Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Curso Superior de Tecnologia em Segurança da Informação

Jéssica Oliveira Muniz

Tiago Hessel

Segurança de Software para a Área de Saúde:
Uma avaliação dos requisitos de segurança aplicada em *software* de Registro Eletrônico em Saúde

Faculdade de Tecnologia de Americana – Ministro Ralph Biasi
Curso Superior de Tecnologia em Segurança da Informação

Jéssica Oliveira Muniz
Tiago Hessel

Segurança de Software para a Área de Saúde:
Uma avaliação dos requisitos de segurança aplicada em *software* de Registro Eletrônico em Saúde

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.(a) Daniele Junqueira Frosoni.
Área de concentração: Segurança da Informação

Americana, SP.
2019

Fatec Americana
Ministro Ralph Biasi

Centro Paula Souza

SÃO PAULO
GOVERNO DO ESTADO

Faculdade de Tecnologia de Americana

Jessica Oliveira Muniz
Tiago Hessel

Segurança de Software para a Área de Saúde:
Uma avaliação dos requisitos de segurança aplicada em software de Registro Eletrônico em Saúde

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.
Área de concentração: Segurança da Informação

Americana, 07 de dezembro de 2019

Banca Examinadora:

Daniele Junqueira Frosoni (Presidente)
Especialista
Faculdade de Tecnologia - Americana

Edson Roberto Gaseta (Membro)
Mestre
Faculdade de Tecnologia - Americana

Eduardo Antonio Vicentini (Membro)
Mestre
Faculdade de Tecnologia - Americana

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

M365s MUNIZ, Jessica Oliveira

Segurança de software para a área de saúde: uma avaliação dos requisitos de segurança aplicada em software de registro eletrônico em saúde. / Jessica Oliveira Muniz, Tiago Hessel. – Americana, 2019.

84f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Esp. Daniele Junqueira Frosoni

1 Segurança em sistemas de informação. I. HESSEL, Tiago II. FROSONI, Daniele Junqueira III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.519

DEDICATÓRIA

Dedicamos esse trabalho aos nossos pais e familiares, que com muito amor e zelo, nos guiaram para que alcancemos nossas metas.

AGRADECIMENTOS

Aos nossos professores e mestres, que souberam compartilhar seu conhecimento.

Aos nossos amigos, pessoas que passam em nossas vidas e deixam um pouquinho de história.

A MkDATA e seus diretores, que disponibilizaram o *software* para que fosse analisado.

Ao Scrum-Master Lucas Bovetto, que nos auxiliou na instalação do *software* e nos deu suporte para todas as dúvidas que tivemos do mesmo.

A professora e orientadora, Daniele Junqueira Frosoni, que com muita paciência e sabedoria nos guiou desde o começo da ideia, procurando novas fontes de estudos e mostrando caminhos que podíamos percorrer para que esse trabalho fosse entregue com maestria.

EPÍGRAFE

“As grandes organizações requerem um altíssimo nível de compromisso de todas as pessoas envolvidas.” – Bill Gates

RESUMO

Este trabalho traz os resultados de um estudo avaliativo de requisitos de segurança em *software* na área de saúde, realizado com o *software* MKSAUDE, fornecido pela empresa MkDATA. Para verificar a segurança desse *software* foi necessário ter conhecimento sobre a Lei Geral de Proteção de Dados (LGPD), requisitos de segurança previstos nas normas da ABNT, conhecer as recomendações da ANS e da HIPPA, que são agências reguladoras na área de saúde. No Brasil, o Conselho Federal de Medicina (CFM) em parceria com a S-BIS, fizeram as normas e certificações SG1 e SG2, que são necessárias para garantir a segurança do *software* da área de saúde. Com base nestes estudos, foi possível verificar se o *software* MKSAUDE atende os principais os requisitos necessários para que seus usuários não encontrem problemas de segurança, tais como disponibilidade, integridade e confidencialidade.

Palavras chave: Segurança em *software* de saúde, ISO, ABNT, LGPD, Hipaa, ANS, Certificações, MKSAUDE, MkDATA.

ABSTRACT

This work brings the results of an evaluative study of safety requirements in *software* in the healthcare area, carried out with the MKSAUDE *software* provided by the company MkDATA. To check the security of this *software* it was necessary to have knowledge about the General Data Protection Act (LGPD), safety requirements set out in the ABNT standards, know the recommendations of ANS and HIPAA, which are regulatory agencies in the health area. In Brazil, the Federal Council of Medicine (CFM) in partnership with S-BIS, made the standards and certifications SG1 and SG2, which are necessary to ensure the safety of the health area's *software* Based on these studies, it was possible to verify that the MKSAUDE *software* meets all the necessary requirements so that its users do not find safety issues, such as availability, integrity and confidentiality.

Keys word: Safety in health *software* ISO, ABNT, LGPDP, Hipaa, ANS, Certifications,MKsaúde, MkDATA.

LISTA DE ABREVIATURAS SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
NBR	Norma Brasileira
ISO	Organização Internacional de Padronização
IEC	Comissão Eletrotécnica Internacional
SGSI	Sistema de Gestão da Segurança da Informação
SI	Segurança da Informação
CPF	Cadastro de Pessoa Física
RG	Registro Geral
LGPD	Lei Geral de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
U.E.	União Europeia
CNI	Confederação Nacional da Industria
SBIS	Sociedade Brasileira de Informática em Saúde
PEP	Prontuário Eletrônico do Paciente
S-RES	Sistemas de Registro Eletrônico de Saúde
CFM	Conselho Federal de Medicina
CNPJ	Cadastro Nacional de Pessoa Jurídica
CRM	Conselho Regional de Medicina
ICP	Chaves Públicas Brasileiras
NGS	Nível de Garantia de Segurança
OWASP	Open Web Application Security Project
ZAP	Zed Attack Proxy

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A evolução está ocorrendo há décadas e os processos são alterados e adaptados para agregar produtos, empresas, novas tecnologias, regulamentações e/ou novas situações do dia-a-dia. Por exemplo, o que antes era controlado via cadernos de contas, hoje são utilizados planilhas ou sistemas de controle eletrônico. Como outro exemplo pode-se citar as empresas que possuíam linhas de produção com funcionários que realizavam procedimentos repetidos, hoje estes funcionários foram substituídos por robôs e os humanos passam a gerenciar e analisar a possibilidade de melhoria dos processos.

Dessa forma, é de se afirmar que a mudança pode ocorrer a todo momento, e as metodologias e os processos devem ser adaptados para melhor aproveitamento e obtenção de resultados para as organizações

Uma das áreas que vem sendo fortemente impactada por mudanças de processos e sistemas é a saúde, que presta serviço a milhões de brasileiros nos hospitais públicos, privados, clínicas, laboratórios, dentre outros, nos quais dados ainda são registrados muitas vezes no papel e armazenados em armários ou/e caixas, não havendo rastreabilidade e controle, podendo cair no esquecimento, perda do documento, por ser mal armazenado ou por impacto de alguma catástrofe natural.

Para atender a área da saúde, os *softwares* devem atender uma série de requisitos que serão apresentados no decorrer desse trabalho. Por exemplo, será explicado quais partes da norma NBR ISO 27002, melhor se adequam ao *software* aplicado para área de saúde, desde a sua implementação até sua manutenção após a implantação para o cliente.

O objetivo principal deste trabalho foi estudar os requisitos de segurança do *software* voltados a prontuário eletrônico da área de saúde. O prontuário eletrônico, é utilizado para armazenar dados do paciente de forma segura, garantindo que somente ele e os profissionais de saúde poderão utilizar desses dados. A segurança e disponibilidade desse documento é valiosa, pois o paciente poderá recorrer ao prontuário sempre que necessário para futura consulta.

Com o avanço da Internet e das tecnologias, o mundo lida com um crescente aumento dos números de *softwares* que buscam cada vez mais a rapidez da troca de dados e seu armazenamento. Enfrentando vários problemas com a falta de sigilo com os dados das pessoas físicas, a União Europeia aprovou a Lei de Proteção de Dados, e outros países tais como Brasil e Estados Unidos, estão seguindo está mesma linha.

Também será apresentado no decorrer deste trabalho os principais tópicos que tangem as normas da segurança de dados na área da saúde. As principais normas NGS1 e NGS2, que são certificações requeridas às empresas desenvolvedoras de *softwares* para a área da saúde.

Neste trabalho, consta um estudo de caso, realizado com a empresa MkDATA que é desenvolvedora de *softwares* de saúde, e provê soluções de *software* para hospitais e consultórios médicos. Especificamente este estudo de caso foi voltado ao levantamento de requisitos de segurança para o desenvolvimento de prontuário eletrônico, as normas de segurança que este *software* precisa atender, demostrando que um prontuário eletrônico seguro é aquele que garante a integridade, rastreabilidade e segurança das informações, de forma que se permita a continuidade no tratamento do paciente e agilidade no diagnóstico, assim proporcionando um melhor cuidado ao paciente.

2 NORMAS DE SEGURANÇA EM DESENVOLVIMENTO DE SOFTWARE

Para desenvolver um *software s*eguro, é necessário seguir algumas diretrizes, tais como a ABNT – ISO e outras leis internacionais e nacionais do país o qual o código será comercializado. São estas diretrizes e leis, que definem requisitos universais que dão diretrizes ao desenvolvimento do *software* para que o mesmo seja seguro para as empresas e seus clientes, permitindo que países membros que adotam estas mesmas diretrizes possam, fazer negócios um com os outros.

A segurança tornou-se um dos temas de maior relevância na vida das pessoas, seja para assegurar que a casa seja protegida, que a empresa não seja invadida (física e virtualmente). Também é necessário aplicar a segurança nas indústrias, empresas, no trânsito, hospitais, tudo para prevenir acidentes e incidentes. Por isso a segurança deve ser envolvida em qualquer processo, seja para desenvolver produtos, alimentos, artigos de uso pessoais e nos *softwares* que tornaram -se indispensáveis no uso do dia a dia.

Logo, faz-se necessário buscar ferramentas que possam auxiliar a gestão de segurança em qualquer âmbito, e para isso existem algumas normas internacionais que abordam a gestão da segurança, a qualidade dos produtos e serviço. Tais normas são conhecidas como ABNT NBR ISO/IEC e serão apresentadas na seção 2.1 deste capítulo as normas voltadas para área de tecnologia e segurança da informação.

Na seção 2.2, abordará sobre a Lei de Proteção de Dados Pessoais internacional e seus impactos no Brasil e principalmente sob as empresas desenvolvedoras de *software*.

2.1 ABNT - ISO

A segurança da informação deve ser aplicada para resguardar a empresa de possíveis perdas e tratar a informação como item valioso na instituição.

A norma ISSO 27001 afirma que:

> [...] a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado.

Dessa forma é fundamental analisar quais os riscos existentes, desenvolver processos, criar ações para evitar ou reduzir possíveis efeitos. Por isso foram desenvolvidas algumas normas de segurança da informação que recomendam boas práticas para o desenvolvimento de *softwares* seguro.

A norma ABNT ISO 27001 (2013) trata sobre técnica de implantação de um SGSI (Sistema de Gestão da Segurança da Informação) dentro de uma organização para estruturar processos organizacionais, objetivos e é uma decisão estratégica, pois garante que as informações sejam guardadas, conforme a norma relata:

> O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas [...]. (ABNT,2013)

Para implantação da ISO é importante elencar os requisitos de segurança e definir quais os resultados devem ser alcançados, para isso toda organização precisa estar envolvida para garantir o sucesso da implementação de uma gestão de segurança da informação. Esses levantamentos de requisitos estão descritos na norma ABNT ISO 27002 (2007) que recomenda que a organização busque fontes principais de requisitos de segurança da informação como:

- Análise/avaliação de riscos, consideração de objetivos e estratégias, identificação dos ativos e as vulnerabilidades, considerar o impacto nos negócios.
- Buscar legislação vigente, estatutos, regulamentações e cláusulas contratuais que devem ser atendidas.
- Identificar objetivos e requisitos do negócio.

Depois da analise realizada, deve ser providenciado medidas de gerenciamento do riscos, aplicar os controles necessários para reduzir os riscos a niveis aceitaveis.

A partir da norma 27000, a qual trata sobre SI (Segurança da Informação), abordam-se práticas para serem seguidas e se resguardar de eventos inoportunos de modo mais generico.

A norma ABNT ISO 27001 (2013) alguns pontos específicos para desenvolvimento do *software* testes e suporte e recomenda quais os itens que devem ser controlados e seus objetivos. Ao todo são dezoito recomendações relacionadas a segurança em *software* conforme apresentado na tabela 1:

Tabela 1 - REFERÊNCIA AOS CONTROLES E OBJETIVOS DE CONTROLES

A.9.4 – CONTROLE DE ACESSO AO SISTEMA E À APLICAÇÃO		
OBJETIVO: Prevenir o acesso não autorizado aos sistemas e aplicações		
A.9.4.5	Controle de acesso ao código fonte de programas	Controle: O acesso ao código fonte de programa deve ser restrito.
A.12 Segurança nas operações | A.12.1 RESPONSABILIDADES E PROCEDIMENTOS OPERACIONAIS.		
OBJETIVO: Garantir a operação segura e correta dos recursos de processamento da informação		
A.12.2.1	Separação dos ambientes de desenvolvimento, teste e de produção	Controle: Ambientes de desenvolvimento, teste e produção devem ser separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.
A.12.4 REGISTROS E MONITORAMENTO		
OBJETIVO: Registrar eventos e gerar evidências		
A.12.4.4	Sincronização dos relógios	Controle: Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados com uma fonte de tempo precisa.
A.12.5 CONTROLE DE SOFTWARE OPERACIONAL		
OBJETIVO: Assegurar a integridade dos sistemas operacionais		
A.12.5.1	Instalação de *software* nos sistemas operacionais	Controle: Procedimentos para controlar a instalação de *software* em sistemas operacionais devem ser implementados.

