



Facens

FACULDADE DE ENGENHARIA DE SOROCABA

ESPECIALIZAÇÃO EM SEGURANÇA CIBERNÉTICA

Metodologia da Pesquisa Científica

REVISÃO DE LITERATURA

Filipe Sousa
Gelson Filho
Otávio Marelli

Professor: João Mattar

Sorocaba / SP
24/06/2022

1. INTRODUÇÃO

O presente trabalho tem por objetivo realizar uma breve revisão de literatura com a finalidade de colocar em prática o conhecimento que foi apresentado em sala de aula.

O tema selecionado para o desenvolvimento desta atividade é “Políticas de segurança da informação nas instituições de ensino superior”, e surge diante da necessidade que existe no atual mercado da tecnologia da informação de tratar a segurança dos dados como um recurso estratégico nas instituições. Espera-se alcançar através deste trabalho a contextualização dos principais problemas identificados na implementação de PSI (Política de Segurança da Informação) nas universidades, bem como as principais ações tomadas para mitigar estas ocorrências.

2. METODOLOGIA

As bases de dados selecionadas para realizar a pesquisa dos artigos que seriam revisados foram o Google Scholar (Google Acadêmico), e o Portal de Periódico CAPES, através dos quais, mediante a utilização de alguns recursos e ferramentas específicos, pode-se filtrar os materiais a serem revisados.

2.1 Google Scholar

Ao realizar a pesquisa do tema sem filtros algum, o Google Acadêmico retornou cerca de 600 mil resultados, filtrou-se então por “artigos de revisão”, reduzindo este valor para cerca de 15 mil resultados.

Ao se deparar com tal quantidade, foi necessário utilizar os operadores de pesquisas para limitar as informações a serem analisadas, portanto foram utilizados os operadores “aspas”, que retornam textos exatamente como descritos na frase de pesquisa, bem como o operador “AND”, que faz com que retornem apenas resultados que apresentem ambos argumentos pesquisados. O argumento final utilizado para gerar a pesquisa foi: “Política de segurança da informação” AND “instituição de ensino” AND “IES”. Tal argumento gerou 55 resultados.

2.2 Portal de Periódicos CAPES

A princípio foi inserido na busca o termo "Segurança da informação" no Portal de Periódicos CAPES, tendo como resultado 23.817 itens.

A fim de aplicar alguns filtros, implementaram-se filtros de publicações nos últimos dois anos, e para que se exibisse apenas artigos, obtendo um resultado na segunda busca de 4.111 itens.

Na terceira busca foram aplicados mais filtros, como o de exigência do termo "Segurança da informação" (com aspas), e foram adicionados outros termos que podem aparecer em qualquer campo, sendo estes: "Universidades, ensino, instituições federais" (sem aspas).

Ao término da busca no Portal de Periódicos CAPES, obteve-se um retorno de 15 itens que atendiam aos filtros utilizados.

2.3 Seleção dos artigos a serem revisados

Ao selecionar os textos que seriam revisados, priorizou-se textos que traziam uma abordagem específica acerca da implementação da PSI em instituições de ensino superior, visto que muitos artigos possuíam uma visão mais genérica do assunto abordado.

Foram identificados 8 artigos que poderiam ser utilizados para a realização deste trabalho, porém ao iniciar a leitura dos mesmos, notou-se que alguns apresentavam uma abordagem mais genérica sobre a área de segurança da informação, estes foram então descartados, e permaneceram 3 artigos selecionados pelo grupo a fim de realizar a atividade.

3. ARTIGOS LIDOS NA ÍNTEGRA

3.1 Artigo: Fatores que Influenciam a Predisposição em Seguir uma Política de Segurança da Informação em uma Instituição de Ensino Superior

O artigo publicado expõe que atualmente a informação é vista como um recurso estratégico, e que deve ser protegido para além de medidas como utilização de senhas e antivírus. De acordo com as pesquisas referenciadas, a maior parte dos danos causados na área da segurança da informação provém de ocorrências causadas por funcionários ativos e ex-funcionários. Mediante a pesquisa, constatou-se que o elo mais fraco na implementação de políticas de segurança da informação em uma instituição são as pessoas que fazem parte dessas organizações.

De acordo com o artigo, faz-se necessária a compreensão do comportamento das pessoas que fazem parte da organização a fim de que a implementação da PSI (Política de Segurança da Informação) ocorra com sucesso, investigando o quão dispostos os membros da organização estão ou não em seguir as diretrizes estabelecidas.

