OS TRIBUNAIS DO DISTRITO FEDERAL POSSUEM ESTRUTURAS PARA GERENCIAR RISCOS DE SEGURANÇA DA INFORMAÇÃO? UM ESTUDO À LUZ DAS TRÊS LINHAS DE DEFESA

Transformação digital, ciberespaço e novas tecnologias da informação

Carlos Eduardo Mancini Queiroz (Universidade de Brasília) Renato Solimar Alves (Universidade de Brasília) Aldery Silveira Junior (Universidade de Brasília) Jose Humberto da Cruz Cunha (Universidade de Brasília) Rafael Rabelo Nunes (Universidade de Brasília)

RESUMO

Ataques cibernéticos aumentaram significativamente com a ampliação do trabalho remoto desde a declaração da pandemia do coronavírus. O cenário no Brasil é ainda mais crítico: um levantamento feito em 2020 demonstrou é o país o maior número de vítimas de phishing no mundo (Infomoney, 2021), sendo que, no ano seguinte, foi o 5º que mais sofreu crimes cibernéticos (Prado, 2021). Nesse cenário, o Poder Judiciário tornou-se um alvo para os grupos hackers. Em novembro de 2020, o STJ sofreu o maior ataque de ransomware contra um órgão público do Brasil, resultando na paralisação de suas atividades por quase um mês (Moura, 2022). Em março de 2022, o TRF 3ª Região também sofreu o mesmo tipo de ataque, ficando indisponível por mais de duas semanas. Além dessa classe de ataques, é possível encontrar outras que podem gerar grande impacto, sem tornar indisponíveis os sistemas. São os casos em que os hackers podem, por exemplo, alterar o teor de decisões judiciais (Convergência, 2021) (Conjur, 2021). Sabendo que uma boa gestão de riscos permite a aplicação efetiva do Princípio Constitucional da Eficiência (Nunes, Perini, & Pinto, 2011) e sabendo que um sistema seguro aparenta exatamente da mesma forma que um sistema inseguro para os seus utilizadores, um dos modelos de gestão de riscos de Segurança da Informação (SI) que pode ser útil é o modelo organizacional de divisão em três linhas, onde as responsabilidades pelo risco "mobilizam três grupos separados [...] para trabalhar juntos em diferentes estágios" (Glynn, Hileman, Lerchner, & Sanglier, 2016). Nesse modelo, a primeira linha engloba os profissionais que monitoram e controlam os processos de trabalho, o que inclui a operação diária da Tecnologia da Informação. A segunda linha de defesa serve como apoio para a primeira linha, de modo a supervisionar e facilitar a implementação de práticas de gerenciamento de riscos, e a terceira linha engloba a auditoria interna, que age de forma independente das outras duas linhas, em caráter de supervisor delas (Instituto dos Auditores Internos, 2020). Interessante destacar que a Estratégia de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) se inspira nesse modelo, ao dispor que cada Tribunal, com exceção do STF, deve "[...] constituir estrutura de segurança da informação, subordinada diretamente à alta administração do órgão e desvinculada da área de TIC" (Conselho Nacional de Justiça, 2021). Esse modelo reforça a necessidade de existência de uma segunda linha de defesa independente, com segregação de papéis e funções na gestão desses riscos. Nesse sentido, este trabalho teve como objetivo comparar as estruturas organizacionais para a gestão da SI dos órgãos do Poder Judiciário do Distrito Federal (DF) à luz desse modelo. Esse trabalho é classificado como uma pesquisa de natureza aplicada, qualitativa, com objetivos exploratórios e descritivos. Como procedimentos técnicos se utilizou pesquisa documental onde foram levantados organogramas, portarias, atos normativos, planos estratégicos e demais documentos oficiais entre os meses de fevereiro e abril de 2022. Nos casos em que os documentos não foram suficientes, utilizou-se pedidos de acesso à informação às ouvidorias dos órgãos. No tratamento dos dados, foi utilizada a análise de conteúdo de Bardin (2016) sobre os documentos e informações obtidas, relacionando-as com as definições