A.12.7 CONSIDERAÇÕES QUANTO À AUDITORIA DE SISTEMAS DE INFORMAÇÃO
OBJETIVO: MINIMIZAR O IMPACTO DAS ATIVIDADES DE AUDITORIA NOS SISTEMAS OPERACIONAIS

A.12.7.1	Controles de auditoria de sistemas informação	Controle: às atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar interrupção nos processos do negócio.
A.14 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS		
A.14.1 REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO		
OBJETIVO: Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.		
A.14.1.1	Análise e especificação dos requisitos de segurança da informação	Controle: Os Requisitos relacionados com segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.
A.14.2 SEGURANÇA EM PROCESSOS DE DESENVOLVIMENTO E DE SUPORTE		
OBJETIVO: Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação		
A.14.2.1	Politica de desenvolvimento seguro	Controle: Regras para desenvolvimento de sistemas e *software* devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização
A.14.2.2	Procedimentos para controle de mudanças de sistemas	Controle: Mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas utilizando procedimentos formais de controle de mudanças
A.14.2.3	Análise crítica técnica das aplicações após mudanças nas plataformas operacionais	Controle: Aplicações críticas de negócios devem ser analisados criticamente e testadas quando plataformas operacionais são mudadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.
A.14.2.4	Restrições sobre mudanças em pacotes de software	Controle: Modificações em pacotes de *software* devem ser desencorajadas e devem estar limitadas às mudanças necessárias, e toda as mudanças devem ser controladas
A.14.2.5	Princípios para projetar sistemas seguros	Controle: Princípios para projetar sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados para quaisquer implementações de sistemas de informação
A.14.2.6	Ambiente seguro para desenvolvimento	Controle: As organizações devem estabelecer e proteger adequadamente os ambientes seguros de desenvolvimento, para os esforços de integração e

		desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistemas
A.14.2.7	Desenvolvimento terceirizado	Controle: A organização deve supervisionar e monitorar as atividades de desenvolvimento de sistemas terceirizado
A.14.2 SEGURANÇA EM PROCESSO DE DESENVOLVIMENTO E DE SUPORTE		
OBJETIVO: Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação		
A.14.2.8	Testes de segurança do sistema	Controle: Testes de funcionalidades de segurança devem ser realizados durante o desenvolvimento de sistemas
A.14.2.9	Teste de aceitação de sistemas	Controle: Programas de testes de aceitação e critérios relacionados devem ser estabelecidos para novos sistemas de informação, atualizações e novas versões
A.14.3 DADOS PARA TESTE		
OBJETIVO: Assegurar a proteção dos dados usados para teste.		
A.14.3.1	Proteção dos dados para testes	Controle: Os dados de teste devem ser relacionados com cuidado, protegidos e controlados.
A.10 CRIPTOGRAFIA		
A.10.1 CONTROLES CRIPTOGRÁFICOS		
OBJETIVO: Assegurar o uso efetivo e adequação da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação		
A.10.1.1	Política para o uso de controles criptográficos	Controle: Deve ser desenvolvida e implementada uma politica para o uso de controles criptográficos para proteção da informação
A.10.1.2	Gerenciamento de chaves	Controle: Uma politica sobre o uso, proteção e tempo de vida das chaves criptográficas deve ser desenvolvida e implementada ao longo de todo seu ciclo de vida.

Fonte: Baseada em Norma ABNT (2013)

A tabela 1 é derivada da ABNT NBR ISO/IEC 27002 (ABNT, 2013) que são normas complementares. A norma 27002 serve como um documento de orientações para as instituições implantarem os controles de segurança da informação, incluído políticas, processos organizacionais, procedimentos, funções de *software* e *hardware.*

Dessa forma a ABNT 27002 (2013) explana todos os requisitos necessários e define diretrizes para a implantação e quais os passos que devem ser seguidos, abordando desde contratação de funcionários, controles de acesso, níveis de segurança de sigilo, desenvolvimento de aplicações, segurança de códigos fonte. Um dos itens elencados é a instalação de *software* que a norma descreve qual a melhor maneira para instalação de *softwares* operacionais, recomendando que todo *software* deve ser atualizado e mantido/executado por pessoas treinadas e que recebam autorização gerencial apropriada.

Também orienta que o desenvolvedor deve evitar utilizar compiladores e/ou deixar códigos em desenvolvimento junto ao código executável. Desta forma evita algum tipo de erro ou incompatibilidade ao executar o *script*, pois o cliente pode "sem querer" acessar o *software* em desenvolvimento e ter algum problema com ele por não estar acabado.

É importante o desenvolvedor realizar testes antes de *upload* do *software* conforme é descrito no item:

> [...] convém que sistemas operacionais e aplicativos somente sejam implementados após testes extensivos e bem sucedidos; é recomendável que os testes incluam testes sobre uso, segurança, efeitos sobre outros sistemas como também sobre uso amigável, e sejam realizados em sistemas separados; Convém que seja assegurado que todas as bibliotecas de código fonte dos programas correspondentes tenham sido atualizadas;[...] (ABNT, 2013)

Os testes devem ser realizados sempre atendendo aos requisitos mínimos de configuração do cliente, pois somente dessa forma o desenvolvedor vai saber se o *software* está totalmente seguro e pronto para executar no ambiente que ele foi projetado.

Apesar do desenvolvedor fazer vários testes, é importante ele ter uma estratégia de "retorno às condições anteriores", prevenindo dessa forma algum evento indesejado, podendo desta forma voltar para as configurações anteriores da aplicação.

Caso o cliente necessite utilizar *software* anteriores, por algum motivo de incompatibilidade ou erro na atualização "convém que versões anteriores dos *softwares* sejam mantidas como medida de contingência;" e o desenvolvedor

deve manter um *backup* dos *softwares* e todas as informações pertinentes ao mesmo.

Uma organização, ao manter um *software* ao longo do tempo sem atualizações, deve "[...] considerar os riscos associados à dependência de *software s*em suporte", pois com o tempo a empresa fornecedora deixa de fornecer suporte para o mesmo e a organização passa a correr os riscos que isso possa apresentar.

O cliente deve ficar ciente que não pode efetuar atualizações ou instalação de novos *softwares* sem antes consultar o seu fornecedor, pois:

> *Softwares* para computadores podem depender de outros *softwares* e módulos fornecidos externamente, os quais convém que sejam monitorados e controlados para evitar mudanças não autorizadas, que podem introduzir fragilidades na segurança (ABNT, 2013).

Desta forma, a organização fornecedora do *software* pode garantir a segurança e a integridade dele, visto que, ao implantar ou atualizar um *software* desconhecido sem autorização, o *software* pode deixar de funcionar corretamente.

Deve ser realizada algumas diretrizes para implementação:

> Convém que a organização identifique quais os tipos de *software s*ão permitidos instalar (por exemplo, atualização e segurança de patches ao *software* existente), e quais tipos de instalações são proibidas (por exemplo, *software* que é usado somente para fins pessoais e *software* cuja possibilidade de ser potencialmente malicioso, é desconhecida ou suspeita) (ABNT, 2013).

A organização resguarda-se de eventuais problemas. Dando o mínimo privilégio para instalações de *softwares*. Garantindo desta forma a segurança de seu cliente e do *software* implantando.

As normas sempre irão detalhar os processos que devem ser aplicados para o desenvolvimento e implantação, essas medidas servem de parâmetro para atestar a qualidade do *software* pois o sistema foi desenvolvido para evitar possíveis incidentes e diminuir os riscos que podem ser gerados. Na ABNT 27002 (2013) existe uma consideração sobre segurança da informação:

> Sistemas de informação têm ciclos de vida nos quais eles são concebidos, especificados, projetados, desenvolvidos, testados, implementados, usados, mantidos e, eventualmente, retirados do serviço e descartados. Convém que a segurança da informação seja considerada em cada estágio. Desenvolvimentos de sistemas novos e mudanças nos sistemas existentes são oportunidades para as organizações atualizarem e melhorarem os controles de segurança, levando em conta os incidentes reais e os riscos de segurança da informação, projetados e atuais (ABNT, 2013).

As normas podem ser aplicadas para qualquer sistema independente dá área, pois são diretrizes para práticas de gestão de segurança da informação e também é necessário atender as legislações e regulamentações dos países no qual o *software s*erá disponibilizado.

2.2 LEI DE PROTEÇÃO DE DADOS PESSOAIS

A Internet mudou o mundo e isso alterou a forma como as pessoas pensam e agem, pois, o mundo tornou-se interconectado e toda informação que antes era limitada ou restrita a somente algumas pessoas, organizações, hoje estão disponíveis nas plataformas *web*, nas redes sociais e nos aplicativos. E para ter acesso a essas plataformas, redes sociais, é necessário realizar cadastros e fornecer alguns dados pessoais como CPF, RG, endereço, número de cartão de crédito. E as empresas solicitam esses dados pois precisam identificar o usuário caso ele perca a senha ou login, e ter um cadastro atualizado será mais fácil de resgatar a conta.

Acontece que as empresas não contam o que elas fazem com esses dados e o usuário também não questiona a real necessidade de fazer um cadastro e informar seus dados pessoais, e atualmente está ocorrendo das empresas venderem esses dados para outras empresas utilizarem de alguma forma para gerar lucro, utilizar na propagação de propagandas, manipulação em massas, e direcionar notícias.

Em 2018 ocorreu um escândalo que trouxe a público a forma que uma empresa armazenava os dados e como ela trabalhava com a informação, como podemos ver abaixo a empresa direcionava mensagens políticas:

> [...] mas o episódio envolvendo a *Cambridge Analytica* acaba de revelar o perigo real do tráfico desses dados em redes sociais. E a opacidade dessas plataformas que prometiam criar um planeta mais transparente.
> De posse de dados como curtidas e redes de amigos, essa firma com sede em Londres conseguiu montar perfis de eleitores em potencial, que então eram bombardeados com mensagens política [...] (FOLHA DE SÃO PAULO, 2018).

Com uma forma de proteger os dados pessoais da população a União Europeia iniciou um trabalho em 2016 para criar a Lei Geral de Proteção de Dados.

2.2.1 Regulamento Geral sobre a Proteção de Dados (GDPR)

O Regulamento Geral sobre de Proteção de Dados (GDPR), foi implantada na União Europeia, para atender a nova demanda tecnológica que alcança a todos os cidadãos, e que seus dados sejam preservados em todos os níveis e instancias:

> Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais (GDPR, 2016).

Este regulamento tem como objetivo a preservação da liberdade, segurança e justiça de cada cidadão, respeitando sempre os poderes jurídicos de cada nação.

Com a aplicação dessa lei vários países, empresas e instituições serão afetadas, pois terão que adequar-se para garantir que os dados de seus usuários e funcionários não sejam violados de alguma forma, e isso deve impactar em todos os segmentos do mercado de trabalho desde da área jurídica, financeira, recursos humanos e até os dados mais sensíveis que são da saúde.

A tecnologia e a globalização inovou os modelos de negócios, alterou a forma como as empresas e instituições adquiriam os dados pessoais dos seus consumidores, mudou-se a forma de chegar até o cliente, pois o usuário pode

fazer uma pesquisa de um produto na *web* e a empresa pagar por essa informação e conseguirá direcionar propagandas, anúncios dos produtos ou similares. E isso torna-se um agravante na matéria de proteção de dados. No parágrafo 6 do regulamento informa que:

> [...] as pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais. (GDPR, 2016).

Essas informações pessoais que estão disponíveis na *web* fazem com que o usuário perca a privacidade, uma vez que seus dados estão registrados, qualquer usuário que tenha conhecimento poderá realizar consultas e adquirir o *e-mail*, endereço, número de telefone e existem alguns sites ilegais que divulgam essas informações sem nenhuma autorização, como por exemplo o site TUDO SOBRE TODOS:

> O site Tudo Sobre Todos, que vende dados pessoais - como CPF, local de residência e nomes de familiares - chamou atenção do Ministério da Justiça, do Ministério Público Federal e da Polícia Federal, que deram início a investigações preliminares para apurar a sua legalidade. Em entrevista à reportagem, o responsável pelo site, que não quis se identificar, reforça que sua empresa divulga apenas informações públicas. (AGENCIA ESTADO, 2015).

As informações estão disponíveis a nível global, e o que gera uma preocupação maior é que a empresas informam que os dados pessoais informados no momento do cadastro são restritos, então o que está ocorrendo é a venda de dados e o vazamento das informações quando ocorrem ataques nos bancos de dados.

2.2.2 O Brasil será afetado pela GDPR?

No Brasil, a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

Esta lei foi assinada no dia 28 de dezembro de 2018, sendo que apenas a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, entrou em vigor na data. As demais empresas ou organizações terão até vinte quatro meses após a data de sua publicação para se adequarem a esta lei. As empresas no Brasil já estão se adequando as leis, tanto lei brasileira quanto a lei da União Europeia (U.E.), pois essa é uma exigência da U.E. para que outros Estados que não são membros, se adequem as leis de proteção de dados.

> [...] o tratamento dos dados pessoais de titulares que se encontrem na União por um responsável pelo tratamento ou subcontratante não estabelecido na União deverá ser abrangido pelo presente regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem associadas a um pagamento.

No artigo fica claro que qualquer Estado que queira manter relações bilaterais com a U.E., seja de ordem econômica, segurança ou até mesmo saúde, deve respeitar a lei de proteção de dados.

Portanto, as empresas brasileiras ou/e empresas multinacionais que tem filiais no Brasil, vão precisar segundo as palavras do gerente executivo da Confederação Nacional da Industria (CNI), João Emilio Gonçalves, ter uma equipe “encarregada de proteção de dados”, que faça todo o suporte dentro e fora da empresa, realizando também o suporte e treinamento para todos os funcionários. Além disso, os países que se adequam as leis de proteção de dados, se restringem ao seleto grupo de 100 países que conta com a norma adequada e para o Brasil é importante, pois ajuda a conquistar uma cadeira na Organização para Cooperação e Desenvolvimento Econômico, desta forma, os países que se adequarem a essa lei garantem relações comerciais para suas empresas.

2.2.3 O impacto da LPGD nas empresas de software

Qualquer ramo de negócio que tenha um banco de dados, será afetado como um todo, desde uma rede social, assinatura de pacotes de Internet, qualquer negócio que envolva dados de clientes. Todos os tipos de serviços, públicos ou privados, que recolhem informações de terceiros.

A Lei Geral de Proteção de Dados (LGPD) oferece transparência aos usuários, mostrando ao usuário o que será feito com as informações colhidas e até mesmo que o usuário possa pedir o fim do compartilhamento dela. E empresas que seguem a LGPD tendem a fazer negócios com empresas que possuem leis similares.

As empresas que desenvolvem *softwares* deverão utilizar um recurso para o usuário dar consentimento para autorizar a utilização de seus dados, a empresa deve apresentar um termo de uso e mostrar qual o destino da informação coletada, qual a finalidade e modo de processamento, e caso ocorra alguma mudança no processo a empresa deverá disponibilizar o consentimento novamente para o usuário, para que ele possa autorizar e/ou solicitar a entrega dos dados ou sua eliminação.

