UM ESTUDO SOBRE GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÕES DO ENSINO SUPERIOR PÚBLICAS

A STUDY ON INFORMATION SECURITY MANAGEMENT IN PUBLIC HIGHER EDUCATION INSTITUTIONS

Eliana Maria Quintino[1]
Valter Gustavo Danzer[2]
Joacir Mauro da Silva Junior[3]
Fábio Iser[4]
Alberto Sampaio Lima[5]
Wagner Bandeira Andriola[6]

RESUMO
As políticas de segurança da informação são, de forma geral, expressas por meio de legislações que determinam o *modus operandi* dos usuários e beneficiários das informações. Neste estudo destacamos os avanços dos sistemas de informação no âmbito das instituições, em especial das públicas, com rápida abordagem sobre as instituições de ensino superior. Utilizando metodologia da pesquisa bibliográfica e documental, a finalidade foi desenvolver o tema com o intuito de apresentar as singularidades indispensáveis para a criação das políticas institucionais acerca do tema. Identificados como imprescindíveis no processo de implantação da Política de Segurança da Informação, o fator humano se mostra extremamente relevante ao estudo, identificando assim a necessidade de mudanças culturais e ao mesmo tempo a difusão do conhecimento das tecnologias da informação.
Palavras-chave: Segurança da Informação; Gestão da Informação; Educação Digital.

ABSTRACT
Information security policies are generally expressed through legislation that determines the *modus operandi* of users and beneficiaries of information. In this study we highlight the advances of information systems within institutions, especially public ones, with a quick approach to higher education institutions. Using bibliographic and documentary methodology the purpose was to develop the theme in order to present the singularities indispensable for the creation of institutional policies on the subject. Identified as essential in the process of implementation of the Information Security Policy, the human factor is extremely relevant to the study, thus identifying the need for cultural changes and at the same time the diffusion of knowledge of information technologies.
Key-words: Information Security; Information management; Digital education.

[1] Mestranda em Políticas Públicas e Gestão da Educação Superior pela Universidade Federal do Ceará (UFC). Servidora da UNEMAT.
[2] Mestrando em Políticas Públicas e Gestão da Educação Superior pela Universidade Federal do Ceará (UFC). Servidor da UNEMAT.
[3] Mestrando em Políticas Públicas e Gestão da Educação Superior pela Universidade Federal do Ceará (UFC). Servidor da UNEMAT.
[4] Mestrando em Políticas Públicas e Gestão da Educação Superior pela Universidade Federal do Ceará (UFC). Servidor da UNEMAT.
[5] Doutor em Engenharia de Teleinformática pela Universidade Federal do Ceará. Mestre em Informática Aplicada pela Universidade de Fortaleza. Bacharel em Ciência da Computação pela Universidade Estadual do Ceará.
[6] Professor Titular da Universidade Federal do Ceará (UFC), Pesquisador do CNPq (Nível 1C), Coordenador do Mestrado POLEDUC.

1 INTRODUÇÃO

Com o advento e consolidação do uso da tecnologia e a globalização, as atividades e procedimentos das organizações, sejam elas públicas ou privadas, tendem a abandonar o tradicional modelo pautado no uso de papel, caneta, fichas físicas, passando a ser operadas eletronicamente, revolucionando e alterando a maneira como se entende o trabalho, o ensino, a correspondência, o manuseio de documentos, etc. Bancos de dados gigantescos foram sendo construídos, contendo dados vitais e estratégicos e assim a informação passou a ser um ativo, essencial para o bom andamento em qualquer tipo de negócio.

Neste contexto, a informação passou a ser vista como uma ferramenta a favor do desenvolvimento e crescimento institucional, seja para dar visibilidade ao negócio, empresa ou instituição, seja para proporcionar maior agilidade nos serviços prestados, qualidade, busca de redução de custos, melhorando os processos produtivos, dando maior embasamento para uma tomada de decisão mais precisa, entre outros benefícios que a informação pode propiciar.

Em um cenário que se busca, cada vez mais, expandir negócios, manter-se perenemente no mercado, obter sucesso na competitividade, e ao mesmo tempo em que temos um mercado que precisa de decisões quase que instantâneas ao deparar-se com um problema, a informação representa, portanto, um ativo estratégico e vital para as organizações, assumindo um patamar mais valioso que qualquer outro ativo.

A importância da informação para o contexto atual, cresceu de forma a necessitar proteção especializada e uma Política de Segurança da Informação (PSI), fazendo a área de segurança da informação evoluir aceleradamente. O advento da tecnologia, o seu uso em todas as áreas, os benefícios propiciados, tudo é muito novo dentro da história humana, mas fez-se necessário pensar e buscar meios legais de implantar a PSI, visto que senhas numéricas ou biométricas, *Firewalls* ou antivírus, não representam mais uma segurança efetiva necessária para proteção da informação. Assim, as instituições percebem cada vez mais a relevância da PSI, do estabelecimento de padrões, normas, mecanismos, práticas e leis em busca de reduzir os riscos e vulnerabilidades, bem como proteger-se contra as ameaças.

