Políticas para Segurança da Informação na saúde: uma abordagem baseada na Lei Geral de Proteção de Dados com foco no operador de tratamento

Roberta Cláudia de Jesus Bordalo[1], Mônica Ferreira da Silva[1]

[1]Programa de Pós-Graduação em Informática – Universidade Federal do Rio de Janeiro (UFRJ)
Caixa Postal 2.324 – 21. 941-916 – Rio de Janeiro – RJ – Brasil
{roberta.bordalo, monica.silva} @ppgi.ufrj.br

Abstract. *In the context of security of information, under the General Data Protection Law, this article presents a research project that aims to propose awareness and cultural change related to the culture of information security to operators processing personal and sensitive data ihealth.*

Resumo. *No contexto da segurança da informação, nos termos da Lei Geral de Proteção de Dados, este artigo apresenta um projeto de pesquisa que tem por objetivo propor conscientização e mudança cultural relacionada à cultura em segurança da informação aos operadores de tratamento de dados pessoais e sensíveis, na área da saúde.*

1. Introdução

A Segurança da Informação (SI) concentra-se na proteção dos ativos da informação. Empregando esforços para impedir acessos não autorizados, alterações indevidas e indisponibilidade às informações. Transcende, portanto a segurança em Tecnologia da Informação (TI), pois, além de envolver a TI, envolve também as pessoas, os processos e o ambiente institucional.

A Lei Geral de Proteção de Dados (LGPD) é o instrumento jurídico que garante o direito à privacidade. Anuncia ao cidadão maior controle e transparência sobre seus dados. Entre outras coisas, a lei proíbe o tratamento de dados pessoais e sensíveis para práticas ilícitas ou abusivas.

Segundo a LGPD (2018), entende-se por dado pessoal a informação que pode ser atrelada a uma pessoa identificável. E, por dado sensível, o dado pessoal que pode levá-la a sofrer discriminação, como exemplo: origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Por agente de tratamento, de acordo com a LGPD, entende-se como o

controlador e o operador dos dados. O controlador representa a pessoa, natural ou jurídica, a quem competem as decisões referentes ao tratamento dos dados pessoais. Já o operador, a pessoa natural ou jurídica que realiza o tratamento em nome do controlador.

O fator humano é considerado o elo mais importante e vulnerável em um sistema de informação. O alto investimento no desenvolvimento de soluções tecnológicas costuma dificultar a exploração das vulnerabilidades técnicas. Assim, e por empregar baixo capital, os atacantes apelam cada vez mais para exploração do elemento humano, enquanto um dos pilares estratégicos à gestão de segurança da informação.

A pesquisa TIC Saúde, produzida pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.BR, 2020), analisa o estágio de adoção de TIC e desenvolve indicadores em estabelecimentos de saúde brasileiros. Na Figura 1, podemos observar que, em pesquisa realizada no ano de 2018, do total de estabelecimentos de saúde que utilizaram a Internet nos últimos 12 (doze) meses, 79% (setenta e nove por cento) possuem dados cadastrais dos pacientes disponíveis eletronicamente.

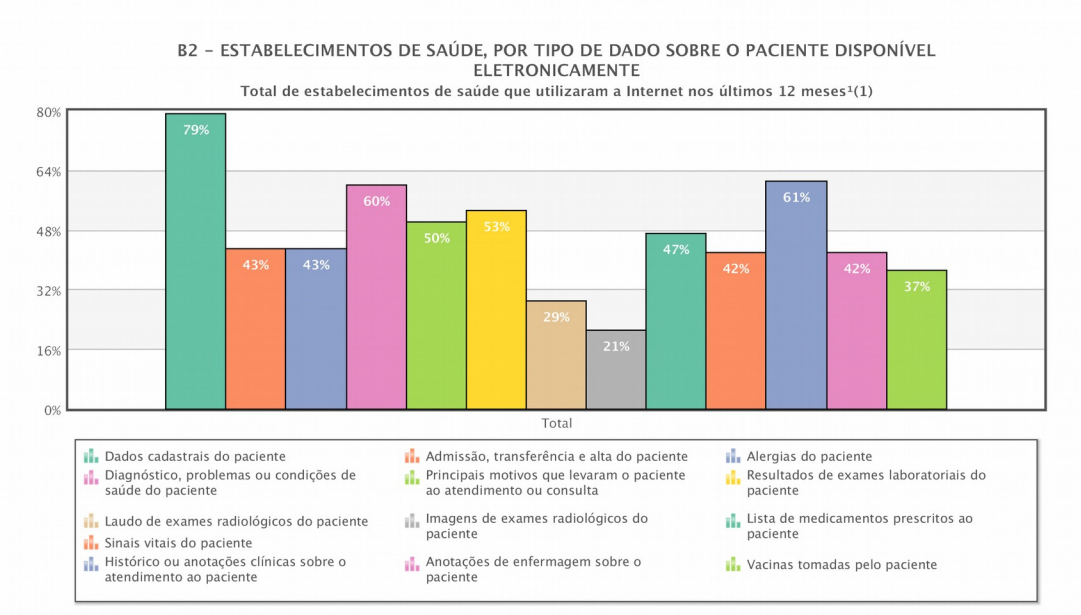

Figure 1. Estabelecimentos de saúde que utilizaram a Internet nos últimos 12 meses (Fonte: CETIC.BR,2018)

