GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: UM RELATO DE EXPERIÊNCIA E SUGESTÕES PARA MELHORIA DO PROCESSO

IV Encontro de Produção de Pesquisa Científica de Servidores Docentes e Técnicos-Administrativos da UFC

Luiz Gonzaga Mota Barbosa, Amarildo Maia Rolim, Paulo Henrique da Silva Franco, Rafael Bezerra Firmo

A Superintendência de Tecnologia da Informação (STI) é responsável pela gestão de parte dos ativos de Tecnologia da Informação da Universidade Federal do Ceará. A fim de monitorar e reduzir as ameaças sobre estes ativos, foi implementado o processo de Gestão de Riscos de Segurança da Informação e Comunicações, conduzido pela, então, Divisão de Segurança da Informação (DSEG). Observando o organograma da STI, durante a pré-análise de seus ativos primários (serviços, processos e informações) foi obtido o Escore de Risco (ER) de cada divisão, considerando a probabilidade das ameaças levantadas e seus respectivos impactos sobre confidencialidade, integridade e disponibilidade. Adotando uma abordagem vertical (aprofundamento em uma divisão por vez) para seleção do escopo e obedecendo a ordem dos ERs obtida na pré-análise, foi selecionada a Divisão_X (ER=8,3), nome omitido por razões de segurança. Através de entrevistas e ferramentas especializadas, a análise de seus 63 ativos secundários apontou os seguintes níveis de risco: 9,4% muito alto, 28,1% alto, 31,4% médio, 10,9% baixo e 10,2% muito baixo. Ao final, foram entregues os Planos de Tratamento de Riscos de cada ativo, com sugestões para o tratamento das ameaças levantadas. Considerando o tamanho da equipe e as demais atividades da DSEG, a abordagem adotada para delimitação do escopo mostrou-se ineficiente, ficando as demais divisões descobertas por um longo período. Sugere-se a adoção de uma abordagem horizontal, aumentando a abrangência do escopo sobre as divisões, e de um percentual em cada nível de risco para a seleção de ativos primários em todas as divisões. Com isso, espera-se uma quantidade menor de ativos por iteração, porém selecionados dentre todas as divisões. A análise de todos os ativos da STI será alcançada incrementalmente, após consecutivas execuções do processo.

Palavras-chave: Gestão de Riscos. Segurança da Informação. Tecnologia da Informação.