Nessa perspectiva, em que se percebe a importância da informação e a necessidade de protegê-la, as instituições públicas têm, também, seu papel de proteger seus bancos de

dados e trabalhar com ele de forma a proporcionar o melhor desempenho dos serviços prestados, resguardando seus arquivos de dados de possíveis ataques.

Quanto às leis sobre o tema, ao longo dos anos as instâncias governamentais têm publicado decretos, normas e manuais visando a proteção necessária para os bancos de dados e a maneira adequada de utilizá-los. No ano 2000 o Presidente da República, percebendo o que vinha acontecendo sob perspectiva mundial quanto a segurança da informação, editou o decreto 3.505, onde instituiu-se a política nacional de segurança das informações. Nesse mesmo ano, criou-se o Grupo de Segurança da Informação (GSI), com o objetivo de apresentar recomendações mínimas para implantar uma Política de Segurança nos órgãos e entidades da Administração Pública Federal, bem como propor a adoção de Infraestrutura de Chaves Públicas do Poder Executivo Federal. (RIOS, TEIXEIRA FILHO e SILVA RIOS, 2017)

Um pouco mais adiante na história da Segurança da Informação, o Tribunal de Contas da União (TCU), buscando evitar a vulnerabilidade e a possibilidade de que os dados institucionais sejam utilizados de forma inadequada, podendo gerar consequência negativas, publicou o Acórdão 1.603/2008 – Plenário, onde se demonstrou a problemática dos quadros de segurança da informação. Diante dessa publicação, cujos resultados pouco mudaram ao longo dos anos, o Conselho de Defesa Nacional (CDN), publicou a Portaria nº 14/2015, onde consta a Estratégia de Segurança da informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018. (GUIMARÃES; SOUZA NETO; LYRA, 2018)

Estão disponíveis em sítios da Administração Pública Federal (APF), instruções, manuais e cartilhas relacionados à segurança da informação. Como exemplo pode ser citada a Cartilha Institucional Segurança da Informação e Comunicações: responsabilidade de todos, publicada em 2011 no site do Planalto, onde apresenta "[...] uma reflexão para mudança de atitudes pessoais e profissionais que assegurem a proteção dos recursos de informação e comunicações do Ministério." (BRASIL, 2011). Sob o prisma das leis, decretos, normativas e instruções, a APF, vem ao longo dos anos, desde o advento tecnológico, buscando implantar PSI em todos os órgãos públicos.

Na seção seguinte abordaremos a segurança da informação voltada para as Instituições de Ensino Superior, buscando enfatizar como o tema vem sendo discutido a partir de pesquisa bibliográfica, focados em Política de Segurança da Informação e Comunicação, Governança em Segurança da Informação e, no fator humano.

3 A GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM IES PÚBLICAS

A partir dos estudos realizados sobre o tema segurança da informação em instituições públicas, abordaremos a seguir, alguns artigos que retratam o tema, fazendo neste capítulo, uma síntese destes estudos para no capítulo seguinte realizarmos nossas considerações a respeito.

Rios, Teixeira Filho e Silva Rios (2017), no artigo Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação, buscaram identificar como se encontra o cenário da gestão de segurança da informação nas instituições pesquisadas, valendo-se da utilização de questionários e estudo de campo em todas as instituições federais de ensino superior do país. Os resultados demonstraram de forma clara que apenas 43% dessas instituições institucionalizaram a PoSIC. Essa situação é extremamente preocupante, pois como os autores citam, que:

> A segurança da informação só poderá ser obtida a partir da implantação de um conjunto de controles adequados, o que inclui a presença de uma PoSIC, estabelecendo, implementando, monitorando e fiscalizando o que for necessário na instituição para que os objetivos e metas institucionais possam ser alcançados. (RIOS; TEIXEIRA FILHO E SILVA RIOS 2017)

Os autores também citam que essa situação, quanto a falta de implantação de PoSIC está diretamente relacionada à alta gestão, e que uma possível solução para o caso seria a elaboração de um documento padrão que "[...] possa auxiliar as instituições de ensino a promoverem as etapas de levantamento, planejamento, desenvolvimento, execução e revisão da PoSIC de forma objetiva, clara e consistente, em conformidade com a legislação e padrões relacionados à segurança da informação, dada sua importância [...]" (RIOS; TEIXEIRA FILHO; SILVA RIOS, 2017).

