Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

IMPLANTANDO CONTROLES DE SEGURANÇA EM UM SISTEMA DE LOUSA ELETRÔNICA PARA HOSPITAIS

DEPLOYING SECURITY CONTROLS IN AN ELECTRONIC WHITEBOARD SYSTEM FOR HOSPITALS

Alisson Lopes de Sousa Freitas [1]
Luciana Andreia Fondazzi Martimiano [1]
Heloise Manica Paris Teixeira [1]

Resumo: Sistemas de informação em saúde gerenciam dados vitais sobre tratamento de pacientes, portanto é fundamental planejar ações no sentido de garantir confidencialidade, integridade e disponibilidade das informações. O sistema de lousa eletrônica denominado SHAVI (*SHared VIew*) foi desenvolvido para o setor de emergência do Hospital Universitário da cidade de Maringá-PR. O sistema provê o armazenamento e a gestão de informações sobre as atividades desenvolvidas pela equipe de saúde do hospital, mostrando informações e alertas importantes em uma lousa eletrônica. Nesse contexto, o principal objetivo deste trabalho foi o estudo e a implantação de controles de segurança para o sistema SHAVI, com vistas às recomendações ISO 27799:2008 e PoSIC/MS, que são voltadas para a área da saúde. A implantação dos módulos de segurança contribui no sentido de melhorar a segurança e confiança da informação utilizada para o atendimento de pacientes na unidade de emergência do hospital.

Palavras-chaves: Sistema de Informação em Saúde; Lousa Eletrônica em Hospitais; Controles de Segurança.

Abstract: *Health information systems control essential data about patient treatment, so it is fundamental to plan actions in order to assurance information confidentiality, integrity and availability. The electronic whiteboard system named SHAVI (SHared VIew) was developed to the emergency department of the University Hospital of Maringá-PR. The system provides storage and management of the information about the activities developed by the hospital's health team, showing important information and alerts on the electronic whiteboard. In this context, the main objective of this work was the study and deployment of security controls for the SHAVI system, based on the recommendations ISO 27799: 2008 and PoSIC/MS, which are focused on health area. The deployment of security modules contributes to improving security and reliability of the information used to care for patients in the hospital emergency unit.*

Keywords: *Health Care Information Systems; Whiteboard in Hospital; Security Controls.*

[1]*Universidade Estadual de Maringá, Campus Sede – Brasil, email:*
alissonlopes3@gmail.com, lafmartimiano@uem.br, hmpteixeira@uem.br

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

1 Introdução

Em Sistemas de Informação em Saúde (SIS), em que os dados gerenciados devem ser confiáveis, confidenciais e íntegros, é de grande relevância a implantação de mecanismos de segurança, que deve ser planejada e realizada seguindo as melhores práticas e protocolos recomendados por organizações na área da saúde. Os SIS são utilizados por especialistas no tratamento dos pacientes na tomada de decisão médica, portanto, a falta de confidencialidade, integridade e disponibilidade dos dados e informações pode levar a erros, dificuldades e atrasos no atendimento aos pacientes.

A ISO 27799:2008 (ISO/EIC, 2008) é a norma que define controles para apoiar a gestão da segurança nas organizações da área da saúde. Ela descreve várias recomendações, que devem ser seguidas tanto por desenvolvedores, por responsáveis pela implementação e manutenção de um SIS, como pelos usuários do sistema. Outra referência é a Política de Segurança da Informação e Comunicações do Ministério da Saúde (PoSIC/MS), regulamentada pela Portaria n° 271, de janeiro de 2017 (SAÚDE, 2017). Estudar e aplicar processos de segurança são essenciais para garantir que as informações sejam usadas com confiança pelos profissionais de saúde em suas atividades.

Este artigo apresenta os resultados obtidos no estudo de normas, planejamento e implantação de controles de segurança em um SIS. O sistema, denominado SHAVI (*SHared VIew*), foi desenvolvido com base no setor de emergência do Hospital Universitário de Maringá (HUM) e possui como principais funcionalidades o armazenamento e a organização dos dados e informações do trabalho realizado pela equipe de saúde para que possam ser apresentadas e compartilhadas em uma lousa eletrônica (ROECKER et al. 2014).

Os principais objetivos foram estudar as normas e implantar controles de segurança para o sistema SHAVI, no sentido de propiciar a disponibilidade de informação íntegra e consistente para os usuários do sistema. Para descrever o trabalho realizado, o artigo está organizado como segue. A Seção 2 apresenta o referencial teórico e descreve recomendações de segurança para um SIS. Na Seção 3 são descritos os procedimentos metodológicos e na Seção 4 as etapas do desenvolvimento deste trabalho. Finalmente, na Seção 5 são apresentadas as considerações finais.

