UNIVERSIDADE FEEVALE

LEANDRO THOMAS

**ANÁLISE DE UM SISTEMA DE PRONTUÁRIO ELETRÔNICO SOB A LUZ DA LGPD (LEI GERAL DE PROTEÇÃO DE DADOS)**

Novo Hamburgo

2022

LEANDRO THOMAS

**ANÁLISE DE UM SISTEMA DE PRONTUÁRIO ELETRÔNICO SOB A LUZ DA LGPD (LEI GERAL DE PROTEÇÃO DE DADOS)**

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Feevale.

Orientador: Marta Rosecler Bez

Novo Hamburgo

2022

**LEANDRO THOMAS**

Trabalho de conclusão do Curso de Sistemas de Informação, com o título **UM ESTUDO DE CASO NA ÁREA DA SAÚDE SOB A LUZ DA LGPD (LEI GERAL DE PROTEÇÃO DE DADOS)**, submetido ao corpo docente da Universidade Feevale, como requisito necessário para obtenção do Grau de Bacharel em Sistemas de Informação.

Aprovado por:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Orientadora: Prof.ª. Marta Rosecler Bez

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Professor avaliador

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Professor avaliador

Novo Hamburgo, junho de 2022.

**AGRADECIMENTOS**

Agradeço a todos que de alguma maneira participaram e contribuíram para a realização deste trabalho de conclusão, em especial:

Minha mãe que sempre colocou em primeiro lugar meus estudos e proporcionou que eu chegasse até este momento importante.

A Prof. Marta que teve paciência e dedicação ao me orientar na construção deste trabalho.

E por fim a empresa que concedeu espaço para a pesquisa deste trabalho.

Muito obrigado a todos!

**RESUMO**

A Lei Geral de Proteção de Dados (LGPD) busca estabelecer normas e primitivas que definem como os dados pessoais devem ser tratados, armazenados, entre outros tipos de manipulação destes. Baseado nestas normas, toda empresa ou instituição deverá tratá-los conforme especificado nesta lei. O prontuário do paciente é documento básico em hospitais ou grandes clínicas e permeia toda a sua atividade assistencial, administrativa, além de permitir a integração entre os vários setores e com seus respectivos profissionais de saúde. Desde que os requisitos legais e os regulamentos de sigilo profissional sejam atendidos, ele pode ser preenchido eletronicamente em sistemas de Prontuários eletrônicos de paciente chamados PEP. O sistema deve garantir a segurança e privacidade de dados do paciente implementando um modelo seguindo as normativas de proteção de dados previstas na Lei n°. 13.709/2018. O objetivo deste trabalho é realizar um estudo de caso de um sistema hospitalar de prontuário eletrônico sob a luz da LGPD evidenciando requisitos e lacunas sobre as diretrizes dispostas na lei. A metodologia utilizada para este trabalho um estudo de caso único, buscando de forma qualitativa validar um conjunto de sistemas de saúde dentro das normativas da LGPD. Os sistemas analisados foram MVSOUL (sistema responsável pelas configurações do sistema de prontuário eletrônico), MVPEP (sistema de prontuário eletrônico), SACR (sistema responsável pela classificação de risco para os atendimentos de urgência e emergência), MVEDITOR (sistema utilizado para criação de formulários eletrônicos personalizados, aplicativos de apoio a enfermagem) e o sistema de diagnóstico por imagem utilizado para visualização de exames de imagem e realização de laudos. Os requisitos TISS que não eram atendidos plenamente foram analisados evidenciando os possíveis problemas, impactos e soluções.

**Palavras-chave:** LGPD. Lei geral de proteção de dados. Prontuário Eletrônico. Segurança. TISS.

**ABSTRACT**

The General Data Protection Law (LGPD) seeks to establish norms and primitives that define how personal data should be treated, stored, among other types of manipulation. Based on these standards, every company or institution must treat them as specified in these laws. The patient's medical record is a basic document in hospitals or large clinics and permeates all their care and administrative activities, in addition to allowing the integration between the various sectors and with their respective health professionals. Provided legal requirements and professional secrecy regulations are met, it can be completed electronically in Electronic Patient Record systems called PEP. The system must guarantee the security and privacy of patient data by implementing a model following the data protection regulations provided for in Law no. 13,709/2018. The objective of this work is to carry out a case study of a hospital system of electronic medical records under the light of the LGPD, highlighting requirements and gaps on the guidelines set out in the new Law nº 13.709, 2018. The methodology used for this work is a single case study, qualitatively seeking to validate a set of health systems within the LGPD regulations. The analyzed systems were MVSOUL system responsible for the electronic medical record system settings, MVPEP electronic medical record system, SACR system responsible for risk classification for urgent and emergency care, MVEDITOR system used to create personalized electronic forms, applications to support nursing and system the diagnostic imaging system used for viewing imaging exams and making reports. TISS requirements that were not fully met were analyzed highlighting possible problems, impacts and solutions.

**Keywords:** LGPD. General Data Protection Act. Electronic Medical Record. Safety. TISS.

**LISTA DE FIGURAS**

[Figura 1 - Classificações dos países quanto a tratamento e proteção dos dados 20](#_Toc105191780)

[Figura 2 - Quadro comparativo dos principais recursos contemplados 30](#_Toc105191781)

[Figura 3 - Integração entre as áreas, os profissionais e os principais recursos do hospital 43](#_Toc105191782)

[Figura 4 - Sistemas integrados ao PEP (prontuário eletrônico do paciente) 46](#_Toc105191783)

[Figura 5 - Categorias protocolo Manchester 49](#_Toc105191784)

[Figura 6 - Descrição cirúrgica criada em MVEditor 50](#_Toc105191785)

[Figura 7 - Tela de configuração de diretivas de segurança 54](#_Toc105191786)

[Figura 8 - Campo descrição versão e sistema oriundo 56](#_Toc105191787)

[Figura 9 - Configuração para desabilitar salvar credenciais de acesso 57](#_Toc105191788)

[Figura 10 - Configuração de senha forte 63](#_Toc105191789)

[Figura 11 - Configuração time out IIS (*Internet Information Services*) 66](#_Toc105191790)

**LISTA DE QUADROS**

[Quadro 1 - Princípios da Lei Nº 13.709 – Art. 6º 17](#_Toc105191588)

[Quadro 2 - Relação de itens e categorias contemplados na ISO/IEC 17799 25](#_Toc105191589)

[Quadro 3 - Princípios para certificação SBIS 28](#_Toc105191590)

[Quadro 4 - Requisitos NGS2 Certificação SBIS 32](#_Toc105191591)

[Quadro 5 - Princípios e seus requisitos 53](#_Toc105191592)

[Quadro 6 - Sistemas e requisitos não atendidos completamente 53](#_Toc105191593)

[Quadro 7 – Requisito 5 TISS (2022) MVPEP e MVSOUL 54](#_Toc105191594)

[Quadro 8 – Requisito 33 TISS (2022) MVPEP e MVSOUL 55](#_Toc105191595)

[Quadro 9 – Requisito 42 TISS (2022) MVPEP e MVSOUL 56](#_Toc105191596)

[Quadro 10 – Requisito 43 TISS (2022) MVPEP e MVSOUL 57](#_Toc105191597)

[Quadro 11 – Requisito 63 TISS (2022) MVPEP e MVSOUL 58](#_Toc105191598)

[Quadro 12 – Requisito 65 TISS (2022) MVPEP e MVSOUL 58](#_Toc105191599)

[Quadro 13 – Requisito 5 TISS (2022) Editor 59](#_Toc105191600)

[Quadro 14 – Requisito 7 TISS (2022) Editor 59](#_Toc105191601)

[Quadro 15 – Requisito 33 TISS (2022) Editor 60](#_Toc105191602)

[Quadro 16 – Requisito 42 TISS (2022) Editor 60](#_Toc105191603)

[Quadro 17 – Requisito 43 TISS (2022) Editor 61](#_Toc105191604)

[Quadro 18 – Requisitos 63 e 65 TISS (2022) Editor 62](#_Toc105191605)

[Quadro 19 – Requisito 4 TISS (2022) Diagnóstico por imagem 62](#_Toc105191606)

[Quadro 20 – Requisito 5 TISS (2022) Diagnóstico por imagem 63](#_Toc105191607)

[Quadro 21 – Requisito 7 TISS (2022) Diagnóstico por imagem 64](#_Toc105191608)

[Quadro 22 - Requisito 33 TISS (2022) Diagnóstico por imagem 65](#_Toc105191609)

[Quadro 23 - Requisito 42 TISS (2022) diagnóstico por imagem 66](#_Toc105191610)

[Quadro 24 - Requisito 43 TISS (2022) Diagnóstico por imagem 67](#_Toc105191611)

[Quadro 25 - Requisito 67 TISS (2022) Diagnóstico por imagem 68](#_Toc105191612)

[Quadro 26 - Requisitos 63 e 65 TISS (2022) - Diagnóstico por imagem 68](#_Toc105191613)

**SUMÁRIO**

[1 INTRODUÇÃO 10](#_Toc105517325)

[1.1 OBJETIVOS 12](#_Toc105517326)

[1.1.1 Objetivo geral 12](#_Toc105517327)

[1.1.2 Objetivos específicos 13](#_Toc105517328)

[1.2 ESTRUTURA DO TRABALHO 13](#_Toc105517329)

[2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) N °. 13.709 / 2018 15](#_Toc105517330)

[2.1 CAPÍTULO I - DISPOSIÇÕES PRELIMINARES 15](#_Toc105517331)

[2.2 CAPÍTULO II - DOS TRATAMENTOS DE DADOS PESSOAIS 19](#_Toc105517332)

[2.3 CAPÍTULO III - DOS DIREITOS DO TITULAR 19](#_Toc105517333)

[2.4 CAPÍTULO IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO 20](#_Toc105517334)

[2.5 CAPÍTULO V - DA TRANSFERÊNCIA INTERNACIONAL DE DADOS 20](#_Toc105517335)

[2.6 CAPÍTULO VI - DOS AGENTES DE TRATAMENTOS DE DADOS PESSOAIS 21](#_Toc105517336)

[2.7 CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS 22](#_Toc105517337)

[2.8 CAPÍTULO VIII - DA FISCALIZAÇÃO 23](#_Toc105517338)

[2.9 CAPÍTULO IX - DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS 23](#_Toc105517339)

[2.10 CAPÍTULO X - DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS 24](#_Toc105517340)

[3 REQUISITOS PARA CERTIFICAÇÃO DE SISTEMAS DE REGISTRO ELETRÔNICO EM SAÚDE (SBIS) - UM OLHAR SOB À LUZ DA LGPD 25](#_Toc105517341)

[3.1 PRINCÍPIOS DO MANUAL DE CERTIFICAÇÃO PARA SISTEMAS DE REGISTRO ELETRÔNICO EM SAÚDE 29](#_Toc105517342)

[4 TRABALHOS CORRELATOS 35](#_Toc105517343)

[4.1 OS DADOS PESSOAIS E A PROTEÇÃO DE DADOS DE SAÚDE: ANÁLISE A PARTIR DAS INICIATIVAS DE E-SAÚDE 35](#_Toc105517344)

[4.2 JURISPRUDÊNCIA E LEGISLAÇÃO SANITÁRIA COMENTADAS LEI GERAL DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO NA ÁREA DA SAÚDE 37](#_Toc105517345)

[5 PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP) 40](#_Toc105517346)

[5.1 SISTEMA MV PEP (PRONTUÁRIO ELETRÔNICO DO PACIENTE) 42](#_Toc105517347)

[5.1.2 Perfis de acesso e processos registrados 44](#_Toc105517348)

[5.1.3 Sistemas relacionados no MVPEP 46](#_Toc105517349)

[5.1.3.1 Soul MV 47](#_Toc105517350)

[5.1.3.2 SACR 49](#_Toc105517351)

[5.1.3.3 Editor 50](#_Toc105517352)

[6 ANÁLISE DE REQUISITOS PADRÃO TISS, SOB A LUZ DA LGPD 53](#_Toc105517353)

[6.1 ANÁLISE DOS REQUISITOS DO SISTEMA MVPEP E MVSOUL 54](#_Toc105517354)

[6.2 ANALISE DOS REQUISITOS DO SISTEMA MVEDITOR 60](#_Toc105517355)

[6.3 ANALISE DOS REQUISITOS DO SISTEMA DE DIAGNÓSTICO POR IMAGEM 63](#_Toc105517356)

[7 CONCLUSÃO 70](#_Toc105517357)

[REFERÊNCIAS BIBLIOGRAFICAS 73](#_Toc105517358)

[ANEXO A – CERTIFICADO SBIS 75](#_Toc105517359)

[APÊNDICE A – TABELA DE ANÁLISE DOS REQUISITOS TISS (2021) 78](#_Toc105517360)

**1 INTRODUÇÃO**

Segundo Piurcosky (2019), com base no GDPR (Regulamento Geral sobre a Proteção de Dados) da União Europeia foi aprovada no direito pátrio a Lei Geral de Proteção de Dados Pessoais (LGPD) n°. 13.709/2018, que dispõe sobre o tratamento de dados pessoais, por pessoas naturais e jurídicas, tanto de direito público quanto privado.

Mulholland (2018) também enfatiza que a referida Lei recebeu uma forte influência do direito comunitário europeu, desde a Diretiva de Proteção de Dados de 1995 até o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em vigor a partir de maio de 2018. No que diz respeito ao tratamento de dados sensíveis, a LGPD conceituou de forma semelhante, senão idêntica ao GDPR, o conceito de dados pessoais sensíveis, sendo certo que a lei brasileira é bastante inspirada no regulamento europeu.

O Art. 5º, do Capítulo I da LGPD, que fala das Disposições Preliminares, apresenta a preocupação com os direitos de intimidade, vida privada e liberdade da pessoa natural. Também aborda aqueles dados ditos sensíveis, que compreendem a origem racial ou ética, convicção religiosa, opinião pública, filiação a organização de caráter religioso, filosófico ou político, mas principalmente aqueles dados referentes a saúde ou à vida sexual, dado genético ou biométrico, dados que digam respeito a saúde (prontuários e laudos médicos) mas também aqueles que dizem respeito ao código genético (BRASIL, 2018).

Majeed (2018) explica que a privacidade é um fator ético bem como o requisito regulamentar em sistemas de *electronic health record* (EHR). Violações de privacidade podem causar divulgação de identidade, perda de informações confidenciais, roubo de identidade e modificação não autorizada dos dados. Evitar essas violações é um desafio para pesquisadores e cientistas que estão explorando e pesquisando os dados do usuário.

Para Rodotà (2008), “a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações” sendo a esfera privada “aquele conjunto de ações, comportamentos, opiniões, referências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo” (RODOTÀ, 2008, p. 92). Bioni (2020, p. 83), conceitua que “os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação”.

Além dos dados pessoais, há ainda, no que tange à prestação dos serviços de saúde, os dados considerados sensíveis. A área da saúde é, provavelmente, um dos setores que mais tratam dados considerados sensíveis pela Lei 13.709 de 14 de agosto de 2018.

Segundo Canedo *et al.* (2020), no Brasil, organizações de desenvolvimento de software, públicas ou privadas e que processam dados pessoais de usuários, devem cumprir um grande número de regulamentos e garantir que os requisitos de negócios e de sistema estejam legalmente em conformidade, ou seja, atendam a todos os requisitos de privacidade e segurança digital regulamentada pela Lei Geral de Proteção de Dados LGPD (Lei nº 13.709, 2018).

Bezerra (2009) relata que a informática na área da saúde é uma das Tecnologias da Informação e Comunicação (TICs) que apresenta maior potencial de crescimento e preocupação atual com a proteção de dados. Esta está cada vez mais forte e levanta diversos aspectos no meio digital, principalmente no âmbito hospitalar, onde tem-se muitas informações sigilosas, elas são armazenadas em sistemas ditos como PEP (Prontuário Eletrônico do Paciente).

A Resolução CFM nº 1.638/2002 (CONSELHO FEDERAL DE MEDICINA, 2002a, p. 184), em seu Art. 1º, define o prontuário médico como: o documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência prestada, de caráter legal, sigiloso e científico, comunicação entre equipe multiprofissional e a continuidade da assistência prestada ao indivíduo.

De acordo com Patrício *et al.* (2011) o prontuário do paciente é o documento básico em hospitais ou grandes clínicas, permeia toda a sua atividade assistencial, administrativa, de pesquisa e de ensino, além de permitir a integração entre os vários setores e com seus respectivos profissionais de saúde. Se os dados forem armazenados em meio eletrônico, seu vasto conjunto de informações é capaz de gerar conhecimento, podendo ser entendido como a sua principal base de dados, a partir da qual são construídos todos os sistemas de informações, sejam estes gerenciais, de apoio à decisão, especialistas, de apoio ao ensino, estatísticos, para pesquisa e etc.

Os controladores de dados, conforme assim definido no artigo 5º da Lei nº 13.709 (2018), sendo os responsáveis pelas decisões a respeito do tratamento de dados nas empresas, devem formular novas políticas para cumprir a lei, estabelecer novas condições para a organização em relação a seus regulamentos operacionais, procedimentos, incluindo os termos de reclamações e petições de titulares de dados. Também a implementação de padrões de segurança, padrões técnicos e obrigações especiais para processadores de dados, ações educacionais dos funcionários e supervisão de risco de negócios e outros aspectos relacionados ao processamento de dados pessoais (Lei nº 13.709, 2018).

Para Bezerra (2009), deve haver um planejamento envolvendo todos os profissionais atuantes em setores onde há coleta de dados dos pacientes. É importante avaliar todo o processo de registro dos eventos realizados durante os atendimentos ou internações. A padronização dos formulários, o estabelecimento dos fluxos de processo da informação em saúde, o treinamento de todos os envolvidos e o controle e avaliação dos resultados devem ser considerados.

Rosa (2019) explica que baseado nas normas da LGPD toda empresa ou instituição que armazenar dados pessoais ou realizar qualquer manipulação e gerenciamento sobre estes, deverá tratá-los conforme especificado nesta lei. Sabe-se que a Lei Geral de Proteção de Dados poderá obrigar aos hospitais a construção de um modelo novo de *compliance* de dados a respeito da relação entre o paciente e a clínica. Busca-se evidenciar a proteção dos dados sensíveis dos funcionários, pacientes, e a todos os frequentadores, os motivos da coleta de seus dados.

1.1 OBJETIVOS

**1.1.1 Objetivo geral**

Realizar um estudo de caso de um sistema hospitalar de prontuário eletrônico sob a luz da LGPD, evidenciando requisitos e lacunas sobre as diretrizes dispostas na nova Lei nº 13.709, 2008.

**1.1.2 Objetivos específicos**

* Estudo sobre a lei geral de proteção de dados (LGPD).
* Revisão bibliográfica sobre a LGPD aplicada em ambiente hospitalar.
* Estudo dos dados considerados pela LGPD como sensíveis em um sistema hospitalar.
* Selecionar um sistema hospitalar a ser analisado.
* Validar aspectos do sistema selecionado sob a luz da LGPD.

