5º Congresso de Responsabilidade Socioambiental da FSG

http://ojs.fsg.br/index.php/rpsic/index

A IMPORTÂNCIA DA CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO NO APRENDIZADO ORGANIZACIONAL

Ricardo Frigo Balbinot, Vinicius Zanchet De Lima*

*Vinicius Zanchet De Lima
Ricardo Frigo Balbinot, endereço: Rua 13 de maio, 1130.
Bento Gonçalves – RS. CEP:95702-002.
E-mail: contato@ricardofrigo.com.br

Palavras-chave:
Conscientização. Segurança. Informação. Treinamento.

INTRODUÇÃO/FUNDAMENTAÇÃO TEÓRICA: A definição de Segurança da Informação consiste em uma área de conhecimento voltada para a proteção dos ativos de informação, a fim de assegurar a confiabilidade, integridade e disponibilidade das informações, evitando, acessos e alterações indevidas (SÊMOLA, 2004). A literatura acerca da Segurança da Informação indica que a criação da Política de Segurança é sempre um dos primeiros passos para se implantar um sistema de gestão de segurança da informação (ISO 27001, 2013). Contudo, somente a criação da Política não é o bastante, o fator humano deve ser considerado, pois são as pessoas que devem cumprir a política estabelecida. Nesse sentido, as campanhas de conscientização são as ferramentas mais apropriadas para engajar as pessoas e garantir que estas recebam treinamento, educação e conscientização apropriados em consonância com as políticas e procedimentos organizacionais. **MATERIAL E MÉTODOS:** O método de pesquisa utilizado neste trabalho foi a pesquisa bibliográfica, que segundo Macedo (1994) é uma busca de informações bibliográficas referente a um tema específico, também pode ser chamada de revisão bibliográfica, pois apresenta o estudo de algo que já é conhecido. A revisão literária possui vários objetivos, tais como proporcionar o aprendizado sobre a área pesquisada e facilitar a identificação dos métodos utilizados (PIZZANI et al., 2012). **RESULTADOS E DISCUSSÕES:** A norma ISO/IEC 17799:2005, em sua seção introdutória, define segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as

oportunidades de negócio". A Segurança da Informação pode ser compreendida por "ações que objetivam viabilizar e assegurar a disponibilidade, integridade, a confidencialidade e a autenticidade das informações" (BRASIL, 2019). Conforme a ISO 27002 (2013) define que "De modo geral, uma segurança da informação eficaz também garante à direção e a outras partes interessadas que os ativos da organização estão razoavelmente seguros e protegidos contra danos, agindo como um facilitador dos negócios." Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos (BRASIL, 2012). Segundo a ISO 27002 (2013) Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. As políticas de segurança da informação devem ser apoiadas por políticas específicas do assunto, que exigem a implementação de medidas de controle de segurança que são estruturadas e visam cobrir as necessidades determinadas. Bada, Sasse e Nurse (2014) destacam que, um programa de conscientização e formação é fundamental, uma vez que é a fonte de divulgação da informação que todos os utilizadores envolvidos com Tecnologia da Informação necessitam. Os autores dizem que, no caso de um programa de segurança da informação, é o método mais comum utilizado para comunicar os requisitos de segurança e o comportamento adequado. Para que um programa de conscientização e treinamento seja eficaz, o material tem de ser interessante, atual e suficientemente simples para ser seguido. Qualquer conteúdo que seja muito comum e genérico para se aplicar ao público pretendido, será tratado pelos utilizadores como apenas como uma obrigação (BADA, SASSE e NURSE, 2014). O trabalho deve começar com seminários, workshops abertos voltados a compartilhar e conscientizar sobre os riscos e impactos ao negócio, principalmente se alguma ameaça se concretizar. Desta forma cada um passa a se enxergar como uma peça responsável para o bom funcionamento da empresa(SÊMOLA, 2014). **CONCLUSÃO:** Em um mundo cada vez mais conectado e digital, a segurança da informação se tornou um tema de extrema importância para empresas de todos os tamanhos e setores. A implementação de medidas de segurança tecnológica, como softwares e equipamentos é essencial para minimizar os riscos de ataques cibernéticos. No entanto, é igualmente importante investir na segurança da informação para os colaboradores da empresa. Ao enfatizar a importância da segurança da informação e mostrar como ela afeta a empresa, os colaboradores podem se tornar mais conscientes e responsáveis em relação ao seu papel dentro da empresa para desenvolver um bom desempenho e comprometimento com a sua organização.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação** — Requisitos, 2a Edição, 2013.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma Visão Executiva. Rio de Janeiro: Elsevier; 2ª Edição, 2014.

MACEDO, N. D. D. **Iniciação à pesquisa bibliográfica.** São Paulo: Edições Loyola, 1994.

PIZZANI, L.; SILVA, R. C.; BELLO, S. F.; HAYASHI, M. C. P. I. A arte da pesquisa bibliográfica na busca do conhecimento. **Revista Digital Biblioteconomia e Ciência da Informação**, v. 10, n. 1, p. 53-66, 2012.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** Uma Visão Executiva. Rio de Janeiro: Elsevier; 2ª Edição, 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 17799:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.** Versão 2. Rio de Janeiro, 2013.

BRASIL. Presidência da República/Gabinete de Segurança Institucional. Portaria no 93, de 26 de setembro de 2019. **Aprova o Glossário de Segurança da Informação.** Brasília, 2019.

BADA, M., SASSE, A. M., & NURSE, J. R. (2014). **Cyber security awareness campaigns:** Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

BRASIL. Tribunal de Contas da União. Secretaria de Fiscalização de Tecnologia da Informação. **Boas práticas em segurança da informação.** Brasília, 4ª Edição, 2012.