2 Referencial Teórico

2.1 Ética e Segurança da Informação na área da Saúde

De acordo com Pereira, Paiva e Souza (2012), a confidencialidade, a integridade e a privacidade das informações devem ser garantidas em qualquer sistema de informação, principalmente na área da saúde. Para a implantação da segurança nestes sistemas, são constantemente desenvolvidos ou atualizados documentos que definem boas práticas e normas que determinam regras e orientações que devem ser seguidas (ISO/IEC, 2008; Saúde, 2017).

A norma ISO 27799:2008 (ISO/IEC, 2008) define requisitos mínimos e essenciais para a proteção de informações pessoais de saúde de qualquer organização voltada para essa área. No Brasil, o Ministério da Saúde publicou a Política de Segurança da Informação e Comunicações, denominada PoSIC (SAÚDE, 2017). O objetivo da PoSIC é garantir mais segurança no processamento, armazenamento e comunicação de dados. Uma das principais abordagens é a conscientização dos usuários sobre a importância de se seguir as regras de segurança estabelecidas. No entanto, além da conscientização, vários outros fatores

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

influenciam na segurança de qualquer sistema de informação, como por exemplo, a ética dos usuários, o tratamento das informações, a classificação das informações, entre outros.

Além da adoção de tecnologias para garantir a segurança, os usuários do sistema também devem respeitar as regras definidas pela organização. Nesse contexto, a ética é um fator importante, e segundo Salvador e Almeida Filho (2005) é entendida como uma meditação sobre o comportamento humano. Os autores destacam que o profissional de saúde, que tem qualquer tipo de contato com dados e informações (recebe, registra, manipula, digita, armazena e processa), é responsável pela sua guarda e integridade e deve estar atento para preservar e assegurar a privacidade da pessoa cujos dados estão sendo manuseados. Portanto, a segurança da informação na área de saúde também é um dever do profissional, que é usuário de um sistema.

O trabalho de Goldschmidt et al. (2019) caracteriza Segurança da Informação na comunicação de dispositivos médicos (destinados a fins de diagnóstico, prevenção, controle ou tratamento de doenças) com o objetivo de identificar como a segurança é tratada. Para atingir o objetivo, os autores apresentam uma revisão quasi-sistemática da literatura e discutem os principais desafios detectados nos últimos anos, tais como questões sobre impacto na segurança, vulnerabilidade, autenticação, entre outras.

A pesquisa de Bortman e outros (2018) discute a necessidade de estudar se a legislação brasileira é suficiente e eficiente para garantir a segurança das bases de dados existentes na rede mundial de computadores. Segundo os autores, é importante ocorrer fiscalização constante para o cumprimento da Lei, que é vasta e suficiente para determinar a proteção dos dados pessoais de pacientes.

2.2 Recomendações da ISO 27799:2008

As recomendações da norma ISO 27799:2008 tiveram como base a norma ISO/IEC 27002, que estabelece diretrizes e princípios gerais para a melhoria da gestão de segurança da informação em uma organização. A ISO 27799:2008 define um conjunto de controles para gerenciar segurança na área da saúde. Descreve também um plano com orientações para a implementação dos controles. A seguir são descritas as principais orientações.

- **Política de segurança:** Deverá ser desenvolvida e comunicada a todos os empregados e partes externas relevantes. Nela deverá conter a necessidade da segurança da informação em saúde, os objetivos da segurança, responsabilidades legais e éticas para os profissionais da saúde protegerem as informações, e definição de um canal confidencial para notificação de incidentes de segurança da informação. Para a construção dos documentos, alguns fatores deverão ser considerados, como as responsabilidades e direitos das pessoas, as obrigações de quem obtém as informações, os limites das pessoas com acesso temporário, voluntário e permanente.
- **Segurança dos recursos humanos:** Todos os envolvidos na gestão da informação da saúde devem documentar seu envolvimento e devem ter no mínimo a identidade, o endereço atual e o emprego prévio documentados.
- **Rescisão ou mudança de emprego:** Deve ser realizado o mais breve possível o cancelamento do acesso de qualquer pessoa, seja ela permanente ou temporário, contratante de terceiros ou voluntário, no momento da cessação do emprego.
- **Proteção contra códigos maliciosos (*malwares*):** Deve-se implementar controles para a prevenção, detecção e resposta de softwares maliciosos, bem como

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

treinamentos adequados de conscientização dos usuários. Deverá também ser realizado um *backup* de todas as informações do SIS.

