Seguridad de la información sensible en organizaciones que contratan outsourcing

Castiblanco, Fernando y Corredor, Julieth.
fernando8511, juliethac@gmail.com
Universidad Piloto de Colombia

Abstract – The outsourcing companies in Colombia and the world have had a growing market over the last century; they are ever more hired to work in specific and specialized areas into the organization, enabled to the customer focus on the core business and growth of its earnings base lines. In this point the outsourcing companies are involved by the natural of their contracts in the managed of sensitive information of the organization. At the juncture of compliance with agreed responsibilities it loses sight of the importance of execute required measures for contain private customer information. Ignoring that into the process information security should prioritize information assets and the risks to which they are exposed, so allow defining a framework in which both parts are contribution to information assurance.

Index Terms — Outsourcing, Information security, procurement, assets.

Resumen — Las empresas de outsourcing en Colombia y el mundo han tenido una gran crecimiento en el mercado en el último siglo, cada vez son más contratadas para enfocarse en áreas específicas y especializadas de una organización, permitiéndole a este última enfocarse en el core de su negocio y el crecimiento de sus líneas base de ganancias. En este punto las empresas de outsourcing se ven involucradas por la índole de sus contratos en la administración de información sensible de la organización. En la coyuntura del cumplimiento de responsabilidades pactadas se pierde de vista la importancia de ejecutar las medidas requeridas para contener la información privada del cliente. Ignorando que dentro del proceso de la seguridad de la información se debe priorizar los activos de información y los riesgos a los cuales están expuestos, y así establecer con el outsourcing un alianza estratégica que permita definir el marco sobre el cual ambas partes contribuyes al aseguramiento de la información.

Índice de Términos — Outsourcing, Seguridad de la información, contratación, activos.

I. INTRODUCCIÓN

Actualmente es muy usual la contratación de un outsourcing para desempeñar funciones puntuales dentro de una organización dada las situaciones económicas o con el fin de permitir que la empresa se enfoque en el core del negocio y que las tareas secundarias sean realizadas por terceros, logrando así una mayor productividad. El problema resultante está ligado a cómo se maneja la información sensible del cliente por parte del tercero, en el cumplimiento de las políticas, procedimientos, auditorías, cláusulas, entrenamiento, y demás, afines a las necesidades de conservar la integridad, confidencialidad y disponibilidad de la información.

Partiendo de la situación actual de un país como la India, el cual es el mayor proveedor de servicios de outsourcing en el mundo se logra dimensionar el impacto económico y social de esta práctica empresarial.

De diferentes formas puede una empresa de outsourcing establecer sus políticas de seguridad con relación a la empresa contratante, con el fin de establecer el tratamiento de la información, la definición de las políticas y los procedimientos que garantizarán el uso adecuado de la información sensible a la cual pueda acceder su personal dado los accesos que se le entregan para el cumplimiento de las obligaciones para las cuales fueron contratados.

Se plantea de igual forma un escenario ideal en el cual el outsourcing está en condiciones de garantizar un manejo integral de la información a la cual pueda tener acceso y sea sensible para el cliente.

¿Pero que debería tener en mente una gran empresa ante la tercerización y la obligación de cuidar los datos que reposan en su poder? “Booz-Allen Hamilton realizó una encuesta en 2006 para evaluar las preocupaciones fundamentales de los ejecutivos en la selección de un proveedor de externalización y encontró la calidad del servicio

ubicada en la primera preocupación, los precios y la seguridad, en segundo y tercer lugar respectivamente.” [1].

Esto deja en evidencia que la seguridad de la información juega un papel secundario en muchas negociaciones de este tipo, no hace parte de la alta gerencia o no se conciben las implicaciones de un mal uso de la información en contrataciones de este tipo.

II. ESTADO DEL ARTE

A. Antecedentes

Al realizar un barrido sobre los antecedentes que se han escrito al respecto de la seguridad con respecto a la contratación de outsourcing primero encontramos a Emilio del Peso Navarro quien dice que “Si la empresa usuaria ha establecido una clasificación de su información y, por lo tanto, conoce la sensibilidad de esta, deberá comunicar al prestador del servicio, que en el caso de los ficheros de datos de carácter personal de nivel medio y alto son obligatorias, bien por la empresa usuaria o por un tercero designado por está, con una periodicidad bienal. Si sobre todo lo que figura en el contrato es necesario efectuar un seguimiento, éste ha de ser aún más firme en el caso de la seguridad, no debiendo admitirse ninguna desviación de lo pactado” [2].

Otro de los que ha escrito al respecto es el doctor Warren Axelrod, expone las preocupaciones principales que surgen en la contratación de un tercero por parte de las compañías. Estableciendo las medidas de seguridad que le provean confianza y puedan cumplir con las reglamentaciones de protección de datos.

