Segurança da Informação em Âmbito Hospitalar: Estudo de Caso no Hospital Unimed Americana

Information Security in Hospital Scope: Case Study at Hospital Unimed Americana

Seguridad de la Información en Ámbito Hospitalario: Estudio de Caso en el Hospital Unimed Americana

Autora: Caroline Pereira dos Santos
Orientador: Renato Kraide Soffner[1]

Curso Superior de Tecnologia em Segurança da Informação – Faculdade de Tecnologia de Americana (FATEC Americana)
Americana – SP – Brasil

caroline.santos.lv@gmail.com, rksoffner@uol.com.br

Abstract. The purpose of this article is to describe the importance of information security in the hospital health area, through a case study performed at a hospital in the city of Americana that will cover the safety of patients' data, as ID, social security number, home address, date of birth, telephone, among others, emphasizing how medical records and exams are stored. Possible problems like system crashes and power outages will also be addressed.

Keywords: Information Security, Case Study, Information Flows, Hospital Environment.

Resumo. O objetivo deste artigo é descrever a importância da segurança da informação na área de saúde hospitalar, por meio de um estudo de caso realizado em um hospital na cidade de Americana que abrangerá a segurança aos dados dos pacientes, como RG, CPF, endereço residencial, data de nascimento, telefone, entre outros, ressaltando também como são armazenados os prontuários e exames. Eventuais problemas como queda do sistema e falta de energia e qual a solução para esses problemas também serão abordados.

Palavras-chave: Segurança da Informação, Estudo de Caso, Fluxo de Informações, Ambiente Hospitalar.

[1] **Renato Kraide Soffner**

Doutor em Educação

UNICAMP

Caroline Pereira dos Santos

SEGURANÇA DA INFORMAÇÃO EM ÂMBITO HOSPITALAR: ESTUDO DE CASO NO HOSPITAL UNIMED

Trabalho de graduaçao apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 03 de dezembro de 2018.

Banca Examinadora:

Renato Kraide Soffner (Presidente)
Doutor em Educação
Fatec Americana

Wagner Siqueira Cavalcante (Membro)
Mestre em Ciência da Computação
Fatec Americana

Luciene Maria Garbuio Castello Branco (Membro)
Mestre em Linguística Aplicada
Fatec Americana

1. INTRODUÇÃO

A tecnologia da informação vem crescendo a cada ano, tornando seu uso inevitável para a sociedade. Praticamente todas atividades executadas no dia-a-dia, seja no trabalho, ambiente de estudo ou em casa, envolvem algum meio digital, transformando, assim, a segurança em um dos bens mais importantes do meio. A segurança da informação vem sendo primordial, principalmente em empresas, e até mesmo no âmbito doméstico, como forma de proteger dados e informações confidenciais de pessoas ou empresas não autorizadas e mal-intencionadas que roubam os dados por diversos motivos sejam eles pelo desafio da quebra de segurança, também pelo roubo de informações privilegiadas que possam fazer com que uma empresa se destaque mais que a outra, aumentando seus lucros. Segundo (DAVIS, 1997) "o custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir".

A utilização da tecnologia na área da saúde trouxe inúmeros benefícios para o setor, bem como redução de gastos, uso exacerbado de recursos, bem como para auxílio na qualidade de vida, frisa-se que por meio da tecnologia foi criado nos Estados Unidos o *paradigm real time*, aparelho responsável por monitorar e controlar a diabetes de pacientes em tempo real. O dispositivo aplica a quantidade de insulina necessária e monitora o nível de glicose a cada cinco minutos. Há diversos impactos na saúde através da tecnologia, como exames mais detalhados, padronização de atendimento, diagnósticos precisos em curto espaço de tempo, eficácia em cirurgias, desde as mais simples até as mais delicadas, entre outros.

A segurança da informação, como já citado anteriormente, é fundamental no mundo tecnológico em que se vive atualmente, e pensando nisso, a ANS (Agência Nacional de Saúde Suplementar) vinculada com o ministério da saúde do Brasil, agência responsável pela normatização e controle no mercado de planos privados de saúde, exige, desde 2006, o cumprimento da ISO/NBR 17799, que é responsável por propiciar o armazenamento correto de documentos digitalizados ou em papel utilizados na área da saúde. Além disso, a SBIS (Sociedade Brasileira de Informática em Saúde) é encarregada por contribuir para melhorar e transformar a saúde, através do uso adequado das tecnologias de informação. Salienta-se que em âmbito internacional existe a Portabilidade de Informações de Saúde (HIPAA), sigla inglesa usada para definir o conjunto de normas que permitem o monitoramento de informações obtidas por organizações no setor da saúde.