A metodologia empregada neste trabalho é um estudo de caso único (YIN, 2005) em uma cooperativa da área da saúde no Rio Grande do Sul. Segundo Yin (2005), para os estudos de caso, o desenvolvimento da teoria como parte da fase inicial do projeto, é essencial para saber se o propósito decorrente do estudo de caso é desenvolver ou testar a teoria. O autor salienta que é fundamental que o investigador reflita sobre as habilidades para a realização de estudos de caso, assim como experiência prévia, sagacidade para fazer boas perguntas, capacidade de não se deixar levar por seus preconceitos e ideologias, flexibilidade para se adequar às situações adversas etc.

Dito isto, observa-se um grande ganho no estudo de caso proposto pois o autor é o analista responsável pelo gerenciamento dos sistemas neste trabalho apresentado, podendo assim desenvolver e testar os processos realizados nos sistemas sob a luz os princípios da LGPD.

1.2 ESTRUTURA DO TRABALHO

No Capítulo 2 são apresentados de forma descritiva os capítulos da Lei Geral de Proteção de Dados Pessoais (LGPD) n °. 13.709 / 2018. No Capítulo 3 são apresentados os requisitos e princípios para a certificação de Sistemas de Registro Eletrônico em Saúde da Sociedade Brasileira de Informática em Saúde (SBIS), buscando relacionar com as normativas da LGPD. Partindo deste estuado realizou-se a pesquisa por trabalhos correlatos sobre a utilização de sistemas de prontuário eletrônico e a proteção de dados sensíveis expostas nestes sistemas, como descrito no Capítulo 4.

Em seguida, no Capítulo 5 é realizado um estudo buscando elucidar o que é um sistema de Prontuário Eletrônico do Paciente (PEP) e suas aplicações, evidenciando benefícios e dificuldades na implementação em uma unidade hospitalar.

Para apoio nas validações de requisitos de um sistema de prontuário eletrônico e a transferência de dados entre sistemas no Capitulo 6 foi utilizada a tabela Padrão TISS, onde foi classificada e analisada sobre os princípios da LGPD, evidenciando os problemas, impactos e soluções para estar *compliance* com os requisitos avaliados. No Capítulo 7 são apresentadas as considerações para adequação e a importância da segurança e transparência no tratamento de dados pessoais e sensíveis em um ambiente hospitalar.

**2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) N °. 13.709 / 2018**

Uma nova lei foi aprovada na legislação nacional Brasileira e entrou em vigor em agosto de 2020, a Lei Geral de Proteção de Dados Pessoais (LGPD) n °. 13.709 / 2018. Esta prevê o tratamento de dados pessoais por pessoas singulares e coletivas de acordo com o direito público e privado. A inovação não se limita a proteger dados, como nome, contato telefônico, endereço residencial, e-mail, etc. As preocupações sobre o direito à intimidade, vida privada e liberdade das pessoas físicas também incluem os chamados dados confidenciais, como raça ou origem moral, crenças religiosas, opinião pública e afiliação a organizações religiosas, filosóficas ou políticas, mas principalmente, esses dados se referem à saúde ou vida sexual, dados genéticos ou biométricos, dados relativos à saúde (prontuários e relatórios médicos). (BRASIL, 2018, S/N).

Para proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural foi criada a Autoridade Nacional de Proteção de Dados (ANPD), conforme estabelecido no [Decreto nº 10.474, de 26 de agosto de 2020](https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10474.htm). **No que se refere a direitos do titular dos dados,** toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da LGPD ([artigo 17 da LGPD](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709compilado.htm)).

A abrangência da lei passa por organizações Públicas e Privadas de todos os setores da economia que tratam dados pessoais em território nacional e estabelece diretrizes com 10 capítulos e mais de 70 artigos. As informações abaixo foram retiradas diretamente da Lei Nº 13.709/2018. (BRASIL, 2018).

2.1 CAPÍTULO I - DISPOSIÇÕES PRELIMINARES

Neste capítulo da LGPD encontram-se do 1º ao 6º artigo da Lei Nº 13.709, conforme abaixo definidos:

O Art. 1º dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O foco da lei é regulamentar o tratamento de dados pessoais, porém, não fica limitado a eles, inclui também o processo de armazenamento de dados físicos e descarte adequado como processos judiciais, prontuários médicos, fichas cadastrais, etc.

O Art. 2º tem como fundamentos:

1. O respeito à privacidade;
2. A autodeterminação informativa;
3. A liberdade de expressão, de informação, de comunicação e de opinião;
4. A inviolabilidade da intimidade, da honra e da imagem;
5. O desenvolvimento econômico e tecnológico e a inovação;
6. A livre iniciativa, a livre concorrência e a defesa do consumidor;
7. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Dados pessoais pertencem a pessoa e não às empresas ou governo, inclusive dados públicos. Os titulares têm o direito de dizer o que querem dispor na rede. Este artigo não visa restringir a inovação tecnológica, porém, é necessário cumprir o *Privacy by Design.* Isso implica em incluir na arquitetura dos sistemas tecnologias e técnicas que protejam a privacidade, de forma que as proteções de dados pessoais orientem a criação do produto desde a sua concepção. Este é um ponto positivo, visto que a GDPR (*General Data Protection Regulation*) não tem esta premissa.

O Art. 3º aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

O Art. 4º indica que esta Lei não se aplica ao tratamento de dados pessoais: realizado por pessoa natural para fins exclusivamente particulares e não econômicos; para fins exclusivamente jornalístico e artísticos; de defesa nacional; de segurança do Estado; ou de atividades de investigação e repressão de infrações penais. Este artigo trata exceções que justificam a não aplicação da LGPD, como no caso de uso de tecnologia de reconhecimento de digital para identificação de pessoa para segurança pública.

O Art. 5º possui um glossário com 19 termos definidos onde se caracterizam os principais como:

O primeiro, Dado pessoal, se refere a qualquer informação que possa identificar uma Pessoa Natural, direta ou indiretamente, por meio físico ou digital, como, por exemplo: nome, CPF, placa de veículo, IP e etc. São considerados, nesta linha, dados pessoais sensíveis os de saúde, genéticos, biométricos (caixas bancários, aplicativos), religiosos, racial, orientação sexual, dados que podem resultar em discriminação. Quando tratar-se de dados de menores, é necessária a autorização do representante legal e a garantia que esse forneceu.

Denomina-se Tratamento de dados toda operação realizada com dados pessoais: coleta, acesso, transmissão, armazenamento, transferência e etc. Para isso podem ser utilizados dados anonimizados, ou seja, aqueles em que se remove ou modifica informações que possam identificar uma pessoa. Estes não são considerados dados pessoais e estão fora do escopo da LGPD. Já os Dados pseudoanonimizados, ou mascarados, recebem um tratamento em que só é possível identificar os titulares por processo de inversão. São considerados dados pessoais: cartão de credito, CPF com \* (134.\*\*\*.87\*-96), pulseira com (\*) para identificação de pessoas com alergia.

A Lei apresenta diversos agentes de tratamentos de dados. Os controladores tomam a decisão referente ao tratamento dos dados. Os operadores realizam tratamento em nome do controlador, não tendo autonomia para decidir. Exemplo de operadores são as empresas de processamento de folha de pagamento, *Data Center*, etc.

O DPO ou Encarregado é o ponto de contato da organização com titulares e Autoridades Nacional de Proteção de Dados - ANPD (comunicações e reclamações). Orienta a organização sobre boas práticas referentes a proteção de dados. A função DPO teve origem na Diretiva 95/46/EC e tornou-se obrigatória em algumas situações da Lei *General Data Protection Regulation* (GDPR), regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu.

A principal função do DPO é garantir que a organização esteja em conformidade com a legislação, seguindo os princípios de comunicação com titulares e ANPD, prestando esclarecimentos referentes a proteção de dados pessoais, prestando treinamentos sobre práticas adequadas de segurança e ainda análises de atividades, produtos e serviços que envolvem proteção de dados pessoais na organização, elaborando as adequações necessárias.

A Lei prevê ainda o DPIA (Relatório de impacto a privacidade) que é utilizado como avaliação e auditoria dos impactos de seus processos, produtos e serviços com requisitos da LGPD.

O Art. 6º indica que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios apresentados no Quadro 1.

Quadro 1 - Princípios da Lei Nº 13.709 – Art. 6º

| **Nro.** | **Princípio** | **Descrição** |
| --- | --- | --- |
| I | Finalidade | Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. |
| II | Adequação | Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. |
| III | Necessidade | Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. |
| IV | Livre acesso | Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. |
| V | Qualidade dos dados | Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. |
| VI | Transparência | Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. |
| VII | Segurança | Utilização de medidas 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 difusão. |
| VIII | Prevenção | Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais |
| IX | Não discriminação | Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos |
| X | Responsabilização e prestação de contas | Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. |

**Fonte: LGPD, Lei Nº 13.709**

2.2 CAPÍTULO II - DOS TRATAMENTOS DE DADOS PESSOAIS

As principais hipóteses de tratamento de dados pessoais são: mediante consentimento (mais fraco pois pode ser revogado a qualquer momento), cumprimento de obrigação legal ou regulatório do controlador, como os órgãos reguladores como CFM (Conselho Federal de Medicina) e resoluções como da ANS (Agência Nacional de Saúde Suplementar) com mais de 20 resoluções; pela administração pública para tratamento e uso compartilhado de dados necessários a execução de políticas públicas, previstas em leis, regulamentos contratos; realização de estudos por órgãos de pesquisa (recomenda-se anonimização quando possível); execução de contrato ou procedimento preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular; no caso de exercício regular de direito em processo judicial, administrativo ou arbitral; proteção da vida ou incolumidade física do titular ou de terceiros (neste caso a LGPD autoriza tratamento sem consentimento desde que a finalidade e a necessidade estejam definidas e sejam utilizadas medidas técnicas para garantir a segurança do dado, evitando incidentes); para tutela da saúde em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; interesse legítimo do controlado ou de terceiros (exceção no caso de prevalecer direitos e liberdades fundamentais do titular que exijam proteção de dados pessoais); para proteção ao crédito.

2.3 CAPÍTULO III - DOS DIREITOS DO TITULAR

Segundo o Art. 17, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei. Já o Art. 18 esclarece que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento, nos termos do 5º do art. 8º desta Lei.

2.4 CAPÍTULO IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

O tratamento de dados pessoais pelos órgãos e entidades do Poder Público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I - Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sites e, que seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

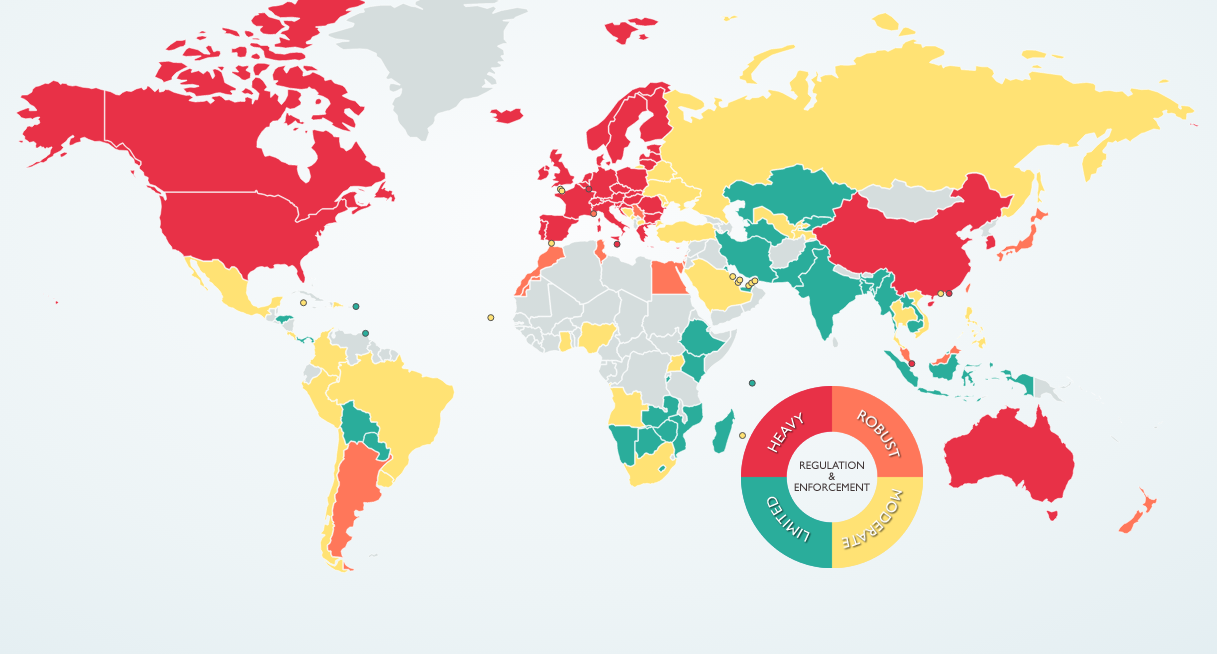
É permitido o uso compartilhado de dados pelo Poder Público, desde que tenha por objetivo atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6° da lei.

2.5 CAPÍTULO V - DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

A Lei considera transferência internacional de dados a realizada em países estrangeiros ou organismos internacionais a qual o país seja membro. A transferência internacional de dados pessoais somente será permitida nas hipóteses do artigo 33 da LGPD, conforme segue: países ou organismos internacionais com grau de proteção de dados pessoais adequado ao previsto na LPGD; controlador oferece e comprova garantias de cumprimento dos princípios e direitos do titular e do regime de proteção de dados previstos na LGPD; cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, de acordo com os instrumentos de direito internacional; para a proteção da vida da incolumidade física do titular ou de terceiros; autorização da ANDP; compromisso assumido em acordo de cooperação internacional; execução de política pública ou atribuição legal do serviço público; consentimento específico do titular; cumprimento de obrigação legal ou regulatória pelo controlador; execução de contrato ou procedimentos preliminares relacionados ao contrato do qual seja parte o titular dos dados; exercício regular de direito em processo judicial, administrativo ou arbitral.

A figura 1 apresenta os países com suas respectivas classificações para tratamento e proteção de dados. O Brasil, por recentemente ter aprovado a LGPD, se enquadrou como moderado no que diz respeito a proteção de dados.

Figura 1 - Classificações dos países quanto a tratamento e proteção dos dados



**Fonte: DLA Piper (2021)**

2.6 CAPÍTULO VI - DOS AGENTES DE TRATAMENTOS DE DADOS PESSOAIS

O controlador, operador e encarregado (DPO) informam as diretrizes para os profissionais atuarem. O Art. 37º indica que o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseadas no legítimo interesse. O Art. 38 indica que a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referentes a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Já o Art. 39 prevê que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

As atividades do encarregado estão descritas no Art. 41º, devendo aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências, orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

2.7 CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS

No que diz respeito a segurança e ao sigilo de dados, o Art. 46 indica que 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. Enquanto o Art. 49 esclarece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Sobre as boas práticas e da governança foram estabelecidos os Art. 50º e 51º que indicam que os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento e os procedimentos. Inclui-se, também, reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

2.8 CAPÍTULO VIII - DA FISCALIZAÇÃO

No Art. 52º são previstas multas em razão das infrações cometidas às normas previstas nesta Lei, ficando sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; multa diária, observado o limite total a que se refere o inciso II; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; eliminação dos dados pessoais a que se refere a infração.

A ANPD (Autoridade Nacional de Proteção de Dados Pessoais) será o órgão que editará e fiscalizará as normas e procedimentos sobre a proteção e tratamento de dados pessoais no Brasil e terá poderes: Regulatórios; de Fiscalização; Sancionatório e Consultivo. Ela é estruturada em seis entidades descritas como: Conselho diretor, Conselho nacional de proteção de dados, Corregedoria, Órgão de assessoramento jurídico e Unidade administrativa e unidades necessárias à aplicação da lei.

2.9 CAPÍTULO IX - DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Esta será composta de 23 (vinte e três) representantes, titulares e suplentes, dos seguintes órgãos: cinco do Poder Executivo Federal, um do Senado Federal, um da Câmara dos Deputados, um do Conselho Nacional de Justiça, um do Conselho Nacional do Ministério Público, um do Comitê Gestor da Internet no Brasil, três de entidades da sociedade civil com atuação relacionada a proteção de dados pessoais, três de instituições científicas, tecnológicas e de inovação, três de confederações sindicais representativas das categorias econômicas do setor produtivo, dois de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; e dois de entidades representativas do setor laboral.

O Conselho nacional de proteção de dados atua com as competências de propor diretrizes estratégicas e fornecer subsídios para a elaboração de Política de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANP; elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; sugerir ações a serem realizadas pela ANDP, elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade, e disseminar o conhecimento sobre estas à população.

2.10 CAPÍTULO X - DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

No Art. 63º diz que a autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados. Já o Art. 64º indica que os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Da mesma forma que é importante conhecer a LGPD, também é imprescindível conhecer os requisitos para Certificação de sistemas de registro eletrônico da SBIS (Sociedade Brasileira de Informática em Saúde. Este tema é apresentado no próximo capítulo.

**3 REQUISITOS PARA CERTIFICAÇÃO DE SISTEMAS DE REGISTRO ELETRÔNICO EM SAÚDE (SBIS) - UM OLHAR SOB À LUZ DA LGPD**

Na área da saúde, no Brasil, existem algumas iniciativas para propor normas para a Segurança da Informação, principalmente aquelas definidas pela Sociedade Brasileira de Informática na Saúde (SBIS), órgão vinculado ao Conselho Federal de Medicina (CFM). No entanto, as instituições hospitalares no Brasil não estão sujeitas a essas regulamentações, sendo que o órgão governamental responsável pelas instituições hospitalares é o Ministério da Saúde (MS) (JANSSEN, 2008).

De acordo com as diretrizes da SBIS, as instituições médicas no Brasil devem passar pelos padrões definidos pela ISO / IEC 17799 (SBIS, 2006) e manter medidas de controle que possam garantir a segurança da informação. Por outro lado, a ANS (Serviço Nacional de Saúde), agência reguladora que complementa o setor de saúde, editou normas para troca eletrônica de informações entre entidades vinculadas à ANS, incluindo regulamentações relacionadas à segurança da informação (JANSSEN, 2008).

O Prontuário Eletrônico do Paciente (PEP) é a principal ferramenta de TICS (Tecnologias da informação e Comunicação) que o médico precisa ou precisará lidar nas suas atividades diárias, seja no consultório, centro diagnóstico ou hospital. É fundamental que o médico utilize uma ferramenta de alta qualidade, segura e que possa auxiliá-lo no registro da história clínica e exame físico, bem como na solicitação de exames e prescrição. Outro conceito importante é o Registro Eletrônico de Saúde (RES), que permite o armazenamento e o compartilhamento seguro das informações de um paciente (SBIS, 2021).

A literatura sobre o tema Segurança da Informação em instituições hospitalares limita-se a abordagens dos conceitos de Segurança da Informação e das normativas aplicáveis ao segmento empresarial de forma genérica, mais especificamente às recomendações baseadas nas normativas internacionais ISO/IEC 17799 e ISO/IEC 27001. Esta caracteriza-se por ser um modelo contendo recomendações de boas práticas em Segurança da Informação. Todavia, a sua característica estrutural não define critérios avaliativos que possam ser usados para uma certificação (JANSSEN, 2008).