Após expor alguns mecanismos que poderiam ser utilizados para influenciar as pessoas a adotarem a PSI, sendo estes: a eficácia percebida; a severidade da punição; a certeza da detecção; o comprometimento moral; o comportamento dos pares; a intenção de conformidade. Os pesquisadores formularam as devidas hipóteses sobre as motivações de predisposição a seguir uma PSI e realizaram uma pesquisa de campo em uma universidade com os estudantes, obtendo 391 observações a serem analisadas.

Com a pesquisa realizada, utilizaram-se de diversos métodos estatísticos e de análise para verificar quais das hipóteses levantadas poderiam ser suportadas ou não, chegando à conclusão de que mecanismos punitivos ou de detecção, como a severidade de punição, e a detecção de infrações são mais influentes na decisão pessoal de seguir as medidas propostas pela PSI.

3.2 Artigo: Análise de tratamento da segurança da informação de uma instituição de ensino público federal.

Há muito tempo a Tecnologia da Informação e sua governança vêm se relacionando cada vez mais com o assunto de Segurança da Informação. Na área educacional de nível superior não é diferente, o setor de TI aprimora a cada dia seus fundamentos com objetivo de manter íntegro, confidencial e/ou com total disponibilidade determinadas informações de caráter institucional.

Diante deste contexto, o artigo apresenta uma pesquisa exploratória quantitativa após entrevista com 6 gestores de TI de 20 a 40 anos, das áreas de Sistemas, Suporte, Infraestrutura e Redes com perguntas previamente planejadas e definidas.

Os 10 questionamentos foram baseados em 5 genéricas dimensões: Organização de segurança e infraestrutura; Políticas de segurança, normas e procedimentos; Programa de segurança; Treinamento e conscientização da cultura de segurança; Adequação. Foram feitos diversos controles estatísticos e análises probabilísticas com as pesquisas feitas e as notas de 1 a 6 (onde 1 é “discordo completamente” e 6 é “concordo completamente”) dadas para cada um dos gestores com relação à pergunta que a eles fora realizada.

Com os dados, observou-se que os todos elementos abordados possuem relevância e que potencialmente melhorariam a compreensão do ambiente de riscos e sua gestão se bem implementados. Ademais, verificou-se que alguns elementos já incorporam com formidáveis resultados os ambientes educacionais de nível superior.

3.3 Artigo: Política de Segurança da Informação: Um modelo voltado para uma instituição de Ensino Superior.

A princípio o autor traça um objetivo geral e três objetivos específicos onde o objetivo geral é a entrega de um plano de Políticas de segurança da Informação baseada na ISO 27001/2005 com uma metodologia para implantação. E como objetivos específicos o autor propõem: O mapeamento dos processos (acadêmicos e administrativos); A realização de uma revisão literária que abrange desde a ISO 27001/2005 até segurança da informação no âmbito de instituições de ensino superior nos últimos dez anos; Mapear em conjunto com a Direção os setores que carecem de segurança afim de determinar quais serão priorizados.

Em seguida o autor já traz um breve resumo dos levantamentos realizados e conhecimentos adquiridos com o cumprimento dos objetivos específicos, em especial a Revisão literária que abrange mais de um tema relacionado a segurança da informação.

Para a etapa de metodologia o autor optou por uma abordagem qualitativa no âmbito de atender o objetivo geral, seguindo a premissa de compreender o comportamento de um grupo social/ organização. E para abordagem do problema o caminho seguido foi da abordagem mista, uma vez que se vê em um ambiente de estudos exploratórios.

Como instrumento de coleta de dados, o autor optou por utilizar um questionário online, hospedado na plataforma SurveyMonkey de 7 questões que abordaram mecanismos e processos basilares de segurança da informação e que foi disponibilizado para todos os funcionários, onde 152 de diversos setores responderam. O formulário serviu para traçar o perfil dos funcionários em relação a conhecimentos sobre segurança da informação.

Durante a descrição do caso o autor comenta sobre como a PSI (Plano de Segurança da Informação) foi elaborada e quais os aspectos que foram adotadas nela, sendo: Propriedade da informação, Controle de acesso, Gerência de usuários e senhas e Segurança Física.

Após a coleta dos dados e interpretação dos mesmos o autor traz suas considerações finais sobre alguns pontos dos objetivos específicos, onde se pode destacar como o estudo da literatura auxiliou na elaboração de uma PSI genuína que entregue bons resultados.

Também foi pontuado pelo autor a falta de políticas de segurança da informação, estado a qual a IES (Instituição de Ensino Superior) se encontrava no início do trabalho, poderia resultar em problemas que poderiam ser facilmente resolvidos com implementação de medidas simples como realização de backups, armazenamentos adequados e reuniões/ treinamentos que conscientizasse os colaboradores sobre questões básicas de segurança da informação.