As ameaças e risco à segurança de dados na área da saúde estão cada vez maiores, tendo como exemplo, o ataque sofrido pelo hospital do câncer de Barretos, localizado no interior do Estado de São Paulo, percebido no dia 27 de junho de 2017 quando *hackers* invadiram o sistema do mesmo afetando não só a unidade do hospital de Barretos, mas também, as unidades de Jales (São Paulo) e Porto Velho (Rondônia). Além de prejudicar ao menos 350 exames que seriam realizados nessas unidades no setor de radioterapia, os *hackers* pediam o valor de 300 dólares por computador para liberar o sistema a serem pagos através de *bitcoins*. Levando em conta que a unidade de Barretos tem aproximadamente mil computadores, o valor do resgate seria de R$ 995,4 mil equivalente ao câmbio do dia ocorrido.

Um dos elementos primordiais para o funcionamento de um hospital é a energia elétrica, uma vez que, todos os aparelhos que abrangem a organização são conectados a ela. Sua falta pode atingir pacientes internados em UTIs (adulto, pediátrica e neonatal), salas de cirurgia, etc. Por outro lado, mas, não menos importante, a queda do sistema também pode prejudicar o bom funcionamento do hospital, tendo como exemplo, a ministração de medicamentos, onde o equipamento conectado ao sistema fornece o medicamento ao paciente automaticamente, além de atrapalhar a emissão de exames, novos atendimentos entre outros.

Para a elaboração deste artigo foi realizado um estudo de caso no Hospital da Unimed na cidade de Americana que foi comunicado no mês de maio de 2018, abordando uma pesquisa realizada com funcionários de diversos setores do hospital tratando como eles usam a segurança da informação no dia-a-dia de trabalho. Realizou-se também, uma entrevista com o responsável da área de informática do hospital, apresentando como é trabalhada a

segurança da informação dentro da organização, juntamente com soluções para possíveis problemas como queda do sistema e falta de energia.

1.1 Objetivo geral

Trazer mais conhecimento sobre segurança da informação na área da saúde. Compreender o funcionamento e possíveis soluções de problemas de tecnologia da informação no hospital citado no estudo de caso.

1.2 Objetivos específicos

Esclarecer ao leitor o quão importante é a segurança da informação, principalmente na saúde. Trazer opiniões de especialistas no assunto, expor casos ocorridos por falta de segurança. Através do estudo de caso, apresentar o que funcionários do hospital Unimed, localizado na cidade de Americana – São Paulo, acham sobre a tecnologia da informação e sua segurança no ambiente da saúde.

1.3 Método Científico

A pesquisa foi realizada através de livros e artigos científicos, mostrando opiniões de escritores especializados no assunto também contendo uma pesquisa geral sobre a tecnologia da informação. Vale ressaltar que para o estudo de caso foi abordado o caráter qualitativo, assim compreendendo o comportamento dos funcionários do hospital diante da tecnologia da informação na saúde.

2. REVISÃO DE LITERATURA

Segurança da informação no ambiente hospitalar é um tema muito estudado, pesquisado e conhecido na maior parte do mundo, mas muitas pessoas não sabem a fundo o quão importante é. No Brasil existem vários portais a respeito do mesmo, como o DATASUS (Departamento de informática do Sistema Único de Saúde do Brasil) e a SBIS (Sociedade Brasileira de Informática em Saúde), entre outros.

O artigo “Saúde: a importância de se investir na segurança da informação dos pacientes” Lopes (2017), explica a relevância da segurança da informação na area da saúde. Eduardo é CSO (*Chief Security Officer*) da empresa *Redbelt,* que se dedica ao ramo de consultoria de segurança cibernética.

> Quando se fala em Saúde, logo se pensa em medicamentos, tratamentos, atendimento médico ou qualidade de vida. Dificilmente nos vem à mente questões relacionadas à segurança de dados de pacientes. Porém, segundo pesquisa realizada pela KPMG, 81% dos executivos de organizações ligadas à Saúde afirmaram que as suas empresas já sofreram ataques virtuais. Somente metade dos gestores entrevistados se sentia preparado para proteger a instituição de futuros ataques e 39% afirmaram não possuir mecanismos confiáveis em segurança da informação para se prevenir de futuras invasões.
>
> O IDC estima que os valores de informações médicas podem valer até 50 vezes mais do que outros dados atualmente roubados em ações criminais

> digitais. E mais: um em cada três pacientes terão seus dados roubados de instituições médicas. Um estudo recente revelou que o setor de Saúde respondeu por 9,2% das violações de dados em 2016, com mais de 4,1 mil violações reportadas, resultando na exposição de mais de 4,2 bilhões de registros médicos.
>
> (LOPES, 2017)

A matéria “Práticas essenciais para segurança da informação na área da saúde” Almeida (2016), elucida as mudanças da area da saúde com a chegada da tecnologia enfatizando a importância da segurança da informação.

