PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL

FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA

MESTRADO EM ADMINISTRAÇÃO E NEGÓCIOS

ODIRLEI ANTONIO MAGNAGNAGNO

MECANISMOS DE PROTEÇÃO DA PRIVACIDADE DAS INFORMAÇÕES DE PRONTUÁRIO ELETRÔNICO DE PACIENTES DE INSTITUIÇÕES DE SAÚDE

Porto Alegre

2015

ODIRLEI ANTONIO MAGNAGNAGNO

MECANISMOS DE PROTEÇÃO DA PRIVACIDADE DAS INFORMAÇÕES DE PRONTUÁRIO ELETRÔNICO DE PACIENTES DE INSTITUIÇÕES DE SAÚDE

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração e Negócios, do Programa de Pós-graduação em Administração da Faculdade de Administração, Contabilidade e Economia.

Professora Orientadora: Dr. Edimara Mezzomo Luciano

Porto Alegre

2015

Catalogação na Fonte

M186m Magnagnagno, Odirlei Antonio
Mecanismos de proteção da privacidade das informações de prontuário eletrônico de pacientes de instituições de saúde / Odirlei Antonio Magnagnagno.- Porto Alegre: PUCRS, 2015 .
138 p. il.

Dissertação (mestrado) Pontifícia Universidade Católica do Rio Grande do Sul. Porto Alegre, 2015.
Inclui bibliografia
Orientador: Profª. Drª. Edimara Mezzomo Luciano.

1. Privacidade da informação 2. Segurança da informação 3. Prontuário eletrônico de paciente – PEP I – Direito à privacidade. 4. Registros médicos – Processamento de dados. 5. Sistemas eletrônicos de segurança.

CDD 005.8
610.28

Bibliotecária
Hebe Negrão de Jimenez
CRB 101/9

Odirlei Antonio Magnagnagno

Mecanismos de Proteção da Privacidade das Informações de Prontuário Eletrônico de pacientes de Instituições de Saúde

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Administração, pelo Mestrado Interinstitucional em Administração firmado entre a Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul e Faculdade Assis Gurgacz.

Aprovado em 31 de março de 2015, pela Banca Examinadora.

BANCA EXAMINADORA:

Profa. Dra. Edimara Mezzomo Luciano
Orientadora e Presidente da sessão

Profa. Dra. Marie Anne Macadar Moron

Profa. Dra. Flávia Mori Sarti

Prof. Dr. Maurício Gregianin Testa

“Para nós os grandes homens não são aqueles que resolveram os problemas, mas aqueles que os descobriram”.
(Albert Schweitzer)

AGRADECIMENTOS

Agradeço à minha esposa Janete e às minhas filhas Gabriela e Rafaela, pela compreensão das ausências necessárias.

Agradeço à professora Edimara pela grande ajuda nas orientações e indicações e pela paciência.

À diretora da Faculdade Assis Gurgacz, Jaqueline, pelo grande incentivo e compreensão nas ausências no trabalho.

À Juliana do comitê de ética da PUC pela agilidade providencial da aprovação do projeto na sua etapa final.

Ao Décio e ao Adriano pelas indicações e auxílio nos contatos dos hospitais que foram realizados os Estudos de Caso.

RESUMO

Ao tratar de privacidade da informação na área da saúde, em virtude do acesso de muitas pessoas às informações do paciente contidas no prontuário eletrônico, o assunto ganha uma maior relevância, uma vez que o vazamento dessas informações pode ser muito impactante para o paciente, para seus familiares e também para as instituições de saúde. Os danos causados podem ser irreversíveis. O trabalho apresenta como tema a proteção da privacidade das informações do prontuário eletrônico de pacientes de instituições de saúde, relacionadas ao sigilo das informações e aos fatores que possam afetar o comportamento seguro dos profissionais que diariamente acessam os prontuários. Leva-se em consideração, como esses colaboradores são treinados ou têm acesso às melhores práticas para proteger essa informação durante o registro, armazenamento e o acesso à informação. O objetivo principal do trabalho é identificar os mecanismos e os processos que podem preservar a privacidade das informações do paciente contidas no prontuário eletrônico, verificando as práticas de tratamento das informações de acordo com a legislação. Uma vez que os hospitais de pequeno e médio porte podem não saber como fazer ou o que fazer para proteger essa informação na integridade, levando em consideração aspectos estruturais, comportamentais e processos do fluxo da informação. O referencial teórico trabalha com os conceitos de privacidade no contexto geral e a privacidade em instituições de saúde, fazendo um *link* com as legislações nacionais e boas práticas internacionais. A pesquisa é do tipo exploratória-descritiva, utilizando-se de duas abordagens metodológicas, isto é, a análise de documentos e o Estudo de Caso. O resultado final foi a localização dos documentos Regulatórios e Normativos que são pertinentes à Segurança da Informação, a identificação dos mecanismos que os hospitais pesquisados utilizam para a Segurança da Informação e a classificação dos 50 mecanismos de privacidade da informação identificados, que os hospitais possam adotar. Esses mecanismos foram identificados através da análise de Documentos Regulatórios e Normativos e através da realização de entrevistas, análise de documentos internos e observações nos dois Estudos de Caso realizados. Posteriormente agrupados e classificados por tipo, requisito e eixo de ação. Chegando-se a conclusão que os mecanismos mais citados são os processos em relação à salvaguarda e os Mecanismos de Relacionamento em relação a conscientização dos colaboradores, o

que se comprovou nos os Estudos de Caso, pois os dois hospitais possuem todos os mecanismos localizados nos Documentos Regulatórios e Normativos, mas isso ainda não é o suficiente, uma vez que nos dois casos ainda ocorrem incidentes com a informação.

Palavras-chave: Instituição de saúde - Segurança da Informação - Privacidade da Informação - Prontuário eletrônico do paciente – PEP

ABSTRACT

Information privacy in the healthcare industry gains a higher relevance, with a large number of individuals with access to the patient medical records, leaks of such information to the public may impact and cause irreversible damages to patients, their relatives and also healthcare institutions. The research focus on information privacy protection in medical records from health institutions, related with information secrecy and human behaviors from professionals which access such information in a daily basis. Is taken in to account how those professionals are trained or have access to the best practices for information protection during recording, storage and access. The main objective is to identify practices and processes that may aid to preserve information privacy in the patient's medical records, verifying vulnerabilities and data processing practices along with applicable legislation. As medium and small medical institutions, may or may not know how to proceed to protect such information as a whole, taking into account aspects such structure, behaviors and processes in the information flux. Theoretical references where worked with privacy concepts in a general context and privacy in healthcare organizations, linking national legislation and international best practices. The research is exploratory and descriptive, making use of two methodological approaches, those being document analysis and case study. The result obtained was the finding of regulations and norms relevant to Information Security, the identification of mechanisms adopted by studied institutions for information security and classify 50 mechanisms found in a manner that hospitals may adopt. These mechanisms where identified by analyzing documents containing norms and regulations, also by interviews, internal documents and observations in the two case studies. Grouped and classified by type, requisite and line of action. Is concluded that the most frequently cited are processes related to safeguards and Relational Mechanisms linked to employees' awareness, proven with case studies, as both hospitals have all mechanisms in the norm and regulations documentation, which still isn't enough as incidents are occurring in both institutions