- **Monitoração:** Todos os SIS devem criar um registro de auditoria toda vez que o usuário acessar ou criar um arquivo. Esse registro deve identificar unicamente o usuário, identificar a função realizada por ele e observar a hora e a data em que a função foi executada. Quando informações referentes à saúde forem atualizadas, deve ser feito um registro contendo as informações anteriores e as informações atualizadas.
- **Controle de acesso:** Deve ser implementado um controle de acesso às informações. Os usuários deverão acessar informações pessoais da saúde apenas: (i) quando existe uma relação entre o usuário e o titular dos dados; (ii) quando o usuário exerce uma atividade em nome da pessoa dos dados; e (iii) quando houver a necessidade de dados específicos para apoiar uma atividade. Para registrar e identificar um usuário do sistema de saúde é preciso: captura precisa da identidade (por exemplo, Gustavo Almeida); captura da credencial e/ou cargo (Susan Freitas, recepcionista); e atribuição de um identificador. Para garantir a confidencialidade e a integridade das informações, bem como os privilégios de acessos, podem ser usadas algumas estratégias: o controle de acesso baseado na função, para restringir o acesso privilegiado às informações; o controle de acesso baseado no grupo de trabalho (como clínicas) para determinar quais dados podem acessar; o controle de acesso discricionário, que identifica quem tem uma legítima relação com o sujeito de cuidado (como um médico da família) para garantir acesso a dados que outro usuário que não tem essa relação. Os usuários que possuem mais de uma função deverão optar por uma única função à cada sessão de acesso.
- **Identificação dos pacientes**: Os pacientes devem ser identificados de forma única. O sistema deve ser capaz de reunir registros múltiplos ou duplicados do mesmo paciente que foram criados involuntariamente ou durante uma emergência médica. Deve-se assegurar que os dados do paciente identificado podem ser obtidos somente se necessário, e que a eliminação, anonimização (processo que torna o sujeito anônimo, não permitindo sua re-identificação) e pseudonimização (processo que permite a identificação da pessoa pelas suas características sem que realmente se saiba quem ele é) sejam utilizadas de forma adequada para minimizar a divulgação não intencional de dados. Informações pessoais de saúde não devem ser usadas como dados de testes.

2.3 Recomendações da PoSIC/MS

A Política da Segurança da Informação e das Comunicações tem como um de seus principais objetivos estabelecer diretrizes a serem seguidas pelo Ministério da Saúde no que diz respeito à adoção de normas e procedimentos relacionados à segurança da informação e comunicações. As principais diretrizes da política são:

- **Propriedade da informação:** Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação vai ser utilizada deverá providenciar a documentação relativa à cessão de informações de terceiros.
- **Tratamento da informação:** A classificação da informação é atribuição do gestor da informação. As informações serão criptografadas de acordo com sua classificação, em especial as informações de autenticação dos usuários.

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

- **Auditoria e Conformidade:** Sempre que possível, serão utilizados softwares específicos para monitoramento e rastreamento do uso dos SIS.
- **Controles de Acesso:** Os usuários terão uma conta de acesso única e intransferível. Fica a cargo do gestor a concessão e revogação dos privilégios de acesso às informações e a identificação deve ser pessoal e intransferível.
- **Preservação de evidência:** Todos os equipamentos e/ou ativo de informação devem ser configurados para armazenar registros históricos de eventos (*logs*). Os logs devem ser armazenados pelo período mínimo de seis meses. Os registros de auditoria devem ser armazenados localmente e também remotamente.

2.4 Sistema SHAVI

No ambiente de emergência hospitalar, cada profissional percebe e interpreta sua atividade individual conforme sua especialidade, porém, na tomada de decisão devem ser consideradas todas as atividades da equipe. Assim, as lousas tradicionais (quadros manuais) estão sendo substituídas pelas digitais (ARONSKY et al., 2008).

A unidade de emergência do Hospital Universitário de Maringá (HUM) de Maringá é composta por um variado grupo de pessoas, especialidades, artefatos, doenças, condições, protocolos, emergências, e outros. Os profissionais de enfermagem, médicos e nutricionistas serão os principais usuários do sistema. A equipe médica, ao realizar o diagnóstico do paciente, prescreve os cuidados necessários (dietas, medicamentos e outros). A equipe de enfermagem realiza as tarefas de sua competência em três salas da unidade de emergência do hospital, de acordo com a prescrição médica de cada paciente. Já a equipe de nutrição administra as dietas, também em conformidade com a prescrição médica.

O sistema SHAVI tem como metas principais o gerenciamento de tarefas, a atualização e o acesso rápido às informações pelos profissionais (ROECKER et al., 2014). Os dados produzidos nos atendimentos de urgência e emergência são gerenciados por meio de 11 módulos: paciente, clínica, leito, internação, prescrição médica, prescrição de enfermagem, relatório de enfermagem, evolução de enfermagem, lembrete, plano assistencial e o módulo da lousa eletrônica. O módulo lousa eletrônica é o responsável por selecionar e mostrar as informações mais relevantes para o atendimento dos pacientes.