La opinión más común de la contratación externa parece ser; que la preocupación generada al ceder el control, anulará cualquier sensación de alivio al no tener las responsabilidades operativas del día al día. Esta tendencia puede deberse a la percepción en relación con los objetivos y las actitudes del personal interno y externo hacia diferentes servicios, beneficios, y la supervivencia. Es evidente que gran parte de la preocupación proviene de las sospechas de los clientes, que pueden estar justificadas con que el subcontratista no tiene el mismo nivel de compromiso de cumplir con los requisitos de servicio como un grupo interno. [3]

Después de todo, como se argumenta, el personal interno está más estrechamente alineado con otros y se adhiere a los objetivos, misión y cultura de la organización del cliente. Sin embargo, esto puede ser compensado en cierta medida por una mayor formalidad, recogido en acuerdos explícitos de nivel de servicio (SLA), que casi siempre existen formalmente [3].

B. Clasificación de activos y control

La clasificación de los activos de información específicos es generalmente la responsabilidad de la organización que posee la información. Sin embargo, estamos viendo cada vez más definiciones impuestas por los reguladores, en particular en lo que se refiere a la información sobre las personas, como clientes o pacientes. Por ejemplo la GLBA e HIPAA en los Estados Unidos, imponer requisitos estrictos para proteger los datos del cliente y paciente, respectivamente.

Junto con la clasificación de los datos vienen los requisitos para su manipulación segura. Los legisladores y los reguladores están poniendo la responsabilidad de proteger la información personal no pública (IPSFL) en manos de las organizaciones que recopilan la información de las personas, independientemente de si o no que la información viaja a terceros. Los reguladores de Europa, el Reino Unido, los Estados Unidos, y otros países están exigiendo cada vez más que las instituciones de servicios financieros y de salud, en particular, ampliar la supervisión y la protección de dicha información al momento de su recepción, procesado, almacenado y distribuido por tercera partes.

Las clases de datos se pueden definir de varias maneras. Un método consiste en evaluar el daño que podría infligir a la institución, sus clientes, socios comerciales y proveedores de servicios si tuvieran el acceso a las información y, posiblemente, mal manejo o mal utilizados por los que no se supone que tienen acceso a ella. Dicho acceso no autorizado podría haberse ganado intencionalmente o por accidente, de cualquier manera, es un hecho infortunado. La estimación en

cuanto a la magnitud de los daños de una perdida de información es muy difícil de calcular debido a que el daño es probable que sea a la reputación que son particularmente difíciles de cuantificar.

La clasificación de la información se puede realizar bajo la siguiente diferenciación, en la cual se incluye el daño para la organización en caso de su mal uso:

1) Publica: La información que está generalmente disponible en el dominio público. La divulgación de la misma no afecta a la organización, sus clientes o sus socios comerciales.

2) Interna: La información que es fácilmente accesible por las personas dentro de la organización, tales como empleados, contratistas, y probablemente los proveedores de servicios, pero que no está generalmente disponible para el público en general, la divulgación de esta categoría no es probable que dañe la organización, sus clientes, o a sus socios comerciales.

3) Confidencial: Información que, de forma inapropiada, divulgada o mal utilizado, podría causar daño sustancial a la organización, sus clientes o sus socios comerciales. Si esos datos confidenciales, tienen que ser compartidos con un tercero, tendrá que ser elaborado y ejecutado, antes de compartir la información, un acuerdo de confidencialidad.

4) Sensible personal: La información altamente personal que por lo general no debe ser recogida sin una razón válida específica, y para la cual la persona ha dado su consentimiento. Si inadvertidamente se divulga o se presenta cualquier otra anomalía, podría causar problemas significativos por los costos de rehabilitación de las personas y/o los principios de la organización.

5) Secreto: Información muy restringido cuya divulgación a personas no autorizadas, podrían producir un gran daño a la organización, sus clientes, empleados, socios comerciales y proveedores de servicios.

6) Ultra Secreto: La información altamente restringida que se pone a disposición a un grupo muy selecto y que, si no se utiliza inadecuadamente, podría resultar en un desastre mayor para la organización.

Una vez que la información ha sido clasificada, es necesario especificar la disposición de dichos datos a través de su creación, procesamiento, almacenamiento, transporte y eliminación, ya que cada categoría se aborda de manera diferente.

C. Estrategia para la adopción de políticas de seguridad

Del mismo modo que para la clasificación de los activos, una organización puede contratar a un tercero para desarrollar su política de seguridad de la información, junto con las normas de acompañamiento, líneas de base, directrices y procedimientos.

