Impacto de aspectos organizacionais, culturais e individuais na vulnerabilidade a falhas de Segurança da Informação

Bruna Raquel Castilhos Martins[1], Edimara Mezzomo Luciano[1] (orientador)

[1]*Faculdade de Administração, Contabilidade e Economia, PUCRS*

Resumo

Esta pesquisa concentra-se no estudo de aspectos não-técnicos sobre a Segurança da Informação, mais especificamente sobre o impacto de aspectos culturais, organizacionais e individuais na vulnerabilidade do ambiente de TI em relação à segurança da informação. O objetivo é identificar o impacto de aspectos culturais, organizacionais e individuais na vulnerabilidade de organizações em relação a falhas de Segurança da Informação. Metodologicamente um modelo de pesquisa foi desenvolvido, e estudos de caso foram realizados no sentido de validar o modelo e encaminhar o desenvolvimento de uma pesquisa survey no sentido de confirmar as hipóteses relacionadas ao modelo. Foram realizados seis estudos de caso, com dados sendo coletados através de entrevistas semi-estruturadas face-a-face com Gerentes/Diretores de TI e de Segurança da Informação, além de coleta de documentos, em especial das políticas de Segurança da Informação. Os seis casos analisados se constituem de empresas de médio e grande porte presentes do estado do RS, tendo sido dada preferencia para empresas cujos controlados sejam empresas multinacionais pela exigência em termos de Governança de TI (outros quatro casos estão em andamento). Os dados estão sendo analisados por meio de análise de conteúdo temática. As principais categorias relacionadas nas entrevistas são as seguintes (por dimensões do instrumento): a) Educação, Treinamento e Conscientização: ausência de familiaridade com os procedimentos; capacitação superficial; falta de conscientização; falta de treinamento; b) Controle Percebido, severidade das ameaças/punições: necessário mais treinamento para evitar a punição; quando não há punição os pequenos problemas se tornam grandes; as regras são válidas para todos os funcionários da empresa; deve-se ter mais orientação do que punição; a incidência não deve ser punitiva, a reincidência sim; c) Comportamento desejável/monitoramento: monitoramento é feito de forma reativa; monitoramento superficial; monitoramento diminui o risco; o monitoramento dificulta, mas não o bastante; verificado se o comportamento da pessoa é bem intencionado. Os dados das políticas de Segurança da Informação apontam a insuficiência de abordagem de aspectos humanos e comportamentais no regramento destas políticas, tornando-as insuficientes como mecanismos orientador e condutor de comportamentos relacionados a Segurança da Informação.