A arquitetura geral do sistema, ilustrada na Figura 1, foi definida segundo o modelo cliente-servidor, como um conjunto de componentes clientes, que realizam requisições a serviços por meio de um protocolo comum; e servidores, que disponibilizam interfaces e serviços. A arquitetura é organizada em camadas hierárquicas, que limitam o comportamento de tal forma que cada componente não pode “ver” o contexto além da camada com a qual ele interage.

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

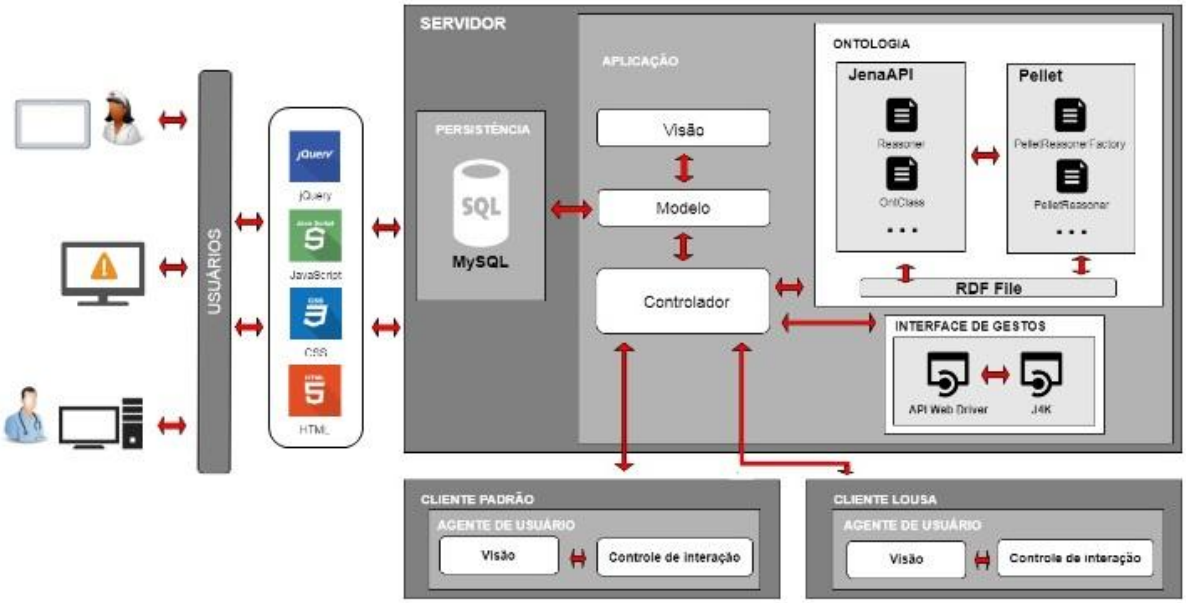

Figura 1. Arquitetura Geral do Sistema

O servidor, composto por dois principais componentes, persistência e aplicação, gerencia o acesso a recursos que são compartilhados entre os clientes. Para persistência das regras de negócio, utilizou-se o sistema gerenciador de banco de dados relacional *MySQL Server*, enquanto que dados multimídia são armazenados por meio do sistema de arquivos local no sistema operacional.

Provisoriamente, os dados estão centralizados em um servidor local, no entanto, após a implantação do sistema, deverá ser utilizado mais um servidor (replicação), desta forma, no caso de falhas, a disponibilidade dos dados seja garantida.

A aplicação fornece um serviço aos clientes por meio de requisições. Este subcomponente é composto de três camadas: o Modelo, o Controlador e a Visão; sua organização arquitetural interna é formada por um híbrido entre os estilos arquiteturais em camadas e MVC (*Model-View-Controller*). A implementação foi feita utilizando tecnologias da *Java™ Enterprise Edition* (Java EE), devido à grande variedade de soluções com licença de uso livre. Foi utilizado o *Apache Tomcat* como container de aplicação.

Os códigos pertencentes ao subcomponente Modelo referem-se às regras de negócio do sistema, tais como restrições dos dados, relacionamento de entidades e controle de acesso e armazenamento. É também responsável por se comunicar com os módulos conectores de persistência. Para sua implementação foi utilizada a especificação *Java™ Persistence API 2.0* (JPA).

O Controlador é responsável por mapear uma requisição para uma funcionalidade disponível na interface do modelo e também para uma representação da camada de visão, retornando a resposta ao cliente. De forma geral, todo o código pertencente ao Controlador foi implementado como *Java™ Servlets*.