> A digitalização das informações médicas é um agente que fomenta a progressão na qualidade do atendimento e com o crescente desenvolvimento de sistemas baseados na web, dados pessoais do paciente, cópias digitalizadas de documentos originais, poderão ser alvos da quebra de privacidade. No Brasil a ISO 27799 é uma norma que trata especificamente da segurança da informação na área da saúde.
>
> A boa notícia é que os sistemas informatizados também têm como um dos seus objetivos proporcionar proteção sobre as informações do cliente que é um ativo muito importante para qualquer empresa. Com isso, os especialistas em sistemas estão sempre procurando implementar práticas que garantam estes princípios essenciais de segurança da informação.
>
> (ALMEIDA, 2016)

3. SEGURANÇA DA INFORMAÇÃO

Na proporção em que os equipamentos tecnológicos passaram a ser fundamentais para operações empresariais e pessoais, também se tornou crescente os ataques cibernéticos. Por conseguinte, para que alguém use um dispositivo é necessário saber se ele está seguro para a conexão à internet. A segurança da informação transformou-se em um conceito-chave para o meio corporativo, e a mesma é formada por um conjunto de normas, políticas, orientações e outros atos que propõem preservar a informação.

A SI (Segurança da informação) é composta por três pilares principais que são:

- Confidencialidade: garante que as informações serão acessadas somente por pessoas autorizadas, sendo assim, só poderão ser visualizadas e utilizadas com a autorização prévia.
- Integridade: Maneiras de que se propõem a identificar se as informações não passaram por modificações durante seu processamento de envio.
- Disponibilidade: Revela que as informações estarão disponíveis para acesso.

Observa-se que a implementação dos três pilares é fundamental para uma política de segurança de qualidade.

Em um ambiente hospitalar as informações são divididas em dois grupos: as informações pessoais e as informações clínicas. As informações pessoais consistem em data de nascimento, nome completo, RG, CPF, endereço, telefone entre outros. Por outro lado, existem as informações clínicas que se baseiam em dados referentes a saúde do paciente, seu tratamento e exames.

A matéria: “Sua Saúde”, da Dra. Beatriz de Faria Leão (LEÃO,2015), consultora de Tecnologia da Informação e membro da Coordenadoria do Curso de Especialização em Informática em Saúde do Hospital Sírio-Libanês, mostra a importância da tecnologia no setor da saúde.

> A tecnologia da informação (TI) tem transformado a forma como o paciente é tratado, aumentando a segurança nos procedimentos médicos e proporcionando um atendimento mais rápido nas emergências. Sua área de aplicação em saúde é vasta e cobre desde o uso de TI para apoio à gestão em saúde até os aspectos mais especializados da assistência, tais como exames e tratamentos médicos.
>
> A TI tem contribuído para melhorar a capacidade de diagnóstico, organizar o atendimento, ampliar os serviços de saúde e fortalecer a relação médico-paciente.
>
> A área vem ganhando cada vez mais participação na assistência e tem como uma de suas principais missões melhorar a segurança do paciente.
>
> O prontuário eletrônico é um instrumento essencial que garante que a informação necessária para estabelecer a melhor conduta - como alergias, medicamentos em uso, fatores de risco e histórico de doenças - esteja sempre disponível.
>
> Outra vantagem é a autonomia que o paciente e sua família ganham para planejar o tratamento. Com acesso às informações de saúde, é possível decidir com mais assertividade quais as melhores opções.
>
> (LEÃO, 2015)

O *backup* (cópia de segurança), consiste na cópia de dados (redundância) para que possam ser restaurados caso ocorram perdas totais ou parciais dos dados originais. Trata-se de um serviço relativo à área de Segurança em Tecnologia da Informação. Os dados podem ser perdidos usualmente por apagamento acidental ou intencional, falhas físicas e lógicas dos sistemas de informação ou catástrofes naturais.

O risco de perda, inacessibilidade ou acesso não autorizado aos dados mantidos nos computadores devido às ameaças, aumenta a preocupação em se manter a disponibilidade, confidencialidade e integridade das informações para a continuidade dos negócios. Para segurança dos dados, além de outras medidas, é necessário que as estratégias para *backup* de dados sejam aplicadas, testadas e analisadas continuamente para serem válidas, mesmo com mudanças no ambiente de negócios.

4. ESTUDO DE CASO NO HOSPITAL UNIMED

4.1 História

A Confederação Nacional das Cooperativas Médicas (Unimed), foi fundada em 28 de novembro de 1975 e é a maior operadora de planos de saúde do Brasil, composta por 346 cooperativas, 2.554 hospitais credenciados e 117 hospitais próprios. Conta também com 114 mil médicos e 18 milhões de beneficiários, além de pronto atendimentos, laboratórios e ambulâncias que garantem a qualidade da assistência médica. Sendo assim, é o maior sistema cooperativo de saúde do mundo.

Figura 1. Hospital Unimed em Americana.

Fonte: Unimed, 2016.

A Unimed Santa Bárbara D'Oeste, Americana e Nova Odessa está próxima de comemorar 42 anos de atividades. O início dela se deu em 10 de novembro de 1976. O hospital na cidade de Americana conta com 9 leitos de UTI adulto, 7 leitos de UTI neonatal, 61 leitos de atendimento cirúrgico, 16 leitos na ala de pediatria, 28 leitos em ginecologia e maternidade e 2 leitos para centro de parto normal, contando ainda com serviço de farmácia, nutrição, pronto atendimento entre outros.