No Brasil, a Associação Brasileira de Normas Técnicas (ABNT), em abril de 2001 disponibilizou, através de um projeto de adaptação e tradução, a norma nacional de Segurança da Informação NBR ISO/IEC 17799:2000. Essa normativa foi aprovada e homologada incluindo o Brasil no conjunto de países que adotam e apoiam o uso desta norma. Esta versão brasileira da ISO/ IEC 17799 também é utilizada por outros países de língua portuguesa, como é o caso de Portugal e Angola (EGAN, 2005).

A NBR ISO/IEC 17799 apresenta as categorias e seus respectivos elementos conforme o Quadro 2:

Quadro 2 - Relação de itens e categorias contemplados na ISO/IEC 17799

| **RELAÇÃO DE CATEGORIAS E ITENS CONTEMPLADOS DA ISO/IEC 17799** | | |
| --- | --- | --- |
| **Categorias** | **Quantidade Elementos** | **Itens Contemplados** |
| 1. Política de  Segurança | 2 | Necessidades do Negócio, Estratégia, Comprometimento, Regras e Responsabilidades, Políticas e Procedimentos. |
| 2. Segurança  Organizacional | 10 | Avaliação, Gestão de Riscos, Liderança do Negócio, Endereçamento e Manipulação, Estoques. |
| 3. Classificação e  Controle de Ativos | 3 | Inventário de ativos, classificação e manipulação de ativos |
| 4. Segurança  Pessoal | 10 | Demissões e Desligamentos, Regras e Responsabilidades, Treinamento, Relatórios e Revisões. |
| 5. Segurança Física e Ambiental | 13 | Perímetros, Ameaças Ambientais, Gestão de Riscos, Controle de Acesso,  Segurança, Destruição e Remoção de Ativos, Monitoramento, Manipulação de  Incidentes, Cooperação e Premiação. |
| 6. Comunicação e  Gerenciamento de  Operações | 24 | Padrões, Métodos de e - Comunicação, Procedimentos de Operação, Monitoramento, Backups, Administração de Exceções, atualizações e Pacotes, *Help Desk*, Gestão de Mudanças, Sistemas de Criptografia, Administração de Mídias, Código Malicioso, Aceitação de Sistemas, Biblioteca de Documentação, Plano de Capacidade |
| 7. Controle de  Acesso | 31 | Perímetros, Gestão de Riscos, Controle de Acesso, Autenticação, Identificação, Responsabilidade de Usuários, Atualização de Acesso, monitoramento, computação móvel, gestão de Incidentes. |
| 8. Desenvolvimento de Sistemas e  Manutenção | 18 | Padrões, Modelo do Ciclo de Vida, Revisões, Análise de Diferenças, Planejamento de Requerimentos, Testes de Integridade e Certificação, Repositório de Código, Lançamento de versão, Liberação. |
| 9. Gestão de  Continuidade | 5 | Gerenciamento de Riscos, Priorização, Backups, Continuidade do Negócio, Plano de Desastre e Recuperação, Testes, Atualizações. |
| 10. Conformidade | 15 | Legal, Contratual, Propriedade Intelectual, Endereçamento e Manipulação, Retenção de Registros, Auditoria, Sanções. |

**Fonte: Adaptado de ISO/IEC 17799 (2005)**

A Norma ISO/IEC 27001 é uma padronização e um guia de gerenciamento para a implementação de controles de Segurança da Informação descritos na ISO/ IEC 17799:2005 (*Information security management systems: Code of practice*), ou sistema de gerenciamento de Segurança da Informação: código de práticas (ISO/ IEC 17799, 2005b). Faz parte de um conjunto de normativas denominada grupo ISO/IEC 27000. Cada uma destas normativas tem um objetivo específico, assim definido:

* ISO/ IEC 27000 - Vocabulário de Gestão da Segurança da Informação (sem data prevista de publicação);
* ISO/ IEC 27001 - Esta norma foi publicada em outubro de 2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de Segurança da Informação;
* ISO/ IEC 27002 - Esta norma substituiu, em 2007, a ISO 17799:2005 (Código de Boas Práticas);
* ISO/ IEC 27003 - Esta norma aborda a gestão de risco, contendo recomendações para a definição e implementação de um sistema de gestão de riscos em Segurança da Informação;
* ISO/ IEC 27004 - Esta norma incide sobre os mecanismos de mediação e de relatório de um sistema de gestão de Segurança da Informação;
* ISO/ IEC 27005 - Esta norma será constituída por indicações para implementação, monitoramento e melhoria contínua do sistema de controles;
* ISO/ IEC 27006 - Esta norma será referente à recuperação e continuidade de negócio. Este documento tem o título provisório de (*Guidelines for information and communications technology disaster recovery services*), ou manual para serviços de recuperação de desastre da tecnologia de comunicações e informação, não estando ainda prevista a sua edição.

Outro ponto forte sobre a ISO/IEC 27001 é a incorporação *Information Security Management System* (ISMS), sistemática composta por um modelo de desenho, implementação, gerenciamento e manutenção dos processos de segurança da informação percorrendo toda a organização (ISO/IEC 27001, 2021).

O início da certificação SBIS/CFM foi em 2004, com o lançamento do Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (S-RES), lista o conjunto de requisitos que se julgava necessários para o S-RES. Nesta fase as organizações desenvolvedoras do S-RES realizavam uma auto declaração de conformidade em relação aos requisitos do manual da certificação (OLIVEIRA, 2013).

A Sociedade Brasileira de Informática em Saúde, em parceria com o Conselho Federal de Medicina, lançou, em 2009, um programa de certificação para S-RES – Certificação SBIS-CFM, (SBIS-CFM, 2009), além de uma resolução determinando que instituições de saúde que pretendam eliminar prontuários com registros em papel estavam obrigadas a utilizar apenas sistemas certificados (CFM, 2007), o que vem estimulando às empresas fornecedoras de S-RES atuantes no mercado brasileiro a investir na adaptação e certificação de seus sistemas (OLIVEIRA, 2013).

Atualmente a SBIS (Sociedade Brasileira de Informática em Saúde) tem publicado a versão 5.0 do documento que apresenta o conjunto de requisitos técnicos especificados e Manual de Certificação de Sistemas de Registro Eletrônico em Saúde (S-RES) específico para sistemas de Prontuário Eletrônico do Paciente (PEP) publicada em 18/11/2020, sendo a versão vigente até o momento (SBIS, 2021).

A Certificação de S-RES SBIS foi concebida como uma maneira de melhorar a qualidade dos softwares e a segurança dos profissionais e instituições de saúde no uso dos mesmos, assim como garantir a legalidade da substituição dos registros em papel pelos seus respectivos registros eletrônicos (SBIS, 2021). Os benefícios que a certificação S-RES SBIS apresenta destacam-se em:

* Conscientizar o mercado quanto à importância de funcionalidades básicas em S-RES;
* Diminuir o risco enfrentado por médicos e instituições de saúde na seleção e compra de S-RES;
* Redirecionar as prioridades de investimentos em informática em saúde, considerando aspectos relevantes para a melhoria da qualidade, segurança e eficiência de sistemas informatizados;
* Contribuir para a confidencialidade e privacidade das informações de saúde ao demandar que os S-RES atendam requisitos de segurança adequados, e garantir a legalidade das informações armazenadas nestes sistemas pelo uso de tecnologia reconhecida no país (ICP/Brasil);
* Aumentar o uso da informática em saúde no Brasil e, consequentemente, melhorar a eficiência e a eficácia do sistema de saúde brasileiro.

3.1 PRINCÍPIOS DO MANUAL DE CERTIFICAÇÃO PARA SISTEMAS DE REGISTRO ELETRÔNICO EM SAÚDE

O manual apresenta princípios que devem ser seguidos para certificação tais como apresentado na Quadro 3.

Quadro 3 - Princípios para certificação SBIS

| **Nro** | **Princípio** | **Descrição** |
| --- | --- | --- |
| I | Imparcialidade | Para que todo o processo seja percebido como tal, as atividades e decisões do processo serão baseadas em evidências objetivas de conformidade e que não serão influenciadas por interesses espúrios. |
| II | Competência | Para oferecer confiança é necessária a utilização de recursos competentes, entendendo-se por competência a capacidade demonstrada de aplicar conhecimentos e habilidades. |
| III | Responsabilidade | Necessária para que o cliente certificado entenda e assume que é ele, e não a SBIS, quem possui a responsabilidade pela conformidade com os requisitos da certificação. |
| IV | Transparência | É um princípio de acesso ou divulgação de informações. Para obter e manter confiança na certificação, a SBIS oferecerá acesso público sobre seu processo de certificação, exceto informações de natureza confidencial, tais como as informações privadas dos Solicitantes e Clientes Certificados. |
| V | Confidencialidade | Princípio que favorece à SBIS obter confiança do solicitante de que não terá sua imagem ou seus interesses, de alguma forma, prejudicados por submeter seus S-RES ao processo de certificação. |
| VI | Capacidade de Respostas a Reclamações | Necessário que tanto a SBIS quanto o Cliente Certificado sejam capazes de prontamente registrar e tratar adequadamente as reclamações a que tiverem acesso. |

**Fonte: SBIS (2022).**

Os conjuntos de conformidade para certificação SBIS estão agrupados em três diferentes conjuntos:

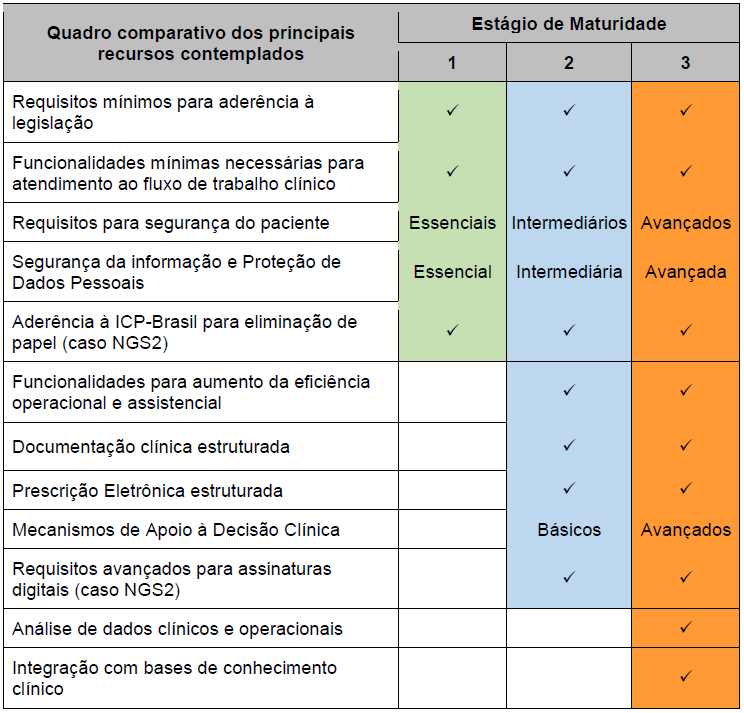
* Requisitos de Estrutura, Conteúdo e Funcionalidades (ECF): são os requisitos que envolvem o fluxo operacional e assistencial. Exemplos são a identificação dos pacientes e/ou profissionais, dados clínicos, entre outros.
* Requisitos do Nível de Garantia de Segurança 1 (NGS1): em termos de segurança, este é considerado o padrão mínimo. Norteia os elementos considerados essenciais para que uma operação seja considerada segura e sigilosa. Estes requisitos não se aplicam aos sistemas que buscam eliminar os registros físicos em papel.
* Requisitos do Nível de Garantia de Segurança 2 (NGS2): contemplam todos os requisitos do NGS1, bem como os recursos de Certificação Digital em sistemas que operem no formato *peprless*.

Existem diversas formas para avaliação de processos. Uma delas é usando modelos de maturidade. Estes possibilitam a identificação de um estágio ou a evolução de um processo em relação ao estágio anterior, demonstrando oportunidades de melhorias. Na certificação da SBIS, o modelo proposto possui três estágios de maturidade do software. Assim, o processo de certificação pode evoluir, atingindo, ao longo do processo, um alto nível de maturidade.

* **Estágio 1**: este é o estágio inicial de maturidade do sistema. As funcionalidades e conteúdos mínimos para o registro e utilização adequados das informações dos pacientes.
* **Estágio 2**: este é o segundo estágio de maturidade do sistema. Este contempla as funcionalidades mínimas do estágio 1 e recursos complementares oferecendo maior eficiência operacional e assistencial.
* **Estágio 3**: em termos de maturidade do sistema este é o estágio mais elevado. Contempla as funcionalidades dos estágios 1 e 2, mais os recursos avançados para registro e utilização de informações sobre a saúde dos pacientes.

Na Figura 2 são apresentados os principais recursos contemplados em cada estágio de maturidade para a categoria PEP.

Figura 2 - Quadro comparativo dos principais recursos contemplados



**Fonte: Requisitos para Certificação de Sistemas de Registro Eletrônico em Saúde (SBIS, 2020)**

A SBIS (2021), em seu documento de requisitos para certificação, informa que para obter o certificado é necessário que o sistema atenda à totalidade dos requisitos de ECF, NGS1.

Sabbatini (2021) cita alguns dos requisitos como principais para os níveis NSG1 são eles:

— O controle de autenticação de acesso às aplicações deve conter senha forte (8 caracteres, pelo menos uma letra e um número), sendo configurável e protegida por criptografia forte no banco de dados e esta senha expirar após determinado tempo. O sistema também deve permitir dois níveis de autenticação (por exemplo, uma senha mais informações biométricas ou um código enviado para um telefone celular). A sessão deve ter um tempo de expiração;

— Implementar um subsistema de trilha de auditoria completo, onde os registros de rastreamento não devem conter dados clínicos ou qualquer informação identificável do paciente (pseudo-anonimato);

— O sistema será responsável por fazer e gerenciar cópias de *backup* e realizar o controle de integridade durante a gravação e recuperação, automatizar alertas quando o limite de ocupação do disco foi atingido;

— Os componentes dinâmicos (ActiveX, Applet, etc.) utilizados no software devem ter origem / autor e controle de integridade;

— Os dados e documentos devem ser armazenados exclusivamente no SGBD de forma criptografada. Após concluída a operação, todos os arquivos gerados temporariamente fora do SGBD (Sistema de gerenciamento de banco de dados), por exemplo, para interoperabilidade, visualização, assinatura, etc., devem ser excluídos, incluindo os arquivos restantes no cache e os arquivos restantes do arquivo XML processado.

— O S-RES deve permitir criptografia de documentos eletrônicos exportados e que contenham dados de saúde como, por exemplo: geração de arquivo do prontuário para visualização ou impressão. Assim como para fins de portabilidade, onde será armazenado em mídia portátil como pen-drive ou CD-ROM ou até mesmo envio por e-mail.

— A comunicação entre os componentes distribuídos do S-RES deve implementar os serviços de segurança de autenticação de parceiro, integridade e sigilo dos dados, assim como nos protocolos HTTPS *(Hyper Text Transfer Protocol Secure* - protocolo de transferência de hipertexto seguro) e SSL (*Secure Sockets Layer*) na comunicação entre cliente e servidor.

— O S-RES deve permitir exportar os registros eletrônicos assinados possibilitando efetuar a validação da assinatura digital externamente ao S-RES. Para a exportação de prescrições/receitas, solicitações de exames, atestados médicos e laudos, o S-RES deve estar coerente com às especificações apresentadas no documento.

Os requisitos NGS2 formam um nível opcional e o mais avançado que exige requisitos conforme descrito no documento Requisitos para Certificação de Sistemas de Registro Eletrônico em Saúde da SBIS (SBIS, 2021), atendendo assim, os 3 níveis de maturidade previstas pela SBIS. Alguns requisitos são listados abaixo no Quadro 4.

Quadro 4 - Requisitos NGS2 Certificação SBIS

|  |  |
| --- | --- |
| NGS2.01.01 | O S-RES deve permitir que certificados digitais ICP-Brasil possam ser utilizados por profissionais de saúde para o processo de assinatura digital de documentos do prontuário do paciente, atendendo às normas de uso definidas pela ICP-Brasil na utilização desses certificados. |
| NGS2.01.02 | O S-RES deverá permitir o uso de um certificado digital (assinatura digital e autenticação no S-RES) por um usuário apenas se o CPF informado no cadastro deste usuário for idêntico ao identificado no certificado digital utilizado. Dessa forma, a cada processo de uso do certificado digital deverá ser verificado se o CPF do usuário executando o processo corresponde ao CPF contido no certificado digital utilizado, e o processo só será finalizado com sucesso em caso de igualdade dos CPFs. |
| NGS2.02.09 | O S-RES deve exibir uma indicação de que um determinado documento foi assinado digitalmente (por exemplo, exibindo um status de “assinado”), deve ainda permitir que o usuário possa visualizar por meio da aplicação as informações sobre a assinatura (minimamente quais profissionais assinaram e registro de tempo). |

**Fonte: SBIS (2022).**

Demais requisitos podem ser verificados diretamente no documento oficial (Manual de Certificação de Sistemas de Registro Eletrônico em Saúde) disponível em: < http://sbis.org.br/documentos-e-manuais/ >.

No Anexo 1 é evidenciado o certificado emitido pela SBIS a um sistema S-RES - Sistemas de Registro Eletrônico em Saúde com nível NGS2 disponível em: < http://sbis.org.br/certificacao/certificados/Certificado\_SBIS\_SRES\_063\_MV.pdf >.

A acreditação SBIS estabelece diferentes padrões para as categorias de PEP e seus respectivos sistemas de registro eletrônico de saúde (S-RES) para estabelecimentos de saúde como hospitais, consultórios e clínicas de atendimento pessoal e ambulatórios, levando em consideração suas especificidades. No entanto, a LGPD tem como objetivo regular, de forma efetiva, clara e transparente, o processamento de dados pessoais, garantindo a proteção. Desta forma busca entregar o poder sobre os dados pessoais, agora trazendo a obrigação para formalizar de que maneira estarão sendo tratados, armazenados, alterados e manipulados estes dados sensíveis e em ambiente hospitalar.

O Artigo 5º, item XII, da Lei Geral de Proteção de Dados Pessoais como traz o conceito como: *"manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"*. Portanto, para que haja o tratamento de dados pessoais por parte de uma organização é necessário o consentimento do titular dos dados, conforme prevê o artigo 7º, inciso I, da LGPD.

Outro ponto forte que a LGPD permeia sobre os sistemas S-RES é definir o conceito de ‘dado’, trazendo duas categorias como o dado pessoal: aquele relacionado a pessoa natural identificada ou identificável como nome e telefone. A segunda categoria, dita como dado sensível que são aqueles que podem discriminar uma pessoa como raça ou orientação sexual e ainda nesta categoria englobam-se os dados sobre saúde como doenças, dados genéticos, tipo sanguíneo. Estes presentes em todos os sistemas hospitalares sejam públicos ou privados, pois são o repositório de informação a respeito da saúde de indivíduos. Tudo isso vem ao encontro do que já pregava a normatização da SBIS, porém, sem a obrigatoriedade.

No próximo capítulo são apresentados trabalhos correlatos quem veem de encontro com o tema de proteção de dados em iniciativas e-Saúde no Brasil e explicitando os objetivos da LGPD.