A camada Visão transforma os dados adquiridos de um modelo em uma representação que será transmitida como resposta ao cliente requisitante. A implementação foi feita utilizando-se *Java™ Server Pages* (JSP) com HTML (*HyperText Markup Language*), e a biblioteca Google Gson com JSON (*JavaScript Object Notation*).

Os componentes clientes da arquitetura, Cliente Padrão e Cliente Lousa, possuem várias características arquiteturais em comum. Ambos são formados por um subcomponente Agente de Usuário, definido como qualquer software que age em nome do usuário para o

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

acesso ao sistema, sendo definido na implementação como um navegador Web. Ambos os clientes também possuem estrutura interna organizada em um estilo derivado da Arquitetura em Camadas, composto pelas camadas de Visão e Controle de Interação.

3 Procedimentos Metodológicos

Para o desenvolvimento da pesquisa, em uma primeira etapa foram estudadas as recomendações da ISO 27799:2008 e da PoSIC, e também o ambiente do hospital onde o sistema SHAVI será implantado. Também foram considerados o perfil e o tipo de tarefas desenvolvidas pelos principais usuários do sistema (técnicos, enfermeiros, médicos, nutricionistas, dentre outros).

Com base no estudo, foram implantados os seguintes módulos de segurança: controle de acessos, geração e armazenamento de *logs* de auditoria, *backups* e filtro de pacotes (firewall). Para cada módulo, foram estudadas diversas ferramentas e selecionada àquela que melhor atendesse os requisitos de segurança do sistema e do ambiente em que ele será implantado. Para escolha de cada ferramenta foram considerados fatores como integração com a linguagem Java, facilidade de uso (configuração), licença gratuita, dentre outros. Os softwares utilizados foram: IDE Netbeans 8.0.2, MySqlBackupFTP, Backup MySQL, FBackup, Uranium Backup Free, ZoneAlarm Free Firewall e o Comodo Firewall.

4 Desenvolvimento

O desenvolvimento dos módulos de segurança foi baseado nas recomendações da ISO 27799:2008, da POSIC/MS e de Salvador e Almeida Filho (2005). Para que seja possível definir os controles implementados no sistema, é importante conhecer quais são os riscos que devem ser gerenciados e mitigados. A seguir são descritos os riscos potenciais que podem ocorrer e os controles de seguranças que foram implantados no sistema do Hospital.

1. **Riscos:** Perda de dados devido a erros de hardware e *malwares* (códigos maliciosos); Roubo de dados; Roubo dos equipamentos de armazenamento das bases de dados e dos servidores; Erros do sistema; Tentativa de acesso indevido aos serviços e dados do sistema; Tentativa de acesso ao datacenter ou local onde estão os servidores e demais equipamentos; Tentativas de explorar vulnerabilidades; Tentativas de invasão; Erros do sistema; Tentativas de scanning; Tentativas de envio de *malwares*; Tentativas de personificação e spoofing; Tentativa de quebra de senhas por força bruta.
2. **Controles de Segurança:** *Backups*; *Logs* de Auditoria; Firewalls; Manutenção preventivas nos equipamentos; Atualizações constantes; Controle de acesso; Unicidade de Identificação; Criptografia das senhas armazenadas e/ou enviadas via Rede.

A Tabela 1 apresenta os principais controles desenvolvidos, levando em consideração os riscos. A primeira coluna resume os principais controles de segurança que devem ser implementados em um sistema da área da saúde, a segunda descreve as características do controle implementado no sistema e a terceira indica a ferramenta utilizada.

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

Tabela 1 – Controles X Implementação no Sistema

Controle (ISO 27799:2008 e POSIC/MS)	**Implementação**	**Ferramenta Utilizada**
1. Realizar backup de todas as informações do SIS.	Backup dos arquivos e banco de dados. Ferramentas estudadas: Uranium Backup e FBackup.	Uranium Backup.
2. Implementar controle de firewall.	A prevenção, detecção e resposta de *malwares* ficará a cargo de um software específico de firewall. Ferramentas estudadas: Comodo Firewall e o ZoneAlarm Free Firewall.	Comodo Firewall.
3. Criar *logs* de auditoria.	O registro dos eventos é realizado desde a entrada até a saída do usuário no sistema desenvolvido. Ferramentas estudadas: *Log4j* e *Java.util.logging*.	*Java.util.logging.*
4. Implementar um controle de acesso.	O controle de acesso é baseado no papel do usuário. Ou seja, é atribuída uma regra de acordo com a função ou cargo no hospital. Ferramentas estudadas: JAAS (*Java Authentication and Authorization Service*), PhaseListener e Spring Security.	Spring Security.
5. Identificar usuário e paciente de forma única e segura.	A identificação e autenticação do usuário são feitas no momento do login. Ferramentas estudadas: JAAS, PhaseListener e Spring Security.	Spring Security.