> O Hospital Unimed Americana é um dos poucos no Brasil e o único da região que possui o selo de acreditação ONA 3 (Organização Nacional de Acreditação), nível máximo de qualificação destinado apenas a hospitais que dispõem de uma equipe totalmente alinhada com a segurança do paciente, com a qualidade assistencial e com a excelência em gestão.
>
> A Certificação ONA 3 (Organização Nacional de Acreditação), certificada pelo IQG (Instituto Qualisa de Gestão), significa que o acompanhamento e a análise crítica de processos e resultados já estão incorporados ao dia a dia, que os ciclos de melhoria acontecem de forma sistemática e também que diretores, gestores, equipe de colaboradores e corpo clínico estão alinhados com o planejamento estratégico da gestão hospitalar.
>
> É um avanço importante em relação à ONA 1, conquistada em 2012 e renovada em 2014, que garante a segurança do paciente considerando estrutura física, pessoas, materiais, equipamentos, fluxos de trabalho, protocolos clínicos e registros seguros e também em relação à ONA 2, conquistada em 2016, que garante mais segurança para quem trabalha no hospital e, principalmente, para quem usa esse importante recurso da nossa Unimed.
>
> (UNIMED, 2018)

O sistema Unimed já conquistou vários prêmios, entre os quais:

- Prêmio Marca Brasil 2016 nas categorias melhor plano de saúde e setor da segurança e saúde no trabalho.
- Prêmio Top Max Brasil 2016, entregues para empresas que se mantiveram na liderança por no mínimo 8 anos.
- A 15 anos consecutivos é a Liderança Nacional no Setor de Saúde Marcas de Confiança (dados de 2016).
- No prêmio 1.000 maiores empresas 2016 a Unimed conta com 30 unidades. Vale ressaltar que elas ficaram de 2º a 50º colocação.

- No ranking “As 150 Melhores Empresas para Você Trabalhar” (2016), havia 15 cooperativas, sendo que 13 delas são Unimed.
- Pelo 24º ano consecutivo, desde 1993, a Unimed lidera o Folha Top of Mind na categoria Plano de Saúde
- A Unimed está em 21ª no ranking das marcas mais valiosas do país, sendo avaliada em R$ 2,817 bilhões (dados de 2014).

4.2 Entrevista

Esse estudo de caso aconteceu no Hospital Unimed Americana no mês de maio de 2018. Alex Jose dos Santos, analista de negócios assistências (TI) concedeu uma entrevista referente ao hospital.

Durante a entrevista, Alex informou que o hospital, localizado em Americana, possui aproximadamente 1.200 funcionários. Ressaltou também que existem dois setores de atendimento de urgência e emergência, Americana e a cidade ao lado Santa Bárbara D’Oeste. A média de pacientes atendidos por dia no hospital de Americana é de 350 pessoas e 200 atendimentos em Santa Bárbara D’Oeste. Além do intercâmbio de outras Unimeds, o hospital atende outros planos de saúde.

Segundo Alex, o hospital Unimed trabalha em formato digital, onde tudo é gravado eletronicamente, desde a parte de abertura de um atendimento quando o paciente chega na recepção do hospital até o prontuário eletrônico.

A cooperativa de saúde conta com um plano de contingência, no qual há dois momentos de acesso a informações de pacientes, no sistema de gestão hospitalar e no prontuário eletrônico. No sistema de gestão hospitalar, caso venha ocorrer qualquer problema é possível fazer o uso em papel e, assim que o sistema voltar essas informações são passadas para o sistema.

Para o gerenciamento do prontuário eletrônico existem máquinas de contingência, que salvam todas as informações que são feitas por setor. Caso possua um problema de servidor ou rede, a enfermagem ou qualquer outro médico tem acesso a informação em máquinas locais de contingência.

Ao decorrer da entrevista, Alex informou que todos os funcionários do hospital seguem uma política de segurança da informação. Essa política ressalta a segurança de informações pessoais, informações sigilosas (diagnósticos, informações médicas entre outras) e uso de senha, pois tudo o que acontece dentro da cooperativa é feito e assinado digitalmente.

Caso o hospital apresente falta de energia, os geradores são ligados automaticamente, abastecidos com diesel, pois, enquanto houver combustível não existirá parada de energia.

Alex explicou que todo funcionário recebe orientações referente a segurança da informação no momento de acolhimento, que acontece durante a primeira semana de trabalho.

Durante a entrevista, Alex informou que o hospital da Unimed em Americana fez a compra de 50 novos carrinhos beira leitos e explicou o seu funcionamento. O sistema beira leito, consiste em um carrinho que conta com um computador, leitor de código de barras e gavetas para medicamentos.

Figura 2. Carrinho beira leito.

Fonte: Psicobox, 2018.