Keywords: Healthcare Institutions – Information Security – Information Privacy – Medical Records

LISTA DE ILUSTRAÇÕES

Figura 1: Desenho de Pesquisa 41
Figura 2: Total de mecanismos identificados a partir das falas de cada entrevistado– Hospital Beta 81
Figura 3: Total de mecanismos por técnica de coleta de dados–Estudo de Caso Beta 83
Figura 4: Total de mecanismos identificados a partir das falas de cada entrevistado– Hospital Gama.....87
Figura 5: Total de mecanismos por técnica de coleta de dados–Estudo de Caso Gama 89
Figura 6: Total de citação para cada mecanismo nos Estudos de Caso 92

LISTA DE QUADROS

Quadro 1: Prontuário eletrônico do paciente - PEP.....25
Quadro 2: Elementos da Segurança da Informação 35
Quadro 3: Requisitos da Informação Segura 35
Quadro 4: Objetivos x método.....40
Quadro 5: Documentos Regulatórios e Normativos 42
Quadro 6: Variáveis do Roteiro de Entrevistas.....45
Quadro 7: Variáveis e perguntas do roteiro de entrevistas 46
Quadro 8: Identificação dos Documentos Regulatórios e Normativos 51
Quadro 9: Grupos de Trabalho do Comitê ISO TC 215 62
Quadro 10: Publicações da ISO TC 215 referentes à segurança e privacidade 62
Quadro 11: Controles de Segurança da Informação da NBR ISO/IEC 27002 64
Quadro 12: Os 10 princípios da PIPEDA 68
Quadro 13: Mecanismos encontrados nas análises dos Documentos Regulatórios e Normativos 69
Quadro 14: Mecanismos identificados (M) x Documentos Regulatórios e Normativos (D) 71
Quadro 15: Caracterização dos participantes do caso piloto 74
Quadro 16: Caracterização dos entrevistados Hospital Beta 76
Quadro 17: Mecanismos identificados nas entrevistas: Hospital Beta 80
Quadro 18: Mecanismos identificados no Estudo de Caso Beta.....82
Quadro 19: Caracterização dos entrevistados do Hospital Gama.....83
Quadro 20: Mecanismos identificados nas entrevistas: Hospital Gama.....85
Quadro 21: Mecanismos identificados no Estudo de Caso Gama 88
Quadro 22: Mecanismos identificados: Documentos Regulatórios e Normativos x Estudos de Caso.....94
Quadro 23: Relação final dos Mecanismos de Estrutura para a proteção da privacidade do paciente 97
Quadro 24: Relação final dos Mecanismos de Processo para a proteção da privacidade do paciente 98
Quadro 25: Relação final dos Mecanismos de Relacionamento para a proteção da privacidade do paciente 99

LISTA DE TABELAS

Tabela 1: Descrição dos requisitos de segurança e privacidade do TISS.....54
Tabela 2: Características técnicas do Comitê ISO TC 215 61
Tabela 3: Mecanismos identificados nos Estudos de Caso Beta e Gama 90
Tabela 4: Resumo do resultado por tipo de mecanismo 99
Tabela 5: Resumo do resultado por Eixo de Ação x Tipo do mecanismo 101
Tabela 6: Requisitos da informação x Eixo de ação.....102

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ANS – Agência Nacional de Saúde

CFM - Conselho Federal de Medicina

EAD – Educação à Distância

GED - Gerenciamento eletrônico de documentos

HIPAA - H*ealth Insurance Portability and Accountability Act*

HIS - *Hospital Information System*

IBGE - Instituto Brasileiro de Geografia e Estatística

ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira.

IMIA - *International Medical Informatics Association*

ISO - *International Organization for Standardization*

JCI – *Joint Commission International*

ONA - Organização Nacional de Acreditação

PEP - Prontuário Eletrônico do Paciente

PIPEDA – *Personal Information Protection and Eletronic Documents Act*

PIS – Profissionais de Informática em Saúde

PNIIS - Política Nacional de Informação e Informática em Saúde

SBIS - Sociedade Brasileira de Informática em Saúde

SUS – Sistema Único de Saúde

TI – Tecnologia da Informação

TISS - Troca de Informação em Saúde Suplementar

SUMÁRIO

1 INTRODUÇÃO 14

1.1 PROBLEMA DE PESQUISA 15

1.2 OBJETIVOS 19

1.2.1 Objetivo Geral 19

1.2.2 Objetivos Específicos 19

1.3 JUSTIFICATIVA 19

1.4 ESTRUTURA DO DOCUMENTO 22

2 A UTILIZAÇÃO DA TI E A PRIVACIDADE DE INFORMAÇÕES NA SAÚDE .. 23

2.1 USO DE TI NA ÁREA DE SAÚDE 23

2.2 PRIVACIDADE DE INFORMAÇÕES 26

2.2.1 Privacidade de Informações na Saúde 29

2.3 SEGURANÇA DA INFORMAÇÃO 33

2.4 DOCUMENTOS REGULATÓRIOS E NORMATIVOS DE PRIVACIDADE EM HOSPITAIS 36

3 MÉTODO DE PESQUISA 40

3.1 TÉCNICAS DE COLETA DE DADOS 42

3.1.1 Análise de Documentos Regulatórios e Normativos 42

3.1.2 Estudos de Caso 43

3.2 TÉCNICAS DE ANÁLISE DE DADOS 48

4 RESULTADOS 51

4.1 DOCUMENTOS REGULATÓRIOS E NORMATIVOS 51

4.1.1 Análise dos Documentos Regulatórios e Normativos 53

4.1.2 Identificação dos mecanismos provenientes dos Documentos 69

4.2 ESTUDOS DE CASO 73

4.2.1 Caso Piloto 74

4.2.2 Estudos de Caso no Hospital Beta 76

4.2.3 Estudos de Caso no Hospital Gama 83

4.3 CONSOLIDAÇÃO DOS RESULTADOS DOS ESTUDOS DE CASO 90

4.4 CONSOLIDAÇÃO DOS RESULTADOS DOS CASOS E DOS DOCUMENTOS 93

5 CONSIDERAÇÕES FINAIS 104

REFERÊNCIAS **110**

APÊNDICE A – ROTEIRO DE ENTREVISTA ORIGINAL **121**

APÊNDICE B – INSTRUMENTO PARA ENTREVISTAS COM PROFISSIONAIS DE TECNOLOGIA DA INFORMAÇÃO. **124**

APÊNDICE C – INSTRUMENTO PARA ENTREVISTAS COM PROFISSIONAIS DE ASSISTÊNCIA MULTIDISCIPLINAR **127**

APÊNDICE D – REFERÊNCIAS BIBLIOGRÁFICAS QUE CITAM OS DOCUMENTOS REGULATÓRIOS E NORMATIVOS **130**

APÊNDICE E – IDENTIFICAÇÃO E RASTREABILIDADE DOS CÓDIGOS UTILIZADOS NA ANÁLISE DOS DADOS. **133**

APÊNDICE F – READEQUAÇÃO DOS NOMES E CÓDIGOS DOS MECANISMOS **134**

1 INTRODUÇÃO

A privacidade da informação, mesmo quando não discutido com tanta ênfase como nos dias de hoje, já vinha se tornando uma das questões mais importantes na gestão das empresas, principalmente pelo grande volume de dados trafegando em máquinas eletrônicas, através de intranet, extranet ou internet e também pela necessidade de informações completas de clientes e até informações adicionais sendo registrados nos bancos de dados das organizações (MASON, 1986).