De acordo com a norma (item 1 da Tabela 1), deve ser feito ***backup*** de todas as informações do SIS, armazenando-as em um ambiente fisicamente seguro e criptografado. A implementação do *backup* foi organizada em dois tipos: *backup* dos arquivos de auditoria e *backup* do banco de dados. Para o backup dos arquivos, foram considerados dois softwares gratuitos, o Uranium Backup (NANOSYSTEMS, 2017) e FBackup (SOFTLAND, 2017). Após comparadas algumas funcionalidades (agendamento de backups, envio de notificação via e-mail, criação de *logs*, entre outras) e o tempo gasto para a realização do backup de uma pasta de arquivos de cada ferramenta, observou-se que com o Uranium Backup atendeu as necessidades, portanto, essa ferramenta foi selecionada. Com a ferramenta Uranium Backup, foi possível fazer as principais configurações necessárias, como a escolha das pastas de origem e de destino, recebimento de notificações via e-mail, agendamento do *backup*, dentre outras. O *backup* é realizado na máquina física que está rodando o servidor da aplicação, necessitando da configuração manual das pastas de origem e destino na ferramenta para que possa ser realizado o backup automático.

Na implementação do *backup* do banco de dados, foram estudados dois softwares gratuitos: o Backup MySQL (TYTTOSOFT, 2016) e o MySqlBackupFTP (MYSQLBF, 2017). Foram consideradas algumas funcionalidades, como o agendamento de backups, envio de notificação por e-mail, restauração, entre outras. Os dois atenderam de forma satisfatória a tarefa, entretanto, o MySQLBackupFTP apresentou uma interface mais amigável, pela facilidade em encontrar determinadas funções. Com a ferramenta é possível configurar facilmente quais bancos de dados serão considerados para o backup, selecionar a opção de enviar uma notificação por e-mail, agendar *backup*, entre outras.

Outro controle indicado na norma (item 2 da Tabela 1) refere-se à implementação de controles para prevenção, detecção e resposta a **softwares maliciosos**. Na implementação do *Firewall*, foram considerados dois softwares gratuitos: Comodo Firewall (GROUP, 2017) e o ZoneAlarm Free Firewall (ZONEALARM, 2017). Em ambos, foram avaliadas várias funcionalidades, dentre elas o monitoramento em tempo real, filtro de tráfego e filtro Web.

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

Observou-se que o Comodo Firewall possui mais recursos, como a área de trabalho virtual, que permite uma navegação segura, detectando e bloqueando possíveis ameaças que poderiam ocorrer. Com a ferramenta é possível visualizar informações sobre as configurações de segurança atual, como por exemplo, a quantidade de intrusões na rede, quantidade de intrusões bloqueadas, executar a área de trabalho virtual, entre outras. Ademais, o ZoneAlarm Free deve ser usado em conjunto com um software de antivírus separado.

A norma também destaca a importância da criação de **registro de auditoria** sempre que um usuário acessar ou criar um arquivo (item 3 da Tabela 1). Esse registro deve identificar unicamente o usuário, identificar a função realizada pelo usuário e observar a hora e a data em que a função foi executada. A implementação dos ***logs* de auditoria** foi realizada em uma classe específica para tratar segurança no sistema. Tal classe faz a utilização do *java.util.logging*, que provê um framework padrão de *logs* do Java. Além desse framework, foi estudado outro chamado Log4j que também provê métodos para utilizar logs em um sistema. No entanto, os dois frameworks são de fácil uso e a escolha de qual adotar depende da complexidade que os *logs* precisam ter no sistema. Como no contexto do sistema não precisa ter uma grande complexidade, foi escolhido o framework padrão do Java. A criação dos *logs* é feita desde o login até o momento em que o usuário sai do sistema, registrando suas interações. No entanto, em caso de pane ou restauração do sistema, não é possível restaurar o sistema usando a base de *logs*.

De acordo com a norma (item 4 da Tabela 1), é preciso realizar o controle de acesso. No sistema, o processo **de autenticação e autorização do usuário** é realizado no momento do seu login, e fica a cargo de um *framework* denominado Spring Security (SOFTWARE, 2017). Este *framework* é específico para o desenvolvimento da estrutura de controle de acesso, que é baseada em papéis ou grupos de usuários. Para sua implementação, foram necessárias bibliotecas do *framework* Spring. No momento do login, é realizada a autenticação do usuário, em caso de sucesso, são capturados todos os dados do usuário, inclusive o seu identificador único. Todos que são autorizados a usar o sistema devem ter vínculo com o Hospital ou com a Universidade.

