Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Tecnologia da Informação – Segurança da Informação

SEGURANÇA DA INFORMAÇÃO EM AMBIENTE HOSPITALAR

JESSICA DE AMARAL CORREIA LIMA

Americana, SP
2013

Faculdade de Tecnologia de Americana

Curso Superior de Tecnologia em Tecnologia da Informação – Segurança da Informação

SEGURANÇA DA INFORMAÇÃO EM AMBIENTE HOSPITALAR

JESSICA DE AMARAL CORREIA LIMA

Jessicaacl@hotmail.com

Trabalho de Graduação desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da informação, sob a orientação do Prof. Me. Alexandre Garcia Aguado.

Área: Segurança da Informação

Americana, SP

2013

BANCA EXAMINADORA

Prof. Me. Alexandre Garcia Aguado (Orientador)

Prof. Me. Carlos Henrique Rodrigues Sarro

Prof. Me. Leandro Halle Najm

DEDICATÓRIA

Aos meus pais, Adauto e Ivanilde que confiaram no meu potencial para esta conquista. Pelos valores que sempre buscaram me ensinar ao longo da vida, pela dedicação, carinho, apoio, incentivo e pelo exemplo de caráter e simplicidade.

AGRADECIMENTOS

Agradeço primeiramente ao criador do universo, Jeová Deus o centro da minha vida, por tudo que me proporciona e por ter-me dado forças para que eu pudesse concluir mais uma etapa da minha vida.

Aos meus pais, Adauto e Ivanilde, pelo apoio incondicional, carinho, pela educação e formação do meu caráter e por fazer de mim o que sou hoje.

Aos meus amigos e familiares que mesmo distante me apoiaram durante esses três anos e estão torcendo pela minha vitória.

As minhas tias Aidalva, Selma e Priscila por sempre acreditarem e investirem em mim.

Aos amigos que fiz nesses três anos, Priscila e José Paulo, pelas risadas, conversas, histórias, traduções, mensagens, email, amizade e ajuda que sempre me estenderam quando eu precisava. Pelos momentos de convivência e companheirismo durante nossa vida acadêmica

Ao meu orientador, Prof. Alexandre Aguado pelo auxílio e disponibilidade de tempo em ouvir minhas considerações, partilhando comigo as suas ideias, conhecimento e experiências, sempre com sua simpatia contagiante.

“A melhor maneira de ficar em segurança é nunca se sentir seguro”

Benjamin Franklin

RESUMO

A evolução do uso da tecnologia na saúde permitiu o crescente aumento da utilização de sistemas de registro eletrônicos no controlo de dados de saúde dos pacientes armazenados de forma digital. A informação digital assume diferentes aspectos de segurança na área da saúde. Sua maior importância consiste no armazenamento, transporte e manuseio de informações médicas em meio eletrônico. Com o aumento da utilização da informação digital, surge também a criação de novas ameaças à segurança da informação. A informação na área da saúde é um ativo importante e assim como qualquer outro ativo necessita ser adequadamente protegida. A Segurança da Informação protege a informação de diversos tipos de ameaças com o objetivo de minimizar os danos que possam vir a existir. Este trabalho tem como objetivo apresentar os riscos e ameaças existentes em um ambiente hospitalar e a melhor maneira de minimizá-los por meio de diretrizes, normas e procedimentos, a fim de garantir a integridade, disponibilidade e confiabilidade das informações. Foi realizado um estudo de caso em um ambiente hospitalar com a finalidade de identificar as possíveis ameaças existentes e analisar o melhor método possível para a solução de tais problemas. A implementação de melhores práticas de TI deverá conscientizar os profissionais da área de TI, bem como os profissionais das demais áreas do hospital sobre a importância das praticas da segurança da informação para as atividades desenvolvidas no hospital.

Palavras Chave: Segurança da Informação; Informação da saúde; Ambiente Hospitalar.

ABSTRACT

The evolution of the use of technology in health has allowed the increasing use of electronic record systems in the control of patients' health data stored in digital form. Digital information takes different aspects of security in healthcare. Its greatest importance relies in the storage, transportation and handling of medical information in electronic form. With the increased use of digital information, there is also the creation of new threats to information security. The healthcare data is an important asset and like any other asset needs to be suitably protected. Information security protects information from various types of threats in order to minimize the damage that may exist. This paper aims to present the risks and threats that exist in a hospital environment and the best way to minimize them through guidelines, standards and procedures in order to ensure the integrity, availability and reliability of information. A case study was conducted in a hospital setting with purpose of identifying potential threats and analyzing the best possible method for solving such problems. The implementation of improved practices should educate IT professionals in the IT field, as well as professionals from other areas of the hospital on the importance of information security practices for the operations of the hospital.

Keywords: *Information Security, Healthcare Information, Hospital Environment.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAS DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANS	Agência Nacional de Saúde Suplementar
ANVISA	Agência Nacional de Vigilância Sanitária
CFM	Conselho Federal de Medicina
IMIA	International Medical Informatics Association
ISO	International Organization for Standardization
NBR	Norma Brasileira
PEP	Prontuário Eletrônico do Paciente
RES	Registro Eletrônico em Saúde
SBIS	Sociedade Brasileira de Informática em Saúde
SGSI	Sistema de Gestão da Segurança da Informação
SI	Segurança da Informação
S-RES	Sistemas de Registros Eletrônicos De Saúde
TI	Tecnologia da Informação

SUMÁRIO

INTRODUÇÃO

A utilização de computadores é algo cada vez mais frequente nas instituições hospitalares, tendo como principais objetivos o armazenamento, manuseio, trocas das informações médicas e dados dos pacientes por meio de Sistemas de Registros Eletrônicos de Saúde (S-RES). “A informação digital assume diferentes aspectos de segurança na área de saúde. Sua maior importância reside na guarda e manuseio de informações médicas em meios eletrônicos [...]” (ABRAHÃO, 2003. p.131).

Um dos principais benefícios do uso da informação digital vem por meio do prontuário eletrônico do paciente (PEP). O PEP é onde ficam armazenadas todas as informações de um paciente, tanto informações de saúde, como administrativas. Nesse prontuário podem ser encontrados problemas de saúde, intervenções atuais, tomadas de decisão e melhorias de efetividade do cuidado do paciente. (MASSAD, MARIM, AZEVEDO, 2003).

Segundo Rodrigues (2010), as soluções tecnológicas e de telecomunicações empregadas para a utilização nos sistemas que se valem da informação digital são complexas e trazem riscos de segurança à confidencialidade, a integridade das informações, podendo expor os pacientes e a organização.

Devido ao grande número de informações pessoais contidas no prontuário eletrônico, ele passa a ser um dos principais ativos da empresa que necessita de segurança.

> “[...] o mau uso da informática vem facilitando seu extravio e seu acesso indevido; os sistemas que utilizam redes de computadores tornam esses dados vulneráveis a acessos não autorizados; a facilidade de alteração de dados registrados eletronicamente traz perigos adicionais à vida e ao bem-estar de pacientes.” (PINOCHET, 2011, p.278)

Conforme Pinochet (2011) aponta, as organizações atualmente competem em um mundo altamente globalizado, isso faz com que a informação do paciente seja considerada o mais valioso ativo da empresa. A utilização da tecnologia da

informação nas organizações hospitalares traz desafios na gestão da segurança dos diversos ativos, pois a informação do paciente vem sendo considerada como um valioso bem.

Para Abrahão (2003), a informação em saúde, assim como qualquer outro ativo da saúde, precisa de uma segurança adequada para a proteção contra ameaças de diversos tipos, para que seja minimizados os danos que possam vir a existir. Na maioria dos hospitais onde os recursos tecnológicos existem, não há uma política de segurança para a área ou tal política é muito falha.

Considerando esse aspecto e a vivência do pesquisador no contexto de tecnologia da informação na área da saúde, esse trabalho busca enfatizar a importância e os benefícios de uma política de segurança da informação, bem como o cumprimento da mesma na área Hospitalar. Além disso, este trabalho visa apresentar conceitos básicos de segurança da informação voltados para área da saúde, para que o leitor possa entender a real importância de uma política de segurança em um hospital e possa perceber os benefícios da implementação da mesma.

Para a elaboração deste trabalho foi realizado um estudo de caso no Hospital ABC[1] que foi informatizado no ano de 2012 e utiliza o PEP. Cerca de 65% dos profissionais utilizam o computador como ferramenta de trabalho, apesar das dificuldades existentes como usuários da informática, o que compromete a segurança dos dados e informações coletadas e armazenadas.

Os capítulos seguintes abordarão sobre a importância da segurança da informação em um ambiente hospitalar e como se faz necessária a implementação de controles adequados para garantir tal segurança.

