doi.org/10.51891/rease.v9i9.11299

AS POLÍTICAS DE SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

Tácito Augusto Farias Júnior[1]

RESUMO: Atualmente a sociedade se encontra cada vez mais globalizada e em estado de evolução, sendo assim as organizações obrigatoriamente precisam da disponibilidade de informações para o devido funcionamento de forma ágil, eficaz e segura das aplicações e atividades rotineiras, garantindo a confiabilidade e integridade dos dados pessoais. Neste estudo serão abordadas normas e políticas para gestão e monitoramento na proteção de dados, além de medidas essenciais que tratam de atitudes suspeitas nos sistemas de informação. Para atingir o objetivo proposto, foi feita uma revisão bibliográfica de maneira prática, que permitiu o desenvolvimento de um questionário para realizar a coleta de dados, sendo que posteriormente, foram recolhidas respostas de 20 profissionais de Tecnologia da Informação residentes no Brasil. A conclusão do estudo demonstrou que a maioria dos profissionais entrevistados utilizam normas ou políticas para gerenciar e monitorar a segurança dos sistemas de informação dentro das organizações onde trabalham.

Palavras-chave: Disponibilidade. Integridade. Confiabilidade. Normas e políticas. Segurança da Informação.

ABSTRACT: Currently, society is increasingly globalized and in a state of evolution, so organizations necessarily need the availability of information for the proper functioning of applications and routine activities in an agile, effective and safe manner, ensuring the reliability and integrity of personal data. . This study will address standards and policies for data protection management and monitoring, as well as essential measures that deal with suspicious attitudes in information systems. To achieve the proposed objective, a bibliographical review was carried out in a practical way, which allowed the development of a questionnaire to collect data, and responses were subsequently collected from 20 Information Technology professionals residing in Brazil. The conclusion of the study demonstrated that the majority of professionals interviewed use standards or policies to manage and monitor the security of information systems within the organizations where they work.

Keywords: Availability. Integrity. Reliability. Standards and policies. Information security.

1. INTRODUÇÃO

A informação é um ativo importante, como qualquer outro, é um elemento fundamental para os negócios da organização, sendo necessária a sua devida proteção. O resultado da crescente interconexão da informação ocasionou um aumento e uma enorme variedade de ameaças e vulnerabilidades.

[1] Engenheiro de Software pela UniCesumar.

A segurança da informação está associada à existência de ameaças, vulnerabilidades, ataques e riscos que podem comprometer o funcionamento de Sistemas de Informação em organizações, sendo essencial tomar atitudes quanto à identificação e caracterização para obter um resultado positivo e realizar a proteção caso ocorra alguma destas situações indesejáveis. A segurança da informação é definida como a junção entre confidencialidade, integridade, responsabilidade, confiança, honestidade e ética.

Os problemas referentes à segurança se resumem a ausência de medidas relacionadas diretamente à segurança da informação dentro da organização. Como também é possível haver uma estrutura de medidas realizada pela empresa, porém, torna-se necessário repassá-la corretamente aos funcionários através da utilização dos canais de comunicação de maneira adequada. As organizações precisam tomar medidas e realizar adaptações necessárias na estrutura para se prevenir de fraudes, corrupção, danos e adulteração da informação por usuários não autorizados.

A partir do desenvolvimento de um tema, para configurá-lo dentro de uma perspectiva científica, necessitamos considerar em destaque elementos-chave que possibilitam a sua justificativa: a importância do problema, a contribuição do autor para solucionar o problema e a viabilidade da execução.

Na importância do problema, cabe destacar a perspectiva das políticas de segurança da informação em contexto com a sociedade tecnológica atual. A proteção dos dados se apresenta como um elemento fundamental para a solução do problema em pauta.

No que se concerne a contribuição do autor para a solução do projeto em questão, ela, não, necessariamente, precisa ser original, porém, deve ser descrita segundo a capacidade de entendimento do referido autor em relação ao problema em pauta, utilizando a literatura corrente atualizada.

Levando em consideração a questão da viabilidade do projeto, cumpre destacar que o mesmo será desenvolvido utilizando-se da literatura brasileira e internacional consoante o gabarito do tema em pauta, ou seja, teremos uma visualização tanto através da parte escrita (livros, artigos, revistas e outros), como também fazendo o uso da internet. Toda e qualquer atitude não perpassa qualquer custo financeiro que acarrete qualquer problema para o desenvolvimento da temática em pauta.