O enfermeiro fará uso do leitor de código de barras nas pulseiras dos pacientes, aparecendo assim a identidade do mesmo na tela do computador, tendo também acesso ao prontuário eletrônico com as prescrições médicas. Então, o enfermeiro utilizará novamente o código de barras no medicamento e o sistema emitirá um sinal autorizando ou não a ministração do mesmo, evitando, assim, falhas humanas nas aplicações de medicamentos em pacientes.

4.3 Pesquisas

No estudo de caso também foi executada uma pesquisa entre dez funcionários do hospital de diversas áreas, entre elas, administrativa, farmácia, TI e pessoas da equipe de enfermagem. Ao serem perguntadas se tinham acesso à rede de computadores do hospital através de login e senha, todos os entrevistados afirmaram que sim. Em seguida foram obtidos os seguintes dados:

Os funcionários foram questionados se possuíam acesso à internet por meio de algum equipamento do hospital, e 70% deles responderam que sim, conforme observa-se na figura 3.

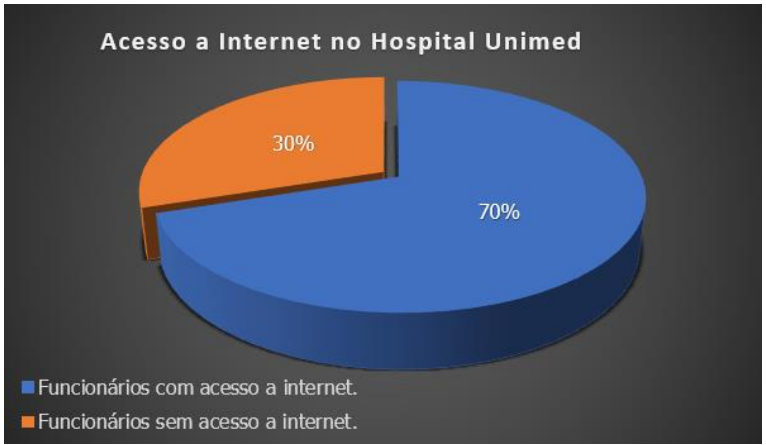


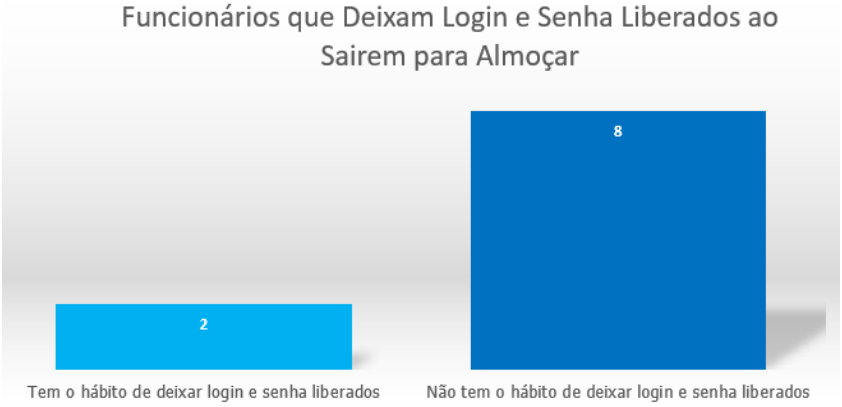
Figura 3. Pesquisa com funcionários

do hospital Unimed referente ao acesso à internet dentro do hospital.

Fonte: Imagem elaborada pelo autor, 2018.

Visando a segurança da informação dos dados do hospital, foi perguntado aos funcionários que aceitaram participar da pesquisa se, ao sair para almoçar ou para uma pequena pausa, possuíam o hábito de deixar o seu computador ligado com o login e senha liberados e 80% das pessoas disseram que não têm esse hábito (figura 4).

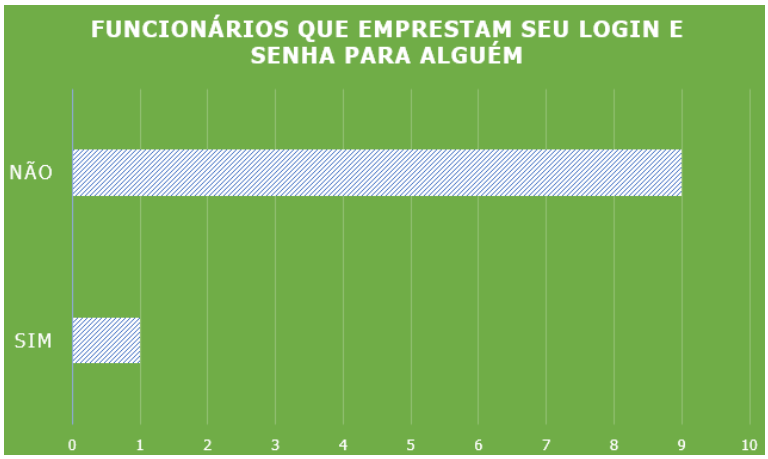
Figura 4. Pesquisa realizada no hospital Unimed sobre funcionários que deixam login e senha liberados para ao saírem almoçar.



