RISCOS DE SEGURANÇA DA INFORMAÇÃO EM HOSPITAIS: PROFISSIONAIS DE ENFERMAGEM E A LEI LGPD

ELOIR MARQUES DA SILVA

RESUMO

O presente trabalho justifica-se pela importância dos profissionais de enfermagem em lidarem com a segurança da informação em hospitais, pois esses ambientes lidam com dados sensíveis e confidenciais de pacientes, além de informações críticas sobre o funcionamento da instituição, uma vez que os incidentes de segurança cibernética representam uma ameaça crescente para o setor da saúde como um todo. Nesse sentido, o objetivo fundamental é que esses profissionais tenham conhecimento sobre a Lei de Proteção de Dados, além de receberem treinamentos em equipe. Afinal, as falhas de ordem humana são um dos pontos fracos na segurança cibernética e é importante aumentar a conscientização entre todos os colaboradores dos hospitais, em todas as áreas. Recomendações práticas também devem ser propostas para os usuários finais, como a prática de alterar sempre as senhas em novos dispositivos, o uso de senhas fortes, evitar deixar dispositivos sem supervisão e evitar a conexão com serviços de WiFi públicos. Este trabalho é uma revisão bibliográfica baseada em pesquisas nas bases de dados da Biblioteca Virtual em Saúde (BVS), Literatura Latino Americana e do Caribe em Ciências da Saúde (LILACS) e *Scientific Electronic Library Online* (SCIELO), bem como em jornais, revistas e artigos. Seu objetivo é enriquecer o meio acadêmico ao sintetizar os resultados encontrados, justificando a importância do conhecimento da Lei Geral de Proteção de Dados (LGPD) no ambiente hospitalar. Tal relevância se fundamenta no crescente número de ataques cibernéticos direcionados a essas instituições. Contudo de maneira mais geral, os hospitais devem ser aconselhados a realizar exercícios simulados anuais para provedores e outros funcionários, incorporando as lições aprendidas com ataques recentes. Embora essas práticas envolvam o engajamento da equipe e sejam recomendadas para manter todos vigilantes, é crucial que os hospitais possuam uma equipe de liderança, governança e tecnologia da informação (TI) dedicada à segurança cibernética.

Palavras- chave: saúde, cibersegurança e Lei de Proteção de Dados.

1. INTRODUÇÃO

Atualmente a segurança da informação é um desafio crucial para os profissionais de enfermagem nos hospitais no século XXI. É fundamental que esses profissionais compreendam os elementos essenciais de um plano de continuidade de negócios, levando em consideração as vulnerabilidades presentes nos sistemas de informação hospitalar atualmente e os padrões de auditoria de privacidade pessoal propostos por regulamentos e leis.

A privacidade é um valor e um direito consagrado na sociedade, e à medida que a área da saúde busca melhorar a qualidade e a eficiência por meio do desenvolvimento de redes de

DOI: 10.51161/conaenf2023/22905

informação em saúde, incluindo a troca eletrônica de informações financeiras e clínicas, torna-se cada vez mais importante proteger a privacidade e a confidencialidade dos pacientes nesses ambientes. Para lidar com essas preocupações, os profissionais de enfermagem devem adotar medidas para garantir a segurança das informações do paciente. Isso envolve a implementação de medidas tecnológicas, programas de orientação e educação, bem como o cuidadoso desenvolvimento e implementação de políticas e procedimentos, juntamente com treinamentos adequados (FRETTA, 2021).

A segurança cibernética demanda a implementação de medidas de segurança altamente eficientes. No entanto, é importante reconhecer que a segurança cibernética absolutamente infalível não existe. Por esse motivo, adotar uma abordagem baseada em riscos através do gerenciamento de riscos corporativos é essencial. Mesmo com uma infraestrutura e práticas de TI (tecnologia da informação) de qualidade, juntamente com uma postura proativa e medidas de segurança da informação, o risco de sofrer um ataque sempre estará presente (FRETTA, 2021).

Logo o presente estudo tem como compreender a segurança da informação por meio de Medidas Tecnológicas, evidenciar os elementos essenciais de um plano de privacidade e os desafios de compartilhamento de informações e identificar como a Lei Geral de Proteção de Dados Pessoais (LGPD) pode auxiliar os registros dos hospitalares. Para mitigar os riscos de ataques cibernéticos os hospitais devem investir em medidas de segurança da informação robustas, incluindo políticas de acesso controlado, treinamento de conscientização em segurança para os profissionais de enfermagem, criptografia de dados, backups regulares, atualizações de software, entre outras práticas recomendadas. A adoção de um programa de conformidade com a LGPD também é essencial para garantir o tratamento adequado dos dados pessoais dos pacientes e evitar penalidades legais.