[1] O nome do hospital é fictício, afim de não expor a real identidade daqueles que participaram do caso.

1 SEGURANÇA DA INFORMAÇÃO

Este capítulo apresentará a parte teórica sobre segurança da informação relacionada com diversos elementos que contribuem para garantir que a informação esteja protegida contra qualquer ameaça no ambiente corporativo.

1.1 Importância da Segurança da Informação

As informações pertencentes a uma empresa são consideradas como ativos. Esses ativos existem em diversos formatos, podem ser impressos, escritos em papel, armazenados eletronicamente, transmitidos através de meios eletrônicos, mostrados em imagens ou falados em conversas. Independente do formato em que a informação se encontra, é necessário que ela seja protegida de maneira adequada (ABRAHÃO, 2003).

A ISO 27002 (2005), define segurança da informação como sendo a “preservação da confidencialidade, integridade e disponibilidade da informação” (P.2) e a autenticidade, responsabilidade, não repúdio e confiabilidade, também são outras propriedades que podem estar envolvidas.

Segurança da informação é definida por Sêmola (2003) como sendo uma área de conhecimento que está voltada à proteção dos ativos da informação contra possíveis ameaças, tendo como principal objetivo garantir a integridade, confiabilidade e disponibilidade da informação. Segundo Abrahão (2003) a segurança da informação é caracterizada pela confidencialidade, integridade e disponibilidade das informações.

De maneira similar Fontes (2006), define segurança da informação como sendo um conjunto de orientações, normas, procedimentos, políticas e demais ações que visam proteger a informação, por garantir a disponibilidade, integridade, confiabilidade, legalidade, não repúdio de auditoria e auditabilidade da informação.

Assim, pode-se concluir que Segurança da Informação é a proteção da informação contra diversos tipos de ameaças. Para que tal segurança seja garantida

é necessária, como já mencionado, a preservação de três atributos básicos: integridade, disponibilidade e confidencialidade da informação.

Conforme pode-se verificar na ISO 27002 (2005), a segurança da informação é feita através da implementação de controles e políticas necessários para assegurar a informação. Estas técnicas precisam ser trabalhadas conforme a necessidade de cada área, visando que sejam atendidos os critérios de segurança estabelecidos.

> "A Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software e hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança organizacional sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio." (ABNT, 2005, p. x).

É impossível afirmarmos que há segurança da informação sem que a informação seja controlada e gerenciada, afirma Quintella e Gonçalves (2013). Por isso, a fim de minimizar os riscos a níveis existentes na proteção da informação faz-se necessária a classificação de risco das informações.

1.2 Princípios de Segurança da Informação

A segurança da informação é constituída por três atributos básicos que juntos formam os pilares da segurança da informação, esses atributos tem como objetivo manter os requisitos básicos e necessários para garantir a segurança da informação. Esses elementos são a confidencialidade, disponibilidade e integridade.

Figura 1 - Pilares da segurança da Informação (MACEDO, 2013)

A figura 1 representa os pilares da segurança da informação, mostrando a relação da segurança da informação com a confidencialidade, disponibilidade e integridade.

1.2.1 Confidencialidade

Confidencialidade é definida por Sêmola (2003), como sendo a garantia de que a informação é acessível somente por pessoas a qual ela é destinada. Toda a informação deve ser protegida conforme o grau de sigilo de seu conteúdo, sendo disponível somente para pessoas autorizadas.

A confidencialidade é a proteção da informação contra a leitura, cópia ou alteração por qualquer individuo que não seja autorizado pelo proprietário da informação. Tal proteção da informação deve ser feita não somente como um todo, mas também por partes da informação que podem ser utilizadas para interferir sobre o todo. No caso das redes de computadores, enquanto as informações estão sendo

trafegadas, não deverão ser vistas, alterados, ou extraídos da rede por pessoas não autorizadas.

1.2.2 Disponibilidade

Conforme Sêmola (2003), disponibilidade visa garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes quando necessário para qualquer finalidade. A disponibilidade também consiste na proteção das informações para que não sejam degradadas ou se tornem indisponíveis, sem autorização.

Se um sistema encontra-se indisponível quando um usuário autorizado necessita das informações, isso pode gerar perdas graves, prejudicando tanto quanto se a informação estivesse sido removida do sistema.

Assegurar a informação também inclui a manutenção dos acessos às informações que estão sendo disponibilizadas. O objetivo é que a informação chegue aos usuários de forma íntegra e confiável.

1.2.3 Integridade

Segundo Sêmola (2003), garantir a Integridade é assegurar que a informação seja mantida na mesma condição em que foi disponibilizada pelo seu proprietário. A integridade consiste em evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação. Somente poderá haver alterações na informação com a autorização do proprietário.

O objetivo é assegurar que os dados não foram modificados por pessoas não autorizadas. A integridade preocupa-se mais com a gravação ou alteração de dados, pois ela é um pré-requisito para outros princípios da segurança. Se a integridade de um sistema pode ser violada, então a confidencialidade de seus arquivos pode ser igualmente violada.

1.3 Classificação da Informação

Para que as informações possam receber a segurança adequada é necessário que exista uma classificação quanto a sua criticidade. (LANVERLY, et al., 2013) A classificação da criticidade da informação é necessária também para manter a privacidade do paciente. Porém, o processo classificatorio das informações pode variar de organização para organização. O nivel de privacidade dessas informações depende do tipo de negocio realizado pela organização.

Segundo a ISO 17799(2005), que trata da classificação da informação:

> "Convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento." (p. 23).

A classificação quanto à criticidade das informações, que visa identificar o risco para o negócio caso uma informação seja divulgada indevidamente, deve ser feito pelo proprietário da informação, juntamente com a organização (LANVERLY, et al., 2013).

Determinar os níveis de criticidade dos ativos de informação em saúde é um processo complexo. Conforme a ISO 27779 (2008), a classificação das informações varia conforme a necessidade do proprietário. A confidencialidade das informações pessoais no setor da saúde é muitas vezes subjetiva, ao invés de objetiva. Ou seja, somente o proprietário da informação é capaz de determinar o grau de confidencialidade necessário para cada caso.

A confidencialidade das informações pessoais de saúde pode mudar ao longo da vida de registro de saúde de um indivíduo. Por exemplo, uma pessoa que busca manter sua identidade em sigilo pode considerar que o grau de confidencialidade do seu endereço e número de telefone é bem maior que a confidencialidade de dados clínicos sobre a definição de seu braço quebrado. Ou o nome e endereço de um

paciente obtido através de uma lista de pacientes que passaram em um atendimento emergencial de um hospital, podem não ser considerados especialmente confidenciais por esse indivíduo, mas o mesmo nome e endereço obtido através em uma lista de pacientes que passaram em uma clínica de tratamento da impotência sexual podem ser considerados altamente confidenciais pelo paciente (ISO 27779, 2008).

Porém é necessário lembrar que toda a informação após passar por alteração de conteúdo, deve ser submetida a um novo processo de classificação para ser colocada um nível adequado (FERREIRA; ARAÚJO, 2008).

1.3.1 Definição

Para que seja feita a classificação é necessário avaliar o negócio, processos e atividades realizadas na organização. Antes que sejam feitas as classificações das informações, é de extrema importância estabelecer algumas definições. Conforme Ferreira e Araújo (2008), a tabela 1 nos mostra algumas definições que devem ser estabelecidas no inicio do processo.

Tabela 1 – Definições das informações (FERREIRA; ARAÚJO, 2008).

Classificação	Atividade que tem como objetivo atribuir o grau de sigilo necessário em cada informação.
Proprietário	Profissional responsável pelo ativo da informação na organização.
Custodiante	Profissional responsável por garantir que as informações estão de acordo com o estabelecido pelo proprietário da informação.
Criptografia	Proteção por meio de codificação que permite proteger a informação de acesso não autorizado.
Perfil de acesso	Responsável por definir os diretitos de acesso às informações.

1.3.2 Níveis de Classificação

Após serem definidos os critérios de classificação das informações é necessário que elas sejam classificadas de acordo com o nível de criticidade. O processo de classificação das informações pode variar conforme a organização.

A tabela 2 apresenta três níveis de classificação das informações conforme Ferreira e Araújo (2008).

Tabela 2 – Classificação das informações (FERREIRA; ARAÚJO, 2008).

Informação Pública	São informações que não necessitam de nenhum sigilo ou proteção. Se forem divulgadas não trarão impacto ao negocio.
Informação Interna	Devem ser protegidas de acessos externos, porem se tais informações se tornarem públicas, as consequências não serão criticas.
Informação Confidencial	São informações que necessitam de recursos de proteção. Só deverão estar acessíveis para pessoas autorizadas. Caso essa informação se torne Pública, as operações da organização poderão ser comprometidas.