Por fim é citado pelo Autor que o sucesso da PSI só pode ser garantido uma vez que as pessoas das instituições acatem de maneira profissional tais políticas. E como planos futuros é abordado a necessidade de dar continuidade da PSI e a implementação efetiva dela.

4. CONCLUSÃO

O artigo 3.2, apresenta um panorama onde os Gestores de TI mostram saber em suma as medidas que precisam ser tomadas dentro de um Plano de Segurança da Informação – PSI como também conseguem dimensiona-las sob o nível de influência sobre resultados finais. Mostram entender que os seguintes itens fazem parte de um PSI: Organização de segurança e infraestrutura, Políticas de segurança normas e procedimentos; Programa de segurança; Treinamento e conscientização da cultura de segurança. Apesar disso o artigo não contempla de fato os fundamentos do problema da segurança da informação sob esfera dos colaboradores de escalão menor e dos estudantes das instituições, apesar de avaliar a partir de uma pesquisa exploratória quantitativa que os itens citados anteriormente são profundamente relevantes.

Entretanto o artigo 3.3 supre de maneira mais significativa a abrangência do assunto com relação aos funcionários das instituições de ensino superior concluindo que a falta de maturidade dos colaboradores é um dos principais fatores que influenciam nos surgimentos de incidentes na área da segurança cibernética em instituições de ensino superior. Este artigo já apresenta mais aspectos sobre um notável PSI: Propriedade da informação, Controle de acesso, Gerência de usuários e senhas e Segurança Física. Bons resultados, segundo o artigo seriam conquistados após a realização de uma revisão literária que abrange desde a ISSO 27001/2005 até segurança da informação no âmbito de instituições

de ensino superior nos últimos dez anos e o mapeamento dos processos acadêmicos e administrativos e determinar por nível de prioridades cada um dos mesmos. Ao final compreende-se novamente que se os funcionários não mudarem o “mindset” e não colaborarem quanto aos hábitos contra incidentes na área de segurança cibernética, qualquer plano não terá satisfatórios resultados.

Outrossim, o artigo 3.1 bem cita o termo “recurso estratégico” para se referir à informação o que já automaticamente leva-nos a concluir que a segurança dela é de ponderada importância. Assim como todos os outros artigos, neste também fora feita pesquisa de campo, desta vez com estudantes. Após discussão dos dados da pesquisa, análises técnicas quantitativas, regressão logística, análise fatorial e de clusters junto a análise de critérios comportamentais do perfil pesquisado, o artigo define que os fatores que de maneira mais contundente predispoem os usuários de contribuírem para qualquer PSI são: severidade da punição, comprometimento moral, eficácia percebida, certeza de detecção e intenção de conformidade. Em suma o artigo 3.1 aborda mais uma relação humana com relação ao tema.

Destarte a pesquisa se baseou em 3 diferentes artigos no que se refere ao perfil das pessoas entrevistadas através de pesquisas de campo. Enquanto no primeiro pode-se verificar o assunto “Plano de Segurança da Informação – PSI” predominantemente sob o ponto de vista dos gestores de TI, no segundo pode-se verificar sob o ponto de vista dos estudantes das instituições e no terceiro pode-se ter conhecimento sob o ponto de vista dos funcionários em geral. Ambos completam uma linha de raciocínio interessante ao complementar com aspectos técnicos, humanos, tecnológicos, mútuos e conclusivos o que de fato configura-se um adequado Plano de Segurança da Informação.

5. BIBLIOGRAFIA

DA SILVA DAMASCENO, Larissa Mayara; RAMOS, Anatólia Saraiva Martins; DE MELO PEREIRA, Fernando Antonio. Fatores que Influenciam a Predisposição em Seguir uma Política de Segurança da Informação em uma Instituição de Ensino Superior. **Revista de Gestão e Projetos**, v. 6, n. 3, p. 01-16, 2015.

ARIMA, Carlos Hideo; BELDA, Francisco Rolfsen; SOUZA, Jackson Gomes Soares. Análise de tratamento da segurança da informação de uma instituição de ensino público federal. **Revista Ibero-Americana de Estudos em Educação**, v. 15, n. 3, p. 1309-1321, 2020.

DE OLIVEIRA, Ione Beatriz Pereira; FIGUEIREDO, Walter Costa Almeida; FARIA, Ana Carolina Cintra. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM MODELO VOLTADO PARA UMA INSTITUIÇÃO DE ENSINO SUPERIOR. **Revista Eletrônica Cosmopolita em Ação**, v. 6, n. 1, p. 21-30, 2020.

OKOLI, Chitu et al. Guia para realizar uma Revisão Sistemática de Literatura. **EAD em Foco**, v. 9, n. 1, 2019.