**4 TRABALHOS CORRELATOS**

Serão apresentados neste capítulo dois trabalhos correlatos que serviram de inspiração para o desenvolvimento deste TCC pois abordam iniciativas de e-Saúde no Brasil e suas fragilidades quanto ao novo contexto de proteção de dados sensíveis.

4.1 OS DADOS PESSOAIS E A PROTEÇÃO DE DADOS DE SAÚDE: ANÁLISE A PARTIR DAS INICIATIVAS DE E-SAÚDE

Siqueira *et al*. (2019), realizaram um estudo bibliográfico com a temática de proteção de dados pessoais com ênfase para dados de saúde, e respeito à vida privada dos pacientes. É utilizado um método comparativo expondo a lei atual brasileira de proteção de dados LGPD em relação as anteriores e de outros países que serviram de base para a produção nacional.

O trabalho foi dividido em duas etapas, onde na primeira buscou-se tratar o direito humano como fundamento do respeito à vida privada do paciente e proteção dos dados de saúde. Siqueira *et al*. (2019) consideram direitos humanos no contexto dos cuidados em saúde e de pacientes, o direito à vida, o de não ser tratado de forma desumana, degradante, cruel ou torturante. Com o direito à liberdade e segurança pessoal, à saúde, de não ser discriminado de nenhuma forma, especialmente relacionado ao propósito atual, de saber e respeitar a vida privada.

Afirma que a partir desta abordagem exposta, os dados médicos são uma ramificação dos dados pessoais e consistem em informações sensíveis e as rotula como informações que apresentam alto potencial discriminatório ou recriminatório ao seu titular, ostentando maiores riscos que a média para o indivíduo e, até mesmo, para a coletividade. Segundo os autores supracitados, aqueles dados que desvelam a origem racial ou étnica do titular, os seus princípios políticos, morais, filosóficos ou religiosos, filiações partidárias ou sindicais, antecedentes criminais, orientações sexuais, além dos dados médicos e de saúde.

Os Estados Unidos da América publicaram um estudo já em 1973, editado por um comitê de especialistas convocado pela *Secretary for health, education and welfare*. O setor de saúde é o pioneiro em demonstrar medo razoável ao manipular dados médicos por meio de um sistema informatizado, estabelecendo relação direta entre o tratamento de dados e o direito de privacidade, criando assim normas para o exercício de controle pelo indivíduo, sobre a divulgação e utilização de suas informações. (SEQUEIRA *et al*., 2019) O autor ainda cita que o Brasil, por outro lado, está em um patamar inferior, visto que somente em 2018 editou a lei que especifica a segurança dos dados pessoais de seus cidadãos: a Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), Lei nº 13.709/2018.

Diante do risco e fragilidade das informações médicas a autodeterminação das informações do paciente, que é a base da LGPD, deve ser protegida de acordo com as disposições do artigo 2, Parágrafo 2, da Lei nº 13.709, 2018, preenchendo o Formulário de Consentimento Livre e Esclarecido, documentos exigidos por ambas as partes para realizar cirurgia ou como prática de pesquisa. O termo deve conter uma notificação clara sobre o grau de confiabilidade, verificar, alertar sobre possíveis riscos, consequências fisiológicas e complicações, objetivos e benefícios da intervenção. Deve ser escrito no idioma simples e decodificado de termos médicos ou científicos para que os pacientes compreendam totalmente o conteúdo da licença.

Na segunda etapa do trabalho buscou-se evidenciar as iniciativas de E-SAÚDE, definidas pela Organização Mundial de Saúde (OMS) como telessaúde ou telemedicina, existente para designar as atividades, no campo da atenção à saúde, que fazem uso das Tecnologias de Informação e Comunicação (TIC) nas práticas como telediagnóstico, os prontuários digitais, os bancos de dados médicos informatizados, as teleconsultorias, as videoconferências, as telecirurgias, a tele-educação, as bibliotecas virtuais de vídeos e imagens.

Para Siqueira *et al.* (2019),no Brasil a prática do E-SAÚDE encontra-se em ascensão e como exemplo cita o Programa Nacional de Telessaúde, parte integrante do Sistema Único de Saúde (SUS), que preza pela ampliação da resolutividade da Atenção Básica. Cita como orientação de segurança a cartilha do Conselho Federal de Medicina (CFM) em parceria com a Sociedade Brasileira de Informática em Saúde (SBIS), lançada em 2012, que orienta os profissionais acerca da necessidade de certificação dos sistemas de registro eletrônico de saúde, como forma de garantir a segurança e a confidencialidade para as informações do paciente.

Ressalta que a recente Lei Geral de Proteção de Dados Pessoais constitui-se como marco normativo para tutela de direitos fundamentais, entretanto, devem ser adotadas estratégias no sentido de que o direito à privacidade do paciente seja efetivamente protegido tanto individual quanto coletivamente. Conclui, desta forma, que a atuação jurídica deve ser aliada das novas tecnologias, especialmente quanto às iniciativas de e-Saúde.

4.2 JURISPRUDÊNCIA E LEGISLAÇÃO SANITÁRIA COMENTADAS LEI GERAL DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO NA ÁREA DA SAÚDE

No trabalho de Leme *et al.* (2020), foi realizado uma análise descritiva da Lei nº 13.709/2018, em especial no aspecto do direito à saúde e suas implicações na segurança do tratamento dos dados decorrentes da revolução tecnológica.

O autor define os objetivos da LGPD como a proteção de dados de qualquer pessoa natural, identificada ou passível de identificação, cujas informações sejam tratadas por controladores e/ou operadores na coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração da informação. Ainda neste contexto afirma que a principal definição advinda da lei foi a definição de *dado pessoal sensível*.

Desta forma no trabalho foi aprofundada a análise do conceito dado pessoal sensível relativo ao tratamento e à segurança das informações concernentes à saúde das pessoas, oferecendo respostas para assegurar o não vazamento de dados pessoais sensíveis na esfera da saúde individual.

No trabalho é citado que no Brasil há um crescente uso de *big data* nos setores de medicina de precisão, prontuários eletrônicos, internet das coisas e telemedicina. Assim, fica claro o crescimento da quantidade e da diversidade de informações que podem ser combinadas e relacionadas, ampliando consideravelmente o risco de re-identificação dos dados, mesmo após a sua anonimização ou desidentificação de bases isoladas.

A ampliação e difusão das grandes bases de dados torna o titular das informações cada vez mais vulnerável, seja pela negligência na coleta de dados, no manuseio, compartilhamento, armazenamento ou descarte, comercialização ou até mesmo vazamento das informações.

Relacionando a LGPD ao contexto, cita-se o artigo 5º inciso XII da Lei 13.709/2018 que apresenta o consentimento do titular onde está condicionado à manifestação livre, informada e inequívoca do titular, que deverá concordar com o tratamento de seus dados pessoais para uma finalidade específica.

No que diz respeito ao processamento de dados sensíveis, o motivo do consentimento qualificado se deve à natureza do seu conteúdo, que requer atenção, especialmente dados médicos, genéticos e sexuais, que devem ser protegidos para garantir o pleno exercício dos direitos humanos básicos.

O consentimento somente será válido se as informações fornecidas ao titular dos dados forem apresentadas de forma transparente, clara e inequívoca. No caso de alteração da finalidade do tratamento dos dados pessoais, o responsável pelo tratamento deve informar previamente o titular da alteração da finalidade. Se o titular não concordar com a alteração da finalidade do tratamento, o consentimento pode ser revogado. O processamento deve ser de acordo com o disposto no Artigo 9º Parágrafo 1 e Parágrafo 2 da LGPD.

Entretanto, o artigo 11° permite que circunstâncias especiais processem dados confidenciais sem o consentimento do titular, por exemplo, para cumprir as obrigações legais ou regulamentares do controlador; compartilhar e processar dados exigidos pelas administrações públicas para implementar políticas públicas estipuladas por leis e regulamentos; instituições de pesquisa conduzem pesquisas para garantir tanto quanto possível o anonimato dos dados; a fim de proteger a vida ou a segurança pessoal do proprietário ou de terceiros; procedimentos executados por profissionais ou autoridades de saúde e entidades da região com o objetivo de proteger a saúde. Está previsto ainda a prevenção de fraudes e a proteção da segurança do titular durante o processo de identificação e registro da certificação no sistema eletrônico, e a proteção dos direitos descritos no artigo 9º da referida lei.

Para Leme *et al.* (2020) outro ponto a ser observado em organizações e que a LGPD trouxe no artigo 46º para fins de segurança da informação são 3 papeis distintos: o controlador responsável pelo tratamento da informação; o operador que executa as ordens do controlador em relação ao processamento das informações e o oficial de dados DPO (*Data Protection Officer*), responsável pela execução das diretrizes definidas pelo controlador e operador.

Conclui-se neste trabalho que a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) foi editada para garantir a transparência no uso dos dados das pessoas físicas, assegurar a privacidade dos titulares das informações, coibir o uso abusivo e discriminatório destes dados. Porém, para alcançar estes propósitos está totalmente relacionado ao desenvolvimento de regras e mecanismos de segurança da informação como o consentimento livre, expresso e informado manifestado pelo dono dos dados e além disso os sistemas devem ser projetados com base em conceitos de *Privacy by Design (*privacidade desde a concepção*) e Privacy by Default (*privacidade por padrão*).*

A seguir, no capítulo 5, são abordados os conceitos de sistemas S-RES elucidando suas variações, vantagens, desvantagens e usabilidade em ambientes hospitalares. Observa-se preocupações na utilização dos sistemas PEP (Prontuário eletrônico do Paciente) pois o mesmo carrega informações sensíveis e, desta forma, origina-se a necessidade de investir esforços em segurança e melhoria contínua.

**5 PRONTUÁRIO ELETRÔNICO DO PACIENTE (PEP)**

A norma ABNT ISO/TR 20514 define o Registro Eletrônico em Saúde (RES) como um repositório de informação a respeito da saúde de indivíduos, em uma forma processável eletronicamente.

Já o **Sistema de Registro Eletrônico de Saúde (S-RES)** é definido como um sistema que captura, armazena, apresenta, transmite ou imprime informação identificada na área da saúde. A informação identificada é aquela que permite individualizar um paciente, o que abrange não apenas o seu nome, mas também números de identificação únicos tais como: RG e CPF, ou outros dados que possibilitem a identificação do indivíduo como o número de prontuário. (SBIS, 2021).

S-RES são variados e entre eles estão: o Prontuário Eletrônico do Paciente (PEP), os sistemas de gestão hospitalar, os sistemas para clínicas e consultórios, os sistemas de resultado de exames laboratoriais, os sistemas para laudos de exames de imagens, os sistemas para saúde do trabalhador e tantos outros (CFM; SBIS, 2021).

A Resolução do Conselho Federal de Medicina (CFM) Nº 1.638/2002 define como Prontuário Médico:

O documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo. (CFM, 2021, art. 1º).

Patrício (2011) afirma que independentemente do conceito adotado, o PEP deve ser um sistema sigiloso útil, ético, legal e científico, além de permitir a comunicação entre os membros da equipe multiprofissional e o cuidado contínuo ao paciente. Complementa que é o documento básico de um hospital ou clínica de grande porte, permeando todas as suas atividades assistenciais, administrativas, de pesquisa e de ensino, e também permite a integração entre diferentes departamentos e com seus respectivos profissionais de saúde. Se os dados são armazenados eletronicamente, seu enorme conjunto de informações pode gerar conhecimento, que pode ser entendido como sua principal base de dados, todos os sistemas de informação, sejam gerenciados ou de suporte à tomada de decisões.

Bezerra (2009) cita que no Brasil, preocupações com a formulação e desenvolvimento do modelo PEP surgiram no ambiente universitário na década de 1990. Em 1999, por iniciativa do Ministério da Saúde, foi proposto um conjunto mínimo de informações sobre os pacientes, que devem ser incluídos no PEP para que possa ser integrado aos diferentes sistemas nacionais de informação em saúde.

Desde a implementação da proposta do PEP até os dias atuais, são evidenciados grandes avanços em melhorias tecnológicas e novas funcionalidades agregadas como a possibilidade de anexar imagens e outros exames complementares. A utilização de sistemas de apoio à decisão e o acesso remoto ao PEP são vantagens do uso da ferramenta no atendimento.

Outras vantagens surgem advindas da utilização do PEP tais como: o acesso mais veloz ao histórico de saúde e as intervenções às quais o paciente foi submetido; disponibilidade remota; uso simultâneo por diversos serviços e profissionais de saúde; flexibilidade do layout dos dados; legibilidade absoluta das informações; eliminação da redundância de dados e de pedidos de exames complementares; integração com outros sistemas de informação; processamento contínuo dos dados, disponíveis para todos os envolvidos no atendimento do paciente; informações organizadas de forma mais sistemática; facilidade na coleta dos dados para emissão de relatórios, seja para pesquisa ou faturamento; acesso ao conhecimento atualizado com consequente melhoria do processo de tomada de decisão e da efetividade do cuidado prestado. (Patrício, 2011).

Bezzera (2009) aponta algumas desvantagens que a utilização do PEP pode causar, como a necessidade de grandes investimentos de hardware, software e treinamento, resistência por parte dos profissionais na utilização dos sistemas e ocorrência de falhas que podem deixar o sistema inoperante, ficando assim, sem acesso a todas a informações inseridas no prontuário eletrônico.

Patrício *et al.* (2011) apresentam que o principal desafio para informatizar o arquivo médico está atrelado à educação dos profissionais de saúde que interagem com o prontuário. Os médicos, muitas vezes, alegam que o PEP pode ameaçar sua autonomia, costumam questionar como serão utilizados os dados pelas seguradoras e pelos administradores dos estabelecimentos de saúde para influenciar, restringir e, até mesmo, ditar como a medicina será praticada.

O sistema de registro eletrônico de saúde deve ser aplicável ao ambiente em que será utilizado (Galvão, 2012). Pode ter como alvo diferentes áreas da saúde e diferentes níveis de cuidados. Por exemplo: um sistema para laboratório, outro para o hospital, outro para a clínica. Para cada contexto o sistema de saúde tem necessidades diferentes e sistemas igualmente diferentes. Cada um tem diferentes usos, usuários e necessidades consideradas no processo de desenvolvimento do sistema, então é necessário identificar e atender às suas necessidades por meio de funcionalidades adequadas.

Para Bezerra (2009), no início o processo de informatização de uma Unidade Hospitalar pode gerar insegurança nos profissionais, porém, com o treinamento adequando e domínio da utilização, este pode auxiliar tanto na coleta quando no armazenamento das informações, proporcionando maior qualidade até mesmo no diagnóstico do atendimento.

Bezerra (2009) ainda enfatiza que com as grandes mudanças da área de informação de saúde, o Ministério da Saúde, assim como as agências reguladoras e os órgãos normatizadores, precisam destinar maiores esforços para apoiar a política de informatização das unidades hospitalares. Visando melhorar a qualidade dos serviços de saúde, o PEP e outros dispositivos, podem ser como um cartão personalizado, que permita o acesso em tempo real às informações dos pacientes a ações a serem realizadas.

Neste trabalho foi selecionado, por conveniência (empresa onde o autor trabalha), um sistema PEP utilizado em uma empresa de prestadora de serviços de saúde para apresentar os recursos e aplicabilidades em um ambiente hospitalar conforme apresentado na próxima sessão.

5.1 SISTEMA MV PEP (PRONTUÁRIO ELETRÔNICO DO PACIENTE)

Será apresentado o sistema MV PEP, o Prontuário Eletrônico do MV SOUL escolhido como estudo de caso para o trabalho. Serão verificadas funcionalidades do sistema, usabilidade, aplicabilidade de requisitos e configurações necessárias para a utilização do sistema.

O sistema MV PEP é utilizado como como prontuário eletrônico, terceirizado e desenvolvido pela empresa MV Sistemas (https://mv.com.br). O mesmo possibilita a integração entre médicos, enfermeiros, técnicos e demais integrantes no cuidado com o paciente, seja em consultas ou em intervenções. Com o prontuário esses profissionais tornam-se capazes de tomar decisões tendo à mão um histórico compreensivo.

O sistema possui inúmeros recursos para facilitar o trabalho dos profissionais que prestam assistência ao paciente, como: interação de medicamento, integração com a farmácia, setores de exames, controle de infeção, nutrição, faturamento, central de guias, entre outros, descritos na seção 5.1.2.1.

Conta com requisitos essenciais como certificação digital (Prontuário eletrônico do paciente certificado pelo CFM/SBIS), governança clínica, que possibilita integração com sistemas de apoio à decisão clínica, bases de conhecimentos, *e-learning* e BI clínico completo, com recursos que vão da prescrição até monitorização e histórico. Segundo os desenvolvedores, é totalmente seguro, com acesso restrito a usuários autorizados e controle absoluto das informações e dados dos pacientes.

Algumas das vantagens do MVPEP é garantir a legibilidade absoluta das informações, assegurando as atividades realizadas otimizando a comunicação entre profissionais de saúde no atendimento ao paciente e proporcionando qualidade no atendimento, assegura também a padronização e a eficiência dos processos clinico-assistências.

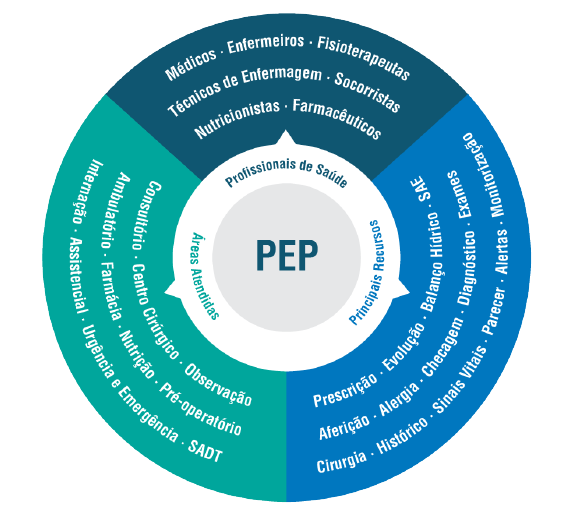
O sistema garante maior controle de acesso aos prontuários dos pacientes com uso de senha criptografada e ainda possibilita a utilização de biometria assim com autenticação de 2 fatores trazendo mais segurança no manuseio de informações sensíveis. O sistema de prontuário eletrônico facilita a análise estatística do paciente por meio da agilidade que proporciona durante o atendimento, desta forma otimizando o diagnóstico do paciente. Ainda contribui para a redução de custos com desperdícios de materiais e medicamentos com todo o controle de dispensação viabilizando um processo 100% digital.

Com a utilização de certificação digital não há necessidade de impressões de papel pois todos os documentos eletrônicos e processos são certificados digitalmente. O certificado digital é um documento eletrônico que contém dados sobre a pessoa que o utiliza para comprovação de autoria e autenticidade, conferindo valor legal aos documentos. Contém nome, CPF, data de nascimento do titular, sua chave pública, dados de controle e seu período de validade.

Os profissionais de saúde que atuam no sistema categorizam-se em médicos, enfermeiros e técnicos de enfermagem, fisioterapeutas, socorristas, nutricionistas e farmacêuticos. Estes atuam com atendimentos de pacientes e registram os seus processos no sistema MVPEP como prescrições, checagem, laudos, anotação de enfermagem, alergias dados estes ditos como sensíveis.