3 SEGURANÇA DO SOFTWARE NA ÁREA DA SAÚDE

Na área da saúde, que é uma área bem sensível caso ocorra perca ou vazamento de dados. Por isto, foram criadas agências reguladoras, tais como a HIPAA e ANS, que tem como responsabilidade definir as diretrizes sobre qualquer produto ou serviço que seja fornecido para área de saúde. Logo, empresas fornecedoras de produtos ou serviços para a área de saúde devem seguir os regulamentos definidos por estes órgãos.

Essas organizações regulamentam em seus países destinos os processos que envolvem os profissionais, os pacientes, o prontuário e a guarda dos documentos, etc.

Além das agências já citadas, existe no Brasil a Sociedade Brasileira de Informática em Saúde (SBIS), que busca aplicar metodologias e desenvolver processos que auxiliam a integração da tecnologia nas áreas de saúde.

Para atender a demanda tecnológica a SBIS desenvolveu requisitos de segurança de *software* para prontuário eletrônico, NGS1 e NGS2, que fornecem uma cartilha de diretrizes a serem cumpridas na construção do *software* na área da saúde. Estas diretrizes estão apresentadas na seção 3.4 deste trabalho.

3.1 LEI DE PORTABILIDADE E RESPONSABILIDADE DE SEGUROS DE SAÚDE | HIPAA

Para regulamentar os serviços de saúde foi criado uma lei para garantir que as operadoras, seguradoras e profissionais que oferecem serviços de saúde garanta uma privacidade nas informações de saúde dos usuários, esta lei estabelece um equilíbrio para proteger os usuários do uso indevido das informações desde os dados demográficos ou relacionado a saúde física, mental, entre outros.

A norma define regras detalhadas em relação a privacidade, acesso e revelação das informações, por exemplo:

> As pessoas devem ser normalmente capazes de ver e obter cópias de seus registros médicos e solicitar correções, se encontrarem erros. Qualquer pessoa legalmente autorizada a tomar decisões de saúde para uma pessoa incapacitada tem o mesmo direito de acesso às informações médicas pessoais dela.
> Os profissionais da área da saúde devem rotineiramente divulgar suas práticas em relação à privacidade das informações médicas pessoais.
> Os profissionais da área da saúde podem compartilhar as informações médicas das pessoas, mas apenas entre eles e apenas o necessário para fornecer o tratamento médico.
> As informações médicas não podem ser divulgadas para fins de mercado.
> Os profissionais da área da saúde devem tomar as medidas razoáveis para garantir que suas comunicações com a pessoa sejam confidenciais. (SABATINO, [s.d.]).

Esta é uma lei federal criada em 1996 que aplica requisitos de segurança do prontuário para o paciente e seu responsável, e caso o usuário perceba que algumas violações ele pode protocolar uma queixa no escritório de direitos civis.

E o profissional de saúde só pode revelar uma informação em alguns casos, como o paciente tenha uma doença infecciosa como: HIV, sífilis, tuberculose, pois essas devem ser relatadas aos agente de saúde pública, ou o paciente tem sinais de maus tratos ou negligência, ou também para os casos de demência ou convulsões e está devem ser relatadas para o departamento de veículos automotores.

3.2 AGÊNCIA REGULADORA DE SAÚDE | ANS

No Brasil existe uma agência reguladora de saúde, a Agência Nacional de Saúde Suplementar (ANS) que regulamenta a venda de planos de saúde em operadoras, seguradoras, serviços de saúde do setor público e outros profissionais da área, este órgão está vinculado ao Ministério da Saúde.

Este órgão também exige que o paciente tenha suas informações confidenciais, conforme a Resolução:

> Subseção IV
> Segurança e Privacidade
> Art. 14. O componente de segurança e privacidade estabelece os requisitos de proteção dos dados de atenção à saúde.
> § 1º O componente de segurança e privacidade visa assegurar o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde.
> § 2º O componente de segurança e privacidade baseia-se no sigilo profissional e segue a legislação vigente no País. (ANS, 2012)

Além da ANS, o Conselho Federal de Medicina também exige que o prontuário seja sigiloso, pois a informação é do paciente e não do médico e só pode ocorrer a quebra de sigilo caso seja do interesse do público, explica Celso Murad, vice corregedor do Conselho Federal de Medicina (CFM).

> A Justiça pode determinar a quebra quando houver uma situação que coloca em risco terceiros ou a sociedade. Alguns exemplos são os casos de doenças de notificação compulsória, como sarampo, HIV, etc*", explica. Ainda nesse sentido, é obrigatória a denúncia, por exemplo, de identificação de maus-tratos a crianças ou adolescentes. (Equipe Conexão, 2017)*

Assim o prontuário tem como regra principal sempre ser sigiloso, pois a informação pode carretar danos aos interessados.

Além do sigilo é necessário garantir a guarda do prontuário e isso gera muitos papeis e muitos processos, sendo o prazo mínimo para eliminação é de 20 anos para prontuários em papel, conforme a Resolução CFM Nº 1.821/07:

> Art. 8° Estabelecer o prazo mínimo de 20 (vinte) anos, a partir do último registro, para a preservação dos prontuários dos pacientes em suporte de papel, que não foram arquivados eletronicamente em meio óptico, microfilmado ou digitalizado. (1821/07, 2007).

Com a evolução da tecnologia o prontuário evoluiu para Prontuário Eletrônico do Paciente (PEP) para que o profissional de saúde possa registrar a evolução do paciente, receitas e solicitar exames, prescrições e assegurar que a guarda do prontuário seja totalmente seguro e dessa forma certificar que a informação seja exclusiva do paciente, conforme a resolução do Conselho Federal de Medicina (CFM):

> Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.
> Considerando que os dados ali contidos pertencem ao paciente e só podem ser divulgados com sua autorização ou a de seu responsável, ou por dever legal ou justa causa;
> Considerando que o prontuário e seus respectivos dados pertencem ao paciente e devem estar permanentemente disponíveis, de modo que quando solicitado por ele ou seu representante legal permita o fornecimento de cópias autênticas das informações pertinentes;
> RESOLUÇÃO CFM) Nº 1.821/2007 (CFM, 2007)

Com a mudança do prontuário físico para o eletrônico o Conselho Federal de Medicina exige que:

> Art. 7ºEstabelecer a guarda permanente, considerando a evolução tecnológica, para os prontuários dos pacientes arquivados eletronicamente em meio óptico, microfilmado ou digitalizado. RESOLUÇÃO CFM Nº 1.821/2007 (CFM, 2007)

E esteja sempre disponível para facilitar e agilizar os atendimentos nas instituições como hospitais, prontos atendimentos, clínicas médicas e caso surja uma solicitação do paciente a instituição tem o dever de ceder os documentos para que sejam utilizados em processos.

3.3 CERTIFICAÇÃO SBIS

Com a importância da informatização na área de saúde surgiu um comitê que faz parte o Conselho Federal de Medicina (CFM) e a Sociedade Brasileira de Informática em Saúde (SBIS) que estabeleceram um convênio em 2002 de cooperação técnica-e-cientifica para desenvolver normas, padrões, regulamentações para o PEP.

A área de saúde tem algumas peculiaridades para tratar informações do paciente, pois o paciente sempre terá que confidenciar seus dados para um profissional para que ele possa tratá-lo, o profissional deve ser extremamente ético e nunca compartilhar o prontuário sem a autorização do paciente ou do responsável, conforme a determinação do CFM quanto ao sigilo profissional:

> É vedado ao médico:
>
> Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente. Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha. Nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento; c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal. (CFM, [s.d.])

Com isso o prontuário tem que ser tratado com o maior cuidado para garantir a segurança e integridade das informações tanto para o prontuário em papel ou eletrônico.

Após a criação do comitê começou a surgir resoluções para atender os processos da saúde, desde o processo de guarda e manuseio do prontuário médico, normas de digitalização e em 2004 eles desenvolveram o primeiro Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) e depois desenvolveram o Manual de Requisitos de Segurança.

O Manual de requisitos de Segurança determina quais os requisitos obrigatórios para o documento eletrônico, reforça a obrigatoriedade da certificação digital (assinatura digital) para validade ética e jurídica.

Além de garantir a segurança da informação o prontuário eletrônico também garante legibilidade e continuidade no tratamento do paciente.

3.4 REQUISITOS DE SEGURANÇA DE SOFTWARE NA SAÚDE

Com intuito de apresentar as normas de maior importância da certificação SBIS-CFM, que é a segurança da informação que contêm os requisitos de segurança, os sistemas devem atender obrigatoriamente.

> •NGS1: define uma série de requisitos obrigatórios de segurança, tais como controle de versão do *software* controle de acesso e autenticação, disponibilidade, comunicação remota, auditoria e documentação.
> • NGS2: exige a utilização de certificados digitais ICP-Brasil para os processos de assinatura e autenticação. (CFM/SBIS, 2012).

Abordagem dos requisitos de segurança que asseguram que o prontuário atenda o tripé da segurança da informação que são:

- Integridade da informação, informação não sofra alteração indevida.
- Confidencialidade, esteja disponível somente às pessoas autorizadas.
- Disponibilidade, estar acessível e utilizável quando necessário.

Para garantir que a ética do prontuário permaneça entre paciente e médico, que seja compartilhada somente com a autorização do paciente ou do responsável pelo mesmo, que só permita o acesso ao prontuário somente os profissionais autorizados e que qualquer resquício de violação e acesso indevido possa ter uma rastreabilidade, também disponibilizar o prontuário eletrônico com assinatura digital do profissional, assegurar que o prontuário eletrônico esteja disponível permanente para que o paciente possa solicitar em qual momento e para que o mesmo possa utilizar do prontuário em casos de processos judiciais a informação seja integra.

A certificação segue muitas normas ISO que são referências internacionais e elas são voltadas para guarda de informação, sigilo e privacidade de documentos, a certificação tem referências da ISO 27002 que é voltada para boas práticas para gestão da segurança da informação e tem um foco na área de saúde.

Com as referências e estudos foram criados os requisitos de segurança NGS1 que ao todo tem 89 itens e a NGS2 que tem 43 itens. Eles estão divididos entre Mandatório e Recomendado.

Esses principais itens da NGS1 e da NGS2 serão abordados nas próximas seções. Serão apresentados os requisitos relacionados a segurança em um *software* voltado para a área de saúde, dentro os quais alguns somente um técnico da área de tecnologia terá acesso e existem outros que o próprio profissional de saúde, que não possui tantos conhecimentos em tecnologia, poderá acessar para verificar se ocorreu alguma violação.

3.4.1 Nível de Garantia de Segurança | NGS1

O primeiro nível de segurança pode ser aplicado no prontuário eletrônico, mas este não elimina o papel impresso, pois não possui a exigência

da assinatura digital. Este requisito está dividido em treze grupos e possui oitenta e nove requisitos que serão explicados neste capítulo.

Um dos primeiros requisitos é saber a versão dos *softwares* implantados no sistema e se eles se encontram atualizados. É importante o domínio local saber o código fonte do *software*.

Nas tabelas abaixo, será identificado com R os requisitos Recomendados e M os requisitos Mandatórios.

Tabela 2 NGS1.01 **Controle de versão do software**

ID	TÍTULO	OBRIGATÓRIO
NGS1.01.01	Versão do software	M
NGS1.01.02	Código fonte	R
NGS1.01.04	Repositório de versões	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

A tabela abaixo trata da identificação do usuário e senhas, qual é a política da identificação dos usuários e de senhas, evitando que um usuário possa ter mais de um login e que sua senha seja fraca.

Tabela 3 NGS1.02 **Identificação e autenticação de pessoas**

ID	TÍTULO	OBRIGATÓRIO
NGS1.02.01	Identificação e autenticação de usuário	M
NGS1.02.02	Método de autenticação de pessoa	M
NGS1.02.03	Proteção dos parâmetros de autenticação de usuário	M
NGS1.02.04	Segurança de senhas	M
NGS1.02.05	Controle de tentativas de login	M
NGS1.02.06	Identidade única da pessoa e responsabilização	M
NGS1.02.07	Autenticação para operações críticas	R
NGS1.02.08	Informações na autenticação	M
NGS1.02.09	Informações em autenticação inválida	R
NGS1.02.10	Revelação de credenciais na interface de autenticação	R
NGS1.02.11	Autenticação forte	R
NGS1.02.12	Uso de SALT	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Na norma NGS1.03 exige o controle de sessões do usuário, pede-se que tenha uma política contra roubo de login, encerramento por inatividade ou bloqueio em caso de férias ou por motivos particulares antes tratados na política da empresa e a retomada da atividade do usuário após esse período Controle de sessão de usuário

Tabela 4 NGS1.03 **Controle de sessão de usuário**

ID	TÍTULO	OBRIGATÓRIO
NGS1.03.01	Bloqueio ou encerramento por inatividade	R
NGS1.03.02	Segurança contra roubo de sessão de usuário	M
NGS1.03.03	Retomada de atividade do usuário	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Na tabela 5 é tratado sobre controle de acesso e de autorização, precisando desta forma, a empresa ter política de restrito para pessoas não autorizadas. E que o controle de acesso aos dados seja limitado para o sujeito da atenção.

Tabela 5 NGS1.04 **Autorização e controle de acesso de pessoas**

ID	TÍTULO	OBRIGATÓRIO
NGS1.04.01	Impedir acesso por pessoas não autorizadas	M
NGS1.04.02	Mecanismo de controle de acesso ao RES	M
NGS1.04.03	Gerenciamento de usuários e papéis	M
NGS1.04.04	Papéis relacionados à T.I	R
NGS1.04.05	Configuração de controle de acesso	M
NGS1.04.06	Usuário mínimo ativo e restrição de autoconcessão de direitos	M
NGS1.04.07	Delegação de poder	M
NGS1.04.08	Acesso ao RES pelo sujeito da atenção	M
NGS1.04.10	Gerenciamento de grupos	R
NGS1.04.11	Controle de acesso ao prontuário indicado pelo sujeito da atenção	M
NGS1.04.12	Inserção de dados pelo sujeito da atenção	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

É preciso ter uma política para a disponibilidade do RES, que o mesmo tenha sempre uma cópia de segurança. Quando se fizer necessário, que ele seja restaurado na integra e, alerte caso esteja perto de ultrapassar o máximo disponível de ocupação.

Tabela 6 NGS1.05 **Disponibilidade do RES**

ID	TÍTULO	OBRIGATÓRIO
NGS1.05.01	Cópia de Segurança	M
NGS1.05.02	Integridade na restauração da cópia de segurança	M
NGS1.05.03	Alerta de limiar de ocupação	M

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Nesse requisito, é importante verificar se todos os componentes do S-RES conversam entre si, verificando a segurança e a disponibilidade e integridade da informação a ser trocada e a confirmação da mesma.