Fonte: Imagem elaborada pelo autor, 2018.

A grande maioria dos funcionários responderam que não emprestam seu login e senha para outras pessoas, conforme demonstra a figura 5.

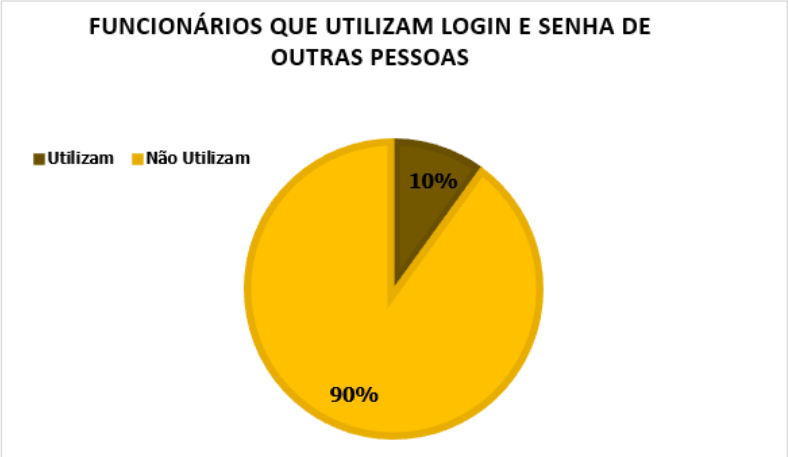
Figura 5. Pesquisa realizada no hospital Unimed referente aos funcionários que emprestam seu login e senha para alguém.



Fonte: Imagem elaborada pelo autor, 2018.

Seguindo a pesquisa e objetivando a política de segurança da informação, foi questionado se o funcionário possuía o hábito de utilizar login e senha de algum colega na empresa para fazer qualquer tipo de acesso de seu interesse de trabalho ou pessoal, e 90% dos colaboradores do hospital informaram que não utilizam login e senha de outras pessoas (figura 6).

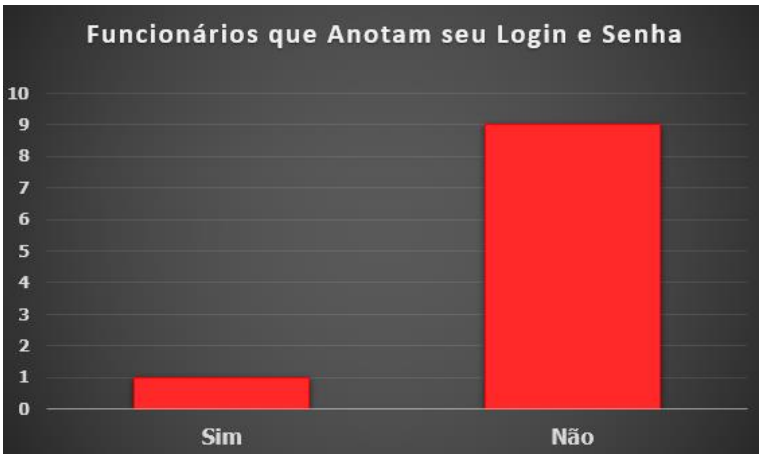
Figura 6. Pesquisa realizada no hospital Unimed referente aos funcionários que utilizam login e senha de outras pessoas.



Fonte: Imagem elaborada pelo autor, 2018.

Visando a política de senha composta na política de segurança da informação o grupo de entrevistados foi questionado se faz uso de lembretes para anotar seu login e senha do computador em algum lugar. A grande maioria das pessoas respondeu que não fazem uso de lembretes (figura 7).

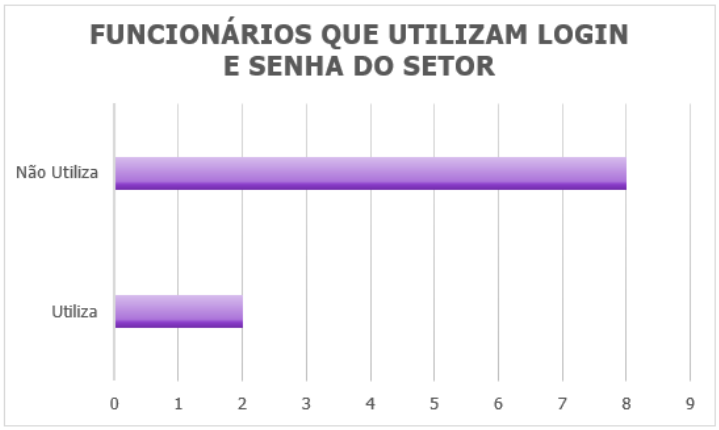
Figura 7. Pesquisa realizada no hospital Unimed referente aos funcionários que anotam seu login e senha.



Fonte: Imagem elaborada pelo autor, 2018.