Na Figura 3 pode ser visto que o PEP está estruturado em diversas áreas de atendimento e disponibilizando vários recursos para os profissionais durante o atendimento em uma unidade hospitalar. Maiores detalhes de processos e perfis de acesso são apresentados na seção 5.1.2, com os recursos para os profissionais como médico, enfermeiro e técnico de enfermagem.

Figura 3 - Integração entre as áreas, os profissionais e os principais recursos do hospital



**Fonte: MV S.A (2022)**

**5.1.2 Perfis de acesso e processos registrados**

É possível configurar perfis diferentes para cada tipo de prestador, assim limitando o acesso de informação (dados sensíveis) para cada nível de atendimento do paciente em um ambiente hospitalar. Neste trabalho, são apresentados os perfis de médicos, enfermeiros e técnicos de enfermagem.

Estes 3 perfis podem registrar e visualizar informações de atendimentos ao paciente em todo seu período no hospital. Desta forma é crucial que a informação seja precisa, o acesso controlado e disponível a qualquer momento. Todos têm acessos as listas de atendimentos iguais assim como internação, urgência, bloco cirúrgico e ambulatorial, porém, cada perfil tem configuradas telas e processos diferentes conforme descrito a seguir.

O perfil de médico possui acesso aos menus como: História Clínica, onde tem acesso a informações como prescrições, sinais vitais, balanço hídrico, checagem de medicamentos, CID (Classificação Internacional de Doenças) e alergias. Conta também com acessos a resultados de exames de imagem e laboratório, que são integradas de sistemas terceiros (laboratório externo e sistemas de laudos e capturas de imagens) no sistema PEP.

O médico em seu processo registra toda a evolução do paciente e prescrições de medicamentos via sistema PEP e tem acesso a todos os registros de atendimentos anteriores, mesmo sendo realizado por outro médico, dentro da empresa e até mesmo evoluções e anotações da equipe de enfermagem.

Integrado ao sistema de prontuário também é disponibilizada uma plataforma *online* de apoio a decisão clínica chamada *UpToDate* que auxilia o médico pois disponibiliza mais de 420 periódicos revisados ​​por pares, diretrizes da sociedade, bancos de dados clínicos e ensaios clínicos para novas descobertas médicas importantes, disponíveis em: https://www.uptodate.com/contents/search.

A empresa conta com protocolos para determinados processos e disponibiliza no perfil de médico, através de um sistema terceiro, documentações dos fluxos definidos para auxilio e consulta a qualquer momento.

Alguns processos realizados no sistema PEP, como descrição cirúrgica, atestados, receituário e formulários variados podem ser customizados por meio de um sistema chamado MV Editor. Neste é possível criar formulários com regras e processos que se adequam a empresa e, desta forma, criar telas para cada processo específico dentro de cada tipo de atendimento. Este sistema será abordado em maiores detalhes na sessão 5.1.3.3 Editor.

A descrição cirúrgica disponível para o médico é realizada em atendimentos do bloco cirúrgico onde o mesmo descreve os passos realizados para aquela cirurgia ou procedimento. Este documento é visível para médicos que estão atendendo o paciente.

Ao final de cada atendimento realizado, o médico deve realizar o processo de alta hospitalar informando as condições do paciente ao término do atendimento, também deve informar o CID, pois é através dele que é traçado o perfil epidemiológico do hospital.

Ao enfermeiro e técnico é liberado acesso as prescrições e evoluções medicas para posteriormente administrar e controlar as medicações. É disponibilizado também para ambos um aplicativo assistencial com recursos do sistema PEP, este auxilia na segurança na administração de medicamentos. O aplicativo torna o processo mais confiável pois é necessário realizar a conferência entre o QR Code do produto dispensado pela farmácia com a pulseira de identificação do paciente, então o aplicativo valida se está prescrito para o paciente para aquele horário e medicamento.

O enfermeiro não pode prescrever medicamentos somente procedimentos de enfermagem e cuidados do paciente, além de realizar evoluções e anotações com orientações sobre o tratamento e demais informações sobre a estadia do paciente no hospital.

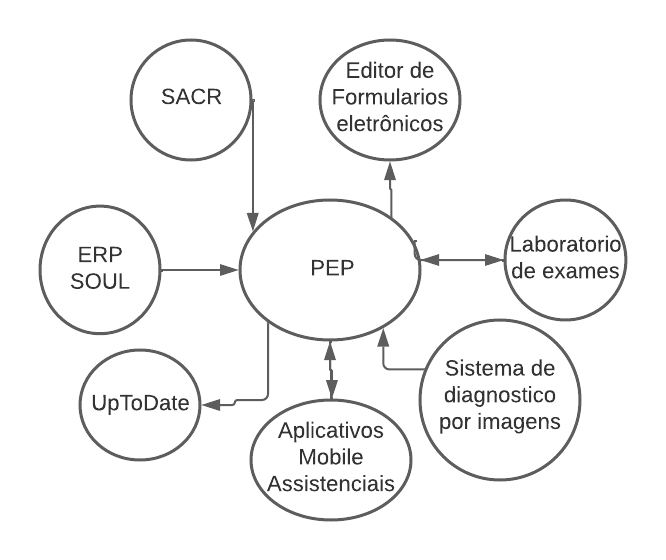
O técnico de enfermagem por sua vez não pode realizar prescrições no sistema, porém, pode visualizar toda a história clínica que o médico registra no atendimento necessária para dar o apoio assistencial necessário conforme orientações médicas. E para registrar o processo de seu atendimento o técnico de enfermagem pode realizar anotações no sistema e o registro de aferições de sinais vitais do paciente.

No sistema MVPEP há diversas integrações, tanto externas quanto internas, que auxiliam no processo desde configuração para utilização até processos de atendimento de pacientes. Estes são detalhados na sessão 5.1.3.1.

**5.1.3 Sistemas relacionados ao MVPEP**

São apresentados, na sequência, os sistemas relacionados responsáveis pela configuração do sistema MVPEP, este segmentado por módulos no ERP MVSOUL. Nele é possível criar atendimentos, configurar os acessos, perfis de usuários e demais processos derivados do MVPEP. Na Figura 4 são apresentados, de forma ilustrada, todos os sistemas que atualmente atuam em conjunto como o PEP para trazer praticidade, tecnologia e segurança.

Figura 4 - Sistemas integrados ao PEP (prontuário eletrônico do paciente)



**Fonte: Do autor (2022)**

*5.1.3.1 Soul MV*

No sistema de almoxarifado, é possível a gestão de estoque do hospital, automatizando os processos que envolvem a solicitação e o atendimento de produtos. Como possui integração com outros sistemas, permite que a lista de produtos prescritos seja impressa ou recebida eletronicamente na farmácia. Depois de aprovados pelo farmacêutico, eles serão dispensados para os pacientes por meio de leitores de código de barras ou registro manual. Essas leitoras geram o débito automático dos produtos no estoque e a atualização dos dados na conta do paciente.

A central de agendamento realiza o agendamento de consultas e exames de forma prática e rápida, possibilitando a redução do tempo de atendimento ao paciente e a eliminação de papéis, por meio de lembretes afixados nos postos de trabalho, com orientações de exames, perguntas de exames, mensagens informativas ao paciente, entre outras opções que poderão ser emitidas via agendamento eletrônico. Além disso, é conferida maior segurança à gerência das agendas médicas e dos agendamentos, aproveitando ao máximo os horários com as agendas dinâmicas, evitando assim, horários ociosos.

No módulo de centro cirúrgico e obstétrico é possível gerenciar todos os procedimentos do bloco cirúrgico, permitindo ao administrador acompanhar com precisão os resultados das cirurgias realizadas a partir do consultório ou pela central de marcação. Poderão ser visualizadas informações como: as cirurgias agendadas no sistema, os procedimentos a serem realizados, a equipe médica responsável, o tipo de anestesia a ser administrada, a necessidade de equipamentos específicos, os materiais e derivados para a cirurgia em questão. Ao término da cirurgia, a folha de sala é registrada com a descrição cirúrgica, debitando o saldo do estoque da farmácia e realizando o faturamento *on-line* dos produtos e das taxas dos equipamentos utilizados.

O controle de Infecção hospitalar é o sistema utilizado para orientar e capacitar o usuário no cadastro e gerenciamento dos processos inerentes ao Controle de Infecção Hospitalar.

O módulo de diagnóstico por imagem possibilita o cadastro e o gerenciamento dos exames de imagem, bem como a emissão de laudos, identificação dos setores de exames e o controle das versões dos resultados.

No módulo de diretoria clínica é possível cadastrar os profissionais que prestam serviços para o hospital, bem como, registrar e consultar algumas características desses prestadores, como conselhos aos quais estão vinculados, suas especializações, especialidades e áreas de atuação, entre outras informações. Também permite o cadastro de ocorrências e licenças médicas, auxiliando no gerenciamento dos serviços prestados.

O sistema de gerenciamento de unidades reúne as funções administrativas realizadas nos Postos de Enfermagem, bem como as configurações para um bom funcionamento do MVPEP (Prontuário Eletrônico do Paciente). Administra a movimentação do paciente, exibindo as admissões médicas realizadas em todas as unidades da instituição. Possibilita também, a opção de informar as ocorrências dos plantões, monitorar os atendimentos, consultar as prescrições e exames solicitados para os pacientes. Além disso, permite configurar o SAE (Sistematização da Assistência de Enfermagem).

As configurações realizadas no menu "PEP" e "SAE" tem impacto direto no sistema MVPEP. A integração dos processos no sistema possibilita aumento na produtividade e eliminação do retrabalho nos setores finais.

O módulo de Gestão de Usuários possibilita o gerenciamento dos sistemas utilizados pelo hospital, dos usuários e de seus respectivos acessos a cada sistema cadastrado. Além disso, permite todo o controle de auditoria e consulta das tabelas cadastradas.

O módulo de Internação permite efetuar o gerenciamento dos processos de admissão dos pacientes no hospital por meio de internação, realizando a emissão de formulários e o controle de reserva e ocupação dos leitos. Fornece informações estatísticas do perfil dos pacientes atendidos, procedimentos realizados, taxas de ocupação do hospital, faturamento e outros tipos mais utilizados. Além disso, possibilita a realização do cadastro dos pacientes e o processo de alta médica e hospitalar. O sistema permite também a integração on-line com as Centrais de Regulação de Leitos.

No módulo de Laboratório de Análises Clínicas é possível cadastrar e gerenciar os exames laboratoriais, bem como emitir laudos, realizar a identificação dos setores de exames e controlar as versões dos resultados.

O módulo de Nutrição e Dietética permite cadastrar as opções de cardápios, refeições e dietas utilizadas no hospital e gerenciar as solicitações de refeições, procurando orientar e esclarecer as necessidades de informações dos clientes e usuários.

No módulo de Urgência e Emergência existe a possibilidade de gerenciamento dos procedimentos relativos ao cadastro dos atendimentos de urgência, à triagem e ao acompanhamento dos pacientes atendidos.

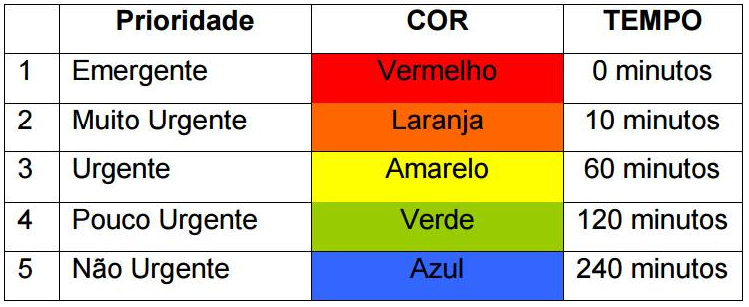
*5.1.3.2 SACR*

O SACR utiliza o protocolo de Manchester, que permite a identificação de prioridade e a definição do tempo alvo recomendado até a avaliação médica para cada caso. Se torna responsável por orientar a classificação e categorização do diagnóstico do paciente.

Para os atendimentos de urgência e emergência inicia-se pela triagem onde o atendimento é realizado no sistema de acolhimento com classificação de risco, é uma ferramenta indispensável para a priorização de atendimento aos pacientes, de acordo com a gravidade clínica de cada um. Nas urgências dos hospitais, a ordem de chegada tem de ser substituída pela ordem de necessidade clínica e a triagem realizada pela equipe responsável é facilmente controlada por esse sistema. Integrado com os sistemas de atendimento ao paciente, o SACR possibilita organizar a lista de atendimento visando a prioridade pelo atual estado de saúde dos enfermos, categorizando aqueles que precisam de uma atenção médica mais rápida.

Na figura 4 é ilustrada a relação de prioridade com cor atribuída e tempo estimado para atendimento médico.

Figura 5 - Categorias protocolo Manchester



**Fonte: Do autor (2022)**

*5.1.3.3 Editor*

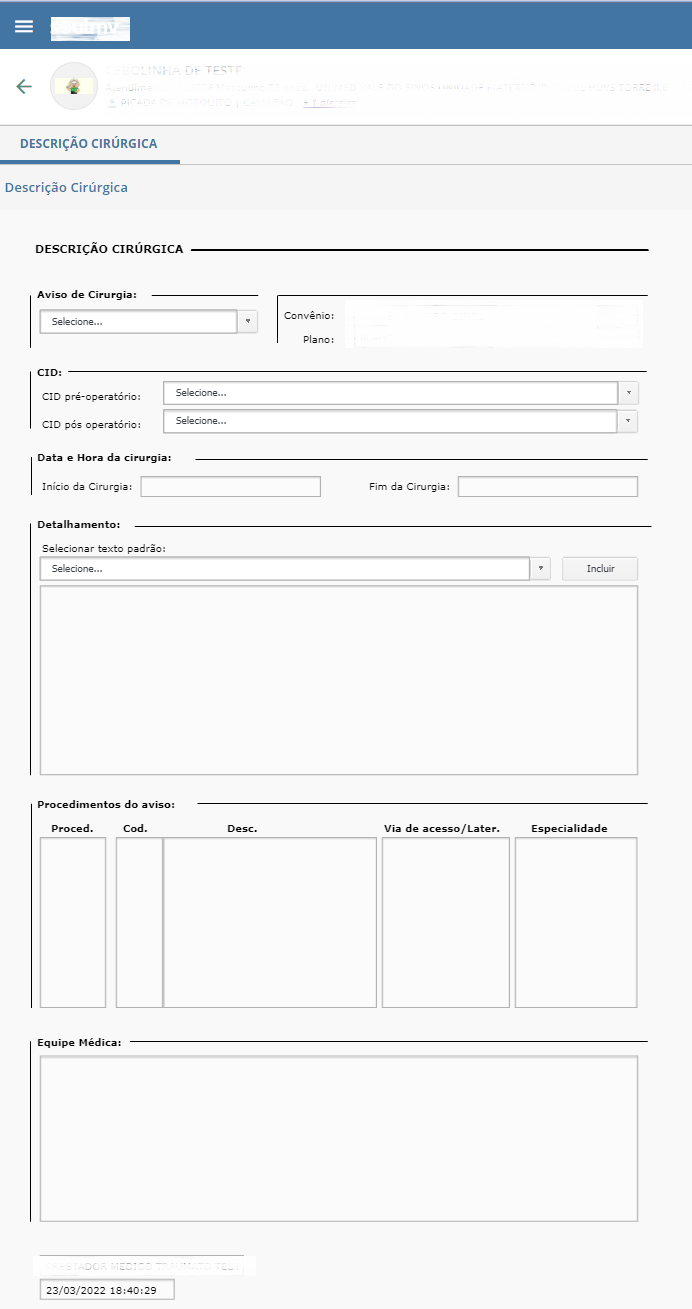
Esta ferramenta foi especialmente desenvolvida para possibilitar a construção de documentos eletrônicos que serão utilizados pelos médicos, enfermeiros e técnicos de enfermagem no sistema de Prontuário Eletrônico do Paciente. Ela propicia que a criação desses documentos seja realizada de maneira rápida, eficaz e uniforme, já que um único campo criado poderá ser utilizado em mais de um documento.

O sistema é composto pelas abas “Campos” e “Documentos”, por meio das quais são criados campos/metadados e elaboradas as telas e os relatórios que serão utilizados no atendimento.

Campos/metadados possibilitam realizar ações como consultas em banco de dados com instruções SQL (*Structured Query Language*) entre outras funções como receber dados para gravação em campos de textos para atender diversas rotinas do hospital. Garantem a legibilidade de informações e possibilitam o armazenamento e controle da informação registrada, pois possibilita gerar relatórios e indicadores de atendimento.

Na Figura 6 é apresentado um exemplo de documento eletrônico criado para realizar descrições cirúrgicas trazendo informações do paciente, dados da cirurgia, como procedimento, equipe medica, início e fim de cirurgia e CID operatório.

Figura 6 - Descrição cirúrgica criada em MVEditor



**Fonte: Do autor (2022)**

Apresentados os recursos do sistema de prontuário eletrônico e suas integrações, observa-se uma grande massa de dados ditos como sensíveis e pessoais, e desta forma busca-se analisar os requisitos que compõem a tabela Padrão TISS que contempla a troca de informações em sistemas e portais na saúde suplementar sobre os princípios da LGPD conforme é apresentado a seguir no Capítulo 6.

**6 ANÁLISE DE REQUISITOS PADRÃO TISS, SOB A LUZ DA LGPD**

Para a análise do sistema de prontuário eletrônico escolhido - MVPEP e suas ramificações com sistemas integrados buscou-se como referência a tabela padrão TISS (Troca de Informações na Saúde Suplementar). Esta contém 78 requisitos desde a comunicação entre sistemas até o tratamento de dados pessoais em um ambiente hospitalar, dividida em cinco componentes conforme apresentado a seguir.

O primeiro componente é o organizacional que é o responsável por estabelecer o conjunto de regras operacionais. No segundo componente, chamado conteúdo e estrutura é definida a arquitetura dos dados utilizados nas mensagens eletrônicas e no plano de contingência, para coleta e disponibilidade dos dados.

Como terceiro item tem-se a representação de conceitos em saúde do Padrão TISS que estabelece o conjunto de termos para identificar os eventos e itens assistenciais na saúde suplementar, consolidados na Terminologia Unificada da Saúde Suplementar - TUSS.

No quarto componente, segurança e privacidade do Padrão TISS são apresentados os requisitos de proteção para assegurar o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde. Tem como base o sigilo profissional e segue a legislação.

Por fim, o quinto componente de comunicação do Padrão TISS estabelece os meios e os métodos de comunicação das mensagens eletrônicas definidas no componente de conteúdo e estrutura. Adota a linguagem de marcação de dados XML - *Extensible Markup Language*.

Inicialmente buscou-se classificar esta tabela sobre os 10 princípios que são previstos na LGPD apresentados no Art. 6. Desta forma, estes 78 requisitos foram classificados dentro de um dos princípios apresentados no Quadro 5.