Cada organização tem sua necessidade quanto à classificação das informações e deverá ter a quantidade de níveis que atenda a sua necessidade.

Visto que as informações que circulam em um hospital são extremamente sigilosas, o ambiente hospitalar apresenta desafios e requer intensificados recursos de proteção da segurança das informações, e uma política de segurança bem estruturada, para que as informações continuem íntegras e seguras. Esse tema será tratado em detalhes no subtópico seguinte.

1.4 Política de segurança

Segundo Ferreira e Araújo (2008), política de segurança da informação é um conjunto de regras e padrões sobre o que deve ser feito para garantir que as

informações da empresa recebam proteção adequada, por meios de métodos e procedimentos utilizados para a manutenção da segurança da informação.

A política de segurança é composta por diretrizes, normas, procedimentos e instruções que estabelecem os critérios de segurança que deverão ser adotados, visando o estabelecimento, padronização e normalização da segurança tanto no âmbito humano quanto tecnológico.

> “Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, a política tem um papel fundamental e, guardadas as devidas proporções, tem importância similar à constituição federal para um país. Desta forma, assume uma grande abrangência e, por conta disso, é subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinadas, respectivamente, às camadas estratégica, tática e operacional.“ (SÊMOLA. 2008 p.105).

A Política de Segurança da Informação é dividida em três níveis hierárquicos distintos: diretrizes, normas e procedimentos. Rodrigues (2010), define cada um deles como:

- Diretrizes de Segurança da Informação: define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- Normas de Segurança da Informação: estabelecem obrigações e métodos definidos de acordo com as diretrizes da política;
- Procedimentos de Segurança da Informação: instrumentalizam o disposto nas normas e na política, permitindo a direta aplicação nas atividades da organização.

A política de segurança deve conter procedimentos para armazenamento, manuseio e descarte da informação. Porém, cada empresa tem sua necessidade e a política de segurança deve ser estruturada de modo personalizado para cada organização.

2 SEGURANÇA DA INFORMAÇÃO EM AMBIENTE HOSPITALAR

Este capítulo constitui nos conceitos sobre segurança da informação, riscos, requisitos, normatização e regulamentação para o setor de saúde.

2.1 Informações da Saúde

A norma ISO 27799 (2008), define informações da saúde como sendo constituídas por várias informações sobre um paciente, contendo informações da saúde física e/ou mental de um individuo, bem como os serviços de saúde utilizados pelo mesmo. Essas informações podem incluir:

- Informação sobre o registro do indivíduo para a provisão de serviços de saúde;
- Informação sobre despesas médicas com respeito ao indivíduo;
- Um número, símbolo ou detalhe particular atribuído a um indivíduo para sua identificação exclusiva;
- Qualquer informação sobre o indivíduo coletada no decorrer da provisão de serviços de saúde;
- Informação derivada de qualquer exame de uma parte do corpo ou substância corporal;
- Identificação de uma pessoa (por exemplo, um profissional de saúde) como o fornecedor da saúde ao indivíduo.

A informação pessoal da saúde contém informações não somente dos eventos relacionados à doença de um individuo, mas também de informações como hábitos alimentares, prática desportiva e atividades de lazer. Todos os eventos relacionados à saúde da pessoa do nascimento até a morte (que estão registrados em um prontuário), agregados em torno de um identificador único (ABRAHÃO, 2003).

É direito do paciente a disponibilidade permanente das informações, como é dever do médico e da instituição guardar o prontuário. O sigilo profissional, que visa preservar a privacidade do indivíduo, deve estar sujeito às regras estabelecidas na legislação e no Código de Ética Médica, independentemente do meio utilizado para o armazenamento dos dados no prontuário, seja eletrônico ou em papel (ABRAHÃO, 2003).

Essas informações podem estar armazenadas em papeis ou por meios de Sistemas de Registro Eletrônico de Saúde (S-RES), que será abordado na próxima sessão.

2.2 Segurança da Informação na Saúde

Os objetivos globais de segurança da informação são manter a confidencialidade, disponibilidade e integridade das informações, incluindo autenticidade, responsabilidade e auditabilidade.

Em ambiente hospitalar a privacidade do paciente depende em grande parte de manter a confidencialidade das informações pessoais de saúde. Para que essa confidencialidade seja mantida, devem ser tomadas medidas para assegurar a integridade dos dados. Além disso, a segurança dos pacientes depende de manter a integridade das informações pessoais de saúde.

A ISO 27779 (2008), contém considerações adicionais que moldam os objetivos de segurança da informação de saúde. Estes são:

- Honrar as obrigações legais de privacidade, como expresso em leis e regulamentos de proteção de dados;
- Manter a privacidade do paciente por meio de práticas de segurança da informação na saúde;
- A organização e os profissionais da saúde tem responsabilidade pelas informações utilizadas;
- Analisar os riscos dentro das organizações de saúde;

- Atender as necessidades de segurança identificadas em situações comuns da área hospitalar;
- Facilitar o aumento do uso da tecnologia de forma segura e bem gerenciada;
- Obter a confiança do público nas organizações de saúde e nos sistemas de informação dessas organizações;
- Inserir padrões e ética a fim de garantir a segurança, confidencialidade e integridade das informações de saúde;
- Operar os sistemas eletrônicos de informação de saúde em um ambiente adequadamente protegido contra ameaças.

Assim como em quaisquer outras organizações existentes, a necessidade de implementar controles de segurança nas organizações hospitalares se dá devido a quantidade e diversidade de informações que necessitam ser armazenadas, processadas e gerenciadas (QUINTELLA; GONÇALVES, 2013).

Os controles de segurança da informação podem ser feitos por meio de políticas, práticas, procedimentos, estruturas organizacionais, *software* de controle entre outros procedimentos que garantem que os objetivos de segurança específicos da organização sejam atendidos (ABRAHÃO, 2003).

Em contrapartida, a falta de tais controles pode deixar a informação exposta a pessoas não autorizadas e o uso indevido dos sistemas de informação dos serviços de saúde, pode comprometer as informações sigilosas dos pacientes e resultar em doenças, lesões ou até mesmo a morte. De acordo com a ISO 27779 (2008), a segurança da informação do paciente depende de integridade das informações pessoais contidas no PEP.

O controle de segurança adequado para a área da saúde assegura a confidencialidade, integridade e disponibilidade das informações do paciente. Esse controle ajuda a evitar erros na prática médica resultantes da incapacidade de manter a integridade das informações de saúde.

A segurança nas instituições de saúde que manipulam informações eletrônicas é essencial pois a privacidade do paciente depende da manutenção da confidencialidade da informação armazenada.

Veremos qual a importância do armazenamento correto da informação na área da saúde, quais riscos existem e quais medidas tomar para evitar uma possível ameaça.

2.3 Armazenamento das Informações

As informações da saúde do paciente podem ser armazenadas em meios eletrônicos, ou em meios físicos. Instituições hospitalares que ainda não foram implementadas a informatização, as informações geralmente ficam armazenadas em um prontuário pessoal em forma de papel, no qual, após a realização de qualquer procedimento com o paciente, é feito um registro. Em instituições que utilizam a informatização, esse prontuário passa a ser digital e as informações são armazenadas em Sistemas de Registro Eletrônico de Saúde (S-RES).

O manual de Certificação para Sistemas de Registro da SBIS traz algumas definições para informações da saúde:

- Registro Eletrônico em Saúde (RES): um repositório de informação a respeito da saúde de indivíduos, numa forma processável eletronicamente.

- Sistema de Registro Eletrônico em Saúde (S-RES): Sistema para registro, recuperação e manipulação das informações de um Registro Eletrônico em Saúde.

Sistemas de registros eletrônicos de saúde é o uso da informática como forma de organizar e armazenar a informação contida no prontuário em papel, ou seja, é um conjunto de informações de saúde no formato digital. O RES deve atender aos requisitos essenciais de integridade, autenticidade, disponibilidade e privacidade da informação.

2.4 Riscos da informação na área de saúde

Risco é a probabilidade que alguma ameaça explore a vulnerabilidade de um ativo, provocando algum dano para a organização. Ameaça pode ser definida como uma causa potencial de um incidente indesejado, que pode resultar em um dano para uma organização. Vulnerabilidade é a fragilidade de um ativo na organização que pode ser explorado por alguma ameaça.

A segurança é uma prática voltada à eliminação de possíveis vulnerabilidades existentes a fim de reduzir os riscos de uma ameaça se concretizar no ambiente que deseja proteger. A figura 2 mostra o relacionamento entre riscos e fontes de riscos. Pode-se observar que a existência do risco é determinada a partir das ameaças e das vulnerabilidades dos ativos de informação contidos na organização.

Figura 2 - Riscos e fonte de risco (ISO 27002, 2008).