Cuando se trata de un proveedor externo, la organización debe asegurarse de que el proveedor de servicios cumple con las políticas de seguridad de los clientes, en su caso. Dicho cumplimiento se puede lograr de las formas que se describen a continuación:

Adoptar políticas del cliente. El outsourcing podría estar de acuerdo en adherirse a la política relevante del cliente en su totalidad. Este es el enfoque más simple desde el punto de vista del cliente, pero podría suponer un esfuerzo considerable por el proveedor externo, dependiendo del número y tamaño de los huecos entre los dos conjuntos de política.

Adoptar políticas del proveedor de servicios. El cliente puede acordar la adopción de la política del proveedor de servicios si éste cumple con los estándares de la industria y se considera superior a la política del cliente. Es muy probable que el proveedor de servicios tenga una mejor política, normas y procedimientos, ya que deben satisfacer muchos clientes.

Importantes preguntas debe hacerse la dirigencia acerca del outsourcing a contratar en relación a la seguridad de la información y deben partir de las políticas ya establecidas en este ámbito por la organización. Si las políticas de seguridad son fuertes ¿hasta qué punto el outsourcing se debe ajuste a ellas? Si por otro lado son débiles ¿no se debería contratar a una empresa con experiencia que permita fortalecer aquellos puntos débiles? Y todo ligado obviamente a la estrategia de la organización en términos económicos, de crecimiento, de penetración, etc.

“Lo ideal sería que en cualquier estructura de gobierno, un proveedor debe adaptarse a la

aplicación de los principios de gobierno y el uso de herramientas de gobierno con los de la organización. Un entendimiento mutuo ofrece a una organización mayor posibilidad de establecer con éxito desde el principio si un potencial proveedor cumplirá sus objetivos." [4].

D. India, país líder en servicios de outsourcing

Gracias al crecimiento del outsourcing la India ha logrado convertirse en el centro más grande de atención al negocio de terceros, aquí un ejemplo: En el campo de la subcontratación, GE es una empresa pionera. Una nueva norma que rige las acciones de GE en alta mar se introdujo en la década de 1990 por Jack Welch, ex CEO de GE. Se llama la regla 70:70:70. Welch estableció que el 70% del trabajo de GE sería subcontratado, y esto fue informado a los empleados de GE en un e-mail. Fuera de esto, el 70% de la obra se completará en los centros de desarrollo offshore, y fuera de este el 70% se envió a la India, lo que resulta en aproximadamente el 30% del trabajo de GE está externalizado a la India.

Treinta unidades de negocio diferentes en los Estados Unidos han entregado más de 450 procesos por los servicios de GE Capital International (GECIS), que emplea a más de 12.000 personas. Sitios en la India en los que opera incluyen Gurgaon, Hyderabad, Bangalore y Jaipur.

El ejemplo de GECIS cambiar la mentalidad de las empresas que solían pensar que trabajo en el extranjero carece de calidad y era difícil de supervisar. En offshoring las empresas pueden ahorrar hasta un 50% en los gastos operacionales en comparación con un centro de llamadas de EE.UU., por lo bajo costo es la ventaja más evidente de la deslocalización. Además del costo, hay más de por qué los centros de llamadas se están estableciendo en otros países como India. Zonas complementarias de tiempo, baja rotación de personal, y una fuerza de trabajo de habla Inglés educada, hacen atractiva la deslocalización. La ubicación geográfica de la India se presta a una operación 24/7, y la India es el hogar de la población de habla Inglés educada más grande del mundo. Acerca de la diferencia de zona horaria de 12 horas que existe entre Estados Unidos y la India. Una fuerza de trabajo altamente motivado es otro aspecto positivo de la India, mientras que la llamada EE.UU. centra a menudo experimentan baja moral y una muy alta rotación, alrededor del 40% al 70% anual. Se hace difícil mantener un servicio de calidad a bajo costo, teniendo en cuenta el tiempo y los costes asociados con la formación de nuevos agentes. Centros de llamadas indias tienen una tasa promedio de facturación de aproximadamente 5%.

Las operaciones de back office para las empresas de GE Capital, Servicios de GE Capital International (GECIS), que se creó en 1997, incluyen la oferta de servicios como la planificación de recursos empresariales (ERP), base de datos Oracle Consulting, ayuda de TI de escritorio, servicios de conocimiento, soluciones de software, análisis, extracción de datos y modelización, e-learning, los centros de contacto con clientes y red de monitoreo remoto.