Tabela 7 NGS1.06 **Comunicação entre componentes do S-RES**

ID	TÍTULO	OBRIGATÓRIO
NGS1.06.01	Segurança da comunicação com componente de interação com o usuário	M
NGS1.06.02	Controle de acesso do cliente ao servidor	M
NGS1.06.03	Processamento de dados no lado servidor	M
NGS1.06.04	Segurança da comunicação entre componentes	M
NGS1.06.05	Controle de acesso entre componentes	M
NGS1.06.06	Comunicação entre S-RES	M
NGS1.06.07	Confirmação de entrega	M
NGS1.06.08	Integridade e origem de componentes dinâmicos	M
NGS1.06.09	Método de autenticação de parceiro de comunicação	M
NGS1.06.10	Segregação de componentes	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Nesse requisito é verificado a segurança dos dados. Desde a importação, integridade. Impedir acesso direto ao SGBD e a reconstrução do RES.

Tabela 8 NGS1.07 **Segurança de dados**

ID	TÍTULO	OBRIGATÓRIO
NGS1.07.01	Importação de dados	M
NGS1.07.04	Verificação de integridade dos dados	R
NGS1.07.05	Utilização de SGBD	M
NGS1.07.06	Impedir acesso direto ao SGBD	M
NGS1.07.07	Impedir reconstrução do RES	R
NGS1.07.09	Manipuladores RES	R
NGS1.07.10	Validação de dados de entrada	M
NGS1.07.11	Segregação dos dados por organização	M
NGS1.07.12	Processo de importação de dados	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Nesse requisito, é demonstrado como deve ser tratada uma auditoria, que ela deve ser continua e os registros devem ser protegidos. Todos os eventos e informações, devem ser registradas numa trilha. De tal forma que a auditoria consiga localizar algum inconveniente caso necessário.

Tabela 9 NGS1.08 **Auditoria**

ID	TÍTULO	OBRIGATÓRIO
NGS1.08.01	Auditoria contínua	M
NGS1.08.02	Proteção dos registros de auditoria	M
NGS1.08.04	Eventos e informações registradas na trilha de auditoria	M
NGS1.08.05	Visualização dos registros da trilha de auditoria	M
NGS1.08.06	Exportação dos registros da trilha de auditoria	M

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

A documentação deve ter todos os dados lançados nela, desde versão do *software* utilizado, horário e idioma. A mesma deve ter uma cópia de

segurança e histórico de alterações na mesma e acesso, mostrando desse modo uma trilha de auditoria caso necessário.

Tabela 10 NGS1.09 **Documentação**

ID	TÍTULO	OBRIGATÓRIO
NGS1.09.01	Documentação	M
NGS1.09.02	Referência à versão do *software* na documentação	M
NGS1.09.04	Operador de backup	M
NGS1.09.05	Restrição de acesso a entidades não autenticadas e autorizadas	M
NGS1.09.07	Configuração da segurança da comunicação entre componentes	M
NGS1.09.08	Sincronização de relógio	M
NGS1.09.09	Guarda da mídia de cópia de segurança	M
NGS1.09.10	Segregação dos componentes	M
NGS1.09.11	Importação de dados de dispositivos externos de saúde	M
NGS1.09.12	Idioma	M
NGS1.09.13	Alertas sobre configurações inseguras	M
NGS1.09.14	Histórico de alteração	M

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Nesse requisito é cobrado que a auditoria seja feita por um tempo uniforme e que seja guardado e demonstrado relatórios dos avanços da auditoria.

Tabela 11 NGS1.10 **Tempo**

ID	TÍTULO	OBRIGATÓRIO
NGS1.10.01	Uniformidade da representação de tempo para auditoria	M
NGS1.10.03	Fonte temporal	M

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Um dos requisitos cobrados, é a interface para notificações ao usuário, que o mesmo receba notificações claras e visíveis sempre que necessário.

Tabela 12 NGS1.11 **Notificação de ocorrências**

ID	TÍTULO	OBRIGATÓRIO
NGS1.11.01	Interface para notificação	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

É tratado a privacidade, desde os termos de concordância do paciente e da associação de saúde. Quais são os motivos do uso da informação e restrições.

Tabela 13 NGS1.12 **Privacidade**

ID	TÍTULO	OBRIGATÓRIO
NGS1.12.01	Concordância com termos de uso	R
NGS1.12.02	Consentimento do sujeito da atenção	R
NGS1.12.03	Associação do consentimento à informação de saúde	R
NGS1.12.04	Acesso de emergência	R
NGS1.12.05	Propósito de uso	R
NGS1.12.06	Restrição de exportação por propósito de uso	R
NGS1.12.07	Restrições para transmissão e exportação de RES	M

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Nesse requisito, é cobrado o certificado digital do usuário, para autenticação do mesmo, o não repudio em caso de acesso e a compatibilidade dos sistemas empregados para a autenticação

Tabela 14 NGS1.13 **Autenticação de usuário utilizando certificado digital**

ID	TÍTULO	OBRIGATÓRIO
NGS1.13.01	Certificado digital	R
NGS1.13.02	Atendimento à ICP-Brasil	R
NGS1.13.03	Validação do certificado digital antes do uso	M
NGS1.13.04	Configuração de certificados raiz do S-RES	M
NGS1.13.05	Verificação do propósito do certificado digital para autenticação	R
NGS1.13.06	Não repúdio da autenticação	M

ID	TÍTULO	OBRIGATÓRIO
	realizada	
NGS1.13.07	Tipos de usuários para autenticação com certificação digital	R
NGS1.13.08	Homologação ICP-Brasil	R
NGS1.13.09	Elemento de prova da autenticação	R
NGS1.13.10	Vínculo entre Certificado Digital e Usuário	R
NGS1.13.11	Compatibilidade com mídias para certificado digital	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

.

3.4.2 Nível de Garantia de Segurança | NGS2

Conforme dito anteriormente a NGS2 possuí 43 itens que aborda a certificação digital que é uma premissa para assinar digitalmente, e é o primeiro item da NGS2.01 – Certificado digital e divide em subclassificações que são a:

Esses requisitos exigem que a assinatura esteja em conformidade com ICP – Brasil, que o CPF seja validado na assinatura do usuário do sistema e da assinatura digital, para essa validação ocorrer deve-se usar criptografia.

Tabela 15 NGS2.01 **Certificado digital**

ID	TÍTULO	OBRIGATÓRIO
NGS2.01.01	Certificado digital	M
NGS2.01.02	Atendimento à ICP-Brasil	M
NGS2.01.03	Validação do certificado digital antes do uso	M
NGS2.01.04	Configuração de certificados raiz do S-RES	M
NGS2.01.05	Tipos de usuários para autenticação com certificação digital	R
NGS2.01.06	Compatibilidade com mídias para certificado digital	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Os requisitos acima detalham sobre a assinatura digital, qual o formato, registros de pendência, indisponibilidade da assinatura e a compatibilidade.

Tabela 16 NGS2.02 **Assinatura digital**

ID	TÍTULO	OBRIGATÓRIO
NGS2.02.01	Formato de assinatura	M

ID	TÍTULO	OBRIGATÓRIO
NGS2.02.02	Verificação do propósito do certificado digital para assinatura	M
NGS2.02.03	Referência temporal para revogação	M
NGS2.02.04	Validação da assinatura digital	M
NGS2.02.06	Propósito da assinatura	R
NGS2.02.07	Visualização das informações a serem assinadas	M
NGS2.02.08	Homologação ICP-Brasi	R
NGS2.02.09	Exportação de registros assinados	M
NGS2.02.11	Resultado da validação da assinatura digital	M
NGS2.02.12	Validação com objeto de revogação ideal	R
NGS2.02.13	Indisponibilidade de acesso a serviços externos	M
NGS2.02.14	Validação e adequação da assinatura de documentos recebidos	M
NGS2.02.15	Instante da assinatura	M
NGS2.02.16	Inclusão e validação de certificado de Atributo	R
NGS2.02.17	Informações sobre assinatura	M
NGS2.02.18	Encadeamento de registros assinados digitalmente	R
NGS2.02.19	Verificação do encadeamento de registros	R
NGS2.02.20	Indisponibilidade da chave privada	R
NGS2.02.21	Aviso de registro pendente de assinatura	M
NGS2.02.22	Uso dos formatos AD-RV e AD-RC	R
NGS2.02.23	Exportação de registros eletrônicos identificados	R
NGS2.02.24	Formato de assinatura em formato AdES	R
NGS2.02.25	Compatibilidade com os dispositivos ICPBrasil	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Estes requisitos descrevem sobre os documentos que são digitalizados e devem ser assinados digitalmente no modelo ICP- Brasil, também exige que o documento digitalizado tenha um par de chaves simétricas.

Tabela 17 NGS2.04 **Digitalização de documentos**

ID	TÍTULO	OBRIGATÓRIO

ID	TÍTULO	OBRIGATÓRIO
NGS2.04.01	Assinatura digital do sistema de GED	R
NGS2.04.02	Assinatura digital do operador	R
NGS2.04.03	Assinatura digital do responsável	R
NGS2.04.06	Termo de conduta para digitalização	R
NGS2.04.07	Homologação ICP-Brasi	R
NGS2.04.08	Certificado digital do sistema GED	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

O requisito de tempo que é tratado no requisito NGS2.05 - Carimbo de tempo, exigem a validação da hora/minuto/segundo no momento da assinatura.

Tabela 18 NGS2.05 **Carimbo de tempo**

ID	TÍTULO	OBRIGATÓRIO
NGS2.05.01	Carimbo de tempo	M
NGS2.05.02	Verificação do carimbo de tempo	M
NGS2.05.04	Carimbo de tempo ICP-Brasil	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

O requisito de atributado permite configurar uma autoridade para assinar digitalmente, por exemplo o conselho federal de medicina.

Tabela 19 NGS2.06 **Certificado de atributo**

ID	TÍTULO	OBRIGATÓRIO
NGS2.06.01	Configuração das fontes de autoridade	R
NGS2.06.02	Tratamento de certificado de atributo	R

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Apesar do usuário assinar digitalmente e mantiver o arquivo armazenado, ele pode imprimir o registro, assim existe o requisito NGS2.07 – Impressão de registro assinado digitalmente.

Tabela 20 NGS2.07 **Impressão de registro assinado digitalmente**

ID	TÍTULO	OBRIGATÓRIO
NGS2.07.01	Impressão de registros assinados digitalmente	M
NGS2.07.02	Impressão de mensagem de rodapé	M

NGS2.07.03	Impressão de relatório de assinaturas	M

Fonte: Baseada no manual de certificação SBIS – CFM (2019)

Quando o usuário imprimir um documento assinado digitalmente, na impressão deverá conter algumas informações do profissional, por exemplo nome completo, CPF, data e hora da assinatura.

Com a implantação dos requisitos NGS2 permite a eliminação dos papeis nos processos na área de saúde, também substitui a preservação das informações de meios físicos por meio eletrônicos, esse item foi aprovado na:

> RESOLUÇÃO CFM Nº 1.821/2017
> Art. 7º Estabelecer a guarda permanente, considerando a evolução tecnológica, para os prontuários dos pacientes arquivados eletronicamente em meio óptico, microfilmado ou digitalizado. (CONSELHO FEDERAL DE MEDICINA, 2007).

É uma premissa para garantir a eliminação do papel é assinar digitalmente o prontuário.

4 ESTUDO DA APLICAÇÃO DOS REQUISITOS DE SEGURANÇA

Neste capítulo será apresentado um estudo de caso foi realizado como *software* de saúde, MKSAUDE, produzido pela empresa MKDATA, que forneceu o *software* para a realização deste estudo.

A empresa em questão está em processo de implementação dos requisitos das Normas SG1 e SG2 que estão sendo implantados no *software* MKSAUDE, *software* este voltado para prontuário eletrônico.

A empresa disponibilizou um ambiente teste para verificar se os requisitos implementados estão de acordo com a certificação e realizar um teste de segurança na aplicação este teste foi realizado somente na aplicação sem acesso ao código fonte.

O teste realizado teve como principal objetivo verificar possíveis vulnerabilidades que ainda poderiam existir na aplicação, e fazer recomendações que poderiam aumentar a segura.

4.1 SOBRE A EMPRESA MKDATA

A empresa MKDATA surgiu em 1998 na cidade de Americana/SP com um produto para área de controle financeiro e após o seu primeiro produto começou a expandir e desenvolver sistemas para outras áreas comerciais e prestar consultoria nas empresas da região.

Atualmente a empresa tem filiais no estado de São Paulo, Mato Grosso, Paraná, Manaus, Espírito Santo e Minas Gerais.

Sempre em evolução a empresa busca conhecer novos conceitos de negócios, novas tecnologias para aplicar nos sistemas e atender da melhor forma os clientes.

Os *softwares* são separados para área administrativa (MKADM) e saúde (MKSAUDE). Na área administrativa o sistema possui módulos para: vendas, estoque, financeiro, nota fiscal eletrônica e produção. E os módulos de saúde são voltados para: pronto atendimento, consultórios, centros de especialidades, medicina preventiva, domiciliar, atenção primária a saúde, estoque, central de agendamento e agenda *online* integrada com os consultórios, possui

aplicativos mobile para venda dos planos de saúde, desospitalização, agendamento e atendimento do médico.

4.2 SOBRE O SOFTWARE MKSAUDE

Em 2010 surgiu uma parceria com um consultório médico para desenvolver um prontuário eletrônico, o sucesso foi tanto que a empresa expandiu para outras clínicas e desenvolveu outras aplicações para área hospitalar, farmácias de manipulação, centros de especialidades e operadoras de saúde, ao todo são doze mil usuários que utilizam o produto MKSAUDE.

O sistema foi desenvolvido para retirar o que era feito no papel e aplicar os processos do dia a dia no sistema, desde a parte do agendamento e até o atendimento médico, assim o médico consegue gerenciar o histórico de atendimento do paciente.

Os profissionais e as operadoras de saúde passaram a informatizar todos os processos com a utilização do sistema e isso gerou uma confiança no cuidado, pois o médico tem à disposição um:

> Histórico de saúde completo: A proposta do prontuário eletrônico é coletar as informações de saúde durante toda a vida do paciente e garantir o fácil acesso a esses dados...torna-se mais fácil fazer diagnósticos e identificar patologias com maior precisão.
> Economia de tempo: Preencher dados como resultados de exames ou prescrições médicas no prontuário eletrônico toma um tempo bem menor do que nos registros em papel...
> Prescrição segura: ... O prontuário eletrônico pode disparar alertas na ocorrência de interações medicamentosas perigosas ou até mesmo no caso de alergias.
> Segurança dos dados: O prontuário de papel pode ser perdido e visto por qualquer pessoa. Já a utilização de um prontuário eletrônico elimina o risco de perdas e garante a privacidade dos dados do paciente. Apenas aqueles com permissão têm acesso ao prontuário, além de existirem diversos níveis de acesso para diferentes profissionais envolvidos.
> Compartilhamento dos registros: Os dados armazenados no prontuário eletrônico podem ser compartilhados entre diferentes instituições, departamentos e profissionais, permitindo uma integração e coordenando o atendimento para benefício do paciente.
> O prontuário eletrônico é uma tendência que promete grande impacto na área da saúde. Sua utilização pode promover uma relação melhor entre o médico e os seus pacientes. (UNIMED, 2017).