do modelo extrapolando ao contexto de SI. Foram estudadas 4 (quatro) dimensões para cada um dos órgãos, sendo elas: se existia setor específico de SI; se esse setor era separado do setor de TIC; se havia comitê de SI; e se o comitê se reunia regularmente. Essas dimensões foram estudadas em seis tribunais do DF, a saber: TJDFT, TRF1, TST, STM, STJ e STF. Os resultados demonstraram que para a primeira dimensão, quatro tribunais tinham um setor específico de SI (STF, STJ, STM e TST). Na segunda dimensão, apenas o STF demonstrou ter um setor específico vinculado diretamente à alta administração. Nas terceiras e quartas dimensões, identificou-se um comitê de SI ativo em todos os tribunais, contudo, apenas 4 deles (STF, STJ, TRF1 e TST) demonstraram que os comitês estavam ativos, reunindo-se periodicamente. Dessa forma, não foram encontradas evidências de que os tribunais subordinados à ENSEC-PJ atendem a exigência de segregação em três linhas com um setor apartado da TI, já que apenas o STF possui essa estrutura. A literatura ressalta que a estrutura utilizada pelo STF aumenta a chance de que riscos e controles sejam gerenciados com eficiência (Anderson & Eubanks, 2015), podendo reagir de forma rápida às ameaças com tendência de ser mais inteligente perante os riscos (Potter & Toburen, 2016). Dentre as limitações desse trabalho, destaca-se que não foi possível aferir, de acordo com os documentos consultados, se os comitês realmente funcionam conforme declaração realizada pelos Tribunais, e se, porventura, os riscos da temática são identificados e apreciados por seus membros. Como sugestão para trabalhos futuros, pode-se ampliar o escopo de estudo dos Tribunais de forma que se conheça melhor a realidade da estrutura para gestão de SI em todo o país.

PALAVRAS-CHAVE: Segurança da Informação, Tribunais, Três linhas de defesa, Estratégia Nacional de Segurança Cibernética.

REFERÊNCIAS

Anderson, D. J., & Eubanks, G. (2015). Leveraging COSO Across The Three Lines of Defense. Carolina do Norte.

Bardin, L. (2016). Análise de Conteúdo. São Paulo: Almedina Brasil.

Conjur. (2021, maio 19). Polícia Federal prende dois suspeitos de tentar hackear a Justiça de São Paulo. Retrieved maio 10, 2022, from Consultor Jurídico: https://bit.ly/3Pp4TRg

Conselho Nacional de Justiça. (2021, jun 7). Resolução 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Brasilia, DF, Brasil.

Convergência. (2021, jul 13). Hacker que alterou decisões de quase R$ 1 milhão é denunciado na Justiça de São Paulo. (Convergência Digital) Retrieved maio 10, 2002, from Convergência Digital: https://bit.ly/3PbkmUN

Glynn, C., Hileman, D., Lerchner, H., & Sanglier, T. (2016). Practice guide: Internal audit and the second line of defense. Florida: Altamonte Springs.

Infomoney. (2021, mar 4). Brasil é o país com maior número de vítimas de phishing na internet. Retrieved maio 10, 2022, from Infomoney: https://bit.ly/37z6qTA

Instituto dos Auditores Internos. (2020). Modelo das três linhas do IIA. Flórida, EUA. Retrieved from https://bit.ly/3w3qQ0l

Moura, R. (2022, mar 28). A impunidade dos hackers que colocaram o Judiciário de joelhos. Retrieved maio 10, 2022, from Veja: https://bit.ly/3M7y6Om

Nunes, R., Perini, M., & Pinto, I. (2011). A gestão de riscos como instrumento para aplicação efetiva do princípio constitucional da Eficiência. Revista Brasileira de Políticas Públicas, 11(3). doi:10.5102/rbpp.v11i3.7903

Potter, P., & Toburen, M. (2016). The 3 lines of defense for good risk management.

Prado, F. (2021, dez 20). Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais. Retrieved maio 10, 2022, from Isto é Dinheiro: https://bit.ly/3L8Y3Me