2. REFERENCIAL TEÓRICO

A obra de (BEAL, 2005) trata da proteção de ativos ligados à informação que ao decorrer do tempo alcançam o status de um ponto estratégico para as organizações, principalmente, quando se trata do elevado valor atribuído aos ativos, como os impactos prejudiciais causados pela destruição, modificação ou repercussão inadequada de informações acarretando problemas para a organização. O trabalho da autora apresenta boas soluções para realizar o tratamento das questões ligadas à segurança da informação de forma geral, utilizando como base os princípios de boas práticas, sendo assim, as organizações terão como projetar estratégias eficientes para uma melhor proteção dos seus ativos digitais. Por mais que a obra tenha um ótimo conteúdo e boas intenções, acaba limitando-se muito na questão de políticas de segurança, sem fazer uma abordagem mais profunda em ferramentas ou métodos que possam ser úteis e ajudem a solucionar problemas que possam vir a ocorrer dentro do contexto de segurança da informação da organização.

Os autores (FUGINI; BELLETINI, 2004) ressaltam a importância que os sistemas de informação têm obtido dentro das empresas e que estão se transformando em heterogêneos, já que os dados e as demais aplicações abrangem diversos locais e distintas plataformas. Os problemas da segurança nos sistemas vão além da privacidade ou confidencialidade dos dados, existem muitos processos que lidam diretamente com o usuário e também com a autenticidade de dados, seja quando se trata da segurança física, ou de questões relacionadas à organização. O trabalho demonstra diversas pesquisas atuais que abordam sobre os sistemas integrados, como também as novas exigências de segurança da informação. A obra se limita em retratar problemas que são enfrentados dentro das organizações, sendo assim não retratando um melhor cenário para a resolução de falhas que possam ocorrer com constância nos sistemas de informação da organização.

A primeira hipótese trata-se do desenvolvimento de políticas relacionadas à segurança da informação, sendo assim estruturando a organização contra possíveis ataques que ocorram sendo originados internamente ou não (KNAPP; MORRIS; MARSHALL; BYRD, 2009).

A segurança da informação apresenta uma composição repleta de modelos e características, a gestão impõe que sejam consideradas questões técnicas, da organização, da estrutura, do comportamento e também relacionadas aos aspectos que envolvem a sociedade (DHILLON, 2004).

Segundo (KNAPP; MORRIS; MARSHALL; BYRD, 2009), a definição, o planejamento e o controle de políticas relacionadas a segurança da informação são hipóteses estabelecidas para tipos de comportamentos considerados aceitáveis, além de influenciar nas tomadas de decisão e no conjunto de padrões, levando em consideração à implementação de um plano de boas práticas para realizar a segurança na organização.

Para (KRUGER e KEARNEY, 2008), ao realizar a abordagem para implementação dos controles de segurança, é necessário criar e divulgar o conjunto de métodos e normas de boas práticas e de comportamentos para que sejam vistos e adotados por completo. As organizações, definem os métodos aplicados na segurança dos Sistemas de Informação, os quais são motivados pelos usuários a realizar as aplicações desejáveis, demonstrando através do uso de simulações que as ações tomadas podem ocasionar vulnerabilidades e, por consequência, ataques que possam comprometer o funcionamento dos Sistemas de Informação da organização (WORKMAN; BOMMER; STRAUB, 2008).

Realizar cópias de segurança ou backups, é um método fundamental que visa garantir a disponibilidade da informação, se porventura as bases de dados nas quais as informações estão armazenadas sofram algum tipo de dano ou forem roubadas. O backup irá obter pelo menos duas ou mais cópias sendo armazenadas em locais diferentes e seguros. Podendo ser armazenados tanto em dispositivos físicos, como também servidores de backup, pen drive, Hard Disk (HD) externo, ou então, em Cloud (nuvem). Sendo mais relevante assegurar que tenha sempre mais de uma cópia armazenada em local seguro (POSITIVO, 2017).