Quadro 5 - Princípios e seus requisitos

|  |  |
| --- | --- |
| **Principio** | **Total** |
| III - Necessidade | 3 |
| IV – Livre acesso | 2 |
| V – Qualidade dos dados | 6 |
| VI – Transparência | 2 |
| VII – Segurança | 47 |
| VIII – Prevenção | 1 |

**Fonte: Do autor (2022)**

Após esta classificação foi realizada a análise dos requisitos sob os sistemas MVPEP, MVSOUL, MVEDITOR, MVSACR, APLICATIVOS e DIAGNÓSTICO POR IMAGEM citados no Capítulo 5. Neste trabalho foram avaliados os impactos, riscos, ações e sugestões para correções ou melhorias para os requisitos que os sistemas não atendem ou que atendem parcialmente onde o sistema disponibiliza funcionalidades para atender ao requisito porem a empresa não utiliza ou utiliza de forma incorreta. O Apêndice A apresenta a tabela completa com todos os requisitos analisados neste trabalho. O Quadro 6 apresenta os sistemas e os requisitos que não são totalmente atendidos.

Quadro 6 - Sistemas e requisitos não atendidos completamente

|  |  |  |
| --- | --- | --- |
| **Sistema** | **Não atende** | **Parcial** |
| MVPEP | 4 | 2 |
| MVSOUL | 4 | 2 |
| MVEDITOR | 6 | 1 |
| SACR | 4 | 1 |
| APLICATIVOS | 4 | 1 |
| DIAGNÓSTICO POR IMAGEM | 9 | 2 |

**Fonte: Do autor (2022)**

6.1 ANÁLISE DOS REQUISITOS DO SISTEMA MVPEP E MVSOUL

Nesta seção são descritos os requisitos não atendidos completamente e parciais no sistema MVPEP e MVSOUL, SACR e Aplicativos apresentando o problema, o impacto e a solução. Ambos sistemas compartilham dos mesmos requisitos que não atendem ou atendem parcialmente, desta forma, a apresentação dos dois sistemas será conjunta.

Quadro 7 – Requisito 5 TISS (2022) MVPEP e MVSOUL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 5 | Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a um ano. O sistema deve permitir que o usuário troque sua senha a qualquer momento. | Obrigatório | VIII | Parcial |

**Fonte: Do autor (2022)**

* Problema: Aumenta possibilidades de exploração e vazamento de dados com senha de usuários.
* Impacto: Configurando conforme previsto no requisito 5 observa-se um impacto positivo, evitando exploração de senhas.
* Solução: O sistema disponibiliza esse requisito, cabe ao responsável pela administração do sistema que realize a configuração adequada para que atenda de forma completa este requisito. A Figura 7 demonstra que o sistema permite esta configuração e como forma de maior proteção indica-se o período de 365 dias (um ano) para trocar a senha obrigatoriamente, atualmente está configurado para 999 dias.

Figura 7 - Tela de configuração de diretivas de segurança



**Fonte: Do autor (2022)**

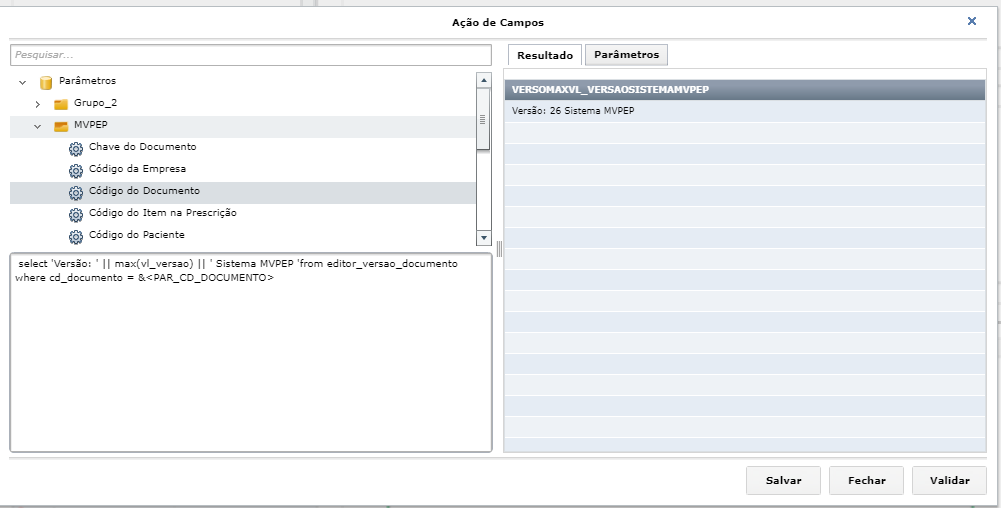
Quadro 8 – Requisito 36 TISS (2022) MVPEP e MVSOUL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 36 | O sistema deve apresentar minimamente as informações de identificação do software, contendo obrigatoriamente o nome do software, nome do fornecedor, identificação completa da versão e/ou *release* e/ou *build*.  Essas informações deverão estar disponíveis minimamente:  • na tela inicial do sistema;  • nas telas de cada módulo de modo que quando o sistema esteja em uso essas informações sejam sempre visíveis;  • impressões geradas oriundas do sistema. | Obrigatório | V | Parcial |

**Fonte: Do autor (2022)**

* Problema: Requisito atende parcialmente devido a não exibir em relatórios e documentos eletrônicos personalizados a informação de versão e sistema gerados.
* Impacto: Dificulta a identificação da versão impressa do documento e de alterações de novas versões dos documentos eletrônicos e origem do documento impresso.
* Solução: É possível incluir a informação de identificação do sistema e versão do documento criando um campo com uma *query* (*Structured Query Language*) e incluir este campo no rodapé ou cabeçalho do documento oriundo do sistema. Na Figura 8 é apresentado o campo criado com o retorno desejado para o documento de atestado médico que é gerado no sistema MVPEP e desenvolvido no MVEditor.

Figura 8 - Campo descrição versão e sistema oriundo



**Fonte: Do autor (2022)**

Quadro 9 – Requisito 42 TISS (2022) MVPEP e MVSOUL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 42 | Assim que completada uma autenticação com sucesso, o sistema deve exibir à pessoa usuária as seguintes informações:  • Data e hora da última autenticação com sucesso de seu usuário;  • Data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso.  Nota: Considera-se como “última autenticação” a autenticação anterior à que está ocorrendo. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Usuário não tem informações de últimos acessos com sucesso e tentativas invalidas de acesso.
* Impacto: Sem a informação de último acesso ou tentativa de acesso o usuário não consegue identificar possíveis tentativas de acesso indevido, podendo até resultar em vazamento de informações sensíveis.
* Solução: Para este requisito o sistema MVPEP não possui a funcionalidade, será necessário abrir chamado de implementação com o fornecedor.

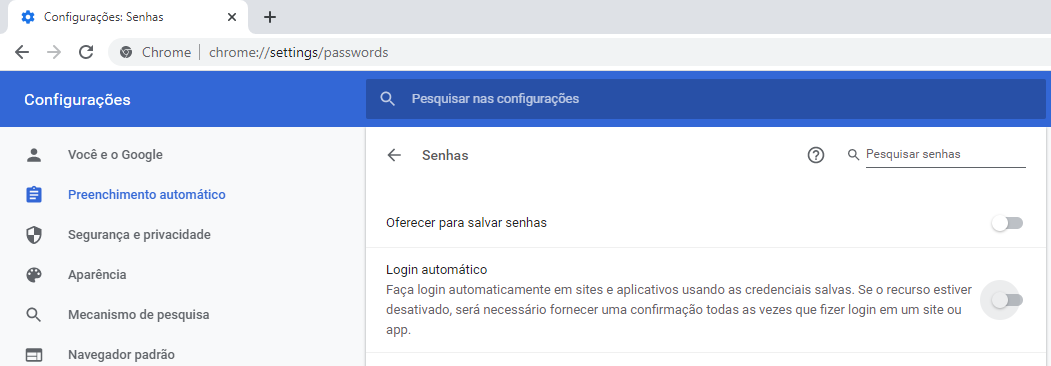
Quadro 10 – Requisito 43 TISS (2022) MVPEP e MVSOUL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 43 | Condição: Arquitetura cliente-servidor e autenticação por *login* e senha. A interface de usuário utilizada para digitação de credenciais de acesso ao sistema (*login* ou nome do usuário, senha secreta de acesso, PIN) deve impedir a memorização e a visualização de dados anteriores (lista de *logins* já digitados, lembrança automática de senhas associadas a um *login*, etc.). Além disso, toda e qualquer digitação direta de senhas deve ser feita por meio de máscara de caracteres que impeça sua visualização por outras pessoas. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Atualmente o sistema é executado no *browser* Google Chrome e o mesmo está habilitado para oferecer que a senha e usuário sejam salvos.
* Impacto: Em computadores compartilhados, caso um usuário salve a senha, é possível acessar o sistema com credencias salvas anteriormente por outro usuário ocasionando em acesso indevido.
* Solução: É recomendado, principalmente em áreas assistenciais de atendimento ao paciente, que seja removida a opção que permite salvar senhas. A configuração para desabilitar tal recurso é apresentada na Figura 9 a seguir.

Figura 9 - Configuração para desabilitar salvar credenciais de acesso



**Fonte: do autor (2022)**

Quadro 11 – Requisito 63 TISS (2022) MVPEP e MVSOUL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 63 | Utilização de *captcha* na tela de acesso ao sistema vinculada ao método de autenticação por *login* e senha. Não deve ser permitido autenticar o usuário sem a validação simultânea do *login*, senha e *token* do *captcha*. | Recomendado | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Tentativas automatizadas podem ser usadas por fraudadores para acesso não autorizado.
* Impacto: Através de ataques do tipo *Brute Force* (Ataque de força bruta) é possível ter acesso a aplicações e dados não autorizados.
* Solução: Devido ao sistema estar configurado para acesso somente a domínio interno não há necessidade de utilização de *captcha*, somente acesso por *login* e senha, como já utilizado.

Quadro 12 – Requisito 65 TISS (2022) MVPEP e MVSOUL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 65 | Utilização de *captcha* na tela de recuperação de senha de acesso do sistema para evitar ataques do tipo *Brute Force*. | Recomendado | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Tentativas automatizadas podem ser usadas por fraudadores para acesso não autorizado.
* Impacto: Através de ataques do tipo *Brute Force* (Ataque de força bruta) é possível ter acesso a aplicações e dados não autorizados.
* Solução: Devido ao sistema estar configurado para acesso somente a domínio interno não há necessidade de utilização de *captcha*, somente acesso por *login* e senha. O sistema está atualmente configurado para permitir somente 5 tentativas de acesso, após isso usuário será bloqueado e somente o administrador pode ativar o acesso novamente.

6.2 ANALISE DOS REQUISITOS DO SISTEMA MVEDITOR

Nesta seção são descritos os requisitos não atendidos completamente no sistema MVEDITOR, apresentando o problema, o impacto e a solução.

Quadro 13 – Requisito 5 TISS (2022) Editor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 5 | Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a um ano. O sistema deve permitir que o usuário troque sua senha a qualquer momento. | Obrigatório | VIII | Parcial |

**Fonte: Do autor (2022)**

O usuário de acesso ao MVEditor é o mesmo de acesso ao MVSOUL, portanto aplica-se a mesma solução descrita na seção 6.1, não sendo necessária outra configuração para solução deste requisito ao sistema MVEditor.

Quadro 14 – Requisito 7 TISS (2022) Editor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 7 | Bloquear, ao menos temporariamente, o usuário após um número máximo de tentativas inválidas de *login*, por qualquer meio de acesso. Este número de tentativas não deve ser superior a cinco. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

Foram realizados testes onde evidenciou-se que mesmo após mais de 5 tentativas o sistema não bloqueava o acesso. Desta forma o sistema pode ser alvo de ataques como *Brute Force*.

* Problema: Tentativas automatizadas podem ser usadas por fraudadores para acesso não autorizado.
* Impacto: Através de ataques do tipo *Brute Force* (Ataque de força bruta) é possível ter acesso a aplicações e ter dados não autorizados.
* Solução: Para correção deste problema será necessário abrir um chamado com o fornecedor pois não há como solucionar internamente.

Quadro 15 – Requisito 33 TISS (2022) Editor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 33 | a) A sessão de usuário deve ser automaticamente bloqueada ou encerrada forçadamente pelo aplicativo após um período de inatividade. Este tempo não deve ser superior a 30 minutos.  b) após o bloqueio ou encerramento da sessão de usuário, as informações em tela não deverão mais estar visíveis, sendo necessária uma nova autenticação para a retomada da atividade.  c) não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Acesso não autorizado ao sistema de usuários que esqueceram de realizar *logout.*
* Impacto: Com o acesso não autorizado é possível causar danos a empresa pois o sistema armazena os formulários personalizados utilizados em prontuário eletrônico para auxilio em atendimentos de pacientes. É possível então com acesso não autorizado, ter acesso a dados sensíveis.
* Solução: Atualmente sistema não possui configurado *time out* na aplicação, será necessário em conjunto com fornecedor do software realizar a configuração para que a sessão seja encerrada após 30 minutos de inatividade e obrigue novo acesso com autenticação de *login* e senha para novas alterações.

Quadro 16 – Requisito 42 TISS (2022) Editor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 42 | Assim que completada uma autenticação com sucesso, o sistema deve exibir à pessoa usuária as seguintes informações:  • Data e hora da última autenticação com sucesso de seu usuário;  • Data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso.  Nota: Considera-se como “última autenticação” a autenticação anterior à que está ocorrendo. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Usuário não tem informações de últimos acessos com sucesso e tentativas invalidas de acesso.
* Impacto: Sem a informação de último acesso ou tentativa de acesso usuário não consegue identificar possíveis tentativas de acesso indevido, podendo até resultar em vazamento de informações sensíveis.
* Solução: O sistema MVEditor não possui a funcionalidade será necessário abrir chamado de implementação com o fornecedor do software.

Quadro 17 – Requisito 43 TISS (2022) Editor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 43 | Condição: Arquitetura cliente-servidor e autenticação por *login* e senha. A interface de usuário utilizada para digitação de credenciais de acesso ao sistema (*login* ou nome do usuário, senha secreta de acesso, PIN) deve impedir a memorização e a visualização de dados anteriores (lista de *logins* já digitados, lembrança automática de senhas associadas a um *login*, etc.). Além disso, toda e qualquer digitação direta de senhas deve ser feita por meio de máscara de caracteres que impeça sua visualização por outras pessoas. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Atualmente o sistema é executado no *browser Google Chrome* e o mesmo está habilitado para oferecer que a senha e usuário sejam salvos.
* Impacto: Em computadores compartilhados, caso um usuário salve a senha, é possível acessar o sistema com credencias salvas anteriormente por outro usuário, ocasionando em acesso indevido.
* Solução: A solução para este requisito e sistema pode ser a mesma sugerida na seção 6.1 da análise dos sistemas MVPEP e MVSOUL.

Quadro 18 – Requisitos 63 e 65 TISS (2022) Editor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 63 | Utilização de *captcha* na tela de acesso ao sistema vinculada ao método de autenticação por *login* e senha. Não deve ser permitido autenticar o usuário sem a validação simultânea do *login*, senha e *token* do *captcha*. | Recomendado | VII | Não atende |
| 65 | Utilização de *captcha* na tela de recuperação de senha de acesso do sistema para evitar ataques do tipo *Brute Force*. | Recomendado | VII | Não atende |

**Fonte: Do autor**

Os requisitos 63 e 65 são apenas recomendados, desta forma avaliado que devido o sistema estar disponível somente em domínio interno da empresa e de acesso para desenvolvedores de formulários eletrônicos não é necessária a implementação de *captcha* pois o acesso ao sistema utiliza *login* e senha.

6.3 ANALISE DOS REQUISITOS DO SISTEMA DE DIAGNÓSTICO POR IMAGEM

Nesta seção é apresentado a análise dos requisitos não atendidos e não atendidos completamente para o sistema de Diagnóstico por Imagem utilizado para visualização de imagens de exames e laudos no prontuário eletrônico MVPEP.

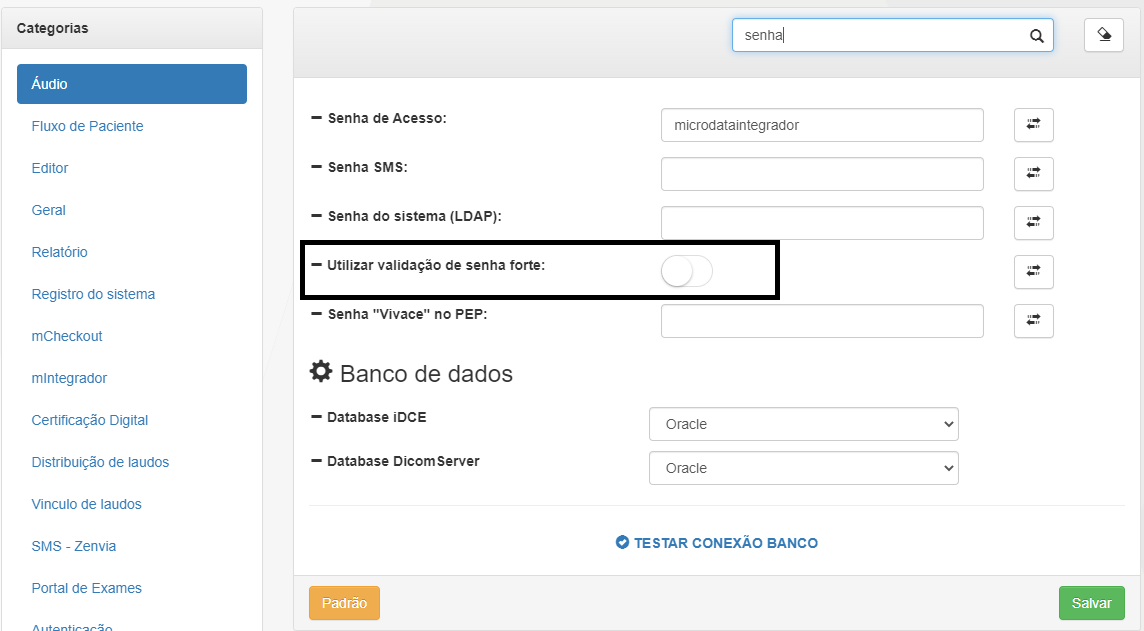
Quadro 19 – Requisito 4 TISS (2022) Diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 4 | Verificar a qualidade de segurança da senha no momento de sua definição pelo usuário obrigando a utilização de, no mínimo, 8 caracteres dos quais, no mínimo, 1 caractere deve ser não alfabético. | Obrigatório | VII | Não atende |

**Fonte: Do autor**

* Problema: Atualmente o sistema permite criar senhas fáceis de decifrar, assim como por exemplo senha123 ou até mesmo 123.
* Impacto: O Sistema fica suscetível a invasões por utilização de senhas consideradas fracas e assim tendo dados sensíveis vazados ou até corrompidos.
* Solução: O Sistema possui configuração de senha forte assim como apresentado na Figura 10, onde obriga no próximo acesso a troca para uma senha forte com 8 caracteres entre letras, números e no mínimo um caractere especial.