2. METODOLOGIA

Trata-se de um estudo de revisão bibliográfica, realizada através de pesquisa nas bases de dados da Biblioteca Virtual em Saúde (BVS), Literatura Latino Americana e do Caribe em Ciências da Saúde (LILACS), *Scientific Eletronic Library* (SCIELO), por jornais, revistas e artigos com o propósito de enriquecer o meio acadêmico sintetizar os resultados, justificando a importância do conhecimento da LGPD no ambiente hospital. Em função do crescimento de ataques cibernéticos nestas instituições.

O presente estudo buscou estabelecer critérios de inclusão que basearam- se em: artigos publicados no período de 2018 a 2022 em português, que apresentassem textos completos na íntegra e publicações que respondessem ao tema proposto de modo a categorizar os artigos, analisar criteriosamente, interpretar os resultados e apresentar os resultados da revisão.

Logo foram os critérios de exclusão deste estudo foram: artigos na forma de resumos, relatos de casos, dissertações, teses, publicações não correspondentes ao período e artigos repetidos em uma das outras bases de dados pesquisadas. Os descritores utilizados para a busca de dados foram definidos de acordo com os Descritores com operador booleano *AND* caracterizando-se em: ataques cibernéticos, tecnologia da informação e profissionais de enfermagem, para melhor refinar a busca de artigos nas bases de dados escolhidas para a revisão.

3. RESULTADOS E DISCUSSÃO

A abordagem de compartilhamento de informações e colaboração entre as partes interessadas no setor hospitalar é fundamental para fortalecer a cibersegurança nos sistemas

DOI: 10.51161/conaenf2023/22905

de saúde. Permite uma compreensão abrangente das ameaças e dos atores envolvidos, além de promover a consciência situacional e a preparação dos tomadores de decisão para lidar com incidentes cibernéticos. A troca de informações entre provedores de serviços de saúde, fabricantes, fornecedores, pagadores, provedores de registros eletrônicos e até mesmo governos é crucial para identificar ameaças potenciais, indicadores de compromisso, melhores práticas, vulnerabilidades e lições aprendidas. Essas informações podem ajudar a desenvolver estratégias eficazes de mitigação e políticas de gerenciamento de risco corporativo.

Com a crescente frequência e gravidade dos ataques cibernéticos nos últimos anos, é essencial que as unidades de saúde estejam preparadas para responder a incidentes e manter a continuidade dos negócios. Isso requer a criação de planos de resposta a incidentes e continuidade de negócios que sejam regularmente testados, exercitados e armazenados *offline*. Esses planos devem envolver um processo acordado com as partes interessadas relevantes, garantindo que todos os envolvidos estejam cientes de suas responsabilidades e tenham as medidas apropriadas em vigor para lidar com um incidente cibernético. A colaboração entre as partes interessadas no planejamento e execução desses planos é essencial para garantir uma resposta eficiente e coordenada (AMARAL et al., 2021).

A crescente incorporação de tecnologia na área da saúde está resultando em avanços nas medidas de segurança cibernética. As informações de saúde acessadas por meio de violações de dados são de grande interesse para criminosos, devido à sua natureza imutável. Os registros médicos de um indivíduo contêm dados como tipo sanguíneo, cirurgias anteriores, diagnósticos e outras informações pessoais de saúde. Esses registros incluem dados privados, como nome, data de nascimento, informações do seguro e provedor de saúde, além de informações genéticas e de saúde. Quando essas informações privadas são comprometidas, a privacidade não pode ser restaurada e os danos são irreversíveis (HAWRYLISZYN; COELHO; BARJA, 2021).

Esses ataques não representam apenas uma ameaça à identidade e às finanças dos pacientes, mas também podem prejudicar as operações do hospital e colocar em risco a saúde e o bem-estar dos pacientes. Por exemplo, um hospital privado que sofra um ataque cibernético pode experimentar atrasos nos planos de tratamento e até mesmo o redirecionamento inadequado de ambulâncias devido à perda de acesso aos sistemas de informação hospitalar. Esses atrasos operacionais e as consequências financeiras das violações de dados e ataques, como o *ransomware*, têm efeitos prejudiciais de longo prazo na reputação e na receita de hospitais e instalações de saúde (HAWRYLISZYN; COELHO; BARJA, 2021).