Ainda objetivando a segurança dos usuários e senhas compostos na rede de computadores do hospital Unimed, foi perguntado se o colaborador utilizava login e senha de determinado setor, onde mais de uma pessoa o utilizava, e 80% deles responderam que não manuseiam login e senha de determinado setor (figura 8).

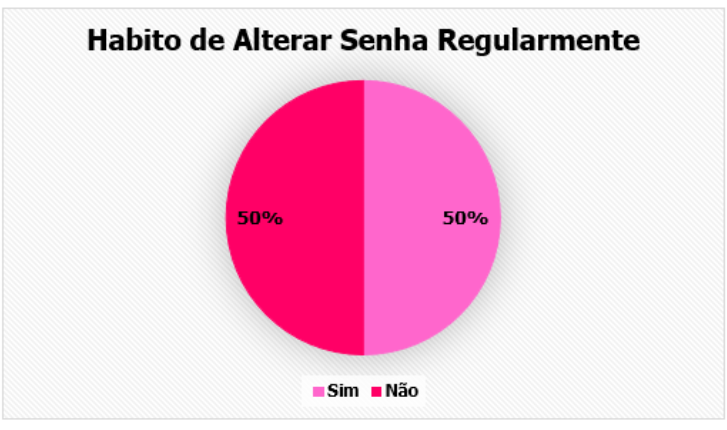
Figura 8. Pesquisa realizada no hospital Unimed referente aos funcionários que utilizam login e senha do setor.



Fonte: Imagem elaborada pelo autor, 2018.

A pergunta que mais obteve divergência na pesquisa, onde 50% dos colaboradores responderam que sim e os outros 50% informaram que não, foi o quesito referente ao hábito de alterar a senha regularmente (figura 9).

Figura 9. Pesquisa com funcionários do hospital Unimed



referente ao hábito de alterar a senha do login regularmente.

Fonte: Imagem elaborada pelo autor, 2018.

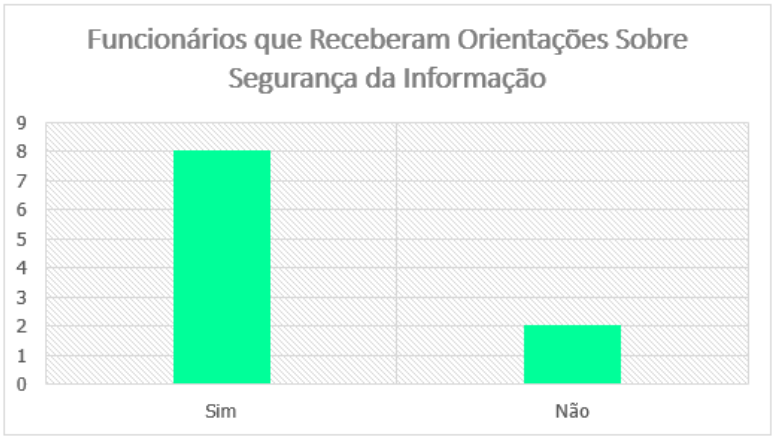
No penúltimo item da pesquisa, foi informado que os funcionários têm acesso às informações dos pacientes através da rede de computadores do Hospital Unimed (figura 10).

Figura 10. Pesquisa com funcionários do hospital Unimed referente as informações que cada um tem acesso pela rede de computadores do hospital.

Fonte: Imagem elaborada pelo autor, 2018.

No último ponto da pesquisa foi questionado se o colaborador obteve orientações referentes à segurança da informação ao entrar na cooperativa. Dentre eles 80% informaram que receberam orientação, mostrando que no Hospital Unimed existe uma política de segurança da informação de dados (figura 11).

Figura 11. Pesquisa realizada no hospital Unimed referente aos funcionários que receberam orientações sobre segurança da informação.



Fonte: Imagem elaborada pelo autor, 2018.

5. CONCLUSÃO

A utilização da tecnologia no setor da saúde é fundamental para resultados e tratamentos mais precisos e rápidos, trazendo grande benefício para as instituições de saúde, seus funcionários e seus beneficiários.

Entretanto, o aumento da tecnologia no meio deve servir de alerta para riscos e vulnerabilidades. Com isso faz-se crescer a necessidade de investimentos e cuidados no setor de segurança da informação, com implementações de políticas, com a finalidade de garantir a integridade, a disponibilidade e a confidencialidade das informações. É de extrema importância que as instituições de saúde sigam a ISO 27799:2008; ISO 27001:2005 e a ISO 27002:2005, que apresentam normas às instituições, referentes à segurança da informação.

Baseando-se nos resultados obtidos no estudo de caso realizado no hospital Unimed em Americana, foi possível observar que grande parte dos funcionários que fazem uso de computadores têm o conhecimento referente à segurança da informação, mostrando que existe uma política de segurança da informação implantada na cooperativa. Foi possível observar que

o hospital Unimed está em busca de melhorar ainda mais seu sistema de tecnologia com a aquisição do projeto beira leito.

Salienta-se que, não se pode eliminar os riscos por completo constantemente, mas devem ser atenuados com normas e regras que propõem-se garantir a segurança da informação.