Com a informatização dos prontuários eletrônicos é necessário garantir que as informações não sejam perdidas e nem violadas. Assim a empresa

MKDATA, que sempre procura atender as legislações do país, procurou desenvolver um sistema que garantisse a segurança das informações, e para atender as normas da LGPD, ANS e as resoluções do CFM.

Com isso a empresa procurou uma certificação de *software* SBIS que estabelece requisitos de segurança, que exige o sigilo do prontuário, a integridade das informações e para o prontuário ter validade jurídica deve ser assinado com um certificado digital padrão ICP – Brasil.

4.3 A IMPLANTAÇÃO DAS NORMAS SG1 E SG2

Em 2016 iniciou-se o projeto para desenvolver e implantar a certificação e por estratégia os primeiros requisitos a serem implantados foram os níveis de garantia de segurança e os mandatórios, conforme o projeto evoluir os recomendados também serão implantados.

A equipe começou a desenvolver os requisitos aplicando parâmetros no sistema, utilizando aplicações já existentes e para atender foi realizado uma integração com as empresas que já fornecem a certificação digital e já atendem os requisitos de segurança.

Alguns requisitos ainda estão em desenvolvimento e outros já foram aplicados no sistema e já estão em produção. A empresa atende 66 requisitos, sendo 58 mandatórios e 8 recomendados.

A primeira etapa deste estudo de caso, foi fazer um levantamento de todos os requisitos que foram implementados no *software* MKSAUDE para atender as normas NGS1 e NGS2, além de verificar o como foram implementados estes requisitos.

A tabela a seguir, apresenta os resultados obtidos nesta primeira etapa do estudo de caso:

Tabela 21 Requisitos da NGS1 e da NGS2 implementados no *software* MKSAUDE .

ID	TÍTULO	OBRIGATÓRIO	COMO?
NGS1.01.01	Versão do software	M	O requisito exige que em todas telas do sistema deve ser apresentado a versão do sistema, assim foi aplicado um campo que mostra a versão, release e pela numeração da versão é possível identificar o mês e o ano da versão gerada. Exemplo da numeração: 19.05.3.6060 (r-6060a), 19(ano), 05 (mês), 3.6060(versão) e caso seja release é identificado através do R e a *build* é identificada por ordem alfabética, então pode existir *release* de A a Z.
NGS1.01.02	Código fonte	R	O controle de versão é realizado através do *Subversion* (SVN) que armazenas as versões.
NGS1.01.04	Repositório de versões	R	A empresa desenvolveu um site que serve como repositório das versões onde os clientes acessam com usuário e senha e em qualquer momento pode visualizar e fazer o download de qualquer versão.
NGS1.02.01	Identificação e autenticação de usuário	M	O requisito é atendido através do login e senha do usuário, caso o profissional não tenha um login e senha liberado o acesso ao sistema não é permitido.
NGS1.02.02	Método de autenticação de pessoa	M	O requisito é atendido através do login e senha do usuário, caso o profissional não tenha um login e senha liberado o acesso ao sistema não é permitido.
NGS1.02.03	Proteção dos parâmetros de autenticação de usuário	M	Foi utilizado o tipo *SHA256* (*secure hash algorithm 256bits*), que são funções criptográficas do *hash*, muito utilizadas na assinatura digital e em outras funções dentro da segurança da informação. É verificado se ocorre vazamento de dados dos parâmetros de autenticação do usuário.
NGS1.02.04	Segurança de senhas	M	Desenvolvido no sistema uma parametrização de requisitos de senhas que uma vez habilitada não é possível voltar atrás, o parâmetro segue os padrões de segurança de senha e tem como exigência

ID	TÍTULO	OBRIGATÓRIO	COMO?
			no mínimo oito caracteres e deve conter pelo menos um caractere alfabético e um numérico. Também foi desenvolvido o parâmetro periodicidade de troca de senha, troca de senha forçada, igualdade de senha e não permite a visualização de senhas por terceiros.
NGS1.02.05	Controle de tentativas de login	M	Nesse requisito foi desenvolvido um parâmetro que determina quantas tentativas pode ocorrer o bloqueio temporário e depois de quantas tentativas pode ocorrer o bloqueio permanente e com isso o sistema envia um email para o usuário com uma senha temporária.
NGS1.02.06	Identidade única da pessoa e responsabilização	M	No sistema o usuário é identificado através do CPF e não é permitido o cadastrar um outro usuário com o mesmo CPF. Quando o usuário informa um CPF o sistema verifica se é um CPF válido.
NGS1.02.08	Informações na autenticação	M	Para o requisito de autenticação o sistema verifica o usuário e senha e caso estejam errado é mostrado uma mensagem que o usuário e/ou a senha estão incorretas e esses registros são salvos em uma tabela do banco e quando o usuário *logar* no sistema corretamente é apresentando uma tela com últimos acessos, mostrando a data, horário e se teve usuário ao logar.
NGS1.02.09	Informações em autenticação inválida	R	Ao tentar *logar* no sistema e errar a senha ou usuário é apresentado na tela uma mensagem que o usuário ou a senha estão incorretos.
NGS1.03.01	Bloqueio ou encerramento por inatividade	R	Esse requisito é aplicado através de um parâmetro de inatividade, o administrador do sistema pode determinar que depois de 10 minutos de inatividade o sistema seja bloqueado e irá solicitar o login novamente.
NGS1.03.02	Segurança contra roubo de sessão de usuário	M	Para a segurança contra roubo de sessão do usuário, a norma recomenda ao auditor, utilizar de um *sniffer* para interceptar a

ID	TÍTULO	OBRIGATÓRIO	COMO?
			comunicação do usuário com a S-RES. Caso seja bem-sucedida a interceptação, é recomendado a utilização de *HTTPS* nas conexões para proteger o usuário de *sniffer* na rede.
NGS1.03.03	Retomada de atividade do usuário	R	Quando o sistema identificado uma inatividade do usuário ele entra em modo inativo e bloqueia a tela e caso o usuário queira retomar o acesso é necessário informar o usuário e a senha novamente
NGS1.04.01	Impedir acesso por pessoas não autorizadas	M	Para atender ao requisito de pessoas não autorizadas o sistema verifica se o perfil de acesso do usuário tem permissão e verifica a regras de sigilos. Exemplo: Prontuários da equipe de psicologia não são compartilhados. E para acessar o sistema é necessário tem um login.
NGS1.04.02	Mecanismo de controle de acesso ao RES	M	O acesso pode ser realizado através do browser e é homologado nos navegadores Chrome e Mozilla
NGS1.04.03	Gerenciamento de usuários e papéis	M	Este requisito é aplicado no sistema através de perfis de acessos do usuário, ao criar um usuário é necessário vincular um perfil de acessos com permissões de leitura, alterar, incluir, excluir
NGS1.04.04	Papéis relacionados à T.I	R	O requisito exige que um usuário tenha acesso ao banco de dados para realizar o backup, para atender a norma registramos um usuário com essa permissão.
NGS1.04.05	Configuração de controle de acesso	M	Esta configuração é realizada através dos perfis de acesso, onde é definido se o usuário pode fazer a leitura, incluir, alterar e excluir.
NGS1.04.06	Usuário mínimo ativo e restrição de autoconcessão de direitos	M	Foi desenvolvido uma verificação onde é obrigatório ter um usuário com perfil de acesso para liberar acessos para outros usuários, mas não permite que o usuário faça um auto concessão de acesso.
NGS1.04.07	Delegação de poder	M	Foi criado uma rotina no sistema para que um usuário possa dar poder a outro

ID	TÍTULO	OBRIGATÓRIO	COMO?
			usuário temporariamente. Exemplo: Liberar a impressão do prontuário para um usuário do jurídico.
NGS1.04.11	Controle de acesso ao prontuário indicado pelo sujeito da atenção	M	Este requisito é atendido através de uma parametrização do sistema onde o usuário poderá configurar grupos de acessos aos prontuários e determinar qual prontuário o profissional poderá acessar.
NGS1.05.01	Cópia de Segurança	M	Nesta norma é recomendado a criação de um perfil similar ao do operador de *backup* no *SGBD*, para que o mesmo possa verificar dentro do Oracle todos os comandos desde *expdp* (exportar) e *impdp* (importar), até os mais complexos, conforme for necessário a auditoria do sistema.
NGS1.05.02	Integridade na restauração da cópia de segurança	M	O banco utilizado é o *Oracle* e quando o usuário executar o comando *Impdp* é gerado um alerta para o usuário caso ocorra algum problema.
NGS1.05.03	Alerta de limiar de ocupação	M	Foi criado um parâmetro no sistema onde o usuário pode definir um limite de ocupação do banco e a partir de quantos porcento um usuário deve ser alertado. Exemplo quando o banco atingir 80% da sua ocupação um email será enviado para o responsável.
NGS1.06.01	Segurança da comunicação com componente de interação com o usuário	M	Para verificar a segurança de comunicação do usuário com o componente de interação, a norma, recomenda que o auditor ao capturar a mensagem, altere alguns dados e reenvie para o servidor e espere a resposta. Como defesa, pode-se utilizar do *HTTPS* para criptografar o tráfego das informações, browser Chrome, Firefox, etc. Utilizar o Tomcat como servidor de aplicação e o Oracle como banco de dados. Aumentando assim o nível de segurança.
NGS1.06.02	Controle de acesso do cliente ao servidor	M	Foi implementado um campo para definir de qual link de acesso o usuário pode entrar no sistema, o link pode ser adicionado no perfil do usuário,

ID	TÍTULO	OBRIGATÓRIO	COMO?
			o que ainda não foi implementado é a verificação do acesso via *MACs* ou *Ips*
NGS1.06.03	Processamento de dados no lado servidor	M	O requisito exige que o processamento dos dados seja feito previamente do lado do servidor, o desenvolvimento do requisito seguiu a norma, com isso o processamento é feito no servidor, usando o banco de dados e o *backend* e a validação de alguns campos são feitos no front *end*, por questão de performance.
NGS1.06.04	Segurança da comunicação entre componentes	M	O banco de dados só pode ser acessado com usuário e senha autorizados.
NGS1.06.05	Controle de acesso entre componentes	M	O controle de acesso da aplicação e o banco de dados é feito através de usuário e senha autorizados.
NGS1.07.05	Utilização de SGBD	M	A norma exige que toda movimentação realizada no sistema seja gravada em banco de dados, o banco de dados recomentado é o Oracle a partir da versão *10xe*
NGS1.07.06	Impedir acesso direto ao SGBD	M	O banco de dados só pode ser acessado pela aplicação, mediante a bloqueio na porta de comunicação com o banco de dados diretamente
NGS1.07.10	Validação de dados de entrada	M	A norma exige que os dados inseridos pelo usuário nos campos de entrada (*inputs*, caixas de texto) devem ser validados antes de ser processados, prevenir de ataque, por isso foi aplicado no sistema a validação no *front-end*.
NGS1.07.11	Segregação dos dados por organização	M	É exigido a separação de dados por empresa, foi realizada a separação das empresas no banco de dados.
NGS1.08.01	Auditoria contínua	M	A norma exige o registro das informações inseridas no sistema de uma forma contínua, foi criado uma tabela no banco que armazena os registros para que possam ser utilizados na auditoria.
NGS1.08.02	Proteção dos registros de auditoria	M	Para acessar o registro de auditoria o usuário precisa ter um perfil de acesso com essa autorização.

ID	TÍTULO	OBRIGATÓRIO	COMO?
NGS1.08.04	Eventos e informações registradas na trilha de auditoria	M	Este requisito exige que o sistema armazene eventos de alteração de prontuário, alteração de senhas, tentativas de acesso entre outros, para isso foi desenvolvido uma tela para registrar essas alterações e o sistema armazena a horário, dia, usuário, perfil e o *ip*.
NGS1.08.05	Visualização dos registros da trilha de auditoria	M	Conforme explicado acima foi desenvolvido uma tela para consultar as movimentações da trilha.
NGS1.08.06	Exportação dos registros da trilha de auditoria	M	Para exportar um arquivo o sistema utiliza o gerenciador de relatório *Fast Report* que permite a exportação no formato *csv*.
NGS1.09.02	Referência à versão do *software* na documentação	M	Os requisitos exigem que alterações no *software*sejam documentadas, quando uma versão é gerada a equipe faz um documento explicando as novas funcionalidades e este documento também está disponível no repositório de versões.
NGS1.09.14	Histórico de alteração	M	
NGS1.10.01	Uniformidade da representação de tempo para auditoria	M	Foi aplicado o formato *RFC* 3339 para apresentar a data e hora, esse formato é uma exigência da norma.
NGS1.10.03	Fonte temporal	M	O requisito de fonte temporal exige que o sistema registre o dia e horário do acesso conforme o fuso horário do local, para isso foi criado um campo para salvar a data completa com fuso horário *GMT* utilizando uma função do *java*(*Timezone*) para retornar se a data na localização do usuário é horário de verão ou não.
NGS1.12.01	Concordância com termos de uso	R	Foi desenvolvido um cadastro de termo de aceite no sistema onde o usuário poderá adicionar um documento explicando sobre o uso das informações de saúde e informando que os dados são sigilos.
NGS1.13.03	Validação do certificado digital antes do uso	M	A MkDATA precisando atender a normas que exigem o certificado digital procurou uma empresa que já possuí os requisitos implantados da
NGS1.13.04	Configuração de certificados raiz do S-RES	M	

