Segurança da Informação para um Sistema de Anamnese Neurológica Infantil (Hestia)

Palavras-Chave: POLÍTICA DE SEGURANÇA, LGPD, PROPOSTA DE ARQUITETURA.

Autores/as:

Juliana Almeida Morroni - Unicamp

Prof. Dr. André F. de Angelis (Orientador) – Unicamp

INTRODUÇÃO

Sistemas médicos estão entre aqueles que manipulam dados pessoais sensíveis e devem receber proteção adequada, segundo a Lei Geral de Proteção de Dados (LGPD).

Um projeto conjunto da Faculdade de Ciências Médicas (FCM) e do Centro Superior de Educação Tecnológica (Ceset, atual FT), com apoio da FAPESP, desenvolveu o Sistema Hestia [1] para anamnese neurológica infantil, entre 2003 e 2007, atendendo às necessidades dos ambulatórios da área na Unicamp e auxiliando APAEs e médicos no país.

O Hestia tem como principal ponto forte o conjunto único de indicadores que registra, definido após um longo trabalho de pesquisa e adaptação das práticas médicas ao cenário brasileiro. Na época de sua criação, tinha como diferencial em relação a programas de mesmo propósito a utilização de uma interface gráfica para o usuário. Adicionalmente, fazia uso de um Sistema Gerenciador de Banco de Dados (SGBD), característica que permitia um nível sem precedentes de consultas de informação para diagnóstico e pesquisa médica.

Sua última atualização foi feita em 2006 e, desde então, houve mudanças significativas nas tecnologias de redes, bancos de dados e programação, assim como nos requisitos dos sistemas médicos e nas demandas legais, particularmente com as resoluções do Conselho Federal de Medicina e a LGPD. Logo, uma nova versão se faz necessária. No entanto, deseja-se um redesenho completo do sistema para que possa usufruir dos recursos tecnológicos atuais, especialmente a computação em nuvem e a comunicação pela Internet. Para o desenvolvimento dessa almejada atualização, é necessária uma arquitetura de segurança robusta e bem definida para o sistema.

Este projeto de Iniciação Científica teve por objetivo estudar a questão e definir uma proposta de arquitetura de segurança (AS) para subsidiar a criação de novas versões do Sistema Hestia.

METODOLOGIA

Pesquisas e levantamento bibliográfico foram feitos para se obter conhecimento, consolidar normas, leis e recomendações técnicas para que a ferramenta atenda diretrizes de segurança de sistemas médicos, em especial à LGPD [2], às Resoluções CFM 1.821/2007, 2.227/2018 e 2.056/2013 do Conselho Federal de Medicina, à norma ABNT NBR ISO/IEC 27002:2013 [3] e à *Health Insurance Portability and Accountability Act* (HIPAA – Lei de portabilidade e responsabilidade de provedores de saúde) (USA) [4]. Atenção particular foi dada aos conceitos de privacidade, criptografia, banco de dados e métodos de arquitetura de sistemas [5, 6].

Testes de execução do Hestia foram feitos em bancada, com objetivo de inspeção do tráfego de rede gerado pelo sistema.

Houve uma série de dificuldades intransponíveis em função da virtualização do ambiente de teste e nem todas as observações pretendidas se efetivaram.

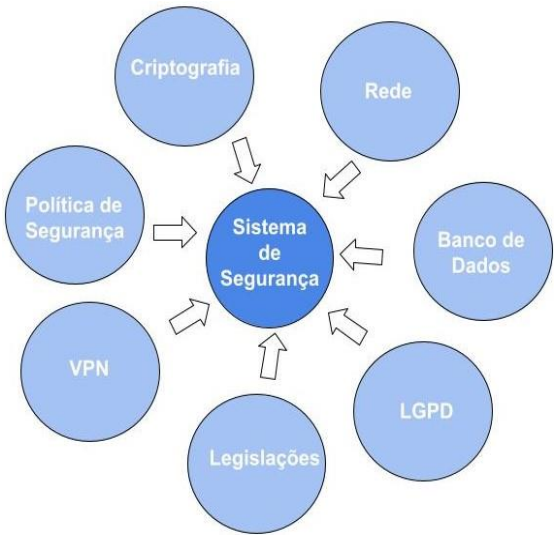
A partir dos levantamentos feitos, preparou-se uma proposta para a AS do Hestia, dividida em seções de recomendações: para o sistema em si, para a rede e para o banco de dados. A proposta também indica a necessidade de uma política de segurança. Elaborou-se um documento próprio com a proposta, que está disponível em *https://github.com/jumorroni/Proposta-de-Arquitetura-para-o-sistema-Hestia*.

disponibilizado em repositório público e permanente.