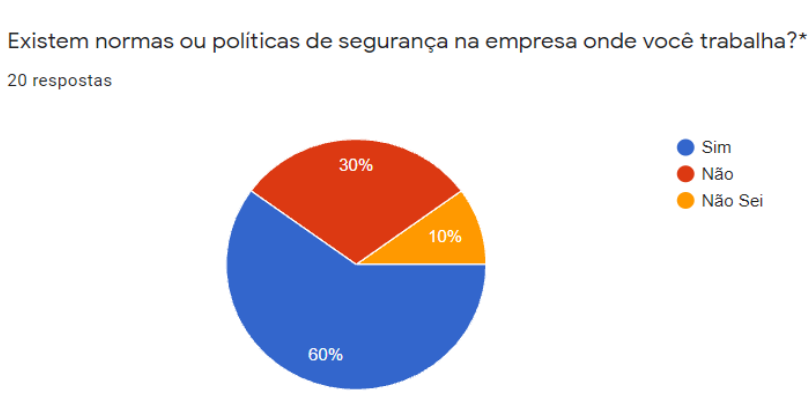
3. METODOLOGIA

A metodologia implantada no projeto inicialmente foi de caráter exploratório com uma revisão da literatura, sendo assim obtendo uma maior familiarização sobre como realizar o uso de normas e políticas de segurança para a proteção de dados. Posteriormente, houve a realização da coleta de dados através de um questionário voltado à segurança da informação no ambiente de trabalho composto por 4 perguntas, sendo respondido por 20 profissionais atuantes na área de tecnologia da informação.

4. ANÁLISE DE DADOS

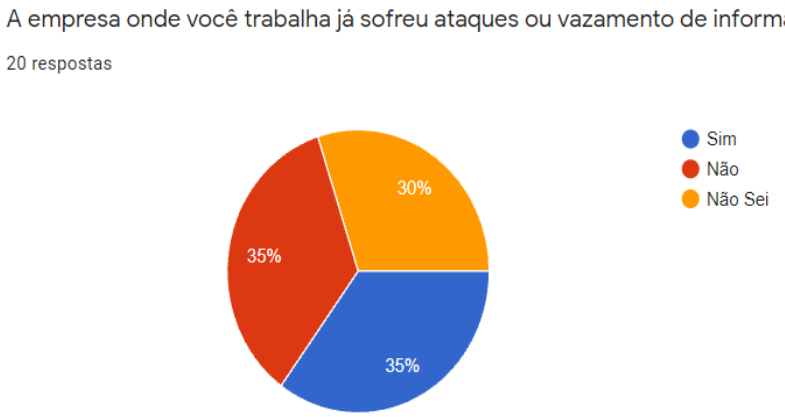
O questionário a seguir, foi elaborado de forma objetiva como proposto. Na coleta dos dados foram recolhidas respostas de 20 profissionais de TI que atuam diretamente com

Tecnologia da Informação no ambiente de trabalho. A seguir, será apresentado um gráfico em formato de pizza, demonstrando os resultados que foram obtidos na primeira pergunta do questionário.



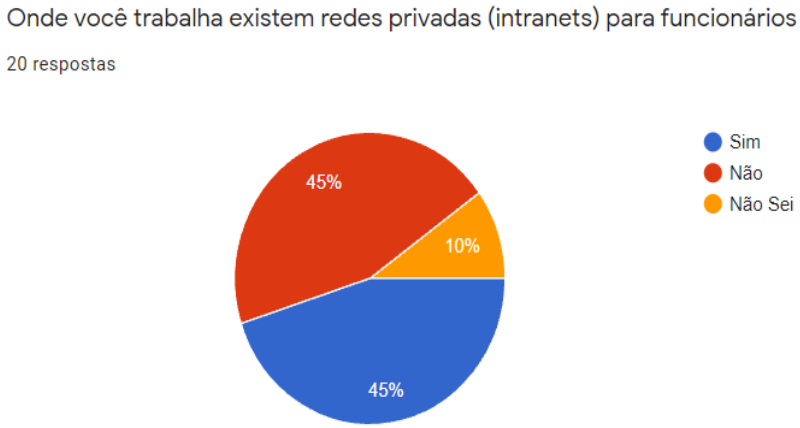
Conforme os dados expostos acima, podemos constatar que 60% dos entrevistados confirmaram o uso de normas ou políticas de segurança da informação no ambiente de trabalho. É importante ressaltar que 30% dos entrevistados declararam não haver qualquer uso de norma ou política de segurança, sendo assim, é possível afirmar que essas empresas correm sérios riscos de segurança e podem tornar-se alvos extremamente fáceis para os invasores. Os outros 10% disseram que não sabem se há algum tipo de regulamentação voltada para segurança da informação.

Na pergunta seguinte, podemos relacionar diretamente a implementação da nova Lei Geral da Proteção de Dados, conforme a mesma fonte de dados foi questionado aos entrevistados sobre ataques ou vazamentos de informações que tenham ocorrido no ambiente interno da empresa.