Nas grandes organizações hospitalares, existe grande volume de pessoas que se deslocam por áreas operacionais. Levando em conta que a maioria das pessoas que circulam por esse ambiente sofre de alguma instabilidade física, emocional ou mental, o risco de vulnerabilidade dos sistemas de informação

aumenta significantemente. Também o fato de que há funcionários que são muitas vezes obrigados a trabalhar sob stress significativo, eleva a taxa de erro humano, com isso a probabilidade de risco aumenta (ISO 27779, 2008).

O ambiente de saúde, contém ameaças e vulnerabilidades únicas, que devem ser consideradas com cuidado especial, a fim de garantir que nenhum risco relacionado a informação venha a existir.

2.4.1 Avaliação de Riscos

A ISO 27779 (2008) apresenta 25 tipos de ameaças existentes em um ambiente hospitalar. Analisaremos os tipos de ameaça que devem ser considerados pelas organizações de saúde quando forem avaliar os riscos para a confidencialidade, integridade e disponibilidade da informação existentes no S-RES:

- Funcionários internos utilizando dados de acesso de outros funcionários: constitui uma avaria na autenticação segura do usuário. Um funcionário utiliza o S-RES com *login* e senha de outro funcionário. Essa usurpação pode ser feita por profissionais da saúde ou equipe de apoio, intencionalmente ou não.

- Uso não autorizado por indivíduos disfarçados de prestadores de serviços: o uso do S-RES por profissionais prestadores de serviços não autorizados com *login* e senha de outro funcionário. Prestadores de serviços que estão encarregados de manutenção de *software* e *hardware*, ou outras pessoas que podem ter uma razão profissional para acessar sistemas e dados.

- Uso não autorizado por estranhos: ocorre quando terceiros (estranhos) não autorizados tem acesso a dados ou recursos do sistema, seja através da personificação de um usuário autorizado ou fraudulentamente se tornar um usuário autorizado. Uso não autorizado por estranhos constitui uma falha de um ou mais dos controles de segurança, por exemplo, a Identificação do usuário, autenticação do usuário, autenticação da origem e controle de acesso e gerenciamento de privilégios.

- Pedido de informações não autorizado: são obtidas informações confidencias por pessoas não autorizadas por meio de um pedido não autorizado de uma determinada informação. O uso não autorizado de um pedido de informações de saúde é uma maneira surpreendentemente fácil de obter acesso não autorizado à determinada informação sigilosa de algum paciente. O uso não autorizado dos pedidos de informação de saúde constitui uma falha do controle de acesso de grupo de trabalho, prestação de contas e controle de auditoria e/ou segurança pessoal.

- *Software* prejudicial: a Introdução de *software* prejudicial ou perturbador que podem inserir no computador vírus e outros *"malware"* é a causa da maioria dos incidentes de segurança de TI.

- Uso indevido de recursos do sistema: usuários que utilizam sistemas de informação e serviços de saúde para uso pessoal, usuários que fazem download de informações não relacionadas ao trabalho a partir da Internet em computadores destinados exclusivamente para apoiar os sistemas de informação de saúde, criação de bancos de dados ou outras aplicações para assuntos não relacionados ao trabalho.

- Infiltração: um determinado indivíduo (um *cracker*, por exemplo) tem acesso ao fluxo de dados através de uma rede. A forma mais comum é um ataque de DOS (negação de serviço). Porem, outras formas de infiltração são possíveis.

- Não confidencialidade da informação: comunicações não criptografadas durante a transmissão não garantem a confiabilidade das informações contidas em uma mensagem, pois a mensagem pode ser interceptada e a informação compartilhada com alguém não autorizado.

- Repúdio: usuários que negam o envio uma mensagem (repúdio da origem) e os usuários que negam o recebimento de uma mensagem (recusa de recebimento). Repúdio pode constituir uma falta de aplicação de controles, tais como assinaturas digitais (um exemplo de repúdio de origem) ou controles, como recibos de leitura nas mensagens de e-mail (um exemplo de repúdio de recepção).

- Falha de conexão: falha de conexão na rede de computadores. Todas as redes estão sujeitas a interrupções de serviço. Falhas de conexão pode ser resultado da má administração dos serviços de rede. Essas falhas podem facilitar a divulgação de informações confidenciais, forçando os usuários a enviar mensagens através de um mecanismo menos seguro, como via fax ou através da Internet.

- Código malicioso: esta ameaça inclui vírus, e-mail e códigos hostis em uma rede sem fio. O uso crescente de tecnologias sem fio e móveis por profissionais de saúde aumenta o potencial desta ameaça de danos.

- Envio de informações acidentalmente: esta ameaça inclui a possibilidade de que a informação possa ser entregue a um endereço incorreto quando está sendo enviado através de uma rede. Isso poderia acontecer devido a um deslize do usuário ou a incapacidade de manter a integridade dos diretórios de provedores de saúde (ou ambos).

- Falha técnica de rede: falhas de *hardware*, falhas na rede, falhas nas instalações ou armazenamento de dados. Uma única falha na rede, levando a perda de conexão no sistema de informação de saúde, e a indisponibilidade de tal sistema, pode ter consequências fatais para os pacientes.

- Falha devido a recursos naturais: falha devido a recursos naturais inclui as falhas de energia elétrica e interrupções do serviço resultantes de catástrofes naturais ou provocadas pelo homem. Sistemas de informação de saúde podem ser cruciais durante os desastres naturais e outros eventos que podem ser fatais para um grande número de pessoas.

- Falha na segurança da rede: ataques de negação de serviço podem ser facilitados pelas fraquezas ou erros de configuração, sistema operacional ou *software* de sistema operacional de rede. Testes de *software* ou sistema de controle de manutenção de *software* deverão ser feitos periodicamente para evitar ou diminuir tal vulnerabilidade.

- Falha de *software* voltado para sistemas da saúde: falhas na aplicação de *software* podem ser exploradas em um ataque de negação de serviço e

também podem ser usadas para comprometer a confidencialidade dos dados protegidos.

- Falha humana: tem um percentual pequeno em comparação às outras falhas, mas um percentual significativo nas divulgações não intencionais de informações confidenciais. Falha humana constitui em uma ou mais falha seguintes: erro ao controlar as operações, segurança pessoal (incluindo treinamento eficaz dos funcionários) e/ou recuperação de desastres (incluindo dados de backup e restauração).

- Erro de Manutenção: constitui na falha nos controles de manutenção de *hardware*, controles de manutenção de *software*, controles de alteração de *software* ou alguma combinação dos anteriores. Esses erros podem ser cometidos por pessoas responsáveis pela manutenção de *hardware* e *software* de sistemas, por membros da equipe, bem como por funcionários terceirizados contratados para executar tarefas de manutenção. Configuração incorreta de *software* durante a instalação é uma causa comum de vulnerabilidades que mais tarde podem ser exploradas por *hackers*. Tais erros podem, por sua vez, colocar em perigo a confidencialidade dos dados protegidos.

- Erro de Usuário: erros cometidos por usuários podem, por exemplo, resultar em informações confidenciais sendo enviadas para o destinatário errado. Erros de usuários podem se dar devido a falhas no controle de usuário ou na segurança pessoal (incluindo treinamento).

- Falta de profissionais: profissionais capacitados e habilitados são fundamentais para o funcionamento do sistema eletrônico. A falta de tais funcionários se dá devido a dificuldade de encontrar pessoais habilitadas, colocando em risco a disponibilidade de tais sistemas por serem utilizados por profissionais não capacitados.

- Roubo de equipamento ou dados por funcionários: funcionários geralmente têm maiores acesso a informações confidenciais de pessoas de fora e, portanto, estão em uma posição favorável para roubar as informações, a fim de vendê-la ou divulgá-la para os outros. Roubo por funcionários constitui

uma falha de um dos muitos controles possíveis, incluindo controles sobre saída de impressão, documentos ou meios de comunicação, segurança física, ou a proteção física do equipamento.

- Roubo de equipamento ou dados por estranhos: roubo de equipamento ou dados por estranhos constitui um grave problema, em alguns hospitais. Roubo pode acontecer porque os dados confidenciais residem em um servidor ou computador portátil que é roubado ou porque os próprios dados são o alvo do roubo, isso resulta em quebra de confidencialidade. Roubo por pessoas de fora pode acontecer devido a uma falha em um dos muitos controles, incluindo controles de computação móvel, transporte seguro mídia, tratamento de incidentes, verificações de conformidade ou proteção contra roubo material.

- Danos intencionais por funcionários: danos intencionais causados por funcionários da instituição podem incluir atos de vandalismo e outros casos em que os prejuízos são causados aos sistemas de TI ou seu ambiente de apoio por pessoas a quem foi concedido acesso.