ID	TÍTULO	OBRIGATÓRIO	COMO?
NGS2.01.01	Certificado digital	M	certificação, com isso realizou uma integração com a empresa, que é uma empresa de *softwares* de segurança, que oferece serviços de Assinatura Digital, Autenticação e Proteção de dados, gerenciamento e armazenamento de chaves criptografadas
NGS2.01.02	Atendimento à ICP-Brasil	M	
NGS2.01.03	Validação do certificado digital antes do uso	M	
NGS2.01.04	Configuração de certificados raiz do S-RES	M	
NGS2.02.01	Formato de assinatura	M	
NGS2.02.02	Verificação do propósito do certificado digital para assinatura	M	
NGS2.02.03	Referência temporal para revogação	M	
NGS2.02.04	Validação da assinatura digital	M	
NGS2.02.07	Visualização das informações a serem assinadas	M	O sistema sempre permite visualizar as informações que são impressas.
NGS2.02.11	Resultado da validação da assinatura digital	M	A MkDATA precisando atender a normas que exigem o certificado digital procurou uma empresa que já possuí os requisitos implantados da certificação, com isso realizou uma integração com a empresa, que é uma empresa de *softwares* de segurança, que oferece serviços de Assinatura Digital, Autenticação e Proteção de dados, gerenciamento e armazenamento de chaves criptografadas
NGS2.02.13	Indisponibilidade de acesso a serviços externos	M	
NGS2.02.15	Instante da assinatura	M	
NGS2.02.17	Informações sobre assinatura	M	O sistema salva as informações em um banco de dados, registrando o profissional que assinou e data/horário. Ao imprimir novamente o sistema apresenta esses dados
NGS2.02.21	Aviso de registro pendente de assinatura	M	Para o requisito acima foi desenvolvido uma tela que mostra quais são os prontuários pendentes de assinatura, dessa o profissional consegue visualizar as pendencias.
NGS2.05.01	Carimbo de tempo	M	A MkDATA precisando atender a normas que exigem o certificado digital procurou uma empresa que já possuí os requisitos implantados da certificação, com isso realizou uma integração com a
NGS2.05.02	Verificação do carimbo de tempo	M	
NGS2.05.04	Carimbo de tempo ICP-Brasil	R	

ID	TÍTULO	OBRIGATÓRIO	COMO?
			empresa, que é uma empresa de *softwares* de segurança, que oferece serviços de Assinatura Digital, Autenticação e Proteção de dados, gerenciamento e armazenamento de chaves criptografadas
NGS2.07.01	Impressão de registros assinados digitalmente	M	Estes requisitos exigem que a assinatura seja impressa no documento, foi desenvolvido a assinatura no rodapé da página.
NGS2.07.02	Impressão de mensagem de rodapé	M	

Fonte: Autoria Própria

A tabela a seguir, apresenta os requisitos da NGS1 e da NGS2 que não implementados no *software* MKSAUDE , e a justificativa da empresa para não implementação destes requisitos:

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS1.02.10	Revelação de credenciais na interface de autenticação	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.02.11	Autenticação forte	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.02.12	Uso de SALT	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.04.08	Acesso ao RES pelo sujeito da atenção	M	Este requisito ainda não foi desenvolvido pois a empresa está em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS1.06.06	Comunicação entre S-RES	M	Este requisito ainda não foi desenvolvido pois a empresa está em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES
NGS1.04.10	Gerenciamento de grupos	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.04.12	Inserção de dados pelo sujeito da atenção	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.06.07	Confirmação de entrega	M	Este requisito ainda não foi desenvolvido pois a empresa está em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES
NGS1.06.08	Integridade e origem de componentes dinâmicos	M	Este requisito ainda não foi desenvolvido pois estamos em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES
NGS1.06.09	Método de autenticação de parceiro de comunicação	M	Será implementado futuramente
NGS1.06.10	Segregação de componentes	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.07.01	Importação de dados	M	Este requisito ainda não foi desenvolvido pois a empresa está em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES
NGS1.07.04	Verificação de integridade dos dados	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS1.07.07	Impedir reconstrução do RES	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.07.09	Manipuladores RES	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.07.12	Processo de importação de dados	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.09.01	Documentação	M	Os requisitos exigem que manuais dos processos sejam criados e disponibilizados para os clientes, os manuais estão em processos de construção
NGS1.09.04	Operador de backup	M	
NGS1.09.05	Restrição de acesso a entidades não autenticadas e autorizadas	M	
NGS1.09.07	Configuração da segurança da comunicação entre componentes	M	
NGS1.09.08	Sincronização de relógio	M	
NGS1.09.09	Guarda da mídia de cópia de segurança	M	
NGS1.09.10	Segregação dos componentes	M	
NGS1.09.11	Importação de dados de dispositivos externos de saúde	M	
NGS1.09.12	Idioma	M	
NGS1.09.13	Alertas sobre configurações inseguras	M	

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS1.11.01	Interface para notificação	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.12.02	Consentimento do sujeito da atenção	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.12.03	Associação do consentimento à informação de saúde	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.12.04	Acesso de emergência	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.12.05	Propósito de uso	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.12.06	Restrição de exportação por propósito de uso	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.12.07	Restrições para transmissão e exportação de RES	M	Este requisito ainda não foi desenvolvido pois a empresa está em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES
NGS1.13.01	Certificado digital	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS1.13.02	Atendimento à ICP-Brasil	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.13.05	Verificação do propósito do certificado digital para autenticação	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.13.06	Não repúdio da autenticação realizada	M	Ainda não foi desenvolvido a autenticação do usuário por certificado digital, será implementado futuramente.
NGS1.13.07	Tipos de usuários para autenticação com certificação digital	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.13.08	Homologação ICP-Brasil	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.13.09	Elemento de prova da autenticação	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.13.10	Vínculo entre Certificado Digital e Usuário	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS1.13.11	Compatibilidade com mídias para certificado digital	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS2.01.05	Tipos de usuários para autenticação com certificação digital	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.01.06	Compatibilidade com mídias para certificado digital	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.06	Propósito da assinatura	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.08	Homologação ICP-Brasi	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.09	Exportação de registros assinados	M	Este requisito ainda não foi desenvolvido pois a empresa está em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES
NGS2.02.12	Validação com objeto de revogação ideal	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.14	Validação e adequação da assinatura de documentos recebidos	M	Este requisito ainda não foi desenvolvido pois a empresa está em processo para realizar a integração com outros sistemas de prontuário eletrônico - S-RES
NGS2.02.16	Inclusão e validação de certificado de Atributo	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS2.02.18	Encadeamento de registros assinados digitalmente	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.19	Verificação do encadeamento de registros	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.20	Indisponibilidade da chave privada	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.22	Uso dos formatos AD-RV e AD-RC	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.23	Exportação de registros eletrônicos identificados	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.24	Formato de assinatura em formato AdES	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.02.25	Compatibilidade com os dispositivos ICPBrasil	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.

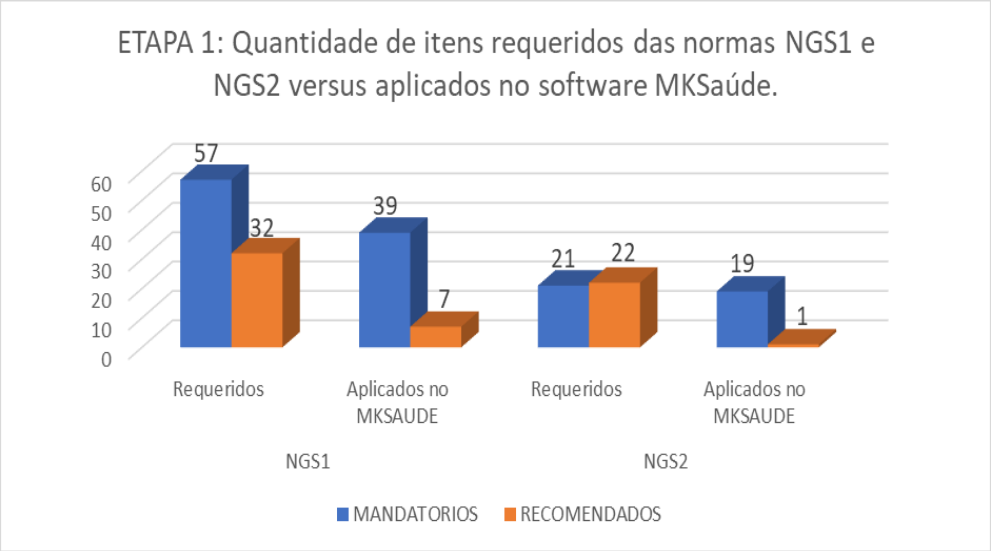
ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS2.04.01	Assinatura digital do sistema de GED	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.04.02	Assinatura digital do operador	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.04.03	Assinatura digital do responsável	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.04.06	Termo de conduta para digitalização	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.04.07	Homologação ICP-Brasi	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.04.08	Certificado digital do sistema GED	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.06.01	Configuração das fontes de autoridade	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.

ID	TÍTULO	OBRIGATÓRIO	MOTIVO DE NÃO ADESÃO
NGS2.06.02	Tratamento de certificado de atributo	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.
NGS2.07.03	Impressão de relatório de assinaturas	M	Será implementado futuramente
NGS1.02.07	Autenticação para operações críticas	R	O requisito é recomendável (não obrigatório) ter no sistema e por uma definição da empresa será implementado primeiro os requisitos mandatórios e posteriormente os recomendáveis.

Fonte: Autoria Própria

Abaixo, foi acrescentada uma tabela, mostrando a quantidade de itens requeridos das normas NGS1 e NGS2 versus aplicados no *software* MkSaúde.

Figura 1 - Quantidade de Requisitos atendidos



Fonte: Autoria própria

Pode-se observar que a empresa está em constante evolução e está trabalhando para aplicar todos os requisitos NGS1 e NGS2 para garantir a segurança do *software* MKSAUDE.

Muitos clientes que já utilizavam o sistema passaram a assinar digitalmente e com isso eliminaram os papeis, trazendo benefícios para a operadora/consultórios e garantindo que o médico tenha uma maior

resolutividade no atendimento ao paciente e caso o profissional necessite consultar um prontuário ele esteja sempre disponível e integro.

4.4 VALIDAÇÃO DA QUALIDADE DA IMPLEMENTAÇÃO DOS REQUISITOS

O *software* quando é desenvolvido deve passar por uma equipe de teste para verificar as falhas e realizar a correção antes da entrega para o cliente, com isso evita descontentamento por parte dos usuários.

Um sistema entregue com qualidade garante a funcionalidade da aplicação, deve ser de fácil uso para o usuário e de fácil manutenção, pode ocorrer pequenas falhas(*bugs*), mas que são corrigidas assim que encontradas. Mas um sistema não pode conter vulnerabilidade pois pode causar um grande prejuízo a organização.

> Qualidade de *software* é cumulativa, pois considera aceitável certo número de falhas ou bugs até certo ponto e, ainda assim, o aplicativo é considerado bom o suficiente para ser entregue ao usuário. A segurança do *software* por outro lado, é absoluta já que qualquer vulnerabilidade existente no aplicativo pode se tornar aquela que causará um enorme prejuízo ou desastre. (Tiinsideonline, 2007)

Dessa forma, a primeira etapa deste estudo de caso foi realizar uma validação dos requisitos item a item para verificar se a empresa atende total ou parcialmente. Observou-se que de 132 requisitos, sendo que 78 são mandatórios e 54 são recomendados, o *software* MKSAUDE já atende a 58 requisitos mandatórios e 8 recomendados, e essa verificação foi realizado junto com gerente de desenvolvimento da empresa.

Como segunda etapa deste estudo de caso, foi permitido executar um teste de segurança do sistema. A empresa disponibilizou um ambiente teste para executar varreduras e encontrar possíveis vulnerabilidades que podem ser exploradas.

Para isso foi instalado em uma máquina em um ambiente teste, com uma réplica de um banco de produção. Foi instalado neste ambiente: um banco *oracle* xe com uma cópia do *software* de produção, e o serviço de aplicação do *Tomcat* versão 9.

4.4.1 Testes realizados com a Ferramenta Zed Attack Proxy 8.2 (ZAP)

Foi realizado uma pesquisa para verificar quais ferramentas poderiam ser utilizadas para o teste de segurança que executam varreduras ativas em sistemas e foi encontrado a ferramenta que é recomendada pela organização OWASP (*Open Web Application Security Project*) que disponibiliza sem fins lucrativos documentações, referencias e procedimentos que permitem que as empresas melhorarem suas aplicações de segurança.

Foi adquirida a ferramenta Zed Attack Proxy 8.2(ZAP) que permite executar uma varredura ativa que tem como finalidade encontrar riscos que possam ser prevenidos, a ferramenta é de fácil uso e manuais para criar os ataques.

A ferramenta verifica as seguintes vulnerabilidades, de acordo com a owasp.org (2019):

> Avaliação de vulnerabilidade - O sistema é verificado e analisado quanto segurança problemas.
> Teste de penetração - O sistema passa por análise e ataque de simulação invasores maliciosos.
> Teste de tempo de execução - O sistema passa por análise e teste de segurança de um usuário final.
> Revisão de código - o código do sistema passa por uma revisão e análise detalhadas especificamente para vulnerabilidades de segurança.

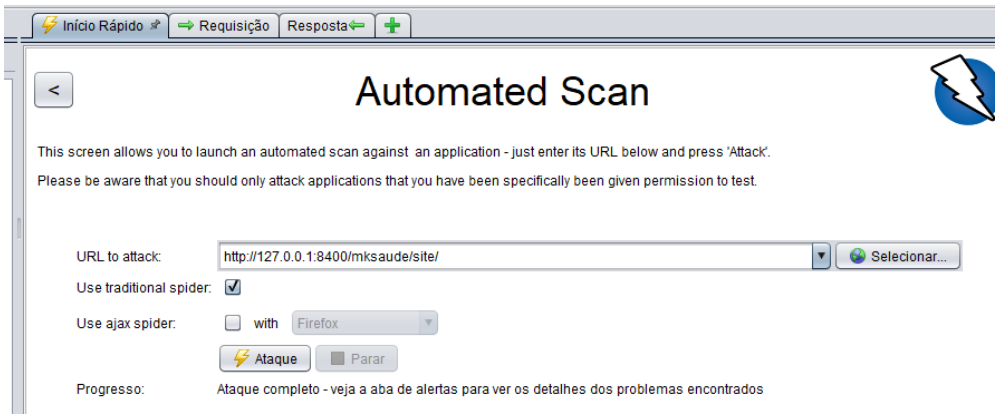
O ZAP inclui um relatório detalhado de seus resultados após o teste, mostrando as vulnerabilidades, como foram exploradas e a dificuldade encontrada para explorar essa vulnerabilidade.

4.4.2 Resultados dos Testes

Foi realizado um teste de varredura ativa que permite encontrar vulnerabilidades que possam ser exploradas. Esse tipo teste é realizado para prevenção, muito simples de realizado e não causa danos à aplicação.