E. Outsourcing en Colombia

Según datos de la revista Portafolio en Colombia se mueven 1,2 millones de dólares al año en el sector económico del outsourcing, potenciado por varios factores como los TLC firmados en los últimos años por el país, lo cual ha incrementado el interés de los países extranjeros de invertir en Colombia. En la misma revista se cita un estudio hecho por la empresa estadounidense Gartner en la cual Colombia está posicionada en el puesto 30 en servicios de outsourcing en el mundo y fundamenta su posición en 10 factores principalmente: el idioma, el sistema educativo, la mano de obra, la infraestructura, la reducción de costos, la compatibilidad cultural, la madurez global y legal, la propiedad intelectual, el ambiente político y económico, y el apoyo gubernamental. [7]-[8].

En un marco tan importante de participación de las empresas de outsourcing en la economía colombiana y mundial es crucial la correcta adopción por parte de las mismas y de las empresas contratantes de normas, procedimientos, políticas para asegurar la información en sus pilares fundamentales de integridad, disponibilidad y confidencialidad dada la inclusión de leyes como la 1581 del 2012 en la legislación colombiana que regulan la protección de los datos personales y el trato que se le debe dar.

III. ESCENARIO IDEAL PARA UNA ORGANIZACIÓN AL CONTRATAR UN OUTSOURCING

Aprovechando las unificación de normativas del manejo de la seguridad de la información se logran potenciar las capacidades del trabajador con el conocimiento especializado y la conciencia de las normativas que rigen la seguridad de la información en la coyuntura de uno o más empresas o de uno o más países, logrando forjar el reconocimiento que catapulte el outsourcing como alianzas estratégicas de bajo costo, capital humano experto, implementaciones de menor tiempo, infraestructuras que combinen políticas de seguridad, estándares, procedimientos y dispositivos acordes a la protección requerida por la línea de negocio manejada por el cliente. Siendo los mayores prestadores de servicios las pequeñas y medianas compañías que logren resaltar sus habilidades con la adaptación de un gobierno de seguridad propio que les permita la contratación de empresas de outsourcing con la seguridad de que su recurso más vital: la información tendrá un riesgo asumible de incumplimiento de alguna de las bases de la seguridad informática: integridad, confidencialidad o disponibilidad.

IV. CONCLUSIONES

Es de vital importancia para las organizaciones tener un gobierno de la seguridad de la información que le permita definir las políticas, los procedimientos, los controles, las auditorías, etc., para mantener la información sensible de la empresa bajo su control, impidiendo fugas de información que pueden conllevar a daños económicos, sociales, legales, etc.

La contratación de outsourcing es de vital importancia en el funcionamiento de las empresas actuales dado que significan personal especializado aun costo admisible teniendo en cuenta los beneficios que trae consigo. Ahora bien, los riesgos que trae para la empresa contratante pueden ser altos y en temas tan relevantes como el manejo de información sensible. Pero no significa lo anterior que las compañías deban abstenerse de contratarlas sino que se deben encontrar las estrategias adecuadas para asegurar los activos de información de posibles fugas o alteraciones que afecten a la compañía.

Cada compañía dada su madurez debe escoger la estrategia que mejor se acomode al instante que vive, es claro que no todas las organizaciones pueden establecer un gobierno de seguridad confiable y estructurado dado los recursos económicos o de personal que se tienen que invertir para lograrlo. Un enfoque inicial podría consistir en contratar una empresa de seguridad de la información que lo apoye en este campo o contratar un outsourcing para un tema específico pero que trae consigo certificaciones o casos de éxito en temas de seguridad de la seguridad en los procesos que realiza y de quienes se puede realizar un aprendizaje paulatino de su modelo para posteriormente adaptarlo a los intereses de la compañía.

REFERENCIAS

[1] AMANT, Kirk St. IT Outsourcing: Concepts, Methodologies, Tools, and Applications. IGI Global, 2010.

[2] NAVARRO, Emilio del Peso. Manual de Outsourcing Informático: Análisis y Contratación, 2003.

[3] C. WARREN, Axelrod. Outsourcing Information Security. Norwood, MA 02062. Artech House, Inc. 2004.

[4] KENDRICK, Rupert, Outsourcing IT: A Governance Guide, Noviembre 26, 2009.

[5] SHARMA, Vivek, Web-Based and Traditional Outsourcing, 2012.

[6] KENDRICK, Rupert, Outsourcing IT: A Governance Guide, Noviembre 26, 2009.

[7] Garcés, Claudia. (2012, marzo). Colombia es la joya de la tercerización en la región. [Online]. Disponible: http://www.portafolio.co/negocios/colombia-es-la-joya-la-tercerizacion-la-region

[8] Garcés, Claudia. (2012, marzo). Colombia es la joya de la tercerización en la región. [Online]. Disponible: http://www.portafolio.co/negocios/outsourcing-mueve-colombia-us12-billones-al-ano

Autores

Fernando Castiblanco T.
Ingeniero de Sistemas
2008

Julieth M. Corredor R.
Ingeniera de Sistemas
2008