Figura 10 - Configuração de senha forte



**Fonte: Do autor (2022)**

Quadro 20 – Requisito 5 TISS (2022) Diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 5 | Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a um ano. O sistema deve permitir que o usuário troque sua senha a qualquer momento. | Obrigatório | VIII | Parcial |

**Fonte: Do autor (2022)**

* Problema: Aumenta possibilidades de exploração e vazamento de dados com senha de usuários.
* Impacto: Configurando conforme previsto no requisito 5 observa-se um impacto positivo, evitando exploração de senhas.
* Solução: Atualmente o sistema não dispõem de configuração para obrigar a troca de senha por período definido. Como solução neste caso seria necessário que o fornecedor criasse essa rotina padrão no sistema. Outra solução sugerida seria a realização de um *UPDATE* e base de dados na tabela RS\_SEG\_USUARIO para exigir a troca no próximo *login* a cada 365 dias conforme recomendado no requisito. A seguir é apresentado o comando SQL para esta rotina.

**UPDATE** RS\_SEG\_USUARIO **SET** SN\_TROCA\_SENHA = 'S' **WHERE** SN\_ATIVO = 'S';

Quadro 21 – Requisito 7 TISS (2022) Diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 7 | Bloquear, ao menos temporariamente, o usuário após um número máximo de tentativas inválidas de *login*, por qualquer meio de acesso. Este número de tentativas não deve ser superior a cinco. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Atualmente o sistema não possui rotina para bloquear usuário após 5 tentativas invalidas de acesso.
* Impacto: Sem esta validação de número máximo de acessos inválidos o sistema fica vulnerável a ataques de *Brute Force* (Força Bruta), e ainda agregado ao problema de o sistema não exigir senha forte descrito no requisito 4, se torna muito mais fácil a descoberta de senha de qualquer usuário, assim expondo dados sensíveis de qualquer paciente.
* Solução: Para solução deste problema será necessário abrir chamado de correção e melhoria com o fornecedor do *software*, criando rotina onde valide a quantidade de tentativas invalidas de acesso ao sistema.

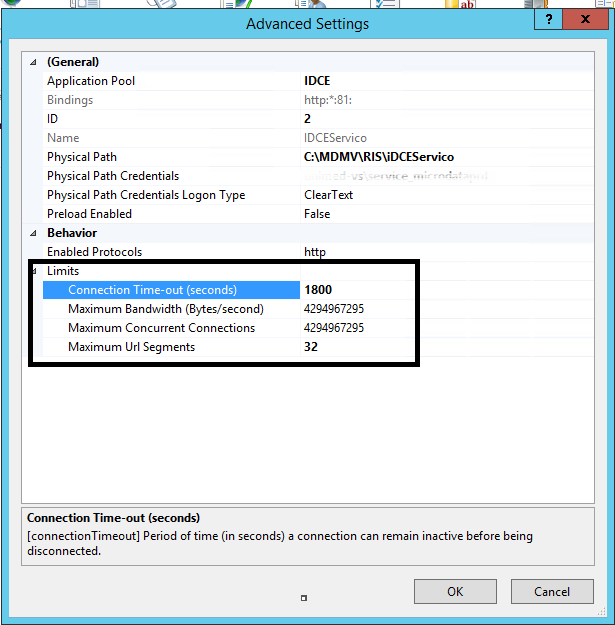
Quadro 22 - Requisito 33 TISS (2022) Diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 33 | a) A sessão de usuário deve ser automaticamente bloqueada ou encerrada forçadamente pelo aplicativo após um período de inatividade. Este tempo não deve ser superior a 30 minutos.  b) após o bloqueio ou encerramento da sessão de usuário, as informações em tela não deverão mais estar visíveis, sendo necessária uma nova autenticação para a retomada da atividade.  c) não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles. | Obrigatório | VII | Parcial |

**Fonte: Do autor (2022)**

* Problema: Sem atender este requisito, caso usuário deixe o sistema aberto em um local público sem devidos cuidados pode dar acesso indevido e brechas para vazamento de dados sensíveis.
* Impacto: Caso ocorra acesso indevido o impacto será negativo pois sistema armazena imagens e laudos de exames de pacientes.
* Solução: É possível configurar o *timeout* da aplicação através do IIS (*Internet Information Services*) servidor web disponibilizado pela Microsoft Windows, onde o sistema está hospedado. A Figura 11 apresenta a configuração necessária para atender completamente este requisito.

Figura 11 - Configuração *timeout* IIS (*Internet Information Services*)



**Fonte: Do autor (2022).**

Quadro 23 - Requisito 42 TISS (2022) diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 42 | Assim que completada uma autenticação com sucesso, o sistema deve exibir à pessoa usuária as seguintes informações:  • Data e hora da última autenticação com sucesso de seu usuário;  • Data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso.  Nota: Considera-se como “última autenticação” a autenticação anterior à que está ocorrendo. | Obrigatório | VIII | Não atende |

**Fonte: Do autor (2022)**

* Problema: O sistema atualmente não exibe informações referentes ao último acesso do usuário
* Impacto: Sem as informações do último acesso o usuário não pode identificar possíveis acessos indevidos gerando grande impacto negativo caso ocorra tal falha.
* Solução: Para atender este requisito será necessário abrir chamado de melhoria com o fornecedor do *software* para que apresente as últimas autenticações ou falhas de acesso daquele usuário.

Quadro 24 - Requisito 43 TISS (2022) Diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 43 | Condição: Arquitetura cliente-servidor e autenticação por *login* e senha. A interface de usuário utilizada para digitação de credenciais de acesso ao sistema (*login* ou nome do usuário, senha secreta de acesso, PIN) deve impedir a memorização e a visualização de dados anteriores (lista de *logins* já digitados, lembrança automática de senhas associadas a um *login*, etc.). Além disso, toda e qualquer digitação direta de senhas deve ser feita por meio de máscara de caracteres que impeça sua visualização por outras pessoas. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: O sistema atualmente utiliza o *browser* Google Chorme e desta forma está habilitado a oferecer para gravar credenciais de usuários.
* Impacto: Caso usuário deixe suas credenciais salvas em um computador compartilhado pode deixar disponível acesso indevido a pessoal não autorizado e por se tratar de laudos e imagens de exames de pacientes considera-se crítico este impacto.
* Solução: Sugere-se, assim como apresentado na secção 6.1 e Figura 9, bloquear que o browser ofereça para gravar credenciais de acessos impedindo assim acesso não autorizado ao sistema.

Quadro 25 - Requisito 67 TISS (2022) Diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 67 | Mínimo de 08 caracteres utilizando pelo menos um (01) caractere de cada um dos quatro (4) tipos de caracteres listados abaixo:  • Letras Maiúsculas (AZ)  • Letras Minúsculas (az)  • Números (0-9)  • Símbolos ASCII (`~! @ # $% ^ & \* () \_ + - = {} | \:"; '<>?,. / e espaço) e caracteres *unicode*. | Obrigatório | VII | Não atende |

**Fonte: Do autor (2022)**

* Problema: Na configuração de senha forte apresentada na solução do requisito 4 foi identificada uma falha onde o sistema não está realmente obrigando o cadastro de senha com caracteres especiais assim como prevê o requisito 67.
* Impacto: Usuários podem criar senhas fracas deixando assim o sistema vulnerável, gerando um impacto negativo para a empresa caso alguma senha seja exposta.
* Solução: Para este requisito será necessária a abertura de chamado de correção com fornecedor do *software* para validar a utilização de caracteres especiais na criação da senha forte.

Quadro 26 - Requisitos 63 e 65 TISS (2022) - Diagnóstico por imagem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Requisito** | **Descrição** | **Condição** | **Princípio** | **R** |
| 63 | Utilização de *captcha* na tela de acesso ao sistema vinculada ao método de autenticação por *login* e senha. Não deve ser permitido autenticar o usuário sem a validação simultânea do *login*, senha e *token* do *captcha*. | Recomendado | VII | Não atende |
| 65 | Utilização de *captcha* na tela de recuperação de senha de acesso do sistema para evitar ataques do tipo *Brute Force*. | Recomendado | VII | Não atende |

**Fonte: Do autor**

Os requisitos 63 e 65 são apenas recomendados, desta forma como é não possível implementação por parte da empresa de saúde este requisito pode ser tratado como chamado de melhoria com o fornecedor do software possibilitando a configuração caso optado pelo cliente.

# 7 CONCLUSÃO

A LGPD tem como objetivo garantir a proteção dos dados pessoais dos titulares, assegurando assim que os direitos fundamentais da liberdade e da privacidade sejam levados em consideração. A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, está sendo um grande marco na tecnologia pois com as novas regras trazidas pela lei, as empresas tiveram que inovar, investir, se adaptar e estruturar o negócio para garantir a proteção dos dados.

Apesar desta lei abranger todos os setores que utilizam dados em meio digital e físico para pessoas singulares e coletivas de acordo com o direito público e privado, no ambiente da saúde ela é ainda mais importante pois clinicas, hospitais, operadoras, laboratórios e consultórios armazenam, manipulam e transferem dados pessoais ditas como sensíveis assim como: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Atualmente com a utilização de sistemas de prontuário eletrônicos é necessário que as empresas empenhem cuidados com a segurança oferecida pelos sistemas utilizados e em adequar as tecnologias já utilizadas à nova lei. Profissionais da saúde precisarão rever a segurança na troca de informações em alguns processos.

Um exemplo comum é que as clínicas médicas enviem os dados dos pacientes para hospitais em casos de internação, assim como é comum a troca de informações entre laboratórios e hospital ou laboratórios e clínica.

Com a LGPD isso ainda é possível, porém, somente com o consentimento do paciente. Contudo, deve haver um cuidado maior por parte das organizações em relação a informar os pacientes sobre o motivo da coleta de suas informações, para quem estes dados poderão ser passados e com qual finalidade.

Além disso, todas estas informações precisarão ser criptografadas e os softwares utilizados no ambiente hospitalar devem estar aprovados por instituições como a Sociedade Brasileira de Informática em Saúde (SBIS).

A SBIS é uma organização sem fins lucrativos que reúne profissionais de saúde, tecnologia da informação para desenvolver padrões para produtos e serviços dentro do ecossistema de saúde. É com base nestas normas que a SBIS desenvolveu os parâmetros de acreditação concedidos pelas entidades, que o mercado entende como indicadores de boas práticas em estabelecimentos de saúde.

O processo de certificação S-RES foi criado por meio de uma colaboração entre SBIS e CFM para avaliar e certificar sistemas de registro eletrônico de saúde (S-RES) para qualidade, segurança e privacidade, incluindo conformidade regulatória.

Este trabalho realizou o estudo de caso em uma empresa que atua como operadora e prestadora de serviço de saúde, onde, a utilização de sistemas de prontuário eletrônico integrado a demais aplicações e recursos eletrônicos traz a preocupação com a segurança na utilização de dados sensíveis.

Desta forma buscou-se avaliar todos os requisitos obrigatórios da tabela Padrão TISS para as trocas eletrônicas de dados de atenção à saúde dos beneficiários de planos. Dito isso, verificou-se a necessidade da validação dos requisitos sob a luz da LGPD e seus princípios apresentados neste trabalho.

Sobre a análise dos requisitos identificou-se o que atende, não atende ou atende parcialmente, apresentando então os problemas, impactos observados caso o requisito não esteja atendido e as devidas providencias para solução e atendimento dos requisitos de segurança padrão em integrações.

Evidencia-se neste trabalho requisitos de grande impacto negativo em segurança onde a correção destes cabe a empresa fornecedora do software, ou analistas responsáveis pela gestão do interna do software. De qualquer forma é necessário disponibilizar recursos para atuar e prevenir incidentes de segurança digital no ambiente hospitalar.

Ainda, percebem-se oportunidades de continuação para melhorias e adequações necessárias para estar *compliance* com todos os princípios da LGPD e requisitos de segurança dentre eles como possibilitar de forma segura e prática ao indivíduo obter o poder de consentimento de toda operação realizada com seus dados assim como o poder de fácil revogação do consentimento sobre seus dados disponibilizados.

É de grande valia para empresa e indivíduo que contrata seus serviços estarem cientes de todos os processos realizados para garantir a segurança dos dados pessoais e dados sensíveis, dito isto é proposto como parte do trabalho futuro criar um guia de segurança baseado na LGPD estando assim claro e objetivos os princípios de coleta, acesso, transmissão, armazenamento, transferência e etc.

A partir deste estudo de caso conclui-se que é de grande valor e útil a empresa que utiliza os sistemas analisados buscar melhorar, aprimorar e disseminar dentre todos da empresa os riscos, práticas de segurança, treinamentos e ainda buscar prevenir e corrigir qualquer possível fonte falha de segurança.

# REFERÊNCIAS BIBLIOGRAFICAS

AVASUS. Lei Geral de Proteção de Dados (LGPD): conceitos e aplicações na área da saúde. 2020. Curso online. Disponível em: <https://avasus.ufrn.br/grade/report/user/index.php?id=378>. Acesso em 01 de abril de 2021.

BEZERRA S. L. Prontuário Eletrônico do Paciente: uma ferramenta para aprimorar a qualidade dos serviços de saúde. Rio de Janeiro: CESGRANRIO 2009.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: <http://www.planalto.gov.br/ccivil\_03/\_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 23 de outubro de 2020.

EGAN, M. *The Executive Guide to Information Security. New Jersey: Symantec Corporation*, 2005.

GALVÃO, M. C. B.; RICARTE, I. L. M. Prontuário do paciente. Rio de Janeiro: Guanabara Koogan, 2012. 322 p.

*International Standards Organization*. Disponível em: <http://www.iso.org/>. Acesso em 12 abril de 2021.

*International Standards Organization*. Disponível em: <https://www.iso.org/standard/39525.html>. Acesso em 18 maio de 2021.

ISO/IEC 17799:2005a*. Code of practice for information security management. International Standards Organization e British Standards Institute*. Disponível em: <http://www.iso.org>. Acesso em 12 abril de 2021.

ISO/IEC 17799:2005b. *Information technology . Security techniques . Code of practice for informaton security management. International Standards Organization*. Disponível em: <http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>. Acesso em 12 abril de 2021.

ISO/IEC 27001. *Information technology . Security techniques . Code of practice for informaton security management. International Standards Organization*. Disponível em: <http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>. Acesso em 12 abril de 2021.

ISO/TR 20514*. Information technology . Security techniques . Code of practice for informaton security management. International Standards Organization*. Disponível em: <http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html>. Acesso em 12 abril de 2021.

JANSSEN, L. A. Instrumento para avaliação de maturidade em processos de Segurança Da Informação: Estudo de Caso em Instituições Hospitalares, dissertação de Mestrado PPGAd/MAN/PUCRS, Porto Alegre: PUCRS, 2008.

LEME, R. S. *et al,* Jurisprudência e legislação sanitária comentadas Lei Geral de Proteção de Dados e segurança da informação. Universidade de São Paulo, São Paulo 2020.

OLIVEIRA, M. E. S. QUALI-RES: Modelo de avaliação para sistemas de registro eletrônico de saúde. Universidade Federal de Pernambuco, Recife 2013.

PATRÍCIO, C. M. *et al*, O prontuário eletrônico do paciente no sistema de saúde brasileiro: uma realidade para os médicos? Porto Alegre: Scientia Medica. Volume. 21 2011.

SABBATINI, R. M. E. A LGPD e a Proteção de Dados em Sistemas de Informação em Saúde e Telemedicina. Disponível em: <https://cryptoid.com.br/identidade-digital-destaques/a-lgpd-e-a-protecao-de-dados-em-sistemas-de-informacao-em-saude-e-telemedicina-por-renato-sabbatini/>. Acesso em 27 abril de 2021.

SBIS. Sociedade Brasileira de Informática na Saúde. Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES). Disponível em: <www.sbis.org.br>. Acesso em 12 abril de 2021.

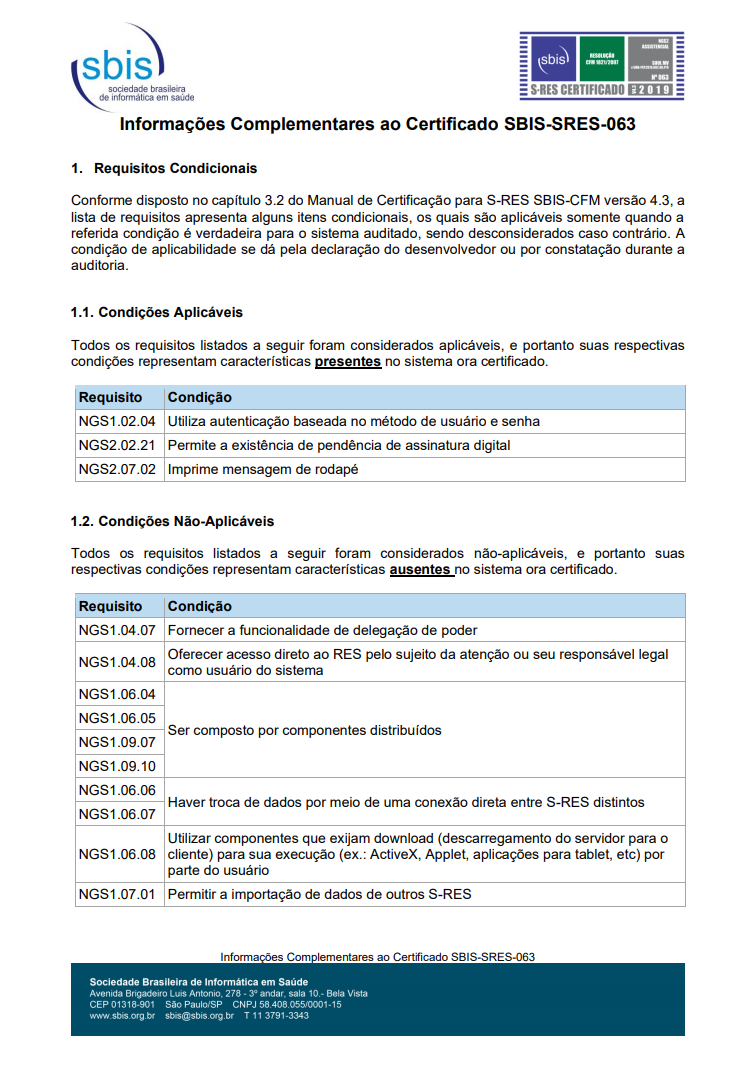
SIQUEIRA, L. S. OS DADOS PESSOAIS E A PROTEÇÃO DE DADOS DE SAÚDE: ANÁLISE A PARTIR DAS INICIATIVAS DE e-SAÚDE. Santa Maria, 2019.