Essa coleta dos dados dos clientes causa preocupações por parte das pessoas pelo fato de estarem suscetíveis a ameaças de privacidade em algum grau (PETRISON e WANG, 1995), sendo questionado muitas vezes pelas próprias pessoas se as informações que foram recolhidas se justificam e se foram cadastradas no banco de dados e armazenadas de maneira segura.

Em seu estudo, Degirmenci, Guhr e Breitner (2013) citam que é quase impossível para os usuários evitarem a exposição relativa à sua identidade e por isso podem sentir-se desconfortáveis com o fornecimento de informações relacionadas aos seus dados pessoais. Na pesquisa realizada por Li (2012) também é tratada a questão de privacidade da informação, trazendo a preocupação dos consumidores *on-line* quanto à coleta, manutenção ou acesso inadequado às informações pessoais por outras empresas, sem seu consentimento.

Na busca de melhorar o aspecto da privacidade da informação, as organizações têm se preocupado muito com adoção de Tecnologias da Informação, com a intenção de gerenciar os seus dados e fornecer um melhor produto ou serviço ao seu cliente de forma segura. Assim como em outros ramos de atividade, no ambiente hospitalar também há uma grande preocupação com a privacidade das informações, e ainda com um agravante, já que as informações relacionadas aos seus clientes são de extrema particularidade, pois envolvem aspectos a respeito de sua saúde. E muitas vezes, como afirmam Acquisti e Grossklags (2007) essa informação que deveria ser protegida, pode estar sendo utilizada sem que se saiba onde e como, porém, as informações do prontuário do médico estão entre os tipos de informações que mais se deseja proteger e preservar (GAERTNER e SILVA, 2005).

Todas estas informações são armazenadas no prontuário do paciente, que mais recentemente tem se transformado em um prontuário eletrônico. O prontuário eletrônico, segundo o *Institute of Medicine* (IOM, 1997), é um registro eletrônico que fornece alerta, dados, sistemas de apoio à decisão e outros recursos com a função de apoiar os usuários. Para minimizar esse agravante, Francisconi e Goldim (1998) propõem que a equipe de saúde tenha como base a política de informações sempre pensando quem necessita saber, profissionalmente, o quê, para quê, e de quem, visando aspectos da privacidade das informações no prontuário do paciente.

Segundo Luciano; Bragança e Testa (2011), os aspectos de privacidade na área da saúde têm relação com o sigilo das informações do prontuário eletrônico, e o comportamento dos profissionais que acessam estas informações constantemente, podendo apresentar diferentes níveis de atitudes em relação às políticas e mecanismos de privacidade de um hospital, devido à individualidade de cada um.

O tema abordado é a privacidade das informações tendo como foco principal a privacidade das informações dos pacientes no prontuário eletrônico em instituições de saúde, buscando identificar mecanismos através de duas abordagens metodológicas. A análise de documentos regulatórios e normativos que é a primeira abordagem, busca meios de proteção que contribuem privacidade. Já os Estudos de Caso, que é a segunda abordagem, buscam estruturas, processos e meios que são utilizados no cotidiano dos hospitais, para a privacidade das informações dos pacientes no prontuário eletrônico. Levando em consideração a atitude comportamental, conscientização penalidades, benefícios e instruções aos colaboradores. Todas as informações identificadas nas abordagens, assim como nas técnicas de entrevistas, análise de documentos e observações, utilizados nos Estudos de Caso focalizam no tema de proteção da privacidade das informações dos prontuários eletrônicos.

1.1 PROBLEMA DE PESQUISA

Segundo Luciano e Klein (2014), a Segurança de Informação é a proteção dos ativos de informação de uma organização contra a perda, vazamento indevido ou alterações. Pode ser conceituada de acordo com Anderson (2003) como uma garantia de que os riscos da informação e o controle estão equilibrados. Esse

equilíbrio é válido devido ao grande impacto que o vazamento dessas informações pode causar aos pacientes, aos médicos e às instituições de saúde. Há três abordagens que atuam em conjunto, com a intenção de proteger os ativos da informação, que segundo Luciano e Klein (2014), são: A abordagem técnica, que é a proteção do *hardware* e do *software*; a abordagem normativa que envolve a aderência de normas e regulatórios e a abordagem comportamental, que são os fatores do comportamento do usuário no papel da Segurança da Informação.

Normalmente se ouve que o componente mais fraco da Segurança da Informação é o usuário, uma vez que os recursos de TI já estariam protegidos por diversas ferramentas. O cumprimento das orientações, regulamentos e regras de Segurança de Informação por parte dos funcionários é o fator de fortalecimento da Segurança da Informação (BULGURCU et al., 2010). Porém de acordo com Da Veiga e Eloff (2010), se os funcionários não conseguirem entender algum item da Política de Segurança da Informação ou fizerem um juízo de valor e considerá-lo não aplicável ao seu trabalho, podem não cumprir as determinações, podendo gerar ameaças tanto intencionais como não intencionais ao ambiente de trabalho.

De acordo com Arce (2003), os sistemas operacionais das estações de trabalho e seus usuários seriam os mais vulneráveis a ataques internos e externos, mas Albrechtsen e Hovden (2009) enxergam o usuário como uma vulnerabilidade quando este não possui habilidades e conhecimentos necessários, ao realizar atos inseguros na instituição ou ao utilizar de forma imprudente as conexões de rede e as informações. Porém, Marciano (2006) coloca que devido à grande complexidade da segurança, para se manter seguro é necessário ter atenção à configuração de todos os níveis de usuários e também aos sistemas. Mas a preocupação com as pessoas não deixa de ser grande, pois Goldim e Francisconi (2005) afirmam que em um hospital de grande porte, durante uma internação, até 75 pessoas diferentes chegam a lidar com o prontuário de um paciente.

