Gestão de Riscos Digitais

ERNANI BAIER

Os riscos digitais estão cada vez mais presentes no dia a dia de todas as organizações, pois todas estão de um modo ou outro inseridas no mundo digital. Tendo em vista que a Lei Geral de Proteção de Dados (LGPD) veio para ficar e, cada vez mais, temos informes sobre ataques digitais às organizações, cremos ser importante analisar alguns aspectos (dos muitos existentes) relacionados à proteção de dados digitais, sejam de pessoas físicas (para atendimento à LGPD) sejam dados e informações corporativas.

O termo gestão pode ser definido como o ato de administrar ou gerir uma organização. Risco é qualquer resultado diferente daquilo que foi planejado ou é esperado, sendo que aqui trataremos dos resultados que podem afetar negativamente a organização. O COSO (The Comitee of Sponsoring Organizations) define gerenciamento de riscos como sendo um processo aplicado no estabelecimento de estratégias visando a identificar eventos em potencial e capazes de afetar o atingimento dos objetivos da organização.

Entre os riscos digitais que podem afetar negativamente uma organização, podemos citar vírus de computador, ataque de hackers, sequestro de dados, vazamento de dados pessoais e financeiros, furto de informações, fraudes, não cumprimento de requisitos legais como os propostos pela LGPD etc. Todos esses eventos podem causar perdas financeiras, danos à imagem e reputação da organização, processos judiciais e, no pior cenário, interrupção temporária ou permanente da operação.

A literatura menciona que alguns dos atributos da segurança da informação são confidencialidade (informação é acessível somente a pessoas autorizadas), integridade (garantia de exatidão), disponibilidade (usuários autorizados têm acesso quando requerido), autenticidade (garantia de veracidade da fonte das informações), não repúdio (gerador da informação ou transação não poderá negar autoria), responsabilidade (habilidade de identificar responsável por ação). E todos estes atributos devem ser considerados no processo de avaliação e gestão dos riscos digitais corporativos.

Por outro lado, a análise de riscos à segurança de dados digitais deve considerar potenciais ameaças, vulnerabilidades, impactos e probabilidade de ocorrência. Uma vez feita a listagem de eventos possíveis de impactar negativamente a organização, e com a atribuição de pesos numéricos, é possível identificar aqueles que requerem maior atenção por parte dos gestores, os quais, em última instância, têm a responsabilidade sobre a organização.

Para se proteger destas ameaças, algumas medidas que podemos citar são a utilização de firewall adequado, ter um programa antivírus atualizado, e a implementação de uma política de segurança da informação, que irá reunir regras, normas e procedimentos a serem seguidos por todos os colaboradores, gestores, proprietários e eventuais terceiros que interajam na organização.

Entre as ações a serem previstas na política de segurança da informação podemos citar: nível de dificuldade da senha, controle de acesso físico a servidores da organização, existência de logs de auditoria nos sistemas, existência de rotina de back-up, realização periódica de teste de retorno de back-up, existência de unidade de back-up externa à organização, regra quanto a uso de unidades de USB, regras claras para o acesso de terceiros a sistemas da organização.

Em resumo, a gestão deve identificar tudo aquilo que pode dar errado em relação à segurança digital, priorizar ações para minimizar aqueles riscos que possam trazer maiores danos e monitorar continuamente o ambiente digital quanto ao gerenciamento de riscos.

CONTADOR, INTEGRANTE DA COMISSÃO DE ESTUDOS DE AUDITORIA INDEPENDENTE DO CRCRS