- Danos intencionais por estranhos: a ameaça de dano intencional por estranhos inclui atos de vandalismo e outros casos em que os prejuízos são causados aos sistemas de TI ou seu ambiente de apoio por pessoas que não tenham obtido o acesso a tais sistemas.

- Terrorismo: inclui atos por grupos extremistas que desejam danificar ou interromper o trabalho das organizações de saúde, para prejudicar os profissionais de saúde ou para interromper as operações de sistemas de informação em saúde.

2.4.2 Tratamento de Riscos

Antes de considerar o tratamento que deve ser aplicado a um determinado risco, é importante definir os critérios que determinam se esse risco pode ser ou não aceito. Nesses critérios deve-se levar em conta os objetivos da empresa, requisitos e

regulamentos, custo de implementação e a operação em relação aos riscos, necessidade de balancear o investimento na implementação de controles, entre outros.

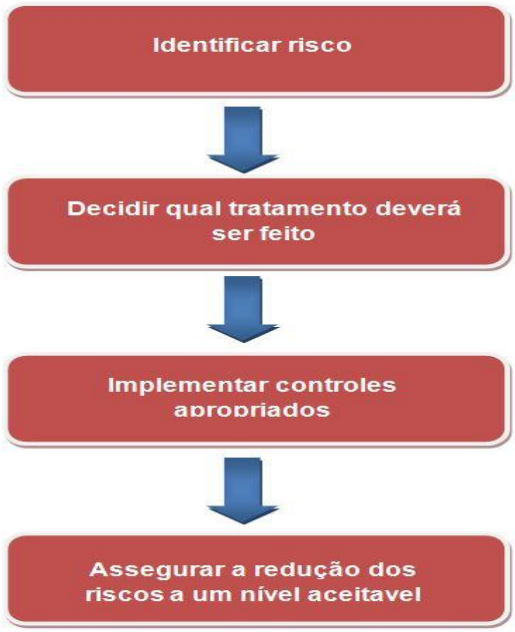

Figura 3 - Tratamento de risco (Autoria própria, 2013).

A figura 3 mostra os passos que devem ser tomados para avaliar o tratamento de risco em uma organização. Após identificar o risco é necessário decidir qual tratamento deverá ser tomado, só então serão implementados controles adequados que assegurarão assim a redução dos riscos a um nível aceitável.

A norma australiana AS/NZ 4360:2004 (Gestão de Riscos - diretrizes para a Implementação) introduziu o conceito de "tratamento de risco". Esse conceito foi posteriormente adotado pela norma ISO / IEC 27001:2005.

Quando se refere a "tratamento de risco", o termo se refere à atividade de reduzir o risco a níveis aceitáveis. O conceito de tratamento de riscos é particularmente pertinente para as organizações de saúde, implementando o conceito de tratar, transferir ou tolerar os riscos. A avaliação e definição do que é ou não aceitável deve ser definido pela organização.

Caso a organização decida não implementar um determinado controle de tratamento de risco, isso é inteiramente válido, mas convém que seja formalmente

registrado na sua política de segurança. Para as organizações da área de saúde é extremamente necessário que sejam documentados os riscos aceitos, visto que se tratam de instituições que lidam com riscos relacionados a saúde.

2.5 Política de Segurança da Informação para ambiente hospitalar

Para que haja um controle adequado de segurança da informação é necessária à implementação de uma política de segurança escrita que seja aprovada pela administração, Publicada e comunicada a todos os funcionários da organização e as partes externas relevantes. O conteúdo da política será impulsionado pelos resultados da avaliação de risco feita pela organização.

A política de segurança em um ambiente hospitalar tem o propósito de fornecer orientação e apoiar às ações de gestão da segurança, podendo ser subdividida em três segmentos: diretrizes, normas e procedimentos.

Deve deixar claro que cada colaborador é responsável por usar os recursos tecnológicos disponíveis de forma a aumentar sua produtividade e contribuir para os resultados e a imagem pública da organização, no caso hospitalar (PINOCHET, 2011).

2.5.1 Criação da Política

As normas ISO/IEC 27002(2005) e ISO 27799(2008) possui orientações sobre o que uma política de segurança da informação deve abordar. Com base nessas informações, analisaremos o que uma política de segurança da informação voltada para a área da saúde deve abordar:

- Abordar a necessidade de segurança da informação na área da saúde;
- Abordar as metas de segurança da informação em saúde;
- A política deve ser amplamente divulgada, revista e, adotada pela organização;

- Abordar os requisitos regulamentares, legislativos e contratuais, inclusive para a proteção de informações pessoais de saúde e as responsabilidades legais e éticas dos profissionais de saúde a fim de proteger essas informações;
- Procedimentos de notificação de incidentes de segurança da informação, incluindo um canal para levantar preocupações em matéria de confidencialidade, sem medo de culpa ou recriminação;
- Abordar a amplitude das informações da saúde;
- Abordar os direitos e as responsabilidades éticas dos profissionais, tal como abordado na lei e como aceito pelos membros dos órgãos profissionais;
- Abordar os direitos do paciente, quando aplicável, à privacidade e ao acesso aos seus registros;
- Abordar as obrigações de médicos no que diz respeito à obtenção do consentimento informativo de assuntos relacionados ao paciente, e manter a confidencialidade das informações pessoais de saúde;
- Abordar as obrigações da organização de saúde onde as informações estão entregues em um "cuidado compartilhado" por todos da organização;
- Abordar os protocolos e procedimentos a serem aplicados para o compartilhamento de informações para garantir a segurança da mesma;
- Abordar as limitações que devem ser colocadas sobre o acesso a informações pessoais de saúde por voluntários e pessoas de apoio.

2.5.2 Revisão da Política

A Política de segurança da informação da organização de saúde, assim como em outras organizações, deve estar sujeita a periódicas revisões. A empresa deve especificar o tempo em que essas revisões deverão ser realizadas. Mas, conforme a ISO 27799, a política de segurança deverá ser revisada pelo menos anualmente.

Caso ocorra um grave incidente de segurança, a política deve ser revista imediatamente após o incidente.

Para a realização da revisão de tal política, faz-se necessário segui as orientações dadas pela ISO 27002(2005). Tal revisão deve abordar:

- A natureza mutável das operações da organização de saúde e as necessidades de mudança gerenciamento de perfil e de risco;
- As alterações feitas à infraestrutura de TI da organização;
- As mudanças identificadas no ambiente externo que podem impactar no perfil de risco da organização;
- Recentes controles, conformidade e requisitos disponibilizados pelos órgãos jurisdicionais de saúde ou por uma nova legislação ou regulamento;
- As últimas orientações e recomendações das associações de profissionais de saúde e de organizações existentes que visam garantir a privacidade e proteção de informações pessoais de saúde;
- Os desafios relacionados com a segurança da informação existentes na política anterior.

2.5.3 Disponibilização da Política

Muitas organizações disponibilizam seu documento de política de segurança eletronicamente, através da intranet da instituição. Quando a organização de saúde utiliza os serviços de empresas terceirizadas, ou contribui com terceiros, o documento de política de segurança deve incluir controles e procedimentos que cobrem tais interações e que especificam as responsabilidades de todas as partes, e essa política também deve estar à disposição desses colaboradores. O importante é a política de segurança esteja disponível a todos os colaboradores da empresa.

2.6 Normas de Segurança da Informação Voltadas para o Setor de Saúde

Devido a frequente preocupação relacionada à segurança da informação nas instituições hospitalares, fez-se necessário a criação de leis e resoluções a fim de garantir a proteção de informações da saúde.

O setor da saúde no Brasil é regulamentado por três órgãos: ANVISA (Agência Nacional de Vigilância Sanitária), ANS (Agência Nacional de Saúde Suplementar) e CFM (Conselho Federal de Medicina). Na área da Tecnologia da Informação, existe a SBIS (Sociedade Brasileira de Informática em Saúde) que juntamente com o CFM, desenvolve, orienta, Pública processos e normas técnicas sobre o uso da informática na área de saúde (RODRIGUES, 2010).

SBIS é o representante brasileiro na IMIA - International Medical Informatics Association (Federação Internacional de Informática em Saúde). O objetivo da SBIS é promover o desenvolvimento de todos os aspectos da Tecnologia da Informação aplicada à Saúde por meio de elaboração da política de saúde e a promoção e incentivo na utilização de padrões para a representação da informação em saúde.

O CFM publicou em 2002 a resolução CFM n°. 1638/2002 onde define formalmente o que é prontuário eletrônico e também torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Em 2002 também foi Públicada a resolução "Normas Técnicas para o Uso de Sistemas Informatizados para o armazenamento e manuseio do Prontuário Médico”- CFM n°. 1639/2002, que apresenta normas sobre o tempo de armazenamento dos prontuários, estabelece critérios para certificação dos sistemas de informação e dá outras providências relacionadas a isso (CONARQ, 2002).