Em resposta a ataques cibernéticos, é necessário realizar reuniões conduzidas por equipes multidisciplinares de especialistas. Também pode ser proposto um workshop com o objetivo de identificar ameaças, promover discussões interdisciplinares e propor recomendações práticas para o hospital.

Portanto, é essencial contar com ferramentas adequadas para proteger os dados compartilhados entre os diferentes departamentos de um hospital, de maneira consciente e segura, reduzindo o risco de violações intencionais ou não autorizadas por meio da distribuição de confiança. Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) estabelece que profissionais e unidades de saúde são obrigados a armazenar as informações de seus pacientes, impedindo o uso e compartilhamento com o objetivo de obter vantagem econômica, garantindo assim a natureza privada das informações pessoais e sua posse pelo titular.

A LGPD brasileira, em seu artigo 2º, apresenta uma série de fundamentos, incluindo o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, informação, comunicação e opinião, a inviolabilidade da intimidade, honra e imagem, o desenvolvimento econômico e tecnológico, a livre iniciativa, concorrência e defesa do consumidor, além dos

DOI: 10.51161/conaenf2023/22905

direitos humanos, desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

A LGPD abrange uma ampla gama de questões, incluindo um conjunto robusto de princípios, regras para aplicação extraterritorial, disposições de segurança sólidas, regulamentação de transferências de dados transfronteiriças, obrigações de designação de funcionários responsáveis pela proteção de dados e realização de avaliações de impacto de proteção de dados, entre outras características positivas. Essas disposições unificam e complementam o atual quadro de proteção de dados, abordando questões como a aplicação extraterritorial das leis de proteção de dados, que antes da aprovação da LGPD eram uma lacuna comum (BRASIL, 2018).

Anteriormente, a estrutura consistia em uma combinação de diferentes leis setoriais, como a Lei do Consumidor, que poderia ser aplicada para garantir a privacidade do consumidor em qualquer relacionamento entre um consumidor e um fornecedor, e a Lei de Informações de Crédito, que se aplicava a questões relacionadas a bancos de dados de informações financeiras.

Outra lei que trata da proteção de dados pessoais é o Marco Civil da Internet, também conhecido como Lei 12.965/2014. Essa lei se aplica aos usuários da Internet em geral, provedores de conexão à Internet (responsáveis pela transmissão de pacotes de dados entre terminais na Internet) e provedores de aplicativos de Internet (que disponibilizam recursos acessíveis por terminais conectados à Internet). O Marco Civil estabelece que qualquer tratamento de dados pessoais realizado no Brasil, mesmo que parcialmente ou apenas coletados por meio de um terminal localizado no país, deve estar em conformidade com a legislação brasileira (BRASIL, 2018).

Com base nesse maior conhecimento sobre a LGPD, é possível observar que informações de identificação pessoal e informações de saúde protegidas são encontradas em todos os departamentos de um hospital privado. Todos os profissionais de enfermagem, como médicos, assistentes médicos, equipes de enfermagem, nutricionistas e fisioterapeutas, utilizam registros eletrônicos de saúde, software de prescrição eletrônica, monitoramento remoto de pacientes ou sistemas de informação laboratorial. O departamento de faturamento lida com informações financeiras por meio de *software* de faturamento médico, os departamentos de agendamento e administração trabalham com dados clínicos no *software* de agendamento, e assim por diante.

A cibersegurança na área da saúde é única devido ao tipo de informação em risco e às consequências para a segurança do paciente. Quando um número de cartão de crédito é roubado, o banco cancela o cartão, emite um novo e reembolsa o cliente. No entanto, quando as informações de saúde de um paciente são roubadas, o paciente não pode alterar, por exemplo, sua data de nascimento, tipo de sangue e informações genéticas e de saúde (FRETTA, 2021).

Uma vez que os dados de saúde são roubados, eles têm ampla aplicabilidade e valor para uma variedade de crimes, desde roubo de identidade até fraude médica. As informações de saúde de um indivíduo são significativamente mais valiosas na *dark web* do que seu número de previdência social ou número de cartão de crédito, podendo ser vendidas por 10 a 20 vezes mais do que esse tipo de dado (MARTINS et al., 2022).

