CEST Centro de Estudos Sociedade e Tecnologia
USP Universidade de São Paulo
Boletim - Volume 1, Número 9, Março/2017

Segurança da Informação na Administração Pública

Vera Kerr

Nas últimas décadas, temos testemunhado o surgimento da sociedade da informação como resultado da constante evolução tecnológica que trouxe consigo profundas mudanças nas relações interpessoais.

Com o desenvolvimento da tecnologia da informação e comunicação e o surgimento da Internet, a Administração Pública também tem sido alvo dessas profundas transformações, deparando-se com o enorme desafio da inclusão digital no ambiente governamental.

É imperativo que o servidor público tenha um comportamento adequado ao lidar com os dados públicos abertos e principalmente com os dados públicos sigilosos ao utilizar-se das tecnologias da informação e comunicação.

Todavia, disponibilizar as novas tecnologias sem a devida orientação e controle, tem gerado ao ente público e aos servidores envolvidos, responsabilidade civil e até mesmo criminal como as decisões dos tribunais têm revelado. Isto porque a Administração Pública está sujeita a ataques externos ou mesmo a atos ilícitos praticados por seus próprios servidores ou por terceiros estranhos aos seus quadros por meio do uso das novas tecnologias. Sem contar que o ente público, além de trabalhar com dados públicos, ou seja, informações acessíveis à sociedade, também trabalha com dados protegidos pelo sigilo legal. Desse modo, é imperativo que o servidor público tenha um comportamento adequado ao lidar com os dados públicos abertos e principalmente com os dados públicos sigilosos ao utilizar-se das tecnologias da informação e comunicação. Para tanto, considera-se imprescindível a implantação de planejamento estratégico em segurança da informação no ambiente governamental. Tal medida visa divulgar as normas de boas práticas relacionadas aos direitos e deveres do servidor, ao acesso e uso de dados e às penalidades relacionadas à sua violação.

Nesse sentido, de acordo com as instruções propostas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), os órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) devem elaborar a política de segurança da informação e comunicação, implementá-la e capacitar os servidores a atendê-la. Também é fundamental que, diante de um incidente de ataque, invasão ou violação do sistema informático, o servidor saiba quais devem ser os cuidados mínimos para se preservar a informação e a prova até a chegada de um perito. No entanto, é importante frisar que tanto o regulamento de segurança da informação quanto auditorias sistemáticas, embora imprescindíveis, não são suficientes para solucionar a questão. Isto porque, o humano continua sendo o elo mais vulnerável na cadeia de segurança. Programas de capacitação consistentes em treinamento e conscientização de servidores, conforme anteriormente mencionado, são essenciais para reduzir a ação dos engenheiros sociais e mitigar as vulnerabilidades do sistema.

O Tribunal de Contas da União (TCU), em seus Acórdãos 1603/2008 e 2308/2010, recomenda que seja elaborada política de segurança da informação e comunicações, bem como normatização complementar referente ao órgão ou entidade da Administração Pública Federal onde forem implantadas. A recomendação registrada no item 9.1.3 do Acórdão nº 1.603/2008-

TCU-Plenário aos órgãos governantes superiores consiste em:

"Orientação sobre a importância do gerenciamento da Segurança da Informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos, a área específica para gerenciamento da Segurança da Informação, a política de Segurança da Informação e os procedimentos de controle de acesso".

Além dos acórdãos acima registrados, há outras decisões do Tribunal de Contas da União relacionadas a várias instituições governamentais que passaram por processo de auditoria e que deverão implementar tais políticas de segurança. Com o fim de possibilitar o fácil acesso e promover a cultura de segurança no ambiente da Administração Pública, o Departamento de Segurança da Informação e Comunicações do GSI/PR disponibiliza em seu site uma compilação da legislação vigente para servir como referência para o trabalho de juristas, servidores públicos, técnicos e especialistas na área. Há normas da família ISO/IEC 27000 que tratam da gestão de segurança da informação, sendo referência a órgãos ou entidades da Administração Pública Federal, direta e indireta, tais como: ISO 27001 – que estabelece um Sistema de Gestão de Segurança da Informação e ISO 27002 – que é o Código de Práticas para a Gestão da Segurança da Informação e ISO 27005 – que descreve a gestão de riscos em Segurança da Informação. Além dessas normas ainda existem normas internacionais da ISO/IEC como, por exemplo, a norma ISO/IEC 15408 (*Common Criteria*) que tem por objetivo avaliar a segurança de TI, entre outras.

No que diz respeito à estrutura de gestão de segurança da informação e comunicação, o GSI/PR recomenda que os órgãos governamentais possuam:

I. Comitê de Segurança da Informação e Comunicação;

II. Gestor de Segurança da Informação e Comunicação; e

III. Equipe de Tratamento e Respostas a Incidentes.

Devido à sua importância, a Coordenação-Geral de Segurança da Informação da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento (SLTI/MP) recomenda que a estrutura de segurança da informação e comunicação do órgão ou entidade esteja definida no organograma institucional em nível estratégico com o envolvimento de todas as áreas da organização. Estabelece ainda que a referida estrutura trate o tema nos níveis estratégicos (comitê de segurança), tático (diretorias) e operacional (grupos de trabalho e equipes de segurança da informação e comunicação específicas como segurança de TI e segurança patrimonial).

Constata-se, portanto, que a mera aquisição de novas tecnologias não representa necessariamente maior eficiência e segurança aos serviços executados pelos gestores e servidores públicos. É necessário implementar planejamento estratégico em segurança da informação no ambiente da Administração Pública. Do mesmo modo, é imperativo capacitar o servidor público, usuário das novas tecnologias, quanto às boas práticas e normas relacionadas com o fim de criar uma cultura corporativa quanto ao uso responsável, seguro e ético dessas ferramentas à luz da legislação vigente, de forma educativa, preventiva e colaborativa.

Vera Kerr, *advogada, doutoranda pela Escola Politécnica da Universidade de São Paulo e pesquisadora do CEST-USP.*

Coordenador: Edison Spina

Este artigo resulta do trabalho de apuração e análise da autora, não refletindo obrigatoriamente a opinião do CEST.