Como esse número de pessoas é expressivo, vale ressaltar o estudo de Klein (2014), no qual teve o objetivo de desenvolver um modelo teórico para entender se o contentamento com colegas, superiores ou com a organização influencia positivamente o comportamento seguro em relação à Segurança da Informação. Após a sua análise, o autor verificou que o contentamento tem um efeito significativo, com um papel importante do comportamento seguro. A não ser que o

funcionário esteja descontente com a organização, seus colegas ou superiores, ao enfatizar a gravidade dos incidentes de segurança, os colaboradores terão motivação para prática de um comportamento adequado as instruções de acordo com as normas.

Os fatores que levam a comportamentos potencialmente inseguros, segundo Silva e Stein (2007), têm sido pouco pesquisados e se tem feito pouco para identificar e principalmente tentar resolver o problema. Todavia, o estudo de LUCIANO et al. (2010) desenvolve um modelo teórico para entender como o comportamento com a Segurança da Informação, a familiaridade com as políticas, a consciência, o ambiente organizacional e as condições de trabalho podem contribuir para a violação da Segurança da Informação. E Herath e Rao (2009) complementam, que a intenção do comportamento e a severidade da punição são influenciadas em relação à certeza da detecção do não cumprimento das normas, porém, segundo Boss et al. (2009), as organizações enfrentam um desafio muito grande para promover as normas e as políticas e os procedimentos de segurança de uma forma eficaz.

Muitas delas procuram se proteger através de uma boa Política de Segurança da Informação, que, segundo a RFC (2002) é um conjunto de regras com a finalidade de regulamentar e proteger os recursos de um sistema. Para Pelissari (2002), a sua utilidade é definir as responsabilidades do uso de recursos computacionais. É importante nessa política a preservação da privacidade com a análise de riscos, pois Finne (1998) define os riscos como sendo a soma das ameaças, ou seja, que causam danos. As organizações de maneira geral, incluindo-se as instituições de saúde, têm se esforçado para minimizar os riscos e os incidentes de segurança, a fim de maximizar a Segurança da Informação. Em especial no caso de hospitais, com um grande volume de dados sigilosos registrados no prontuário eletrônico que necessitam ser protegidos (ABRAHÃO, 2003).

Porém, é difícil para os hospitais saberem exatamente como garantir a privacidade das informações de uma maneira integra. Um dos meios utilizados, além das políticas de segurança é a criação de normas, que podem ser formais ou informais, que orientem os colaboradores de uma instituição de saúde quanto à privacidade de informação, sendo ela da instituição como um todo, ou

especificamente das informações dos pacientes contidas nos prontuários eletrônicos. As normas que orientam os profissionais de uma instituição de saúde quanto à privacidade da informação, podem ser internas, mas também podem ser utilizadas normas externas. Os códigos de ética médica e de enfermagem são um exemplo de documentos normativos e que tratam em seu conteúdo as questões legais e éticas da profissão.

Há diversos desafios que devem ser solucionados para que se tenha uma maximização das vantagens da utilização do prontuário eletrônico, que vão desde o problema legal e ético até o problema técnico, como por exemplo, a legislação e a priorização da privacidade, para garantir a integridade da informação do paciente, desde o seu registro, acesso e armazenamento. Outro fator segundo Ng et al. (2009), é a explicação da gravidade e da possibilidade dos danos às informações do hospital aos funcionários. Pode tornar ainda mais eficaz a orientação fornecida sobre a Segurança da Informação, quanto ao controle de acesso das informações do prontuário, seja ele fisicamente ou eletronicamente.

O controle de acesso e a segurança física podem ser usados como um mecanismo de proteção da privacidade das informações. Para Szuba (1998) o controle de acesso é um conjunto de procedimentos que impedem ou liberam a utilização a sistemas de computador, limitando o acesso a pessoas não autorizadas, pois de acordo com Lemos (2001), nem todas as pessoas devem ou precisam ter acesso a todas as áreas e ou setores da organização. Para Haical (2002), o controle físico é o procedimento ou utilização de equipamentos para proteger ambientes ou informações com acesso restrito.

Os Mecanismos segundo Guldentops, Van Grembergen e De Haes (2004), podem ser de estrutura, processos e relacionamento. Os mecanismos de estrutura têm a responsabilidade de criar regras e papéis, os mecanismos de processos têm a função de implementar os sistemas de tomada de decisão e também gerenciar as práticas e procedimentos voltados à estratégia de TI e o mecanismo de relacionamento é entendimento dos objetivos entre negócio e TI.

Os mecanismos para esse trabalho são as estruturas, processos e relacionamentos que possam ser utilizados para maximizar a privacidade da informação do paciente no prontuário eletrônico durante o registro, armazenamento

e o acesso a informação, sob o ponto de vista de médicos, enfermeiros, instituições de saúde, profissionais de TI da saúde e governo.

Para Goldim e Francisconi (2005) as instituições de saúde são obrigadas a manter seguro os documentos que contenham os registros de informação do paciente, porém, devido ao grande crescimento de tecnologias com recursos de transmissão de dados, inúmeros desafios estão sendo propostos aos hospitais, e um deles as são novas situações de quebra de privacidade. Neste contexto, a pergunta de pesquisa que norteia este estudo é: Quais mecanismos podem ser adotados para preservar a privacidade das informações contidas no prontuário eletrônico?

1.2 OBJETIVOS

Nesta seção são apresentados o objetivo geral e os objetivos específicos deste trabalho.

1.2.1 Objetivo Geral

Identificar os mecanismos que podem contribuir para preservar a privacidade das informações registradas no prontuário eletrônico do paciente.

1.2.2 Objetivos Específicos

Com o objetivo geral definido, segue abaixo os objetivos específicos deste trabalho:

a) Identificar os documentos regulatórios e normativos que possam conter mecanismos de privacidade das informações;
b) Identificar e classificar as práticas de privacidade das informações dos casos estudados;
c) Classificar os mecanismos identificados nos Documentos Regulatórios e Normativos e os mecanismos encontrados nos Estudos de Caso.

1.3 JUSTIFICATIVA

Com o avanço das tecnologias, a acessibilidade às máquinas está aumentando velozmente, assim como os seus recursos tanto de armazenamento quanto de processamento de informações (SIMIONATO et al., 2013). Os hospitais,

assim como qualquer organização, têm a necessidade de uma resposta rápida frente às mudanças tecnológicas, e para isso é importante um registro eletrônico das informações. Dentre vários outros, como gestão de estoques, administração de recursos humanos, tem-se o registro do prontuário eletrônico, o qual traz vantagens, que segundo Perondi et al. (2008) são: controle do fluxo de pacientes, priorização do atendimentos à pacientes mais graves, inexistência de extravio de fichas, maior agilidade, e com ele há um melhor controle de medicações, podendo diminuir os erros no atendimento. Novaes e Belian (2004) e Zandieh et al. (2008), completam que há uma disponibilidade atualizada do conhecimento a fim de melhorar a efetividade do cuidado na tomada de decisão.