Públicada em 2008 a norma internacional ISO 27799 trata das orientações específicas do setor de saúde, no âmbito da segurança das informações. Ela apresenta controles e normas específicas do setor de saúde a fim de garantir a confidencialidade, integridade e a disponibilidade das informações por meio de controle de segurança da informação. Dividida em duas partes, ela apresenta o plano de ação de implementação do sistema de gestão da segurança da Informação (SGSI) e traz o código de prática, conjunto de controles a serem implementados (LEITE, 2013).

A ISO 27799 fornece guias de implementação da norma ISO/IEC 27001:2005 e apresenta controles que visam garantir a segurança da informação prevista na ISO/IEC 27002:2005. A ISO 27799 é complementar para o setor da saúde, e auxiliar à execução e implementação da ISO 27002.

O objetivo das normas e resoluções existentes é ressaltar a importância da segurança da informação e garantir a sua integridade, disponibilidade e autenticidade das informações nas instituições hospitalares.

3 ESTUDO DE CASO

Como procedimento de pesquisa, este trabalho se baseia em um estudo de caso, cujo principal objetivo é verificação de possíveis ameaças e falhas existentes concernentes à segurança da informação.

Foi escolhido o hospital ABC para a realização dessa pesquisa tendo em vista o grande fluxo de informações que circulam diariamente entre os funcionários. O procedimento de coleta de dados adotado foi à utilização de um questionário estruturado (anexo A) submetido aos funcionários com perguntas claras e objetivas, garantindo a uniformidade do entendimento dos entrevistados. O questionário contém dezoito perguntas, que foi respondido por vinte funcionários, com o objetivo de coletar informações sobre o conhecimento e entendimento dos funcionários que utilizam computadores em seus ambientes de trabalho sobre o tema Segurança da Informação.

Esta pesquisa teve o objetivo de identificar o nível de conhecimento dos funcionários de um hospital no que se refere à segurança da informação. Para que se obtivessem informações completas e precisas, bem como para evitar um possível constrangimento enquanto concediam suas respostas, foi conferida a plena liberdade de resposta aos entrevistados, já que a identificação dos mesmos não foi solicitada, Para todos os participantes foi garantido sigilo, anonimato e liberdade de participar e sair da pesquisa.

O estudo de caso foi realizado no decorrer do mês de maio de 2013. A coleta de dados foi realizada pelo próprio pesquisador entre os dias 24 e 28 de maio de 2013 e os questionários foram recolhidos entre os dias 27 e 28 de maio de 2013. Entre os participantes estavam profissionais da saúde como médicos e enfermeiros, funcionários que lidam com o departamento financeiro da empresa e funcionários que tem o primeiro contato com os pacientes. Após serem recolhidos os dados, foi efetuada a respectiva análise.

3.1 Apresentação e discussão dos resultados

Após a análise dos dados, obtiveram-se os seguintes resultados:

- Acesso à rede de computadores: 95% dos entrevistados tem acesso à rede de computadores da empresa através de *login* e senha própria;
- Acesso à internet: 90% dos entrevistados possuem acesso à internet;
- *Login* e senha liberado: metade dos entrevistados (50%) afirmou que tem o hábito de deixar seu computador ligado com *login* e senha liberado ao sairem pra almoçar ou para uma pequena pausa, conforme observa-se na figura 4;

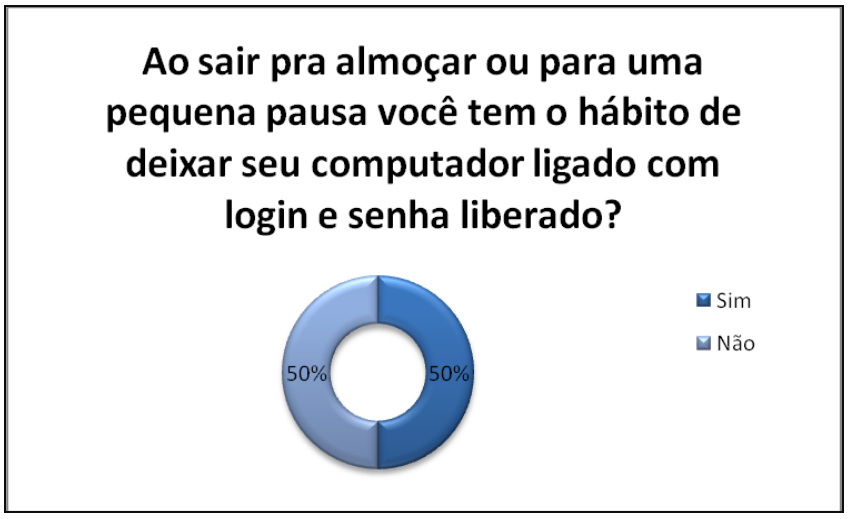

Figura 4 – Hábito de deixar *login* e senha liberados (Autoria própria, 2013).

- Emprestar seu login e senha : dos entrevistados, 20% confirmaram que tem o costume de emprestar seu *login* e senha para outros funcionários;
- Permite que outra pessoa utilize o computador com seu *login* e senha: 35% afirmaram que permitem que outra pessoa utilize o computador sua autenticação ativa, conforme observado na figura 5;

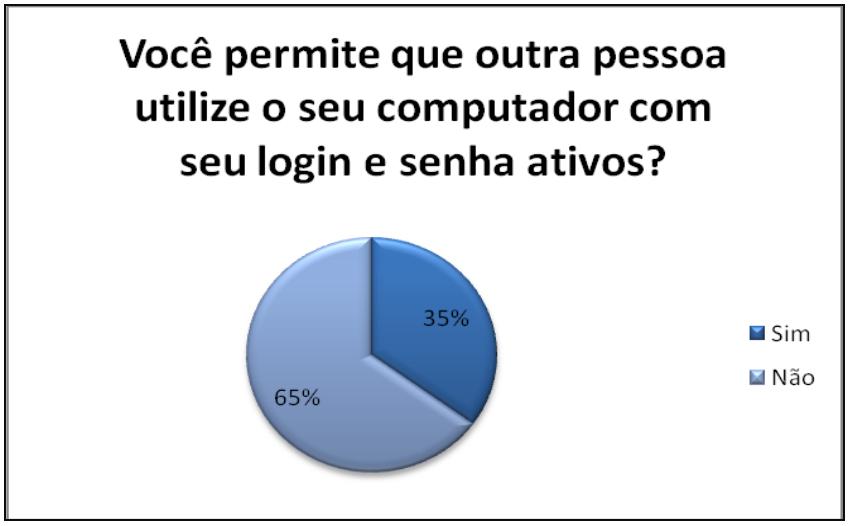

Figura 5 – Utilização de *login* e senha (Autoria própria, 2013).

- Utilização de *login* e senha de outro funcionário: 15% têm o hábito de utilizar *login* e senha de algum colega de trabalho;
- Lembrete se senhas: 20% dos entrevistados utilizam anotações de senhas de acesso como lembrete;
- Alteração de senhas: conforme pode ser observado na figura 6, 100% dos entrevistados não alteram suas senhas regularmente;

Figura 6 – Alteração de senhas (Autoria própria, 2013).

- Significado de “*backup*”: 75% afirmaram que sabem o significa da palavra *“backup*”;

- Cópia de documentos: 25% tem o costume de fazer uma cópia extra dos seus documentos, conforme figura 7. Esse percentual é muito pequeno comparado com o percentual que afirmou saber o que significa a expressão *“backup*”;

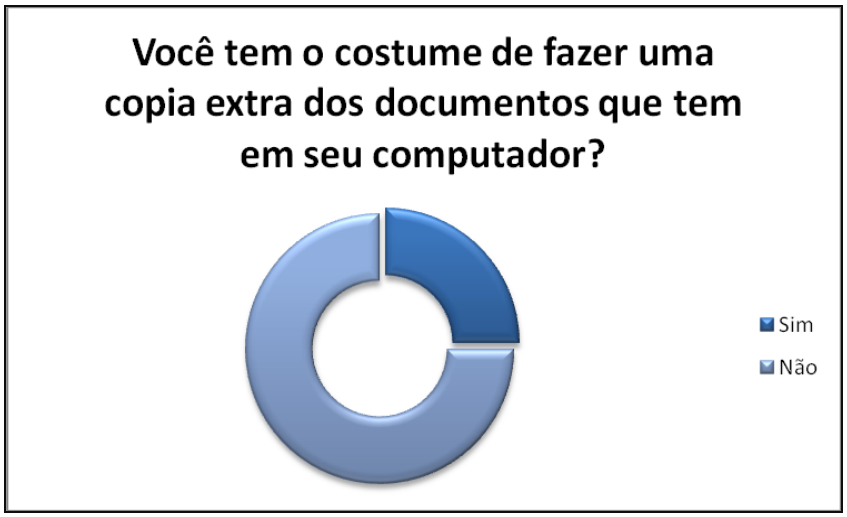

Figura 7 – Cópia de segurança (Autoria própria, 2013).