Após a autenticação do usuário, o Spring Security atribui uma regra de acesso baseada na função deste usuário no HU. No processo de autorização, é verificado se o usuário autenticado tem privilégios (permissões) de acordo com seu papel/função no hospital para acessar a página requisitada. Se o usuário possuir a permissão, a página é acessada normalmente. Senão, é emitida uma mensagem de aviso para o usuário. O controle de acesso dos usuários é baseado no papel (cargo) de cada um dentro do hospital, conforme já descrito.

A norma também destaca que a **identificação de um usuário/paciente** deve ser única e segura (item 5 da Tabela 1). O processo para a identificação do paciente é baseado no ID (Identificador único) e no seu CNS (Cartão Nacional de Saúde). Tanto o ID quanto o CNS são individuais, o que permite a identificação única de cada paciente. Os usuários do sistema são profissionais da saúde e estudantes que possuem algum vínculo com a Universidade. Todos possuem um código único, RA (Registro Acadêmico) se aluno ou uma matrícula se servidor. Esses códigos são utilizados para identificar unicamente cada usuário do sistema.

Os testes dos módulos foram realizados com base na simulação da interação do usuário. No módulo de *backup*, seja de dados ou do banco de dados, foram agendados backups que deveriam ser realizados em determinado horário e em seguido foi verificado se de fato o *backup* foi realizado. No módulo de *logs*, foi simulada a interação que o usuário teria com o sistema e verificado se o *log* gerado continha todas as interações realizadas por aquele usuário. Já no módulo de controle de acesso foi testado o login com credenciais inválidas e tentativa de acessar páginas restritas para determinados usuários.

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

5 Discussão e Considerações Finais

Este artigo apresentou os resultados obtidos com o estudo, planejamento e implantação de controles de segurança para o sistema de informação em saúde descrito. Para o desenvolvimento dos módulos de segurança, primeiro foi realizado um estudo das recomendações da ISO 27799:2008 e da Política de Segurança da Informação e Comunicações do Ministério da Saúde (PoSIC/MS). Com base no estudo, foram implantados os módulos de controle de acessos, de geração e armazenamento de *logs* de auditoria, de realização de *backups* e de filtro de pacotes (*Firewall*) Como o sistema foi implementado na linguagem Java, somente foram consideradas as ferramentas que pudessem ser utilizadas com esta linguagem e que fossem gratuitas.

A implantação dos módulos de segurança no sistema contribuiu no sentido de melhorar a segurança e confiança da informação utilizada para o atendimento de pacientes na unidade de emergência do hospital. O sistema não é um prontuário eletrônico, portanto, não armazena informações sobre o paciente, resultados de exames, consultas, dentre outras. Foi projetado para gerenciar as tarefas dos profissionais no atendimento dos pacientes que estão internados na emergência.

As tarefas são compartilhadas por diferentes profissionais de saúde. Se por algum motivo algum procedimento não for executado em um paciente na hora indicada pelo profissional de saúde responsável, o sistema deverá gerar um alerta. A geração de *logs* de auditoria permite, caso seja necessário, saber quem executou (ou deixou de executar) uma tarefa ou quem foi alertado pelo sistema.

O controle de acesso ao sistema também é essencial para garantir a segurança. O fluxo de pessoas é grande no hospital, incluindo profissionais da saúde, estudantes, residentes, pacientes, visitantes, dentre outros. O controle de acesso do sistema está ligado com o controle de acesso da Universidade, o qual é gerenciado utilizado o LDAP *(Lightweight Directory Access Protocol*), devolvendo além das informações pessoais, o perfil do usuário (estudante, servidor técnico, servidor docente, etc). Dessa forma, se ocorrer o desligamento de um servidor ou estudante, imediatamente ele perde o acesso ao sistema. Adicionalmente, apenas é permitida a inclusão ou a alteração de informações no sistema a partir da rede da Universidade. Assim, não é possível que um usuário fora do hospital faça qualquer atualização no sistema.

O nível de acesso também é controlado e baseado no perfil do usuário, isto é, cada usuário consegue acessar apenas sua área de trabalho. Foram definidos níveis (papéis) de acesso para três tipos de usuários (médico, enfermagem e nutrição) e para cada nível foram atribuídas permissões. Ao fazer login no sistema, ficam acessíveis ao usuário apenas as telas que se referem às suas atividades.