Damasceno, Ramos e Pereira (2015) publicaram o artigo Fatores que Influenciam a Predisposição em Seguir uma Política de Segurança da Informação em uma Instituição de Ensino Superior, cuja pesquisa, pautada em estudos que revelam o fator humano como o maior desafio e ameaça à segurança da informação, demonstrou através dos dados coletados por meio de um *survey*, de análise quantitativa que, embora as políticas de segurança tenham um importante papel na proteção desse ativo, a severidade da punição pelo erro ou conduta, é o fator de maior influência na predisposição em seguir as normas, "[...] a pessoa se sentirá mais inclinada a seguir uma política ao saber que é monitorada e,

por consequência, haver a possibilidade de punição em caso de comportamento abusivo." (DAMASCENO; RAMOS; PEREIRA, 2015)

No estudo Segurança da informação na rede educacional IFF, publicado por Cunha, Gomes e Martins (2015), os autores aplicam técnicas de mineração de dados para identificar ameaças oriundas de tráfegos maliciosos que possam deixar vulneráveis dados de pesquisas, informação ou históricos acadêmicos ou mesmo congestionar a rede. Observa-se que identificar essas ameaças ou esses tráfegos indesejados, é o primeiro passo para aumentar a segurança, auxiliando ainda a traçar o perfil das ameaças, bem como proteger a rede bloqueando tais tráfegos e ainda, propicia a geração de regras de bloqueio.

> Pode-se concluir que a utilização das técnicas mineração de dados para a análise e extração de conhecimento a partir dos logs de segurança do tráfego de rede armazenados em banco de dados é de extrema valia para a ciência da informação, com foco especial na segurança da informação, protegendo o ativo principal do instituto, sendo que a aplicação deste trabalho já está sendo realizada com sucesso no Instituto Federal Fluminense. (CUNHA; GOMES; MARTINS, 2015).

Nessa perspectiva de tentar solucionar os problemas de segurança da informação, é que encontramos o artigo Modelo de Governança de Segurança da Informação para a Administração Pública Federal de Guimarães, Souza Neto e Lyra (2018). Publicado recentemente, nesse artigo os autores se propuseram a apresentar um modelo de GovSIC de acordo com as normas vigentes no país e, "[...]compatível com a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018." Após a identificação dos elementos concernentes a um modelo de GovSIC que atenda o que foi proposto, valendo-se da Norma ABNT NBR ISO/IEC 27014:2013, da NIST 800-100, de estudos comparativos frameworks de GOVSI de Mellado et al. (2011) e das normas brasileiras vigentes (DSCI). A base da proposta de modelo comparou modelos baseados na NIST, DSIC e ABNT e o modelo de melhor aplicabilidade após análise foi o modelo proposto pela ABNT, "Esta prioridade deve-se ao fato de o modelo da ABNT ser reconhecido como "boa prática" pelos órgãos fiscalizadores da APF e por ser uma norma reconhecida no mercado brasileiro."(GUIMARÃES; SOUZA NETO; LYRA,(2018).

O modelo proposto por Guimarães, Souza Neto e Lyra (2018), apresenta princípios de tanta relevância, que faremos um breve apanhado, dada sua importância.

Princípio 1: Aprimorar a segurança da informação em toda a APF, garantindo que as legislações sobre SI sejam entendidas e internalizadas;

Princípio 2: Estabelecer uma estratégia de investimento, promovendo o planejamento dos investimentos em SIC;

Princípio 3: Manter a conformidade legal, assegurando que a PoSIC, gestão de SI e APF cumpram as leis e normas;

Princípio 4: Desenvolver a cultura de SIC:

> A GovSI deve estimular a educação e conscientização da importância de SIC, promovendo, assim, mudanças comportamentais, de pessoas e das instituições, de forma a obter uma postura humana responsável e consciente, e elevar o grau de maturidade das instituições. A GovSI deve considerar que o comportamento humano é essencial para o alcançamento dos níveis de segurança desejados, portanto os objetivos, papéis, responsabilidades e responsabilizações devem ser explicitamente divulgados e conhecidos. (GUIMARÃES, SOUZA NETO e LYRA, 2018).

Princípio 5: Estabelecer ações colaborativas, promovendo a articulação e desenvolvimento de parcerias para o "[...] desenvolvimento dos profissionais de SIC da APF, a adoção de boas práticas, novas soluções tecnológicas e de estímulo ao desenvolvimento de novos produtos e serviços que aprimorem a SIC." (GUIMARÃES; SOUZA NETO; LYRA, 2018).

Princípio 6: Monitorar o desempenho da segurança, garantindo que as ações realizadas para a proteção da informação sejam adequadas e se mantenha nos níveis acordados e legais.