Porém, esse manuseio do prontuário eletrônico do paciente dentro das instituições de saúde deve ser realizado somente por pessoas habilitadas e autorizadas, pois tem que ter a garantia da preservação da informação, não perdendo o controle e evitando o vazamento dos dados. Mas dentro desse contexto, tem-se o erro humano como um fator de vulnerabilidade, que segundo Liginlal et al. (2009) pode acontecer por falta de atenção ou sobrecarga de trabalho. O erro pode ter uma consequência muito grave, como por exemplo, o funcionário da TI liberar o acesso a todos os colaboradores para visualização do prontuário eletrônico de um paciente.

Dois aspectos podem influenciar o comportamento de uma pessoa. O primeiro é no que a pessoa acredita: suas convicções, seus princípios e valores, e o segundo é o meio ambiente: tais como os valores organizacionais, opinião dos colegas e a cultura organizacional, (LUCIANO; MAÇADA e MAHMOOD, 2010). A intenção de comportamento e a severidade da punição de acordo com Herath e Rao (2009) são influenciados em relação a certeza da confirmação do não cumprimento de normas, ou seja, se o funcionário tem a certeza de que a organização irá saber a respeito do não cumprimento das normas, ele tende a segui-las. Isso significa que em instituições de saúde que não possuem normas definidas, ou que não tem o hábito de divulgá-las, estão mais suscetíveis à vulnerabilidade.

Essa intenção no comportamento pode influenciar a Segurança da Informação, uma vez que a informação é um ativo, como qualquer outro ativo importante para procedimentos de saúde, e tem um valor para o meio e consequentemente necessita ser protegida de forma adequada (ABRAHÃO, 2003),

principalmente porque segundo Hamelink (2000), as informações pessoais, têm se tornado uma grande moeda de troca em sociedades capitalistas.

Como concluíram Acquisti e Grossklags (2005) em sua pesquisa, mesmo que se tenham diversas tecnologias a fim de garantir a privacidade das informações, muitas delas, aparentemente, não têm obtido sucesso neste sentido. A informação limitada pode explicar parte desta contradição no comportamento.

Porém, o vazamento dessa informação também pode acontecer de maneira involuntária, através da técnica de Engenharia Social, que, segundo Mitnick e Simon (2003), é o uso da persuasão e influência para enganar as pessoas e conseguir informações. E isso pode ocorrer com o auxilio da tecnologia ou não. O autor também completa que:

> Os engenheiros sociais habilidosos são adeptos do desenvolvimento de um truque que estimula emoções tais como medo, agitação, ou culpa. Eles fazem isso usando os gatilhos psicológicos – os mecanismos automáticos que levam as pessoas a responderem as solicitações sem uma análise cuidadosa das informações disponíveis (MITNICK; SIMON, 2003, p.85).

Segundo Abrahão (2003), os prontuários eletrônicos devem ter níveis muito mais eficientes de segurança e preservação de informação em comparação com os prontuários em papel, uma vez que deve ser observado um rigor de normas técnicas com a utilização de sistemas de manuseio, armazenagem e recuperação das informações desses prontuários eletrônicos, garantindo que sejam preservadas com integridade. Porém, essa integridade não ocorre apenas devido a questões técnicas, mas como menciona Trcek et al. (2007), somente a tecnologia não consegue fornecer Segurança de Informação em níveis aceitáveis, e complementam dizendo que, devido ao crescimento, a tecnologia sozinha não conseguirá fornecer uma segurança adequada aos Sistemas de Informação. Já Ng, Kankanhalli e Xu (2009) escrevem que a tecnologia é necessária para garantir a Segurança da Informação, mas ela depende também do comportamento do indivíduo no aspecto de segurança.

O Brasil não conta com uma legislação específica a respeito de privacidade de informações de saúde, dizendo o que deve se feito para garantir a privacidade dos registros médicos dos pacientes nos prontuários. Para isso são utilizadas normativas e resoluções dos conselhos de Medicina, mesmo que eles não tratem diretamente do assunto, abordando apenas questões de disponibilidade de informações médicas, mostrando assim poucos mecanismos. Os documentos que

tem uma grande contribuição para a privacidade da informação são os manuais de acreditações hospitalares, mas apesar de tudo, não existe um documento que compile todos os mecanismos, que protejam a informação do prontuário eletrônico.

Embora muitos indivíduos tenham acesso ao prontuário eletrônico (GOLDIM e FRANCISCONI, 2005), aumentando a vulnerabilidade da informação, as instituições de saúde procuram minimizar o vazamento de informações, seja por acesso indevido ao sistema ou vulnerabilidade de pessoas (LIGINLAL, et al., 2009), porém, elas podem não saber como fazer ou o que fazer, uma vez que os mecanismos transformam as definições conceituais em fatos práticos.

Com isso a relevância do trabalho se justifica, pois tem a finalidade de identificar mecanismos que possam ser adotados pelas instituições de saúde para a preservação da informação do paciente registrada no prontuário eletrônico, e também como preparação para a adoção de telemedicina, mesmo que a aplicação de todo o conjunto de normas seja dificultosa e não se adeque a todas as organizações, principalmente pelas pequenas e médias instituições, devido à falta de estrutura e processos adequados.

1.4 ESTRUTURA DO DOCUMENTO

Esta dissertação seguirá a seguinte estrutura: O primeiro Capítulo apresenta a introdução, delimitação do tema, problema de pesquisa, a justificativa e os objetivos. O Capítulo 2 é utilizado para o embasamento teórico, sendo que no Capítulo 3 são apresentados os procedimentos metodológicos. No Capítulo 4 será exposta a Análise dos Resultados e por fim o Capítulo 5 apresenta às considerações finais, as contribuições, as limitações do estudo e as sugestões para próximas pesquisas.

2 A UTILIZAÇÃO DA TI E A PRIVACIDADE DE INFORMAÇÕES NA SAÚDE

Neste capítulo serão abordados os conceitos que fornecem a fundamentação do trabalho, dispostos em quatro tópicos principais sendo eles: uso de TI na área da saúde; privacidade de informações; privacidade de informações na saúde e documentos regulatórios e normativos de privacidade em hospitais.

2.1 USO DE TI NA ÁREA DE SAÚDE

Os Hospitais enfrentam muitos desafios para administrar e controlar os seus processos, por serem instituições complexas (GOLDSTEIN, 2010). Para o mesmo autor, a adoção da Tecnologia da Informação e Comunicação (TIC) possibilita a compreensão da realidade referente às tecnologias existentes e auxilia a realização dos trabalhos fornecendo suporte ao hospital, garantindo resultados positivos através da interligação dos vários departamentos. Segundo Oliveira (2012) as TICs assumem um papel bastante importante na transferência de conhecimento e compartilhamento de informações entre os profissionais que trabalham na saúde, assim como também no armazenamento, uma vez que cresce a cada dia a necessidade da disseminação dos conhecimentos oriundos desta área.