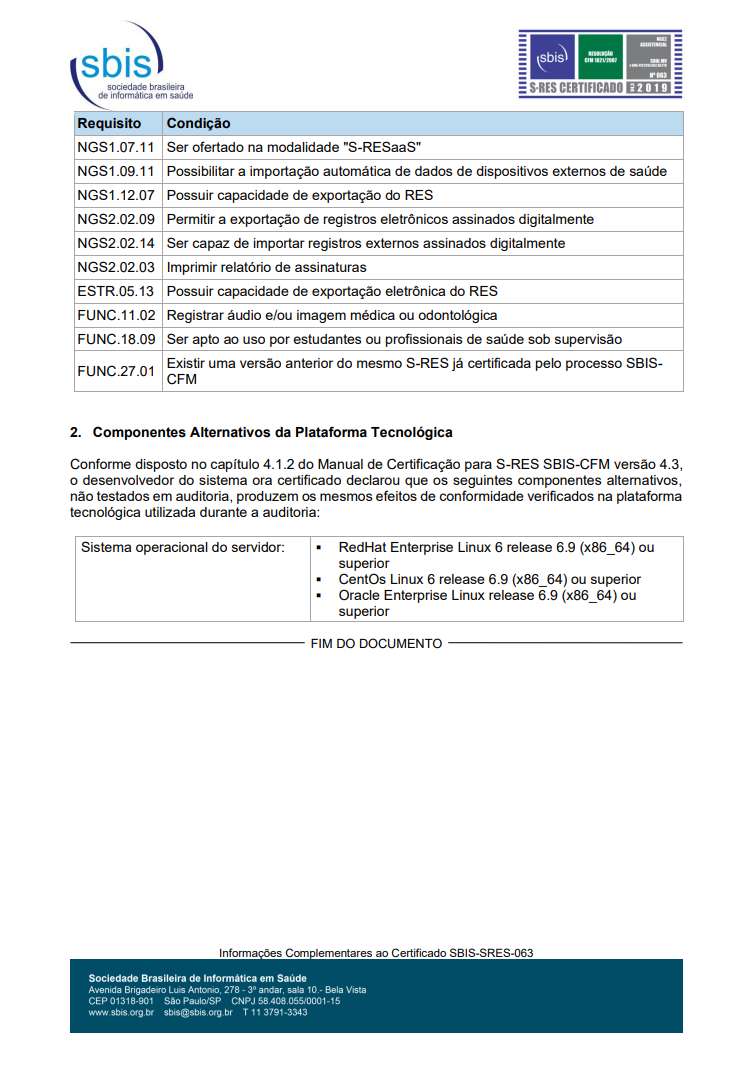
YIN, Robert. Estudo de Caso: Planejamento e Métodos. 2014. Bookman; 5 ed.

TISS, Padrão para Troca de Informação de Saúde Suplementar. Disponível em: <https://www.ans.gov.br/prestadores/tiss-troca-de-informacao-de-saude-suplementar/>. Acesso em 01 março de 2022.

# ANEXO A – CERTIFICADO SBIS







# APÊNDICE A – TABELA DE ANÁLISE DOS REQUISITOS TISS (2021)

Na tabela a seguir a letra A significa Atende, N não atende, P parcial e NA não se aplica. As condições são representadas por O obrigatório, R recomendado. Os sistemas estão identificados como: (1) MVPEP, (2) MVSOUL, (3) EDITOR, (4) SACR, (5) APPS, (6) Diagnóstico por imagem.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nro | Descrição | Condição | Princípio | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | Identificar e autenticar todo usuário antes de qualquer acesso a dados com identificação do beneficiário. | O | VII | A | A | A | A | A | A |
| 2 | Utilizar para autenticação de usuários a site e páginas da Internet (portais) *login* e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital. | O | VII | A | A | A | A | A | A |
| 3 | Utilizar para autenticação de usuários, via utilização de *webservices*, *login* e senha podendo opcionalmente, desde que acordado entre as partes, ser utilizada a certificação digital em substituição ao *login* e senha. | O | VII | A | A | A | A | A | A |
| 4 | Verificar a qualidade de segurança da senha no momento de sua definição pelo usuário obrigando a utilização de, no mínimo, 8 caracteres dos quais, no mínimo, 1 caractere deve ser não alfabético | O | VII | A | A | A | A | A | N |
| 5 | Definir o período máximo de troca de senha como controle do sistema. Este período não deve ser superior a um ano. O sistema deve permitir que o usuário troque sua senha a qualquer momento. | O | VIII | P | P | P | P | P | P |
| 7 | Bloquear, ao menos temporariamente, o usuário após um número máximo de tentativas inválidas de *login*, por qualquer meio de acesso. Este número de tentativas não deve ser superior a cinco. | O | VII | A | A | N | A | A | N |
| 11 | Registrar log de acessos e de tentativas de acesso ao sistema de informação. | O | VII | A | A | A | A | A | A |
| 12 | Utilizar certificado digital sempre dentro do período de validade além de não aceitar o certificado se o mesmo estiver na lista de certificados revogados da AC. | O | VII | A | A | A | A | A | A |
| 13 | Utilizar certificado digital que identifique o endereço eletrônico para o qual foi emitido | O | V | A | A | A | A | A | A |
| 14 | Utilizar certificado digital que contemple em identificação da autoridade certificadora emissora. | O | V | A | A | A | A | A | A |
| 15 | Utilizar certificado digital que contemple em sua estrutura a identificação do titular do certificado | O | V | A | A | A | A | A | A |
| 16 | Utilizar certificado digital que utilize protocolo criptográfico SSL ou TLS | O | VII | A | A | A | A | A | A |
| 18 | Utilizar certificado digital que implemente autenticação por algoritmo *HASH* | O | VII | A | A | A | A | A | A |
| 19 | A interrupção do serviço de troca eletrônica de informações entre prestadores de serviços de saúde e operadoras de planos privados de assistência à saúde deve ser solucionada em até 48 (quarenta e oito) horas, salvo em caso fortuito ou de força maior devidamente justificado. | O | VII | A | A | A | A | A | A |
| 21 | As operadoras de planos privados de assistência à saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial à toda informação identificada individualmente. | O | VII | A | A | A | A | A | A |
| 26 | Os prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir acesso impróprio à informação de saúde, eletrônico ou manual, em especial a toda informação identificada individualmente. | O | VII | A | A | A | A | A | A |
| 30 | Deve conter a assinatura digital do prestador de serviços na mensagem enviada à operadora para assegurar a autenticidade, o não repúdio, a integridade e a garantia de origem. | R | VII | A | A | A | A | A | A |
| 31 | Deve conter a assinatura digital da operadora na mensagem enviada ao prestador de serviços para assegurar a autenticidade, a integridade do conteúdo e o não repúdio das informações ali contidas. | R | VII | A | A | NA | NA | NA | NA |
| 32 | Igualdade de senha: os processos de troca de senha devem exigir que a nova senha seja diferente da imediatamente anterior àquela já utilizada pelo usuário. | O | VII | A | A | A | A | A | A |
| 33 | a) A sessão de usuário deve ser automaticamente bloqueada ou encerrada forçadamente pelo aplicativo após um período de inatividade. Este tempo não deve ser superior a 30 minutos. b) após o bloqueio ou encerramento da sessão de usuário, as informações em tela não deverão mais estar visíveis, sendo necessária uma nova autenticação para a retomada da atividade. c) não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles. | O | VII | A | A | N | A | A | A |
| 34 | A sessão de comunicação remota entre cliente e servidor deve possuir controles de segurança que impeçam o roubo ou reuso da sessão do usuário. a) As credenciais de acesso não devem ser transmitidas entre as partes na forma de texto claro. b) Devem haver controles que impeçam o reuso de identificadores de sessão do usuário (por exemplo: ataques de replay e *covert*-*channel*) e roubo da sessão. c) Não deve ser possível para qualquer usuário do sistema desativar ou desabilitar tais controles. | O | VII | A | A | A | A | A | A |
| 35 | Utilizar certificado digital que utilize criptografia de, no mínimo, 256 bits. | O | VII | A | A | A | A | A | A |
| 36 | O sistema deve apresentar minimamente as informações de identificação do software, contendo obrigatoriamente o nome do software, nome do fornecedor, identificação completa da versão e/ou release e/ou build. Essas informações deverão estar disponíveis minimamente: • na tela inicial do sistema; • nas telas de cada módulo de modo que quando o sistema esteja em uso essas informações estejam sempre visíveis; • impressões geradas oriundas do sistema. | O | V | P | P | A | A | A | A |
| 37 | Todo usuário do sistema deve ser identificado e autenticado antes de qualquer acesso a dados ou funcionalidades do sistema. | O | VII | A | A | A | A | A | A |
| 38 | Utilizar, nos processos de autenticação de usuário para acesso aos sistemas, um dos seguintes métodos: • Identificação de usuário e senha secreta de acesso; • Certificado digital; • Validação biométrica; • OTP. | O | VII | A | A | A | A | A | A |
| 39 | Armazenar de forma protegida todos os dados ou parâmetros utilizados no processo de autenticação de usuário. Método: Nome de usuário e senha a) A senha deve ser armazenada em banco de dados, de forma codificada por algoritmo de *hash* aberto (público) de no mínimo 160 bits. b) As codificações das senhas de acesso dos usuários devem ser protegidas contra acesso não autorizado. Método: Biometria (condição: somente para pessoas) c) Os *templates* biométricos das pessoas devem ser protegidos contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos. d) as amostras biométricas coletadas e transmitidas durante o processo de autenticação devem ser protegidas contra acesso não autorizado. Método: *One-time* *password* (OTP).  e) as sementes de geração dos valores numéricos devem ser protegidas contra acesso não autorizado. Apenas o usuário do banco de dados utilizado pela aplicação deve ter acesso aos mesmos. | O | III | A | A | A | A | A | A |
| 40 | a) O sistema deve possuir, em todos os processos de autenticação de usuário, independentemente do método de autenticação utilizado, mecanismos para bloquear a conta deste usuário no sistema após um número máximo configurável de tentativas consecutivas de *login* com autenticação inválida, que não exceda a 05 (cinco) tentativas. b) após o bloqueio de conta de um usuário, o sistema só deve permitir *login* deste após o desbloqueio de sua conta de usuário. | O | VII | A | A | A | A | A | A |
| 41 | a)Identidade única: toda pessoa usuária do sistema deverá ser identificada individualmente. b)Vinculação a número legal e único: toda pessoa usuária do sistema deverá ser vinculada minimamente a um documento de identificação pessoal unívoco. c)Unicidade de identificação de usuários: a informação de identificação de tal documento deverá ser validada na inclusão ou alteração de pessoas para garantir a unicidade, ou seja, o sistema não deve permitir a associação de um mesmo documento de identificação a dois usuários no sistema. d)Exclusão de usuários: Para fins de responsabilização, não deve ser possível remover o cadastro ou vínculo de usuários e profissionais de saúde do sistema, caso alguma operação tenha sido realizada pelo mesmo. Que seja possível inativar usuário, apesar de não poder excluir, e que o inativo não consiga fazer *login*/acessar. | O | VI | A | A | A | A | A | A |
| 42 | Assim que completada uma autenticação com sucesso, o sistema deve exibir à pessoa usuária as seguintes informações: Data e hora da última autenticação com sucesso de seu usuário; Data e hora das tentativas de autenticação sem sucesso depois da última autenticação com sucesso. Nota: Considera-se como “última autenticação” a autenticação anterior à que está ocorrendo. | O | VII | N | N | N | N | N | N |
| 43 | Condição: Arquitetura cliente-servidor e autenticação por *login* e senha. A interface de usuário utilizada para digitação de credenciais de acesso ao sistema (*login* ou nome do usuário, senha secreta de acesso, PIN) deve impedir a memorização e a visualização de dados anteriores (lista de logins já digitados, lembrança automática de senhas associadas a um login, etc.). Além disso, toda e qualquer digitação direta de senhas deve ser feita por meio de máscara de caracteres que impeça sua visualização por outras pessoas. | O | VII | N | N | N | N | N | N |
| 44 | Impedir acesso ou visualização dos dados por pessoas não autorizadas no sistema. | O | VII | A | A | A | A | A | A |
| 45 | Garantir que o acesso aos dados do sistema seja somente possível por meio de canais de interação pré-definidos (ex.: web, console local, interface entre aplicativos), com atuação obrigatória de mecanismos de controle de acesso. | O | VII | A | A | A | A | A | A |
| 46 | a) A sessão de comunicação entre o componente de interação com o usuário (ex.: browser ou executável cliente) e os outros componentes do sistema (ex.: servidor de aplicação, banco de dados, etc) deve oferecer os seguintes serviços de segurança: autenticação do servidor, integridade dos dados e confidencialidade dos dados. b) O serviço de segurança empregado deve implementar criptografia dos dados em trânsito. | O | VII | A | A | A | A | A | A |
| 46 | a) A sessão de comunicação entre o componente de interação com o usuário (ex.: browser ou executável cliente) e os outros componentes do sistema (ex.: aplicação) deve oferecer as seguintes funcionalidades de segurança: autenticação, integridade dos dados e confidencialidade dos dados. b) O componente de segurança empregado deve implementar criptografia na comunicação utilizando algoritmo de, no mínimo, 256 bits. | O | VII | A | A | A | A | A | A |
| 47 | A comunicação entre componentes distribuídos (como, por exemplo, entre a aplicação e o banco de dados) deve oferecer os seguintes serviços de segurança: autenticação de parceiros (ambas as partes), integridade dos dados e confidencialidade dos dados (criptografia). | O | VII | A | A | A | A | A | A |
| 48 | Dados estruturados devem ser armazenados por Sistema (s) de Gerenciamento de Banco de Dados (SGBD) e dados não estruturados e não armazenados em SGBD devem ser criptografados. | O | IV | A | A | A | A | A | A |
| 49 | Os dados inseridos pelo usuário nos campos de entrada (inputs, caixas de texto, etc.) devem ser validados antes de serem processados, de forma a prevenir ataques de buffer overflow e injeção de dados. | O | VII | A | A | A | A | A | A |
| 50 | O sistema deve permitir o gerenciamento (criação, ativação/inativação e modificação) de usuários e papéis (perfis), por meio da aplicação, de forma a possibilitar o controle de acesso às funcionalidades do sistema conforme os papéis aos quais o usuário possui. Um usuário pode possuir um ou mais papéis. | O | VII | A | A | A | A | A | A |
| 51 | Em caso de autenticação inválida em tentativa de acesso, a mensagem de erro emitida pelo sistema para o usuário não deve informar qual o motivo do erro. | O | VII | A | A | A | A | A | A |
| 52 | Para as transmissões remotas de dados identificados, os sistemas das operadoras de planos de saúde deverão possuir um certificado digital de servidor emitido por uma Autoridade Certificadora. AC certificados de servidor homologada *WebTrust for CAs*, *WebTrust for CAs - SSL Baseline with Network Security e WebTrust for* CAs - EV SSL (se emitir EV), e ETSI TS 102 042, ETSI EN 319 411-1 e ETSI EN 319 411-2. | O | VII | A | A | A | A | A | A |
| 53 | Todos os processos de validação das regras de negócio (ex.: validação de dados, conteúdo, tamanho, domínio, etc.) devem ser realizados no back- end. Opcionalmente, poderá haver tais validações no front-end, desde que seguidas das validações no back-end. | O | VII | A | A | A | A | A | A |
| 54 | A arquitetura do sistema deverá estar disposta em camadas e seus componentes distribuídos. O banco de dados deverá estar segregado das aplicações (ex.: componentes, segmentos de rede, API). | R | VII | A | A | A | A | A | A |
| 55 | O acesso de usuários ao SGBD deve ser permitido somente por intermédio do componente de autenticação e controle de acesso com usuário exclusivo para esse fim, exceto nas atividades de cópia de segurança (suporte de maneira geral). | R | VII | A | A | A | A | A | A |
| 56 | Componentes que manipulam dados identificados do sistema para fins de interoperabilidade, visualização, assinatura e outros, não devem manter tais dados fora do SGBD após o término da operação. | O | III | A | A | A | A | A | S |
| 57 | Gerar trilhas de auditoria das ações realizadas no tratamento de dados pessoais e pessoais sensíveis. | O | VI | A | A | A | A | A | A |
| 58 | Os registros de auditoria gerados devem ter garantia de integridade e serem protegidos contra acesso não autorizado. | O | VII | A | A | A | A | A | A |
| 59 | O sistema deve possuir uma interface para visualização dos registros de auditoria em ordem cronológica. | R | IV | A | A | A | A | A | A |
| 60 | Toda pessoa usuária do sistema deve ter a autenticação confirmada no momento da realização de operações críticas ou sensíveis, mesmo que já tenha se autenticado previamente para ingresso ao sistema. | R | VII | A | A | A | A | A | A |
| 61 | Condição: sistema permite a retomada da atividade após bloqueio de sessão de usuário por inatividade ou manualmente pelo usuário. O sistema deverá permitir a retomada da atividade do usuário após bloqueio de sessão. Essa operação é permitida apenas quando o desbloqueio for realizado pelo mesmo usuário bloqueado. Para que o desbloqueio de sessão seja realizado, o sistema deve requerer novo processo de autenticação do usuário bloqueado. | R | VII | A | A | A | A | A | A |
| 62 | As bases de dados, mídias ou arquivos que contém dados pessoais e/ou dados pessoais sensíveis devem ser protegidas para garantir a confidencialidade (por exemplo: criptografia, somente acessos autorizados, etc.) | O | VII | A | A | A | A | A | A |
| 63 | Utilização de *captcha* na tela de acesso ao sistema vinculada ao método de autenticação por *login* e senha. Não deve ser permitido autenticar o usuário sem a validação simultânea do *login*, senha e *token* do *captcha*. | R | VII | N | N | N | N | N | N |
| 64 | Adotar a criptografia de, no mínimo, 256 bits na comunicação entre as partes da aplicação em redes distintas. | R | VII | A | A | A | A | A | A |
| 65 | Utilização de captcha na tela de recuperação de senha de acesso do sistema para evitar ataques do tipo *Brute Force*. | R | VII | N | N | N | N | N | N |
| 66 | Não permitir alterar e remover registros do log de auditoria de sistema por um tempo mínimo de 90 dias | O | V | A | A | A | A | A | A |
| 67 | Mínimo de 08 caracteres utilizando pelo menos um (01) caractere de cada um dos quatro (4) tipos de caracteres listados abaixo:  • Letras Maiúsculas (AZ) • Letras Minúsculas (az) • Números (0-9) • Símbolos ASCII (`~! @ # $% ^ & \* () \_ + - = {} | \:"; '<>?,. / e espaço) e caracteres Unicode. | O | VII | A | A | A | A | A | N |
| 69 | Bloquear, ao menos temporariamente, o usuário após um número máximo de tentativas inválidas de login, por qualquer meio de acesso. Este número de tentativas não deve ser superior a cinco. Após o número máximo de tentativas, o usuário poderá ser bloqueado por, no mínimo, 5 (cinco) minutos ou ser submetido a outros controles para autenticação. O desbloqueio será feito apenas pelo próprio usuário ou a sessão será encerrada. | O | VII | A | A | A | A | A | N |
| 70 | Registrar log de acessos e de tentativas de acesso ao sistema de informação. O tempo de armazenamento desta informação seja de, no mínimo, 90 (noventa) dias. | O | V | A | A | A | A | A | A |
| 73 | As operadoras de planos privados de assistência à saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso não autorizado à dados pessoais e dados pessoais sensíveis. | O | VII | A | A | A | A | A | A |
| 74 | Os prestadores de serviços de saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso não autorizado à dados pessoais e dados pessoais sensíveis, em especial à toda informação identificada individualmente. | O | VII | A | A | A | A | A | A |
| 78 | A comunicação entre componentes distribuídos do sistema (como por exemplo, entre a aplicação e o banco de dados) devem oferecer controles de segurança para impedir acesso não autorizado. Para tal, deverão ser utilizados componentes de segurança que garantam a autenticação e a confidencialidade entre as partes da aplicação e a integridade dos dados. | O | VII | A | A | A | A | A | A |