- Local de armazenamento dos documentos: 55% salvam seus arquivos e documentos no HD do computador enquanto somente 30% armazenam suas informações na unidade de rede disponível para cada usuário.

- Responsabilidade pela segurança das informações: 37% atribuíram à responsabilidade de garantir que as informações existentes no seu computador não sofra nenhuma alteração a eles mesmos juntamente a equipe de TI e 37% atribuíram a responsabilidade somente à equipe de TI. A figura 8 mostra a porcentagem dos entrevistados sobre que eles acreditam que sejam responsáveis pela segurança da informação.

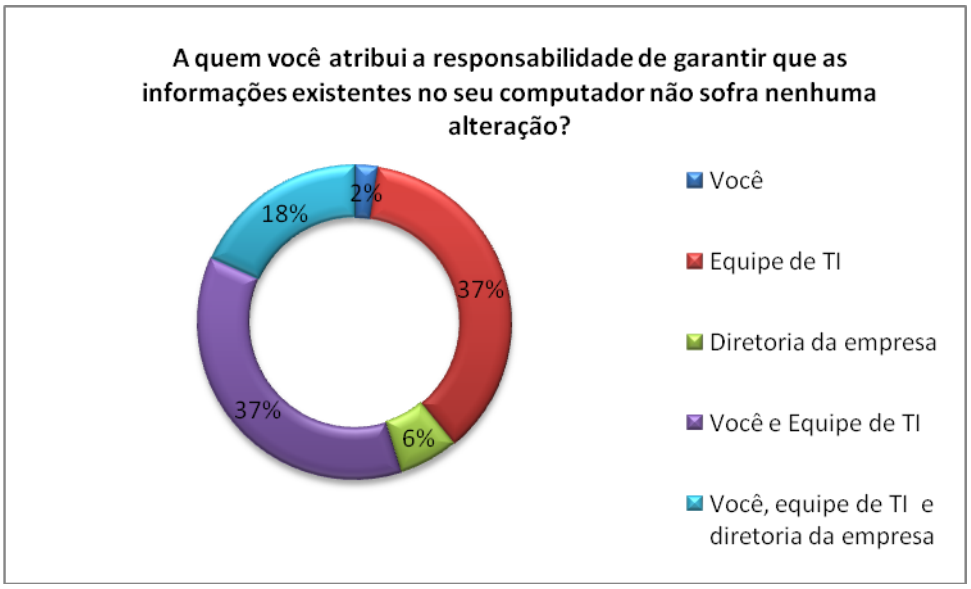

Figura 8 - Responsabilidade pela segurança da informação (Autoria própria, 2013).

- Informações confidenciais da empresa: 45% dos entrevistados trabalham em setores que tem acesso a informações confidenciais e 55% afirmam ser responsáveis por alguma dessas informações.

- Prontuário eletrônico do paciente (PEP): dos entrevistados 100% trabalham com algum tipo de sistema que tem acesso a informações dos pacientes e 25% tem acesso a dados pessoais, receita de medicamentos, informações médicas, processamentos médicos e resultados de exames dos pacientes.

- Segurança da informação: 70% dos participantes afirmam que entendem o significado da expressão “Segurança da informação”.

- Orientação e treinamento: 85% afirmam não ter recebido nenhum tipo de orientação referente à segurança da informação.

Para definir uma estratégia de melhoria, é necessária a realização de um diagnostico e um levantamento de problemas na organização, em que possam ser identificadas as ameaças e as oportunidades, os pontos fracos e os pontos fortes existentes. Somente após a análise dos resultados é possível identificar quais as falhas e ameaças mais evidentes nessa instituição hospitalar.

A tabela 3 apresenta os maiores riscos existentes segundo a pesquisa realizada, concernente a segurança da informação.

Tabela 3 – Maiores riscos da informação no hospital (Autoria própria, 2013).

Maiores Risco da Informação no Hospital	Sim	Não
Login e senha liberado ao sair para almoço ou pequena pausa	50%	50%
Permitem que outra pessoa utilize o seu computador com login e senha ativos.	35%	65%
Alteração de senha regularmente	0%	100%
Backup das informações	25%	75%
Responsáveis por algum tipo de informação importante da empresa.	55%	45%
Orientação/ treinamentos sobre segurança da informação	15%	75%

Metade dos entrevistados tem o hábito de deixar o computador ligados com *login* e senha liberados, esse hábito constitui um risco para a segurança da informação, pois, pessoas não autorizados podem facilmente ter acesso a dados ou recursos do sistema. Conforme a ISO 27779 (2008) o uso não autorizado por estranhos constitui uma falha de um ou mais controles de segurança.

35% dos funcionários permitem que pessoa utilize o seu computador com seu login e senha, conforme a ISO 27779 (2008) avaria na autenticação segura do usuário constitui-se um risco de segurança existente, onde funcionários utilizando dados de acesso de outros funcionários.

O hábito de alterar a senha regularmente é um dos métodos utilizados para prevenir que pessoas não autorizadas tenham acesso indevido às determinadas informações que só o proprietário de *login* tem permissão para acessar. 100% dos

entrevistados afirmaram não ter o hábito de alterar a senha regularmente, este percentual indica uma grande falha nesse aspecto de segurança.

É disponibilizado para cada usuário um espaço de armazenamento na unidade de rede, onde são orientados a salvarem seus documentos nessa unidade. Porém, 55% dos entrevistados afirmam salvar seus arquivos e documentos no HD do computador. A equipe de TI realiza *backup* diário das informações que estão armazenadas nas unidades de rede, ou seja, qualquer problema que o computador do usuário venha a ter, danificando o seu HD, as informações contidas nele serão perdidas. Somente 25% dos entrevistados fazem backup dos documentos que estão armazenados em seus computadores.

Pode-se observar que 37% dos entrevistados atribuíram à responsabilidade de garantir que as informações existentes no seu computador não sofra nenhuma alteração somente à equipe de TI. Esse percentual é um dos motivos pelos quais 75% não tem o costume de fazer uma cópia extra de seus documentos. Com os percentuais dos resultados, é notável a desinformação dos funcionários com respeito à sua responsabilidade em relação as informação da empresa.

Fontes (2006) afirma que o usuário faz toda a diferença que no que se refere à segurança da informação nas empresas. Porém, a existência e explicitação das responsabilidades de cada colaborador fazem parte do processo de segurança da informação. Portanto torna-se de imensa importância à criação e implementação de um programa de conscientização e treinamento de funcionários no que diz respeito às diretrizes corporativas voltadas para a segurança da informação.

Dentre os resultados obtidos nessa pesquisa, é notável a falha referente a procedimentos, normas e capacitação dos funcionários no que diz respeito à segurança da informação. Com isso, torna-se de extrema necessidade adotar práticas de segurança por meio da Implementação de normas e diretrizes que visam garantir a confidencialidade, integridade e disponibilidade da informação.

Quando questionados sobre as falhas existentes na empresa com respeito a utilização e armazenamento das informações, 65% acreditam que não existe falha. 15% dos entrevistaram admitem que não tem conhecimento algum de forma correta de armazenar as informações da empresa.

Assim, conforme explica Fontes (2006), em uma organização deve existir uma política de segurança da informação com o objetivo de explicar aos usuários qual a filosofia e as regras existentes sobre os recursos de TI utilizados.

A integridade, confidencialidade e disponibilidade das informações só podem ser garantidas se forem implementadas diretrizes de segurança. A implementação de controles e praticam voltadas para a segurança da informação garante que a política de segurança se torne eficaz e seja mecanismo eficaz no processo de tomada de decisões sobre o uso dos recursos de TI.

Após o conhecimento das falhas existentes na instituição em estudo, foi possível compreender qual a necessidade da instituição com relação à segurança da informação e quais são os pontos mais importantes a serem abordados na criação de uma política formal de SI.

Conforme os resultados obtidos nas perguntas feitas através do questionário, observa-se que a falta de informação e orientação aos funcionários constitui-se uma das falhas mais graves para o processo de segurança da informação. Tendo o propósito de fornecer orientação e apoio a todos os funcionários que fazem uso de computadores, a política possui uma função fundamental e assume uma grande abrangência com relação à segurança.