Para realizar a varredura ativa a ferramenta pede a URL do *software* que será verificado, conforme apresentado na figura abaixo:

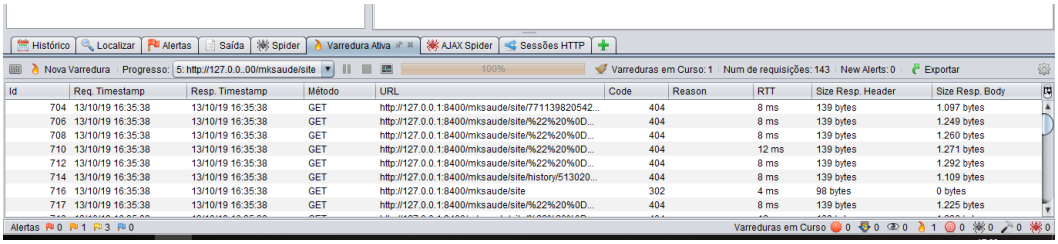
Figura 2 Escaneamento automático.



Fonte:Autoria Própria

Ao clicar em ataque a ferramenta irá vasculhar o site identificando as páginas e os recursos por meio da navegação, conforme apresentado na imagem abaixo:

Figura 3 Resultados do Escaneamento.



Fonte: Autoria Própria

Ao término da varredura a ferramenta apresenta os alertas encontrados e o nivel de vulnerabilidade.

O teste foi realizado em três aplicações, no *software* que está em um ambiente teste, no repositório que armazena as versões e um link de terceiro que armazena os certificados digitais.

Não foi possível testar todos os requisitos, mas em alguns requisitos que foram testados foram encontradas vulnerabilidades.

Na varredura foi possível testar 12 requisitos e alguns requisitos apresentaram mais de uma vulnerabilidade.

Tabela 22 Tabela com requisitos que foram testados.

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
NGS1.01.01	Versão do software	Não	Nenhuma	-	Nenhuma
NGS1.01.02	Código fonte	Não	Nenhuma	-	Nenhuma
NGS1.01.04	Repositório de versões	Sim	Cabeçalho de opções de quadro X não definido	MÉDIO	Os navegadores da Web mais modernos oferecem suporte ao cabeçalho *HTTP X-Frame-Options.* Verifique se ele está definido em todas as páginas da *web* retornadas pelo seu site (se você espera que a página seja enquadrada apenas por páginas do seu servidor (por exemplo, faz parte de um *FRAMESET*), use *SAMEORIGIN,* caso contrário, se você nunca espera a página para ser enquadrado, você deve usar *DENY. ALLOW-FROM* permite que sites específicos enquadrem a página da *Web* em navegadores da *Web* suportados
			Cabeçalho X-*Content-Type-Options* ausente	BAIXO	Certifique-se de que o aplicativo / servidor da *Web* defina o cabeçalho do tipo de conteúdo adequadamente e que o cabeçalho *X-Content-Type-Options* seja *'nosniff'* para todas as páginas da *web*. Se possível, assegure-se de que o usuário final use um navegador da Web moderno e compatível com os padrões que não execute a detecção de *MIME*ou que possa ser direcionado pelo aplicativo *Web* / servidor da *Web* para não executar a detecção de *MIME*.

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
			Proteção *XSS* do navegador da Web não ativada	BAIXO	Verifique se o filtro *XSS* do navegador da *Web* está ativado, configurando o cabeçalho de resposta *HTTP X-XSS-Protection* para '1'.
			Cookie No *HttpOnly* Flag	BAIXO	Verifique se o sinalizador *HttpOnly* está definido para todos os cookies.
NGS1.02.01	Identificação e autenticação de usuário	Sim	Nenhuma	-	Nenhuma
NGS1.02.02	Método de autenticação de pessoa	Sim	Nenhuma	-	Nenhuma
NGS1.02.03	Proteção dos parâmetros de autenticação de usuário	Sim	Nenhuma	-	Nenhuma
NGS1.02.04	Segurança de senhas	Sim	Nenhuma	-	Nenhuma
NGS1.02.05	Controle de tentativas de login	Sim	Nenhuma	-	Nenhuma
NGS1.02.06	Identidade única da pessoa e responsabilização	Não	Nenhuma	-	Nenhuma
NGS1.02.08	Informações na autenticação	Não	Nenhuma	-	Nenhuma
NGS1.02.09	Informações em autenticação inválida	Não	Nenhuma	-	Nenhuma
NGS1.03.01	Bloqueio ou encerramento por inatividade	Não	Nenhuma	-	Nenhuma
NGS1.03.02	Segurança contra roubo de sessão de	Sim	*Cookie No HttpOnly Flag*	BAIXO	Verifique se o sinalizador *HttpOnly* está definido para todos os *cookies*.

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
	usuário		Cabeçalho X-*Content-Type-Options* ausente	BAIXO	Certifique-se de que o aplicativo / servidor da Web defina o cabeçalho do tipo de conteúdo adequadamente e que o cabeçalho X-*Content-Type-Options* seja *'nosniff'* para todas as páginas da *web*. Se possível, assegure-se de que o usuário final use um navegador da *Web* moderno e compatível com os padrões que não execute a detecção de *MIME* ou que possa ser direcionado pelo aplicativo *Web* / servidor da *Web* para não executar a detecção de *MIME.*
NGS1.03.03	Retomada de atividade do usuário	Não	Nenhuma	-	Nenhuma
NGS1.04.01	Impedir acesso por pessoas não autorizadas	Não	Nenhuma	-	Nenhuma
NGS1.04.02	Mecanismo de controle de acesso ao RES	Não	Nenhuma	-	Nenhuma
NGS1.04.03	Gerenciamento de usuários e papéis	Não	Nenhuma	-	Nenhuma
NGS1.04.04	Papéis relacionados à T.I	Não	Nenhuma	-	Nenhuma
NGS1.04.05	Configuração de controle de acesso	Não	Nenhuma	-	Nenhuma
NGS1.04.06	Usuário mínimo ativo e restrição de autoconcessão de direitos	Não	Nenhuma	-	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
NGS1.04.07	Delegação de poder	Não	Nenhuma	-	Nenhuma
NGS1.04.11	Controle de acesso ao prontuário indicado pelo sujeito da atenção	Não	Nenhuma	-	Nenhuma
NGS1.05.01	Cópia de Segurança	Não	Nenhuma	-	Nenhuma
NGS1.05.02	Integridade na restauraçã o da cópia de segurança	Não	Nenhuma	-	Nenhuma
NGS1.05.03	Alerta de limiar de ocupação	Não	Nenhuma	-	Nenhuma
NGS1.06.01	Segurança da comunicação com componente de interação com o usuário	Sim	Informação sobre o tomcat	BAIXO	Quando o atacante obtém uma informação da aplicação ele pode buscar conhecimento para explorar as falhas que podem conter no serviço *web*, não é interessante repassar essa informação. Existe uma medida para ocultar a informação que é simples de ser resolvida, o administrador do serviço poderá adicionar uma linha no arquivo server.xml:
NGS1.06.02	Controle de acesso do cliente ao servidor	Não	Nenhuma	-	Nenhuma
NGS1.06.03	Processamento de dados no lado servidor	Não	Nenhuma	-	Nenhuma
NGS1.06.04	Segurança da comunicação entre componentes	Não	Nenhuma	-	Nenhuma
NGS1.06.05	Controle de acesso entre	Não	Nenhuma	-	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
	componentes				
NGS1.06.06	Comunicação entre S-RES	Não	Nenhuma	-	Nenhuma
NGS1.07.05	Utilização de SGBD	Não	Nenhuma	-	Nenhuma
NGS1.07.06	Impedir acesso direto ao SGBD	Não	Nenhuma	-	Nenhuma
NGS1.07.10	Validação de dados de entrada	Não	Nenhuma	-	Nenhuma
NGS1.07.11	Segregação dos dados por organização	Não	Nenhuma	-	Nenhuma
NGS1.08.01	Auditoria contínua	Não	Nenhuma	-	Nenhuma
NGS1.08.02	Proteção dos registros de auditoria	Não	Nenhuma	-	Nenhuma
NGS1.08.04	Eventos e informações registradas na trilha de auditoria	Não	Nenhuma	-	Nenhuma
NGS1.08.05	Visualização dos registros da trilha de auditoria	Não	Nenhuma	-	Nenhuma
NGS1.08.06	Exportação dos registros da trilha de auditoria	Não	Nenhuma	-	Nenhuma
NGS1.09.02	Referência à versão do *software* na documentação	Não	Nenhuma	-	Nenhuma
NGS1.09.14	Histórico de alteração	Não	Nenhuma	-	Nenhuma
NGS1.10.01	Uniformidade da representação de tempo para	Não	Nenhuma	-	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
	auditoria				
NGS1.10.03	Fonte temporal	Não	Nenhuma	-	Nenhuma
NGS1.12.01	Concordância com termos de uso	Não	Nenhuma	-	Nenhuma
NGS1.13.03	Validação do certificado digital antes do uso	Realizado teste de varredura no site que armazena os certificados	Cabeçalho de opções de quadro X não definido	MÉDIO	Os navegadores da Web mais modernos oferecem suporte ao cabeçalho *HTTP* X-Frame-Options. Certifique-se de que esteja definido em todas as páginas da web retornadas pelo seu site (se você espera que a página seja enquadrada apenas por páginas do servidor (por exemplo, faz parte de um FRAMESET), use SAMEORIGIN, caso contrário, se você nunca espera a página para ser enquadrado, você deve usar DENY. ALLOW-FROM permite que sites específicos enquadrem a página da Web em navegadores da Web suportados).
NGS1.13.04	Configuração de certificados raiz do S-RES		Cabeçalho X-*Content-Type-Options* ausente	BAIXO	Certifique-se de que o aplicativo / servidor da Web defina o cabeçalho do tipo de conteúdo adequadamente e que o cabeçalho X-Content-Type-Options seja 'nosniff' para todas as páginas da web. Se possível, assegure-se de que o usuário final use um navegador da Web moderno e compatível com os padrões que não execute a detecção de MIME ou que possa ser direcionado pelo aplicativo Web / servidor da Web

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
					para não executar a detecção de MIME.
NGS2.01.01	Certificado digital		Proteção *XSS* do navegador da *Web* não ativada	BAIXO	Verifique se o filtro *XSS* do navegador da *Web* está ativado, configurando o cabeçalho de resposta *HTTP X-XSS-Protection* para '1'.
NGS2.01.02	Atendimento à ICP-Brasil		Conjunto de cabeçalhos *HTTP* incompleto ou sem controle de *cache* e *HTTP* pragma	BAIXO	Sempre que possível, assegure-se de que o cabeçalho *HTTP* de controle de cache esteja definido com no-cache, no-store, must-revalidate; e que o cabeçalho *HTTP* pragma seja definido sem cache.
NGS2.01.04	Configuração de certificados raiz do S-RES		Ausência de tokens *anti-CSRF*	BAIXO	Fase: Arquitetura e Design Use uma biblioteca ou estrutura examinada que não permita que essa fraqueza ocorra ou forneça construções que facilitem essa fraqueza. Por exemplo, use pacotes anti-CSRF, como o OWASP CSRFGuard. Fase: Implementação Verifique se o seu aplicativo está livre de problemas de script entre sites, porque a maioria das defesas de CSRF pode ser contornada usando script controlado por invasor. Fase: Arquitetura e Design Gere um nonce exclusivo para cada formulário, coloque o nonce no formulário e verifique o nonce após o recebimento do formulário. Certifique-se de que o nonce não seja previsível (CWE-330). Observe que isso pode ser ignorado

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
					usando XSS. Identifique operações especialmente perigosas. Quando o usuário executar uma operação perigosa, envie uma solicitação de confirmação separada para garantir que o usuário pretendeu executar essa operação. Observe que isso pode ser ignorado usando XSS. Use o controle ESAPI Session Management. Este controle inclui um componente para CSRF. Não use o método GET para qualquer solicitação que desencadeie uma alteração de estado. Fase: Implementação Verifique o cabeçalho do *HTTP* Referer para ver se a solicitação se originou de uma página esperada. Isso pode prejudicar a funcionalidade legítima, porque usuários ou proxies podem ter desativado o envio do Referer por motivos de privacidade.
NGS2.02.07	Visualização das informações a serem assinadas	Não	Nenhuma	-	Nenhuma
NGS2.02.11	Resultado da validação da assinatura digital	Não	Nenhuma	-	Nenhuma
NGS2.02.13	Indisponibilidade de acesso a	Não	Nenhuma	-	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	NÍVEL DO RISCO	RECOMENDAÇÃO
	serviços externos				
NGS2.02.15	Instante da assinatura	Não	Nenhuma	-	Nenhuma
NGS2.02.17	Informações sobre assinatura	Não	Nenhuma	-	Nenhuma
NGS2.02.21	Aviso de registro pendente de assinatura	Não	Nenhuma	-	Nenhuma
NGS2.05.01	Carimbo de tempo	Não	Nenhuma	-	Nenhuma
NGS2.05.02	Verificação do carimbo de tempo	Não	Nenhuma	-	Nenhuma
NGS2.05.04	Carimbo de tempo ICP-Brasil	Não	Nenhuma	-	Nenhuma
NGS2.07.01	Impressão de registros assinados digitalmente	Não	Nenhuma	-	Nenhuma
NGS2.07.02	Impressão de mensagem de rodapé	Não	Nenhuma	-	Nenhuma

Nos requisitos não implementados, não foi possivel realizar testes, pois exigem integração com outros sistemas ou a funcionalidade requerida ainda não existe no sistema e alguns requisitos exigem a criação de manuais, segue abaixo a planilha:

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	RECOMENDAÇÃO
NGS1.02.10	Revelação de credenciais na interface de autenticação	NÃO	Nehuma	Nenhuma
NGS1.02.11	Autenticação forte	NÃO	Nehuma	Nenhuma
NGS1.02.12	Uso de SALT	NÃO	Nehuma	Nenhuma
NGS1.04.08	Acesso ao RES pelo sujeito da atenção	NÃO	Nehuma	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	RECOMENDAÇÃO
NGS1.04.10	Gerenciamento de grupos	NÃO	Nehuma	Nenhuma
NGS1.04.12	Inserção de dados pelo sujeito da atenção	NÃO	Nehuma	Nenhuma
NGS1.06.07	Confirmação de entrega	NÃO	Nehuma	Nenhuma
NGS1.06.08	Integridade e origem de componentes dinâmicos	NÃO	Nehuma	Nenhuma
NGS1.06.09	Método de autenticação de parceiro de comunicação	NÃO	Nehuma	Nenhuma
NGS1.06.10	Segregação de componentes	NÃO	Nehuma	Nenhuma
NGS1.07.01	Importação de dados	NÃO	Nehuma	Nenhuma
NGS1.07.04	Verificação de integridade dos dados	NÃO	Nehuma	Nenhuma
NGS1.07.07	Impedir reconstrução do RES	NÃO	Nehuma	Nenhuma
NGS1.07.09	Manipuladores RES	NÃO	Nehuma	Nenhuma
NGS1.07.12	Processo de importação de dados	NÃO	Nehuma	Nenhuma
NGS1.09.01	Documentação	NÃO	Nehuma	Nenhuma
NGS1.09.04	Operador de backup	NÃO	Nehuma	Nenhuma
NGS1.09.05	Restrição de acesso a entidades não autenticadas e autorizadas	NÃO	Nehuma	Nenhuma
NGS1.09.07	Configuração da segurança da comunicação entre componentes	NÃO	Nehuma	Nenhuma
NGS1.09.08	Sincronização de relógio	NÃO	Nehuma	Nenhuma
NGS1.09.09	Guarda da mídia de cópia de segurança	NÃO	Nehuma	Nenhuma
NGS1.09.10	Segregação dos componentes	NÃO	Nehuma	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	RECOMENDAÇÃO
NGS1.09.11	Importação de dados de dispositivos externos de saúde	NÃO	Nehuma	Nenhuma
NGS1.09.12	Idioma	NÃO	Nehuma	Nenhuma
NGS1.09.13	Alertas sobre configurações inseguras	NÃO	Nehuma	Nenhuma
NGS1.11.01	Interface para notificação	NÃO	Nehuma	Nenhuma
NGS1.12.02	Consentimento do sujeito da atenção	NÃO	Nehuma	Nenhuma
NGS1.12.03	Associação do consentimento à informação de saúde	NÃO	Nehuma	Nenhuma
NGS1.12.04	Acesso de emergência	NÃO	Nehuma	Nenhuma
NGS1.12.05	Propósito de uso	NÃO	Nehuma	Nenhuma
NGS1.12.06	Restrição de exportação por propósito de uso	NÃO	Nehuma	Nenhuma
NGS1.12.07	Restrições para transmissão e exportação de RES	NÃO	Nehuma	Nenhuma
NGS1.13.01	Certificado digital	NÃO	Nehuma	Nenhuma
NGS1.13.02	Atendimento à ICP-Brasil	NÃO	Nehuma	Nenhuma
NGS1.13.05	Verificação do propósito do certificado digital para autenticação	NÃO	Nehuma	Nenhuma
NGS1.13.06	Não repúdio da autenticação realizada	NÃO	Nehuma	Nenhuma
NGS1.13.07	Tipos de usuários para autenticação com certificação digital	NÃO	Nehuma	Nenhuma
NGS1.13.08	Homologação ICP-Brasil	NÃO	Nehuma	Nenhuma
NGS1.13.09	Elemento de prova da autenticação	NÃO	Nehuma	Nenhuma
NGS1.13.10	Vínculo entre Certificado Digital e	NÃO	Nehuma	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	RECOMENDAÇÃO
	Usuário			
NGS1.13.11	Compatibilidade com mídias para certificado digital	NÃO	Nehuma	Nenhuma
NGS2.01.05	Tipos de usuários para autenticação com certificação digital	NÃO	Nehuma	Nenhuma
NGS2.01.06	Compatibilidade com mídias para certificado digital	NÃO	Nehuma	Nenhuma
NGS2.02.06	Propósito da assinatura	NÃO	Nehuma	Nenhuma
NGS2.02.08	Homologação ICP-Brasi	NÃO	Nehuma	Nenhuma
NGS2.02.09	Exportação de registros assinados	NÃO	Nehuma	Nenhuma
NGS2.02.12	Validação com objeto de revogação ideal	NÃO	Nehuma	Nenhuma
NGS2.02.14	Validação e adequação da assinatura de documentos recebidos	NÃO	Nehuma	Nenhuma
NGS2.02.16	Inclusão e validação de certificado de Atributo	NÃO	Nehuma	Nenhuma
NGS2.02.18	Encadeamento de registros assinados digitalmente	NÃO	Nehuma	Nenhuma
NGS2.02.19	Verificação do encadeamento de registros	NÃO	Nehuma	Nenhuma
NGS2.02.20	Indisponibilidade da chave privada	NÃO	Nehuma	Nenhuma
NGS2.02.22	Uso dos formatos AD-RV e AD-RC	NÃO	Nehuma	Nenhuma
NGS2.02.23	Exportação de registros eletrônicos identificados	NÃO	Nehuma	Nenhuma
NGS2.02.24	Formato de assinatura em formato AdES	NÃO	Nehuma	Nenhuma

ID	TÍTULO	TESTE DE SEGURANÇA	VULNERABILIDADE ENCONTRADA	RECOMENDAÇÃO
NGS2.02.25	Compatibilidade com os dispositivos ICPBrasil	NÃO	Nehuma	Nenhuma
NGS2.04.01	Assinatura digital do sistema de GED	NÃO	Nehuma	Nenhuma
NGS2.04.02	Assinatura digital do operador	NÃO	Nehuma	Nenhuma
NGS2.04.03	Assinatura digital do responsável	NÃO	Nehuma	Nenhuma
NGS2.04.06	Termo de conduta para digitalização	NÃO	Nehuma	Nenhuma
NGS2.04.07	Homologação ICP-Brasi	NÃO	Nehuma	Nenhuma
NGS2.04.08	Certificado digital do sistema GED	NÃO	Nehuma	Nenhuma
NGS2.06.01	Configuração das fontes de autoridade	NÃO	Nehuma	Nenhuma
NGS2.06.02	Tratamento de certificado de atributo	NÃO	Nehuma	Nenhuma
NGS2.07.03	Impressão de relatório de assinaturas	NÃO	Nehuma	Nenhuma
NGS1.02.07	Autenticação para operações críticas	NÃO	Nehuma	Nenhuma

Os riscos de segurança identificados neste trabalho serão reportados a empresa para que possam analisar as recomendações.

5 CONCLUSÃO

Ao implantar o prontuário eletrônico no consultório/operadora o profissional caminha para uma informatização nos atendimentos e tem uma maior segurança na disponibilidade dos dados, pois o arquivo irá conter todos os registros de alteração e inclusão das informações, e caso o paciente solicite a impressão ou cópia para levar em um processo ou disponibilizar para outro médico de confiança o processo será mais rápido.

A informatização do prontuário poderá futuramente abastecer bancos de dados nacionais, caso o paciente permita o compartilhamento, e também poderá gerar indicadores de doenças que devem ser informadas ao Ministério de Saúde Pública ou até descobrir o diagnóstico precoce da doença.

Como pôde ser verificado ao longo deste trabalho, ter um prontuário eletrônico necessita de segurança, pois o ambiente virtual pode trazer consigo problemas que precisam ser corrigidos rapidamente, desde backup de dados, informação violada, acessos indevidos, compartilhamentos sem autorização expressa do paciente e outros.

Foi observado que o *software* MKSaude procurou atender as leis vigentes e normas necessárias para garantir a segurança, integridade e disponibilidade do prontuário eletrônico. Este *software* ainda não atende a totalidade dos requisitos das normas NGS1 e NGS2, mas está se adequando para que até a data que as leis brasileiras de proteção de dados sejam vigentes, estejam de acordo com todos os requisitos. Até a presente data, o *software* MKSaude, oferece aos seus clientes o necessário para atender as leis e está procurando tirar todas as certificações para atuar na área de saúde.

Sugere-se como trabalhos futuros, verificar como irão evoluir as leis de proteção de dados, como serão implementados programas de controle, auditoria ou certificação, assim como a atualização do NGS1 e NGS2 frente estas mudanças. Uma outra sugestão de trabalho futuro seriam estudos para buscar novas ferramentas de teste que consiga validar todos os requisitos e se possível fazer uma validação mais robusta, incluindo a validação dos aspectos de segurança sobre o código fonte. Além destes temas, outra recomendação

de trabalho futuro seria criar manuais de boas práticas para desenvolvimento seguro para a área de saúde.

6 REFERÊNCIAS

1821/07, R. C. (23 de Novembro de 2007). h*ttp://www.portalmedico.org.br/resolucoes/cfm.* Acesso em: 23 de Nov. de 2018, disponível em http://www.portalmedico.org.br: http://www.portalmedico.org.br/resolucoes/cfm/2007/1821_2007.htm

ABNT NBR ISO/IEC 27002:2007. (2007). *Código de prática para a gestão da segurança da informação.* Rio de Janeiro. Acesso em: 23 de Mar. de 2019, disponível em http://www.cienciianasnuvens.com.br/site/wp-content/uploads/2014/09/215545813-ABNT-NBR-177991.pdf

ABNT NBR ISO/IEC 27001:2013. (2013). *Sistemas de gestão da segurança da informação - Requisitos.* Rio de Janeiro. Acesso em: 23 de Mar. de 2019

Charles Sabatino, J. D. (s.d.). *https://www.msdmanuals.com*. Acesso em: 23 de abr. de 2019, disponível em msdmanuals: https://www.msdmanuals.com/pt-br/casa/fundamentos/questões-éticas-e-jurídicas/confidencialidade-e-hipaa

Conselho Federal de Medicina. (s.d.). Acesso em 13 de Maio de 2019, disponível em portalmedico: http://www.portalmedico.org.br/novocodigo/integra_9.asp

CFM. (23 de novembro de 2007). *portalmedico*. Acesso em: 05 de Maio de 2019, disponível em http://www.portalmedico.org.br/resolucoes/cfm/2007/1821_2007.pdf

Da Agência Estado. (28 de 07 de 2015). *https://noticias.uol.com.br/tecnologia/noticias/redacao*. Acesso em 13 de Mar. de 2019, disponível em uol.com.br: https://noticias.uol.com.br/tecnologia/noticias/redacao/2015/07/28/site-tudo-sobre-todos-afirma-que-so-divulga-informacoes-publicas.htm

Diretoria Colegiada da Agência Nacional de Saúde Suplementar - ANS,. (09 de Outubro de 2012). RESOLUÇÃO NORMATIVA - RN Nº 305. *RESOLUÇÃO NORMATIVA - RN Nº 305*. Brasil. Acesso em: 24 de Abr. de 2019, disponível em http://www.ans.gov.br/component/legislacao/?view=legislacao&task=TextoLei&format=raw&id=MjI2OA==

Equipe Conexão. (31 de outubro de 2017). Em que casos é possível a quebra do sigilo médico? *Em que casos é possível a quebra do sigilo médico?* Acesso em: 23 de Abr. de 2019, disponível em: http://conexao.segurosunimed.com.br/em-que-casos-e-possivel-a-quebra-do-sigilo-medico/

Folha de São Paulo. (22 de março de 2018). Acesso em 12 de Mar. de 2019, disponível em https://www1.folha.uol.com.br: https://www1.folha.uol.com.br/mercado/2018/03/entenda-o-escandalo-do-uso-de-dados-do-

facebook.shtml?loggedpaywall&fbclid=IwAR2Bj4nUgfNb67_HFoy5ctigcTmk7HhKsS9_2vT8DDQqA0WoDKDqXmy4C1o

Gestão da Clinica. (23 de março de 2017). Afinal, o que é o prontuário eletrônico? Acesso em: 05 de Maio de 2019, disponível em https://medicalbox.com.br/blog/afinal-o-que-e-o-prontuario-eletronico/

Instituo Nacional de Tecnologia da Informação. (27 de junho de 2017). *ICP-Brasil*. Acesso em: 05 de Maio de 2019, disponível em https://www.iti.gov.br/icp-brasil

Jornal Oficial da União Europeia. (27 de abril de 2016). *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO.* União Europeia. Acesso em: 13 de Mar. de 2019, disponivel em https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT

Manual_Certificacao_SBIS-CFM_2016_v4-2. (14 de Junho de 2016). *http://www.sbis.org.br/certificacao*. Acesso em: 19 de Nov. de 2018, disponível em http://www.sbis.org.br: http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2016_v4-2.pdf

MKDATA. (s.d.). Acesso em: 11 de Maio de 2019, disponível em https://MkDATA.com.br

Paulo, A. L. (19 de Dezembro de 1952). *Dispõe sôbre a criação do conselho Estadual de Assistência Hospitalar, na Secretria da Saúde Pública e da Assistência Social, e dá outras providências.* Acesso em: 23 de Nov. de 2018, disponível em https://www.al.sp.gov.br: https://www.al.sp.gov.br/repositorio/legislacao/lei/1952/lei-1982-19.12.1952.html?fbclid=IwAR28758VMdKnumTLVs3otYqEDH7KXwwQauhUx7v3d3VSvHhrrswxlpyloFg

Qualidade, G. d. (s.d.). *gestao-de-qualidade.info/normas-iso.html*. Acesso em: 23 de Mar. de 2019, disponível em gestao-de-qualidade.info: http://gestao-de-qualidade.info/normas-iso.html

Tiinsideonline. (06 de 09 de 2007). Um nova abordagem em qualidade e segurança de *software* Brasil. Acesso em: 02 de Novembro de 2019, disponível em https://tiinside.com.br/tiinside/06/09/2007/um-nova-abordagem-em-qualidade-e-seguranca-de-software/

SBIS. (s.d.). Manual de Certificação para Sistemas de Registro Eletrônico em Saúde. *Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, Versão 4.3*. Brasil. Acesso em: 24 de Abr. de 2019. Fonte: http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2019_v4-3.pdf

7 ANEXO

TERMO DE AUTORIZAÇÃO DE USO DO NOME EMPRESARIAL E DO PRODUTO

Eu, **Sérgio Augusto Morgan**, portador(a) da Cédula de Identidade RG nº 15.234.513-9, inscrito(a) no CPF/MF sob o nº 101.954.418-00, representante legal da empresa **M.M Ferraz Costa Software Ltda**, com nome fantasia de **MKDATA**, inscrita no CNPJ/MF sob nº 10.971.519/0001-70, localizada na Avenida Campos Sales, 420 – Sala 23, Jardim Girassol, no município de Americana/SP, **autorizo o uso do software e do nome da empresa** para a pesquisa de Trabalho de Conclusão do Curso, *sob o título "Segurança de Software para a Área de Saúde: Uma avaliação dos requisitos de segurança aplicada em software de Registro Eletrônico em Saúde"* da funcionária **Jéssica Oliveira Muniz.**

Americana, 11 de dezembro de 2019.

M.M Ferraz Costa Software Eireli ME
CNPJ: 10.971.519/0001-70

Sérgio Augusto Morgan
Telefone para contato: (19) 9.8109-4691
E-mail: sergio.morgan@mkdata.com.br