RESULTADOS E DISCUSSÕES

O resultado deste projeto é um documento com a proposta de uma AS específica para novas versões do Hestia. A seguir, são discutidos alguns pontos desta proposta.

Figura 1: Elementos envolvidos na AS proposta



Fonte: Juliana Almeida Morroni (2021)

Os dados sensíveis contidos no Hestia devem ser protegidos em seu armazenamento, transferência, consulta e também precisam ser acessados por pessoas de direito. Logo, deve-se manter o uso de um conjunto de recursos de segurança da informação, dado que nenhum componente isoladamente pode garantir um nível de segurança adequado. Com base nisso, o sistema deve atender aos seguintes requisitos:

Sistema

Foi proposta uma AS que para um sistema seguro, que atenda às normas e legislações aqui elencadas, com uma política de segurança adequada. Ela requer elementos como criptografia de banco de dados, rede *Virtual Private Network* (VPN) e outros elementos, como exemplificados na Figura 1. Em função dos requisitos do sistema, é exigida uma interface gráfica de usuário, a ser definida conforme o ambiente de execução, prevendo-se o caso de uso em dispositivos móveis.

Rede

A AS proposta prevê a utilização de uma VPN, esquematicamente exemplificada na Fig. 2, para criar uma rede de comunicações entre computadores e outros dispositivos que possuem acesso restrito a quem possui as credenciais necessárias, pois a passagem de dados sensíveis pela Internet somente se torna possível com o uso de alguma tecnologia que torne esse meio altamente inseguro em um meio confiável.

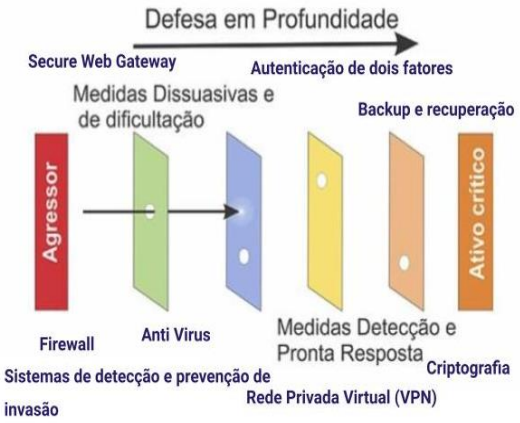
Figura 2: Representação de uma Rede Virtual (VPN)

Fonte: vpnconfiavel.com

Junto a isso, um modelo de Defesa em Profundidade também é proposto para fins adicionais à segurança, pois uma camada única pode não ser eficaz diante da evolução rápida e inteligente dos ataques cibernéticos.

A estratégia de defesa em profundidade (Fig. 3) constrói uma rede mais segura com a implementação de camadas e até a duplicação de certos métodos de proteção para minimizar a probabilidade de vazamentos e exploração de vulnerabilidades. Essas vulnerabilidades podem ser físicas, de hardware, software, de comunicação e humanas.

Figura 3: Defesa em profundidade e seus elementos propostos



Fonte: gestãodesegurancaprivada.com.br

À vista disso, ao implementar uma série de defesas diferentes, podem ser cobertas brechas que existiriam caso se dependesse somente de uma camada de segurança. São exemplos das defesas:

✓ Firewall;

✓ Criptografia;

✓ Autenticação de usuário;

✓ Garantir conexão segura Fim-a-Fim;

✓ Restrição no uso de redes sem fio.

Banco de Dados

A seguir, serão apresentadas as questões relativas à proteção dos bancos de dados para o sistema, divididas em seções sobre criptografia, controle de acesso e backup.

Criptografia: A LGPD exige que medidas de segurança e salvaguardas sejam impostas e destaca a necessidade do uso de mecanismos técnicos e organizacionais adequados de segurança, como métodos de criptografia de banco de dados e iniciativas para o desenvolvimento seguro. [7]

A criptografia é uma técnica bastante utilizada para proteger dados e informações que devem estar em sigilo, pois possuem valor em seu conteúdo. E por meio dela, é possível evitar que pessoas não autorizadas tenham acesso a esses dados armazenados.