A estrutura regulatória em torno das informações de saúde evoluiu nas últimas duas décadas, graças às leis de proteção de dados, fortalecendo a proteção do uso, divulgação, armazenamento e transmissão dessas informações. Essas leis reforçam a notificação de violações e incentivam o uso significativo de registros eletrônicos de saúde, substituindo regulamentações existentes e implementando disposições e requisitos relacionados à proteção de informações de saúde. Isso inclui disposições para notificação de violações e implementação de penalidades. Embora as regulamentações cada vez mais rigorosas

DOI: 10.51161/conaenf2023/22905

representem desafios tecnológicos e organizacionais para as instituições de saúde, seu objetivo é proteger os dados e a cibersegurança dos hospitais, bem como a segurança do paciente (MARTINS et al., 2022).

Os ataques cibernéticos podem atrasar e interromper as operações confidenciais dos hospitais e colocar a vida dos pacientes em risco. Quando os hospitais são alvo de ataques, cirurgias podem ser adiadas e os pacientes podem ser direcionados para hospitais próximos. Os ataques cibernéticos podem ameaçar uma ampla variedade de serviços dentro de um hospital, desde cirurgias até entrega de medicamentos, visando equipamentos avançados, como geladeiras de hemoderivados, equipamentos de imagem, distribuidores automáticos de medicamentos e registros eletrônicos de saúde, bem como sistemas críticos de suporte, como aquecimento, ventilação e ar condicionado.

4. CONCLUSÃO

Construir a resiliência cibernética de um hospital é vital e é uma responsabilidade compartilhada. Os usuários (médicos, enfermeiros, técnicos e a equipe de administração) devem passar por treinamento e praticar a higiene digital, os tomadores de decisão devem aplicar as políticas adequadas e considerar a segurança cibernética nas decisões de compra e os fabricantes devem equipar seus produtos com as medidas de segurança cibernética adequadas. As equipes de segurança da informação dos hospitais também devem aprovar e manter as ferramentas adequadas para proteger o hospital e os pacientes.

As equipes de segurança da informação devem equipar os usuários para combater métodos de engenharia social, por exemplo, filtrando conteúdo de e-mail, verificando automaticamente *URLs* suspeitos em e-mails para códigos maliciosos vinculados, colocando sites e aplicativos confiáveis na lista de permissões, bem como bloqueando *Flash*, anúncios e código JAVA não confiável na Internet, conforme necessário.

Outras táticas para reduzir a exposição devem ser usadas, como alterar intencionalmente as senhas padrão e atualizar regularmente as configurações de segurança em laptops, servidores, estações de trabalho, *firewalls*, entre outros. Finalmente, deve haver ferramentas adequadas para proteger os dados compartilhados entre diferentes departamentos ou instituições médicas de uma forma consciente da privacidade, reduzindo, portanto, o risco de violações intencionais ou não através da distribuição de confiança.

REFERÊNCIAS

AMARAL, Fábio Câmara do et al. **Lei geral de proteção de dados pessoais:** proteção e compartilhamento de dados na área da saúde. 2021. Disponível em: https://www.trt4.jus.br/portais/media/606207/Bibliografia%20atualizada%20LGPD%20-%20agosto%202021%20-%20vers%C3%A3o%2012%20.pdf Acesso em: 17 de mai. de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015- 2018/2018/lei/l13709.htm Acesso em: 2 de set. de 2021.

FRETTA, Darlene dos Santos. **LGPD:** principais aspectos e sua implementação na área da saúde. 2021. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/20852 Acesso em: 12 de mai. de 2023

HAWRYLISZYN, Larissa Oliveira; COELHO, Natalia Gavioli Souza Campos; BARJA,

DOI: 10.51161/conaenf2023/22905

Paulo Roxo. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): O DESAFIO DE SUA IMPLANTAÇÃO PARA A SAÚDE. **Revista Univap**, v. 27, n. 54, 2021. Disponível em: https://revista.univap.br/index.php/revistaunivap/article/view/2589 Acesso em 19 de mai. de 2023.

MARTINS, Marcela et al. A aplicação da LGPD nos hospitais privados e o direito fundamental à saúde e proteção de dados pessoais. **CORPO EDITORIAL**.2022. Disponível em: https://cdea.tche.br/site/wp-content/uploads/2022/05/Estudos-sobre-LGPD.pdf Acesso em: 23 mai. de 2023.

DOI: 10.51161/conaenf2023/22905