar y evaluar el derecho y la capacidad de su empresa de obtener información de la empresa proveedora.
20. Revisar los requisitos para la notificación de violación de seguridad. Garantizar que los requisitos están claramente definidos respecto a Cuándo y cómo el proveedor debe notificar a su empresa en caso de una brecha de seguridad y que su empresa tenga una respuesta claramente definida procedimientos cuando reciban dicha notificación.

Como conclusión, es imprescindible realizar un buen proceso de auditoría para evitar posibles problemas para la empresa, tales como gastos innecesarios, entorpecer o romper la confianza en la relación empresa-cliente, etc. Importantísimo

un plan de gestión de riesgos antes de cualquier proceso de vinculación con el proveedor y establecer métricas para medir el rendimiento de los servicios y actividades proporcionadas por la parte proveedora de forma periódica, y dejar plasmado en el contrato todos los requisitos y objetivos al más mínimo detalle

REFERENCIAS:

[1] Chris Davis, Mike Sheller y Kevin Wheeler (IT Auditing Using Controls To Protect Information Assets 2nd edition, 2011), edicion PDF, Capitulo 14

[2] https://oceano.biblioteca.deusto.es/primo-explore/fulldisplay?docid=TN_proquest1905430789&context=PC&vid=deusto&lang=es_ES&search_scope=default_scope&adaptor=primo_central_multiple_fe&tab=default_tab&query=any,contains,OUTSOURCING%20AUDIT&sortby=rank&offset=0