Para Goldstein (2010), a TIC pode ser eficaz nos diferentes níveis hierárquicos, tais como operacional, estratégico, planejamento ou tomada de decisão, pois pode fornecer informações para qualquer um deles, sendo assim uma ferramenta estratégica para o hospital. E com a possibilidade de tornar qualquer processo relacionado à saúde informatizado e automatizado, devido ao seu atual nível de desenvolvimento (OLIVEIRA, 2012). Isso pode significar uma economia de recursos ao hospital, pois podem melhorar as ações de administração e gerenciamento do Hospital (GOLDSTEIN, 2010).

De acordo com Xu et al. (2012), a utilização de Tecnologias Móveis têm crescido muito, proporcionando um acesso sem precedentes à internet e outros serviços agregados, aumentando também a criação de aplicações de todos os tipos. Essas aplicações podem ser de qualquer natureza, como um simples jogo *on-line*, ou como uma compra utilizando um aplicativo de loja eletrônica. Segundo Kalorama (2007), o setor da saúde também está passando por adoção de novas tecnologias, utilizando-se de internet e dispositivos móveis para realizar monitoramentos remotos,

consultas *on-line*, prescrição via internet e acesso de informações dos pacientes, assim como uma imagem de radiografia. As aplicações de internet podem muito rapidamente, por exemplo, popularizar uma informação para toda a comunidade médica mundial (OLIVEIRA, 2012).

A utilização de dispositivos móveis em ambientes hospitalares tem ocorrido devido à facilidade no acompanhamento e evolução do paciente, pois segundo Abu-Dalbouh (2014) ele permite que médicos e enfermeiros possam verificar as condições dos pacientes, trocando informações com agilidade. Porém, a utilização de aplicativos móveis muitas vezes transmite uma grande quantidade de dados pessoais em tempo real, tornando forte potencial de invasão de privacidade (FTC, 2009). Isso vem aumentando gradativamente em hospitais, mas essa não é a única preocupação acerca da privacidade das informações do paciente. Outra preocupação vem principalmente com acesso e manuseio interno do prontuário eletrônico, pois de acordo com Gaertner e Silva (2005), as informações de um indivíduo, que estão contidas no documento e registradas pela equipe médica é um dos documentos que as pessoas mais têm o desejo e muitas vezes a necessidade de preservar.

Com o crescimento da utilização de dispositivos eletrônicos e a informatização das organizações, aumenta também a necessidade de gerenciamento das informações. No setor da saúde, de acordo com Lohr (2012), o volume de dados captado diariamente dobra a cada dois anos. Devido a isso, a utilização de Sistemas de Informação é importante, para que os dados sejam tratados e transformados em informações úteis para as pessoas responsáveis.

Segundo Oliveira (2012), a tecnologia tem um papel fundamental no exercício da medicina e no atendimento ao paciente, melhorando a qualidade e agilidade de procedimentos clínicos e cirúrgicos, assim como os diagnósticos. A instituição de saúde utiliza a Tecnologia da Informação e Sistemas de Informação em diversos outros setores e serviços, como por exemplo:

a) Monitor de multi-parâmetro, para medir sinais vitais do paciente;
b) Chamada de leito por parte do paciente;
c) Central telefônica integrando ao Sistema de Informação e à conta do paciente;
d) Imagens e laudos de exames;

e) Medicamentos e materiais utilizados;
f) Procedimentos realizados;
g) Informações de evolução da saúde;
h) Prontuário Médico.

O Prontuário Médico, de acordo com Massad et al. (2003), é um documento que tem a finalidade de registrar e armazenar as informações a respeito do tratamento, ou seja, os eventos clínicos que foram prestados aos pacientes. Além dessa finalidade, ele também é importante, pois serve como um meio de comunicação entre os profissionais, uma vez que fornece informações para o cuidado do paciente. Isso independente do meio em que está o documento, ou seja, em papel ou meio eletrônico.

A utilização do prontuário eletrônico do paciente, segundo Costa (2001, 2003) e Alves (2004), tem algumas vantagens e desvantagens, conforme descrito no Quadro 1.

Quadro 1: Prontuário eletrônico do paciente - PEP

Prontuário eletrônico do paciente – PEP	
Vantagens	**Desvantagens**
Acesso mais ágil aos problemas de saúde	Grande investimento em h*ardware*
Disponibilidade de acesso remoto	Grande investimento em s*oftware*
Flexibilidade do *layout* dos dados	Grande investimento em treinamento
Utilização Simultânea	Resistência dos usuários na implantação
Legibilidade absoluta	Demora na obtenção resultados reais na implantação
Eliminação da redundância dos dados	Sujeito a falhas de hardware, *software* e redes, deixando o sistema inoperante
Fim da redigitação de informações	
Integração com outros Sistemas	
Processamento contínuo dos dados	
Organização mais sistemática	
Acesso ao conhecimento científico atualizado	
Melhoria da efetividade do cuidado	
Possível redução de custo	

Fonte: Elaborado a partir de Costa (2001,2003) e Alves (2004)

O prontuário eletrônico, “é um meio físico, um repositório onde todas as informações de saúde, clínicas e administrativas, ao longo da vida de um indivíduo estão armazenadas” (MASSAD et al., 2003, pág. 6). Porém, segundo o mesmo autor, a migração do prontuário em papel para o eletrônico tem trazido diversas mudanças para os profissionais, clientes e gestores. Uma dessas mudanças é a maneira de armazenamento e consulta dessas informações, já que no meio

eletrônico elas ficarão em banco de dados, sendo acessadas através de uma *interface* de aplicação. Além das facilidades de armazenamento, as novas Tecnologias da Informação possibilitam que os dados sejam também processados, transmitidos e publicados, viabilizando as trocas eletrônicas de informações, muitas vezes do interesse do médico e do próprio paciente (ABRAHÃO, 2003). Afetando exatamente a segurança e a privacidade dessas informações.

Segundo Campara et al. (2013), no cenário de informatização da área de saúde, esse registro eletrônico é importante porque permite o armazenamento e o compartilhamento seguro das informações de um paciente, mas para Costa (2003) o uso indevido dessa ferramenta pode colocar a Segurança da Informação e a confiabilidade da informação do paciente em risco, caso a instituição de saúde não esteja preparada para lidar com a privacidade das informações dos pacientes, que serão vistos a seguir.

2.2 PRIVACIDADE DE INFORMAÇÕES

Antes de tratar o que é a privacidade de informações é preciso entender o que é a privacidade em seu conceito geral. Originalmente, o conceito de privacidade, deriva da palavra latina privo ou *privatus*, sendo o significado a palavra privar, ou o que diz a respeito do íntimo do indivíduo, relacionando o estilo de vida com questões relacionadas ao anonimato e ao sigilo (LEIKO-LILLPI et al., 2001). A privacidade tem o seu conceito mostrado sobre dois aspectos, sendo que o primeiro foca no controle que a pessoa exerce sobre o acesso de outros a si mesmo, e o segundo, define a privacidade como uma condição ou estado de intimidade (LOCH, 2003).