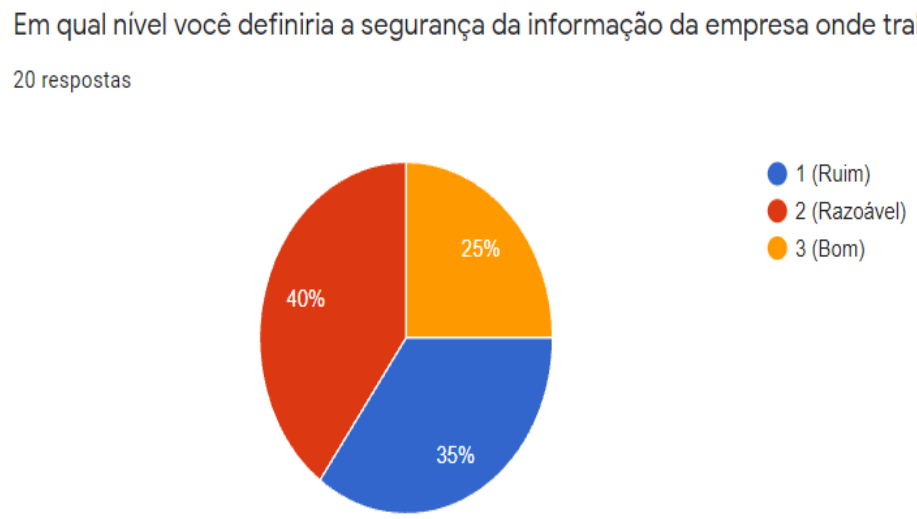


Percebe-se que 35% dos respondentes confirmam ataques ou vazamentos de dados originados no ambiente de trabalho. Sendo que 35% dos entrevistados responderam não para eventuais ocorridos e os 30% restantes disseram não saber.

Na pergunta seguinte foi questionado se existem redes privadas, mais conhecidas como intranets, na empresa onde trabalham.



No gráfico acima demonstra que apenas 45% dos participantes da entrevista informaram sobre a existência das redes privadas para funcionários e fornecedores no local de trabalho. Se tratando da não existência das intranets, a porcentagem obtida também foi de 45% dos entrevistados, restando um total de 10% para aqueles que não sabem se a empresa adota este tipo de procedimento internamente.



Por fim, é possível observar o gráfico acima representando a última pergunta do questionário, onde os entrevistados definem qual o nível de segurança da informação do local de

trabalho. Se tratando do alto nível (Bom) de segurança a porcentagem foi de apenas 35%, sendo que 40% dos entrevistados optaram pelo nível razoável de segurança e os demais 25% por nível baixo (Ruim).

CONCLUSÃO

Na pesquisa, foram explícitas as necessidades do uso das normas e políticas de segurança da informação que devem ser implementadas na infraestrutura de redes de computadores das empresas nos dias atuais, evitando a exposição dos dados e auxiliando na proteção, eliminando o alto risco oferecido por ataques aos sistemas de informação. É possível observar através dos resultados obtidos na pesquisa que muitas empresas ainda hoje não fazem investimentos voltados para adoção de normas e políticas de segurança da informação, sendo assim, possibilitando aos invasores um terreno limpo e de fácil acesso, colocando em risco a integridade, disponibilidade e confidencialidade das informações armazenadas nos bancos de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

BEAL, A. (2005). Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas.

DHILLON, G. (2004). Realizing benefits on an information security program. Business Process Management Journal, 10, p. 260-261.

FUGINI, M., & BELLETINI, C. (2004). Information Security, Policies and actions in modern integrated systems. Idea Group Inc, 2004. 341 p.

GAIVÉO, J. M. (2008). As pessoas nos sistemas de gestão da segurança da informação. Obtido de http://repositorioaberto.uab.pt/handle/10400.2/1272.

ISO/IEC 17799. (2005). Noma ISO. Obtido de http://www.aulasemparedes.com.br/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf.

KNAPP, K. J., MORRIS, R. F., MARSHALL, T. E., & BYRD, T. A. (2009). Information security policy: An organizational-level process model. Computers & Security, 28, p. 493-508.

KRUGER, H. A., & KEARNEY, W. D. (2008). Consensus Ranking - An ICT security awareness case study. Computers & Security, 27, p. 493-508.

POSITIVO (2007). Princípios e práticas da segurança da informação. Obtido de https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao/.

WORKMAN, M., BOMMER, W. H., & STRAUB, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24, p. 2799-2816.