O Hestia em sua atual versão utiliza o SGBD Interbase (opcionalmente, o Firebird). Alternativas para próximos desenvolvimentos são: o SQL-Server, MySQL e Oracle, visto que todos contam com criptografia de dados em repouso.

Controle de Acesso: Uma vez que os requisitos de segurança da informação e os riscos possíveis sejam identificados, convém que controles pertinentes sejam selecionados e executados para assegurar a redução desses riscos a um nível aceitável. Como o gerenciamento de usuários.

Gerenciamento de usuários consiste na tarefa de realizar o controle e verificação de pessoas envolvidas e que interajam com o sistema, bem como: Grupo de permissões de acesso aos recursos oferecidos; Dispositivos; Sistemas de armazenamento (banco de dados); Redes; etc.

Por se tratar de questões de confidencialidade (um dos pilares da LGPD), esse gerenciamento se torna algo fundamental e imprescindível. O nível de controle de acesso influencia diretamente na vulnerabilidade à brechas de segurança. Portanto, quanto mais reforçado, mais difícil será a invasão do sistema. Os elementos para se aplicar esse controle são: processo de autenticação, autorização e auditoria.

Backup: A importância das cópias de segurança está na proteção contra o risco de perda de dado. Essa importância aumenta

proporcionalmente em relação ao valor das informações a serem protegidas.

O Backup manual sempre oferece mais riscos, pois está sujeito a falhas humanas diversas, como esquecimento, armazenamento indevido ou até mesmo conhecimento técnico insuficiente. Por isso, as melhores práticas recomendam automatizá-lo, de modo que ocorra de forma recorrente. Há diversas ferramentas de automação no mercado, que oferecem, além da programação das cópias, a criptografia dos dados.

Uma alternativa para atualizações é a cópia ou a operação direta em nuvem, que propõe a automatização das rotinas de cópias de segurança. Para utilizar este método, deve-se antes fazer um diagnóstico que aponte o espaço de armazenamento necessário, pois é isso que contratos em nuvem levam em conta: preservar as informações quanto à integridade, confidencialidade e disponibilidade.

Dependendo do sistema de backup utilizado, os dados serão automaticamente armazenados e protegidos na nuvem e poderão ser recuperados sempre que necessário.

Política de Segurança

Uma Política de Segurança (PSI) é composta por regras que ditam o acesso, o controle e a transmissão da informação numa organização. Ela define o que é permitido e o que é proibido e deve conter regras e diretrizes que orientem os colaboradores, e usuários com relação aos padrões de comportamento ligados à segurança da informação. [8]

Para a realização da PSI da ferramenta Hestia, deve ser considerada a aplicabilidade a todos os seus usuários: médicos, especialistas, pesquisadores do ramo e colaboradores de TI.

CONCLUSÕES

Este projeto tem o intuito de contribuir para o desenvolvimento de um sistema distribuído de anamnese neurológica infantil de alto nível. Foi elaborada uma proposta de AS que traz recomendações para conformidade com normas atuais de segurança, sendo um guia útil para os desenvolvedores da próxima versão do Sistema Hestia.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANGELIS, André F. **Projeto Hestia.** 2006 Disponível em: <https://sites.ft.unicamp.br/hestia/>. Acesso em: 06 de março de 2020.

[2] BRASIL. LEI nº 13.709, de 14 de agosto de 2018.

[3] ABNT ISO 27002. (2013). ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR/ISO/IEC 27002:2013 tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação.

[4] HIPAA. AWS, 2021. Disponível em:<https://aws.amazon.com/pt/compliance/hipaa-compliance/>. Acesso em:13 de dezembro de 2021.

[5] BASTA, Alfred e BROWN, Mary. **Segurança de computadores e teste de invasão.** 2ª Ed. Editora Cengage Do Brasil, 2014. p 173.

[6] RIBEIRO, Cristiano. **Segurança da Informação**: o desenvolvimento de uma política de segurança da informação em conformidade com a norma ABNT *ISO/IEC* 27002. Ano 2016. 35 páginas. Trabalho de Conclusão de Curso de Sistema de Informação – FAIR Faculdades Integradas de Rondonópolis.

[7] **William Stallings**. 2007. Criptografia e Segurança de Redes: Princípios e Práticas – 4ª Edição.

[8] SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva - 2 ed**. São Paulo: Elsevier, 2014.