AUTORIZAÇÃO PARA USO E APRESENTAÇÃO TRABALHO DE CONCLUSÃO DE CURSO

Venho autorizar a aluna, Caroline Pereira dos Santos portadora do RG: 55.835.383-6 e CPF: 447.035.988-25, estudante da Faculdade de Tecnologia de Americana (FATEC), CNPJ 62.823.257/0016-87, a utilizar o nome da instituição, HOSPITAL UNIMED AMERICANA na defesa de seu trabalho de conclusão de curso "segurança da informação em âmbito hospitalar", que será publicado em canais de comunicação impresso ou digital.

Atenciosamente,

Americana, 03 de dezembro de 2018

Dr. Oscar Kinsui

Diretor Clinico

DR. OSCAR NOBIO KINSUI
CRM - 47737

ANEXO

REFERÊNCIAS

AFRIKA, Equipe. **A segurança da informação é uma necessidade para a área de saúde.** Afrika, [entre 2015 e 2018]. Disponível em: <http://www.afrikatec.com.br/seguranca-da-informacao-e-uma-necessidade-para-a-area-de-saude>. Acesso em: 20 maio 2018

ALMEIDA, Fábio. **Práticas essenciais para segurança da informação na área da saúde.** Pixeon, 2016. Disponível em: <https://www.pixeon.com/blog/praticas-essenciais-para-seguranca-da-informacao-na-area-da-saude>. Acesso em: 20 maio 2018

BUSINESS, Portal Saúde. **O impacto da tecnologia em saúde.** Saúde Business, 2017. Disponível em: <https://saudebusiness.com/noticias/o-impacto-da-tecnologia-em-saude/>. Acesso em: 22 maio 2018

CONSULTING, Gaea. **Guia completo da segurança da informação**. Disponível em: <https://gaea.com.br/guia-completo-da-seguranca-da-informacao/>. Acesso em: 22 maio 2018

DAVIS, Peter T. **Aprenda em 14 dias o windows NT server 4. 1.** Rio de Janeiro: Editora Campus, 1997 pág.683

FESP, Unimed. **Hospital unimed Americana conquista selo de sustentabilidade.** Disponível em: <http://www.unimedfesp.coop.br/hospital-unimed-americana-conquista-selo-de-sustentabilidade>. Acesso em: 15 jun. 2018

FOLHA DE S. PAULO, Equipe. **Hackers invadem sistema do hospital de câncer de Barretos e pedem resgate.** Folha de S.Paulo, 2017. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2017/06/1896638-hackers-invadem-sistema-do-hospital-de-cancer-de-barretos-e-pedem-resgate.shtml>. Acesso em: 15 maio 2018

LEÃO, Beatriz de Faria. **Sua saúde: tecnologia da informação traz cada vez mais benefícios aos pacientes.** Hospital Sírio-Libanês, 2015. Disponível em: https://www.hospitalsiriolibanes.org.br/sua-saude/Paginas/tecnologia-informacao-traz-mais-beneficios-pacientes.aspx>. Acesso em: 10 nov. 2018

LOPES, Eduardo Bernuy. **Saúde: a importância de se investir na segurança da informação dos pacientes.** Portal Hospital Brasil, 2017. Disponível em: <http://portalhospitaisbrasil.com.br/artigo-saude-a-importancia-de-se-investir-na-seguranca-da-informacao-dos-pacientes>. Acesso em: 03 ago. 2018

NOVO MOMENTO. **Unimed faz 38 anos e aposta em tecnologia.** Disponível em: <https://www.novomomento.com.br/Sa%C3%BAde/23771/unimed-faz-38-anos-e-aposta-em-tecnologia>. Acesso em: 25 out. 2018

PSICOBOX. **Carrinho beira leito psicobox.** Disponível em: <http://www.psicobox.com.br/psi/beiraleito/>. Acesso em: 25 out. 2018

TELIUM, Netoworks. **Confidencialidade, integridade, disponibilidade: os três pilares da segurança da informação.** Disponível em: <https://blog.telium.com.br/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao>. Acesso em: 03 ago. 2018

UNIMED. **Hospital unimed: certificado ONA 3.** Disponível em: <https://www.unimed.coop.br/web/santabarbara/hospitais>. Acesso em: 25 out. 2018

- . **Somos o maior sistema cooperativo de saúde do mundo.** Disponível em: <https://www.unimed.coop.br/web/guest/home/sistema-unimed/a-unimed>. Acesso em: 25 out. 2018

WESTON, Americas. **Segurança da informação: quais são os pilares básicos para proteger empresas?**. Disponível em: <https://blogbrasil.westcon.com/seguranca-da-informacao-quais-sao-os-pilares-basicos-para-proteger-empresas>. Acesso em: 10 out. 2018

WIKIPÉDIA, a enciclopédia livre. **Unimed.** Disponível em: <https://pt.wikipedia.org/wiki/Unimed>. Acesso em: 07 nov. 2018