Por Marcos Assi

Tenho lido alguns artigos sobre a lei anticorrupção e a relação com terceiros, e acho que algumas pessoas falam sobre o assunto de gestão de terceiros como se fosse uma novidade, ou não conhecem ou nunca ouviram falar sobre a gestão de terceiros, que desculpem a modéstia já venho alertando há anos sobre o controle de terceirização.

Muitos de meus clientes e algumas empresas que conheço bem, já implementaram em seus processos de contratação e de pagamentos o recebimento de certidões negativas de seus fornecedores, mas será que somente isto basta?

Acredito que não, pois devemos validar os serviços que contratamos e devemos ainda lembrar que não possuir antecedentes criminais não pode ser o item principal na contratação de um terceiro, seja ele para serviços ou produtos, pois muitos mantem a sua empresa “limpa”, mas utilizando outros meios para atos “fora do padrão”.

Afinal em muitos casos contratamos serviços que não sabemos controlar, e para isso citamos a tal do “Cloud Computing” ou computação na nuvem, como auditar esse serviço? E já que estamos falando de compliance, alguém já auditou a empresa que faz a guarda de seus documentos?

Dizem que seria interessante avaliar como manipulam os documentos, onde guardam, seus procedimentos contra incêndio, basta lembra o caso da Interfile, empresa especializada na terceirização de processos de negócios (BPO), admitiu que documentos de mais de cem clientes foram destruídos pelo incêndio que atingiu três dos seus dez galpões em Jandira, no interior de São Paulo, no dia 4 de julho de 2011, e segundo a assessoria de imprensa da companhia, todos os clientes já foram notificados das perdas, porém, não havia previsão para término do relatório sobre os prejuízos provocados pelo acidente, devido à sua grande dimensão, você se lembra?

A empresa informou na época que alguns dos clientes, especialmente instituições financeiras, pediram sigilo total, haja vista que a divulgação de nomes relacionados a arquivos perdidos pode representar risco para seus negócios. A empresa informou também que não há padrão de contingência no armazenamento dos arquivos, pois os planos dependem do serviço contratado – os que preveem cópias de segurança têm custo maior do que aqueles que contemplam armazenagem simples, por exemplo.

Acidentes podem acontecer, mas será que sabemos avaliar os processos de prevenção a catástrofes e se a empresa possui processos de continuidade de negócios? Ainda podemos citar a questão se segurança da informação, pois muitas empresas optam pelo sistema de digitalização para facilitar a pesquisa, mas será que alguém visitou a empresa para entender seu processo de sigilo, quem faz, como faz, como processam os arquivos, haja vista que enviamos contratos sociais de clientes, contratos de negócios, informação cadastrais de clientes, entre outros documentos.

Por esse motivo os controles internos e compliance devem se fazer presentes nestes processos, cobrando das áreas contratantes melhorias nos processos de monitoração, validação e checagem dos serviços prestados, caso tenham dúvidas, procurem pelo DS.2 do CobiT (Control Objectives for Information and related Technology), onde identifica os principais objetivos de controles de terceiros que serve para vários processos, então mãos à obra!

Fonte: administradores.com.br, em 02.07.2014.