No princípio de número cinco, encontramos uma das fortes premissas pregadas por Candeias e Freitas (2017), em sua dissertação Política de Segurança da Informação em uma Instituição de Ensino Superior Pública: Estudo de caso Uneb. Nessa dissertação, o autor toma como princípio básico para a SI, que "A educação digital é indispensável para que a Segurança da Informação seja exercida com efetividade. [...] Padrões de proteção devem ser disseminados nos campi para que os usuários sejam educados e habilitados para utilização correta da computação."

4 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Conforme as abordagens tratadas neste texto, identificamos a necessidade da permanente implementação e aperfeiçoamento das políticas de Segurança da Informação nas instituições públicas com vistas a garantir o acesso e a integridade a essas informações. Permeia em especial por essa atividade a necessidade de capacitação e conscientização na

área com o usuário responsável por tal, visto este ser o elo com os demandantes das informações, assim como serem fundamentais para a tomada de decisões no âmbito da administração público.

Os conceitos de construção de uma política de segurança de informação trazem como elementos basilares a confidencialidade, integridade e disponibilidade, sendo que eles são complementares entre si, desconfigurando-se, portanto, a segurança da informação com a não observância de qualquer destes elementos. A falta de formalidade na definição de normas de Segurança da Informação não propicia o desenvolvimento da área ao mesmo passo que a instituição fica prejudicada no todo, visto não atingir de forma eficaz os objetivos institucionais.

A construção administrativa das instituições públicas, derivadas do seu modelo burocrático de gerenciamento, somado a forma de construção das políticas institucionais de forma participativa e democrática das instituições de ensino superior, gera uma complexidade ainda maior na definição de políticas de sistemas de informação nessas instituições. O uso adequado de ferramentas e a sensibilização do quadro de usuários de acesso as informações é primordial, em especial a instituições que tem por premissa a oferta e o desenvolvimento de qualificação pessoal e de pesquisas (ANDRIOLA, 1997).

Desta maneira é fundamental o desenvolvimento e a implementação de uma Política de Segurança da Informação para que todo o sistema organizacional das informações seja protegido, direcionando essas informações ao seu usuário final, devidamente, para o bem da instituição. Essa política deve definir as diretrizes, os limites de cada integrante do sistema e ainda a direção que a instituição dará ao controle implementado na proteção das suas informações (ANDRIOLA; Mc DONALD, 2003). Como possibilidades de execução de trabalhos futuros, pretende-se realizar uma avaliação da gestão de segurança em uma IES pública, com base nos guias de melhores práticas de gestão de TI e segurança.

5 REFERÊNCIAS

ANDRIOLA, W. B. Expectativas de estudantes do 2º grau sobre a Universidade. **Educação em Debate**, Fortaleza, 33, p. 39-45, 1997.

ANDRIOLA, W. B.; Mc DONALD, B. C. (Org.). **Avaliação. Fiat Lux em Educação**. Fortaleza: Editora da Universidade Federal do Ceará, 2003.

BRASIL. **Segurança da Informação e Comunicações:** Responsabilidades de todos. Brasília, 2011. Disponível em: http://www4.planalto.gov.br/cgd//assuntos/publicacoes/segurancadainformacao_mte.pdf Acesso em 21/07/2019.

CANDEIAS, I. S.; FREITAS, T. P. de. Política de Segurança da Informação em uma Instituição de Ensino Superior. **Revista Gestão Universitária**. v. 8, p. 1-14, 2017.

CANONGIA, C.; MANDARINO JUNIOR, R. Segurança cibernética: o desafio da nova Sociedade da Informação. **Revista Parcerias Estratégicas**, v. 14, n. 29. Ministério da Ciência e Tecnologia, 2009.

CUNHA, A. de A.; GOMES, G. R. R.; MARTINS, S. N. Segurança da informação na rede educacional IFF. **Ibict Ciência da Informação**, v.44, n. 3, p. 475-487, 2015.

DAMASCENO, L. M. da S.; RAMOS A. S. M.; PEREIRA, F. A. de M. 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, 2015.

GUIMARÃES, R.; SOUZA NETO, J.; LYRA, M. R. Modelo de Governança de Segurança da Informação para Administração Federal. **Perspectivas em Gestão & Conhecimento**, v. 8, n. 3, p. 90-109, 2018.

RIOS, O. K. L.; TEIXEIRA FILHO, J. G. A.; RIOS, V. P. S. Gestão de Segurança da Informação: Práticas Utilizadas pelas Instituições Federais de Ensino Superior para Implantação de Política de Segurança da Informação. **NAVUS - Revista de Gestão e Tecnologia**, v. 7, n. 2, p. 49-65, 2017.