Grande parte da literatura disserta com base no primeiro aspecto, como pode-se citar Faden e Beauchamp (1986) que escrevem que a privacidade é um pedido positivo de uma pessoa a um status de dignidade pessoal, a um tipo de liberdade que tem a escolha a respeito de informações ou acontecimentos pessoais que deseja revelar ou não, e qual o momento para isso. Já para Alderman e Kennedy (1995), a privacidade é um direito de cada pessoa e ela abrange desde a intimidade necessária para o pensamento crítico, permitindo que o indivíduo mantenha em segredo fatos sobre si mesmo até a garantia de independência para formar a família de acordo com valores próprios, com direito de sentir-se em segurança no seu lar. Para Rose (2006), a privacidade é observada como o receio da pessoa em perder o

controle do uso e a proliferação das informações pessoais, pois quanto menor é a privacidade, menor é o controle sobre a utilização das informações pessoais.

Para garantir a privacidade de cada pessoa, muitos países têm algum tipo documento ou lei que regulamenta os direitos e deveres dos cidadãos quanto a sua privacidade. A regulamentação da privacidade de informações no Brasil esta contida no Artigo 5º da Constituição Federal, onde rege: “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (CONSTITUIÇÃO FEDERAL, 1988). E também dentro do mesmo artigo a Constituição Federal traz:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes;
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação [...](CONSTITUIÇÃO FEDERAL, 1988).

No ano de 2014 fora aprovado o Marco Civil da Internet, que também regulamenta o acesso a informações no âmbito da internet, no seu artigo 3º, traz: “A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade” (Lei Nº 12.965, 2014). Já em outro artigo descreve:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
>
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
>
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet (Lei Nº 12.965, 2014).

E finaliza as orientações com:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações (Lei Nº 12.965, 2014).

O Canadá tem duas leis federais de privacidade que são a "*Privacy Act"* e a PIPEDA- "*Personal Information Protection and Electronic Documents Act*". Essas leis descrevem além de outras questões o direito de decidir para quem serão fornecidas as informações pessoais e para que finalidade (OFFICE OF THE PRIVACY COMMISSIONER OF CANADA).

A privacidade da informação, segundo Westin (1967) é a reivindicação de pessoas, grupos ou instituições em determinar por si próprios em que momento, qual o meio e a quantidade de informações sobre si mesmos será comunicada aos outros. Anderson e Moore (2006) colocam que a privacidade pessoal como está em constante desmoronamento com os avanços da Tecnologia da Informação e com isso tem afetado o relacionamento tanto de pessoas e profissionais. Isso ocorre devido ao grande crescimento dos riscos de quebra de privacidade, que pode acontecer de diversas formas, como por exemplo, a espionagem por meio eletrônico.

Segundo Henderson e Snyder (1999) com o avanço da Tecnologia da Informação, as informações estão tendo um valor cada vez maior, sendo considerada uma mercadoria de troca, pois a ela tem se destacado cada vez mais na vida pessoal e nas organizações. E segundo Bragança (2010), ao se tratar de privacidade dentro da Tecnologia de Informação, ela pode ser caracterizada como o risco de alimentar as empresas com informações das pessoas e os benefícios que isso gera ao indivíduo.

Para Dourish e Anderson (2006), a Tecnologia da Informação está presente na vida de cada pessoa, como Laptops, PDAS, MP3 players, telefones celulares, tendo uma proliferação de dispositivos com grande poder de processamento e armazenamento, possibilitando um poder maior de pesquisa e filtrando grandes volumes de informações e com um valor econômico acessível. Esse grande volume de informações precisam ser tratadas e compreendidas, para que sejam tomadas decisões mais precisas. Com isso surge o conceito de *Big Data*, que segundo Breternitz e Silva (2013), é um conjunto de tendências tecnológicas, permite esse tratamento e compreensão, e de acordo com Zikopoulos et al. (2012) o *Big Data* se caracteriza por quatro aspectos: volume, velocidade, variedade e veracidade.

Além da ameaça da privacidade da informação que surge devido ao grande volume de dados gerados pela organização, outro aspecto importante está

relacionado com a forma que as organizações atuam em relação á atitude de seus funcionários pelo cumprimento das Políticas de Segurança da Informação, D'Arcy e Hovav (2009) colocam que programas de conscientização, monitoramento, conhecimento das Políticas de Segurança e a percepção de sanções formais, diminuem a intenção de abusos na área de Segurança da Informação.

Uma forma de coibir abusos é deixar claro que o colaborador será severamente punido caso detectado, pois segundo Herath e Rao (2009) a severidade da punição e a certeza da detecção do não cumprimento das normas de Segurança da Informação, são fatores significativos sobre as intenções de comportamento na área de Segurança da Informação, porém para os mesmos autores a existência e a visibilidade de mecanismos de detecção provavelmente sejam mais importantes que a severidade da sanção imposta. Já o estudo de Bulgurcu et al. (2010), concluiu que as crenças de caráter normativo tem maior efeito que a intenção de cumprimento, quando comparadas à severidade das sanções. Ou seja, os funcionários serão mais propensos a seguir as políticas de segurança se percebem que há uma probabilidade alta de serem pegos no ato da violação das políticas de segurança.

A proteção e a maneira de se manter a informação protegida é um fator de extrema importância uma vez que para Dourish e Anderson (2006) a vida cotidiana está cada vez mais *on-line*, aumentado a preocupação tanto para as pessoas, organizações de uma maneira geral, comunidade científica, assim como para as Instituições de Saúde.

2.2.1 Privacidade de Informações na Saúde

As instruções a respeito de Segurança da Informação podem estar contidas nas políticas de segurança, que têm a função de dar suporte, auxiliar no planejamento de implantação de sistemas (no caso da dissertação, de prontuários eletrônicos), sobre como deve agir cada integrante da equipe de assistência médica e como será abordada a política de segurança. Porém, segundo Bulgurcu et al. (2010), a decorrência da vulnerabilidade vem do funcionário que não segue a Política de Segurança da Informação. De acordo com Vance et al. (2012) a vulnerabilidade é a possibilidade de um incidente indesejado ocorrer caso não tenha medidas para evitá-lo. Com isso, "cada organização deve estabelecer quais políticas

serão utilizadas tendo como base suas necessidades, requisitos legais, cultura interna e sistemas informatizados." (FERREIRA; ARAÚJO, 2008, p. 34).

Porém, mesmo com as políticas estabelecidas e com as boas práticas divulgadas para se melhorar a Segurança da Informação de um hospital, se o usuário do Sistema de Informação não colaborar e estiver consciente, não terá um bom êxito (Bragança et al., 2010). Já que essa consciência em relação à informação segura, de acordo com Siponen (2000) é o aumento e o esforço dos resultados das ações realizadas pelas organizações relacionadas à Segurança da Informação, sensibilizando o usuário no cumprimento e bom desempenho, a fim de diminuir as ameaças em relação à Segurança da Informação.