Com relação ao *backup*, este é realizado ao final de cada turno de trabalho. Devido à uma regra interna do hospital, no fim de cada turno um relatório deve ser impresso e assinado pelo enfermeiro responsável. Nesse momento, as informações dos arquivos de *log* de auditoria e também do banco de dados deverão ser copiadas para um segundo disco localizado em um servidor da Universidade. Dessa forma, caso ocorra algum problema com o sistema, será possível recuperar as informações. A proteção de ataques por meio da rede foi implementada com o uso de um *Firewall*.

O desenvolvimento desta pesquisa foi de grande relevância no sentido de implantar controles de segurança da informação gerenciada pelo sistema de lousa eletrônica. Espera-se que os resultados apresentados contribuam com a disponibilidade de informação íntegra e consistente para os usuários do sistema.

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

A próxima etapa da pesquisa é avaliar a segurança do sistema SHAVI por meio de Teste de Invasão, buscando identificar vulnerabilidades de modo que as devidas correções sejam feitas e as falhas solucionadas.

Agradecimentos

Agradecemos à equipe de profissionais da saúde do HUM e à Fundação Araucária pelo financiamento do projeto do sistema SHAVI (Edital PPSUS - Edição 2015) e pela concessão de bolsas de iniciação científica.

Referências

ARONSKY, D., JONES, I., LANAGHAN, K., & SLOVIS, C. M. Supporting patient care in the emergency department with a computerized whiteboard system. **Journal of the American Medical Informatics Association**, v15 p.184–194, 2007.

BORTMAN, Roberto; ALMEIDA, Roberto Luiz Pardini Ferreira de; PATELLA, Karen. Da Cybersegurança para Proteção de Dados de Pacientes. **Anais do Vii Encontro Nacional de Pós-graduação**, Santa Cecília, v. 2, n. 1, p.299-303, 2018.

GOLDSCHMIDT, Guilherme; NOBRE, Jéferson Campos; RIGHI, Rodrigo da Rosa. Segurança da Informação na comunicação de dispositivos médicos: uma revisão quasi-sistemática. **Journal Of Health Informatics**, São Paulo, v. 11, n. 2, p.46-53, 2019.

GROUP, C. (2017). Comodo free firewall. Acessado em: 10/03/2017. Web Page: https://www.comodo.com/home/internet-security/firewall.php.

ISO/IEC (2008). Iso/iec 27799:2008 - health informatics — information security management in health using iso/iec 27002. Acessado em: 14/03/2017. Web Page: http://tc215.behdasht.gov.ir/uploads/244_514_ISO%2027799_2008%20.pdf.

MYSQLBF. (2017). Mysql backup ftp. Acessado em: 10/03/2017. Web Page: https://mysqlbackupftp.com.

NANOSYSTEMS. (2017). Uranium backup. Acessado em: 10/03/2017. Wep Page: http://www.uraniumbackup.com/pt-br/uranium-backup-free.

PEREIRA, Samáris Ramiro; PAIVA, Paulo Bandiera; SOUZA, Paulo Roberto Schoroeder de. Sistemas de Informação para Gestão Hospitalar. **Journal Of Health Informatics**, São Paulo, v. 4, n. 4, p.170-174, 2012.

ROECKER, M. N., RAMALHEIRA, J. L., BALANCIERI, R., MANICA, H., DIAS, M. and MARTINS, J. S. Um sistema de lousa eletrônica para unidade urgência e emergência médica, **XIV Brazilian Congress of Information Technology in Health (XIV Congresso Brasileiro de Informática em Saúde)**, Santos, Brazil, p.125–130. 2014.

SALVADOR, V. F. M. & ALMEIDA FILHO, F. G. V. Aspectos éticos e de segurança do prontuário eletrônico do paciente. In: **II Jornada do conhecimento e da tecnologia**, São Paulo, Brazil, 2005.

Revista Tecnológica - Universidade Estadual de Maringá - ISSN 1517-8048
DOI: 10.4025/revtecnol.v29i1.49002

SAÚDE, M. (2017). Brasil. portaria n 271, de janeiro de 2017 - ministério da saúde. Acessado em: 15/03/2017. Web Page: http://www.lex.com.br/legis_27287736_PORTARIA_N_271_DE_27_DE_JANEIRO_DE_2017.aspx.

SOFTLAND. (2017). Fbackup. Acessado em: 20/03/2017. Web Page: http://www.fbackup.com/br.

SOFTWARE, P. (2017). Spring security. Acessado em: 26/03/2017. Web Page: https://spring.io/projects/spring-security.

TYTTOSOFT. (2016). Sistema de backup automático mysql. Acessado em: 26/03/2017. Web Page: http://tyttosoft.blogspot.com.br/2016/10/sistema-de-backup-automatico-mysql.html.

ZONEALARM (2017). Zonealarm free firewall. Acessado em: 26/03/2017. Web Page: https://www.zonealarm.com/software/free-firewall.