No contexto da Saúde e a sua relação com a LGPD, o estudo pretende conhecer a percepção dos médicos de uma unidade hospitalar, identificando seus conhecimentos sobre os principais conceitos e situações em segurança da informação, em especial, relacionada às políticas do sistema de gestão de segurança da informação ao qual integram.

O objetivo do presente trabalho é indicar ações proativas capazes de mitigar riscos em segurança da informação no que se refere à proteção aos dados do titular, no

âmbito da saúde.

Diante do exposto, almeja-se responder: como as ações proativas podem impulsionar os operadores de dados a uma mudança cultural relacionada à segurança da informação, nos termos da LGPD?

2. Fundamentação Teórica

Segundo Sêmola, segurança da informação é "área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade." (SÊMOLA, 2003, p.43).

Segundo a lei, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (LGPD, 2018, Art.46).

O Código de Ética Médica (CEM) aborda princípios, direitos e deveres dos médicos. A Resolução No. 2.217/2018 entrou em vigor a partir de 30 de abril de 2019, abordando temas como o uso de redes sociais e instrumentos correlatos, no exercício da profissão. Tal uso, de acordo com o Art.37 §2º, deve respeitar as normas elaboradas pelo Conselho Federal de Medicina (CFM).

Segundo o Art. 73, do Capítulo IX, que versa sobre o Sigilo Profissional, é vedado ao médico "Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente." (CRM, 2008, p. 35).

3. Metodologia de Pesquisa

Quanto à abordagem, a pesquisa tem natureza qualitativa. Quanto aos procedimentos, pretende-se utilizar o método de estudo de caso, que, segundo Yin (2001), este método foca nos acontecimentos contemporâneos e não exige controle sobre os eventos comportamentais.

Quanto à unidade de análise da pesquisa, como grupo social participante, pretende-se uma instituição pública hospitalar localizada no estado do Rio de Janeiro. Caracterizando assim, um projeto de caso único de análise.

Com relação aos sujeitos da pesquisa, pretende-se selecionar os médicos, como operadores de dados desta população. E a coleta dados primários, utilizará como instrumentos: documentos, observação direta e entrevistas.

4. Resultados Esperados

O trabalho pretende contribuir para uma mudança cultural relacionada à segurança da informação. De forma que o operador de tratamento de dados aproprie-se da sua

importância e do valor das informações às quais possui acesso.

A proposta de solução, ao final do estudo, ambiciona deixar como legado, ao grupo social participante, o conhecimento sobre ações relacionados a prevenir o comprometimento de informações institucionais, nos ambientes pessoal e profissional. Além de esclarecer sobre os possíveis impactos e efeitos do desconhecimento e/ou da inocência, diante de uma ameaça.

5. Considerações Finais

Este projeto está na fase embrionária e carecerá de ajustes, conforme a pesquisa avance. Entretanto, a proposta inicial é a criação de um produto digital, como: cartilha ou perfil em rede social, ao grupo social participante, com o objetivo de conscientização e mudança cultural relacionada à SI dos dados pessoais e sensíveis dos titulares.

Referências

Associação Brasileira de Normas Técnicas (ABNT). NBR ISO/IEC 27001:2013. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2013.

Brasil. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da República Federativa do Brasil, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em: 02 de julho de 2021.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br). Portal de Dados: TIC Saúde. Disponível em: <https://cetic.br/pt/pesquisa/saude>. Acesso em: 02 de julho de 2021.

Conselho Federal de Medicina (CFM). Código de ética médica: resolução CFM No. 1.931/2009. Brasília: CFM, 2010.

Conselho Federal de Medicina (CFM). Manual de publicidade médica: resolução CFM No. 1.974/11. Brasília: CFM, 2011.

Dias, Donaldo S.; Silva, Mônica F.. Como Escrever uma Monografia: Manual de elaboração com exemplos e exercícios. São Paulo: Atlas, 2010.

Pinheiro, P. P. Proteção de Dados Pessoais. 2a. ed. São Paulo: Saraiva Jur, 2020.

Sêmola, Marcos. Gestão de segurança da informação: uma visão executiva. 3.ed. Rio de Janeiro: Elsevier, 2003.

Yin, Robert K.. Estudo de Caso: planejamento e métodos. Tradução de Daniel Grassi. 2.ed. Porto Alegre: Bookman, 2001.