1.Segurança da informação na relação com fornecedores

Nem todas as atividades que são importantes para uma organização são conduzidas pela própria organização. Tão logo algo seja executado por um terceiro, é importante documentar os requisitos a que a parte tem de atender. Por exemplo, você não pediria a um vizinho de porta para preencher suas declarações de imposto de renda. Quando uma empresa decide terceirizar parte ou a totalidade de sua TI, um contrato efetivo, em que todos os aspectos de segurança recebem a atenção necessária, tem que ser assinado com a parte que fornece o serviço.

É necessário definir os diferentes tipos de fornecedores a que a organização irá permitir ter acesso a suas informações. Serviços são, por exemplo, serviços de TI, utilidades logísticas, serviços financeiros e aqueles envolvidos na implementação e na manutenção dos componentes da infraestrutura de TI.

Já que a organização não pode transferir suas responsabilidades para um provedor de serviços, ela será sempre responsável por controles de acurácia e perfeição que garantem a integridade da informação ou o processamento da informação executada por ambas as partes. Também será responsável por lidar com quaisquer incidentes e contingências associados ao acesso do fornecedor, incluindo as responsabilidades tanto da organização como dos fornecedores.

A informação pode ser posta em risco por fornecedores com uma gestão inadequada de segurança da informação. Controles devem ser identificados e aplicados a fim de administrar o acesso de fornecedores às instalações de processamento de informação. Todos os requisitos relevantes de segurança da informação devem ser estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

É prática comum providenciar um Acordo de Nível de Serviço (SLA), em que as duas partes descrevem os serviços que esperam que sejam realizados e sobre quais circunstâncias. Auditorias são efetuadas regularmente para verificar se esses acordos estão sendo observados. Deve fazer parte do SLA uma seção de segurança em que são detalhados os requisitos legais e regulatórios, incluindo proteção de dados, direitos de propriedade intelectual e direitos autorais, juntamente com uma descrição de como será assegurado que esses requisitos serão atendidos.

Alguns dos requisitos mais importantes na cláusula de segurança do SLA, no entanto, são: a obrigação do fornecedor apresentar periodicamente um relatório independente sobre a eficácia dos controles de segurança; um acordo sobre a correção oportuna de questões relevantes levantadas no relatório; e, por último, mas não menos importante, as obrigações do fornecedor de cumprir os requisitos de segurança da organização.

1.1 Cadeia de suprimentos de tecnologia da informação e das comunicações

A seção 15.1.3 da ISO 27002:2013 descreve a responsabilidade dos fornecedores em relação aos riscos de segurança da informação, associados aos serviços de tecnologia da informação e das comunicações e à cadeia de suprimento do produto. São exemplos: a definição dos requisitos de segurança da informação que se aplicam, à aquisição de produtos ou serviços de tecnologia da informação e de comunicações; além dos requisitos gerais de segurança da informação para os relacionamentos com fornecedores.

A seção 15.1.3-d estabelece que a cadeia de suprimentos deve ser protegida através da implementação de um processo para identificar componentes de produtos, ou serviços, que são críticos para manter a funcionalidade. Eles, portanto, requerem maior atenção e escrutínio quando construídos fora da organização.

O fornecedor deve implementar um processo específico para gerenciar o ciclo de vida e a disponibilidade dos componentes de tecnologia da informação e das comunicações, juntamente com os riscos de segurança associados. Essas práticas específicas são construídas em cima das práticas gerais de segurança da informação, qualidade, gerência de projetos e engenharia de sistemas, mas não as substituem.

2.Gestão da prestação de serviços de fornecedores

Ao monitorar, revisar e auditar regularmente a prestação de serviços dos fornecedores, a organização deve assegurar que os termos e as condições sobre segurança da informação dos contratos estão sendo atendidos, e que os incidentes e problemas de segurança da informação estão sendo gerenciados adequadamente.

Outra forma de assegurar o serviço dos fornecedores é através da certificação por um organismo independente. O organismo independente pode utilizar a ISO 27001, por exemplo, para certificar o sistema de gestão de segurança da informação dos fornecedores e a ISO 9001 para certificar o seu sistema de gestão da qualidade.

As alterações nos serviços de fornecedores devem ser geridos levando em conta a criticidade da informação, dos sistemas e dos processos envolvidos da empresa, e levando em conta uma reavaliação dos riscos. Mudanças podem influenciar acordos. Quando uma organização muda os serviços oferecidos, alterando ou atualizando produtos, ou desenvolvendo novos sistemas, isso leva a SLAs novos ou atualizados.

Por outro lado, quando o fornecedor muda os serviços, melhora ou usa novas tecnologias, ferramentas e ambientes, ou quando um fornecedor utiliza subcontratados que não eram conhecidos no momento em que o SLA foi celebrado, então os riscos devem ser investigados e os SLAs devem ser atualizados para refletir a nova situação. Se a organização concordar com o uso de subcontratados, o SLA deve, pelo menos, incorporar uma seção que declare que o fornecedor é responsável pelo cumprimento da política de segurança da organização por parte dos subcontratados.