Por meio da política de segurança deve-se evidenciar a responsabilidade de cada colaborador referente ao uso de recursos tecnológicos disponíveis de forma a aumentar a garantia de salvaguarda às informações confidenciam da instituição e contribuir para que a política de segurança tenha um resultado pratico. Isso também contribui para a imagem pública da organização.

4 CONSIDERAÇÕES FINAIS

A utilização de sistemas de registro eletrônico nas instituições hospitalares apresenta grandes benefícios tanto para os funcionários, quando para as instituições. O S-RES traz um grande impacto e melhorias de desempenho para as organizações de saúde, visto que facilita o acesso, transporte e manuseio das informações da saúde, que inclui informações administrativas e clínicas do paciente.

Entretanto, o aumento da utilização da informação digital vem trazendo preocupação aos profissionais de TI. Visto que os sistemas de armazenamentos são complexos, passam a introduzir riscos relacionados à segurança podendo expor os pacientes e a organização de saúde. Com isso faz-se necessária a implementação de norma que tem como principal objetivo garantir a confidencialidade, a integridade e a disponibilidade das informações da organização. A ISO 27799;2008 apresenta normas que permite oferecer às instituições hospitalares, orientação sobre a gestão da segurança, por meio de guias de implementação da norma da ISO/IEC 27001:2005 e ISO/IEC 27002:2005.

O estudo de caso apresentado nesse trabalho mostra a importância da implementação de uma política de segurança da informação nas instituições hospitalares, pois, por meio dela é possível inserir um conjunto de normas, regas e procedimentos que visam garantir a confidencialidade, integridade e disponibilidade da informação.

Com base nos resultados através das respostas dos entrevistados, observa-se que um dos problemas existentes é a falta de conhecimento dos funcionários com respeito a segurança da informação. Tendo o propósito de fornecer orientação e apoio a todos os funcionários que fazem uso de computadores é de extrema necessidade a conscientização e treinamento dos funcionários sobre como lidar com a informação.

A política de segurança deve evidenciar a responsabilidade de cada colaborador referente ao uso de recursos tecnológicos disponíveis de forma a aumentar a garantia de salvaguarda às informações confidenciais da instituição e contribuir para que a política de segurança tenha um resultado prático.

O estudo realizado, através do estudo de caso e das bibliografias consultadas, leva a constatação de que as instituições hospitalares não podem desprezar o fato de que estão expostas aos mais variados tipos de riscos, ameaças e vulnerabilidades. O fato é que, nem sempre os riscos podem ser eliminados por completo, mas podem e devem ser mitigadas por meio de normas, regas e procedimentos que visam garantir a Segurança da informação.

5 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. *ISO/IEC 17.799*: Tecnologia da Informação - Técnicas de Segurança - Código de prática para gestão da segurança da informação. Rio de Janeiro, 2005.

ABNT. *ISO/IEC 27.002*: Tecnologia da Informação - Técnicas de Segurança - Código de prática para gestão da segurança da informação. Rio de Janeiro, 2005.

ABRAHÃO, M. S., *A segurança da informação digital na saúde*. São Paulo: Einstein, 2003.

CONARQ, Conselho Nacional de Arquivos. Disponível em:<http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?infoid=155&sid=55 >Acesso em: maio. 2013

FERREIRA, F.; ARAUJO, M., *Política de segurança da informação*. Rio de Janeiro: Ciência Moderna, 2008.

FONTES, E., *Praticando a Segurança da Informação*. Rio de Janeiro: Brasport, 2008.

FONTES, E., *Segurança da Informação o usuario faz a diferença*. São Paulo: Saraiva, 2006.

ISO 27799: *Health informatics — Information security management in health using. Geneva*, 2008.

LANVERLY M. J. B.; Silva E. A.; Souza, J. H.; Neves, R. P.; Nascimento, F. A.; Guimarães, A. P.; Nascimento, H. M., *Proteja o maior bem da sua empresa, a informação, com: política de segurança da informação.* Disponível em:<http://fatec.edu.br/html/fatecam/images/stories/dspti_ii/asti_ii_material_apoio_4_seguranca_informacao_politicas.pdf. >Acesso em: abr. 2013.

LEITE, V., *Segurança da Informação em Instituições de Saúde.* Business Protection Services & Solutions. Disponível em:<http://www.defenda.com.br/ >Acesso em: abr. 2013.

MACEDO, D., *Políticas de Segurança da Informação*. Disponível em:< http://www.diegomacedo.com.br/politicas-de-seguranca-da-informacao/ >Acesso em: abr. 2013.

MASSAD, E.; MARIN, H. F.; AZEVEDO, R. S., *O prontuário eletrônico do paciente na assistência, informação e conhecimento médico*. São Paulo, 2003.

PINOCHET, L. H. C., *Uma visão organizacional na formulação de políticas de segurança.* São Paulo: O Mundo da Saúde, 2011

QUINTELLA, H. L. M. M.; GONÇALVES, A. L., *Fatores críticos de sucesso da segurança da informação em uma organização hospitalar analisados através da cultura organizacional*. Revista Carioca de Produção. Disponível em:< http://www.recap.eng.uerj.br/doku.php >Acesso em: abril. 2013

RODRIGUES, R. S., *Estudo de um processo estruturado de segurança da informação em sistemas de informação do setor de saúde com base na norma ISO 27799:2008*. (Mestrado). São Paulo: Centro Estadual de Educação Tecnológica Paula Souza, 2010.

SÊMOLA, M., *Gestão da segurança da informação*. Rio de Janeiro: Campus, 2003.

SBIS, Sociedade Brasileira de Informática em Saúde. Disponível em:< http://www.sbis.org.br/ >Acesso em: maio. 2013

ANEXO – Questionário de Estudo de caso

QUESTIONÁRIO DE PESQUISA DE ESTUDO DO CASO

Esse questionário é referente a um Estudo do Caso, com a finalidade de identificação do nível de conhecimento dos funcionários quanto à segurança da informação.

1. Você tem acesso à rede de computadores da empresa através de login e senha?

   ( ) Sim ( ) Não

2. Você tem acesso à internet através dos computadores da empresa?

   ( ) Sim ( ) Não

3. Ao sair pra almoçar ou para uma pequena pausa você tem o hábito de deixar seu computador ligado com login e senha liberado?

   ( ) Sim ( ) Não

4. Você permite que outra pessoa utilize o seu computador com seu login e senha?

   ( ) Sim ( ) Não

5. Você empresta seu login e senha para algum?

   ( ) Sim ( ) Não

6. Você tem o habito de utilizar login e senha de algum colega na empresa para fazer qualquer tipo de acesso de seu interesse de trabalho ou pessoal?

   ( ) Sim ( ) Não

7. Você faz uso de lembretes para anotar seu login e senha do computador em algum lugar?

   ( ) Sim ( ) Não

8. Você tem o habito de alterar sua senha regularmente?

   ( ) Sim ( ) Não

9. Aonde você salva seus documentos no seu computador?

   ( ) Na área de trabalho ( ) Meus documentos ( ) Na rede ( ) Pen drive

10. Você sabe o que significa a "backup"?

    ( ) Sim ( ) Não

11. Você tem o costume de fazer uma copia extra dos documentos que tem em seu computador?

    ( ) Sim ( ) Não

12. No setor que você tem trabalha existem informações confidencias com relação à empresa?

    ( ) Sim ( ) Não

13. Você é responsável por algum tipo de informação importante da empresa?

    ( ) Sim ( ) Não

As informações contidas no questionário são extremamente confidenciais.
As respostas das questões são únicas e exclusivas para a realização do estudo de caso, não existe nenhum vinculo com a empresa em que foi aplicada.

14. Você trabalha com algum tipo de sistema que tem acesso a informações dos pacientes?

    ( ) Sim ( ) Não

    Se sim, marque o tipos de informação que você tem acesso.

    ( ) Dados pessoais ( ) Receita de medicamentos
    ( ) Informações médicas ( ) Processamentos médicos
    ( ) Resultados de exames ( ) Informações financeiras

15. Você sabe o que significa a expressão "Segurança da informação"?

    ( ) Sim ( ) Não

16. Você recebeu algum tipo de orientação referente à segurança da informação?

    ( ) Sim ( ) Não

17. A quem você atribui a responsabilidade de garantir que as informações existentes no seu computador não sofra nenhuma alteração

    ( ) Você ( ) Equipe de TI ( ) Diretoria da empresa

18. Em sua opinião quais as principais falhas existem na empresa com respeito à utilização e armazenamento das informações que você utiliza nos computadores:

    1 _____
    2 _____
    3 _____
    4 _____
    5 _____

Obrigado pela sua participação.

As informações contidas no questionário são extremamente confidenciais.
As respostas das questões são únicas e exclusivas para a realização do estudo de caso, não existe nenhum vinculo com a empresa em que foi aplicada.