A NRC (1997) classifica em duas grandes áreas as ameaças com a privacidade do paciente, uma delas é a ameaça sistemática, ou seja, uma intromissão no fluxo da informação, divulgando dados além do necessário. A segunda ameaça se refere ao acesso inadequado aos dados do paciente, tanto por colaboradores que podem se utilizar de privilégios quanto por pessoas externas explorando a vulnerabilidades do Sistema de Informação.

As ameaças de segurança que podem sofrer os Sistemas de Informação relativos ao setor da saúde, segundo Win et al. (2006), é o uso não autorizado de recursos, alteração não autorizada de informações, divulgação não autorizada e a paralização do Sistema de Informação, seja ela por ataques via internet, mau funcionamento dos equipamentos em decorrência de exclusão de arquivo ou de dados corrompidos, como também a ausência de cópias de segurança e de um plano de recuperação de dados (MERCURI, 2004). Esse ataque ao Sistema de Informação e a rede, segundo Appari e Johnson (2008), pode ocorrer por uma pessoa externa que pode ser um ex-funcionário que quer se vingar, um paciente ou um hacker, com a intenção de simplesmente deixar o sistema inoperante ou ter acesso às informações de pacientes.

Todos os participantes do processo de registro, armazenamento ou acesso à informação de um prontuário eletrônico tendem, a saber, o valor da informação e a importância de preservá-la. Segundo Luciano e Klein (2014) a informação é utilizada para a tomada de decisões na organização, podendo trazer prejuízos financeiros caso ocorra algum vazamento. Por isso essa informação deve estar sempre

protegida e controlada, não importando como está sendo armazenada ou compartilhada (SÊMOLA, 2003).

Segundo Mercuri (2004), essa informação do paciente vem se acumulando ao longo do tempo e vai ganhando cada vez mais importância, pois pode conter dados muito importantes como imagens médicas, tratamentos recebidos, anamneses detectadas, hábitos alimentares, informações genéticas, estado mental, além da sua identificação pessoal com documentos, digitais, empregos, rendas, entre outros.

A privacidade na área hospitalar requer principalmente integridade e proteção de dados, tornando-se particularmente importante devido ao crescimento contínuo da tecnologia (SMITH, 1996). Essa privacidade de informações, conforme coloca Leino Kilpi, et al. (1999) em muitos casos têm a ver com o nível de confiança das informações do paciente, sendo que uma das áreas básicas de privacidade em hospitais está relacionada com a proteção de dados e a prevenção de erros de informação.

A privacidade e a confidencialidade das informações têm um grande impacto entre profissionais e instituições de saúde, visto que o potencial risco de violação de um deles compromete o nível de confiança necessária nas relações sociais, conforme coloca Curran e Curran (1991), na sua pesquisa verificou-se que 72% da equipe de enfermagem havia utilizado indevidamente o Sistema de Informação para conhecer dados sobre pacientes que não estavam sob sua responsabilidade profissional. Os autores também colocam que grande parte dos respondentes da pesquisa expressou que a motivação do acesso havia sido a mera curiosidade.

O comportamento humano pode gerar possíveis violações na Segurança da Informação e consequentemente provocar um acréscimo de vulnerabilidade (LIGINLAL et al., 2009). O mesmo autor coloca que a vulnerabilidade também ocorre por erro humano devido à sobrecarga de trabalho ou até mesmo por falta de atenção.

Outra maneira de quebra de privacidade ou confidencialidade, conforme escrevem Goldim e Francisconi (2004) são os comentários a respeito das informações dos pacientes, feitos pelos profissionais de saúde, em qualquer ambiente hospitalar e muitas vezes inapropriado, tais como elevadores, refeitórios e corredores, pois nestes lugares podem ter a presença de pessoas estranhas e que

não estejam ligadas ao atendimento do paciente e ouçam a conversa obtendo assim informações inapropriadas a respeito da saúde e tratamento do paciente.

Com a intenção de evitar esse tipo de situação, os profissionais de saúde possuem documentos regulatórios a fim de tratar de aspectos éticos nas práticas profissionais. Um exemplo é o Código de Ética Médica, de 1988, que diz em seu artigo 102:

> É vedado ao médico: revelar fato que tenha conhecimento em virtude do exercício de sua profissão, salvo por justa causa, dever legal ou autorização expressa do paciente [...] Parágrafo único, que cita: Permanece essa proibição: a) Mesmo que o fato seja de conhecimento público ou que o paciente tenha falecido; e b) Quando do depoimento como testemunha. Nesta hipótese o médico comparecerá perante autoridade e declarará seu impedimento (CÓDIGO DE ÉTICA MÉDICA).

A criação destes documentos tem a finalidade de fornecer diretrizes para a atuação profissional e uma delas é o sigilo, que segundo Massad et al. (2003) o profissional de saúde é responsável pela integridade e pela guarda da informação na qual tem acesso ao registrar, manipular, digitar, armazenar ou processar as informações.

Para Motta (2003), todos os profissionais com acesso aos dados do paciente têm o dever de manter o sigilo e a privacidade das informações e não somente os médicos que têm o acesso direto com o paciente. Isso inclui inclusive funcionários administrativos e a equipe de enfermagem. O vazamento de informações e a invasão da privacidade dos pacientes, para Pupulim e Sawada (2002), é uma questão de ética e que deve ser tratada com mais seriedade pelos profissionais da saúde, pois a ética para eles é a Ciência da Moral e ela por sua vez refere-se ao comportamento do indivíduo.

Cada indivíduo, segundo Moreira (2001), é o responsável e tem o direito às suas informações e a sua privacidade, e por isso, nenhuma empresa (incluindo hospitais e instituições de saúde) deve negligenciar esse direito ao indivíduo, mas devem guardar a informação, com todos os cuidados necessários. Mas para que essa armazenagem e consulta da informação ocorra de uma maneira segura, Fontes (2006) diz que se deve contar com funcionários com capacidade e de confiança.

Motta (2003) escreve que a privacidade é um dos principais problemas éticos quando se trata de prontuário eletrônico do paciente, pois o conteúdo dele pertence

ao paciente, sendo o hospital apenas responsável pela sua custódia, devendo ser utilizado pelas instituições ou profissionais da saúde apenas quando forem para o cuidado do paciente, não podendo revelar informações sem autorização prévia do paciente. O documento fica sob a responsabilidade do hospital, devendo o mesmo buscar meios de garantir a sua segurança e o controle de acesso sobre ele. A pesquisa de Raman (2007) mostrou que nos Estados Unidos, 75% dos pacientes se preocupam com o compartilhamento de seus dados sem a sua permissão em sites relacionados à saúde.

2.3 SEGURANÇA DA INFORMAÇÃO

Von Solms e Von Solms (2004) apresentam componentes que são importantes para que se tenha uma boa Segurança da Informação, sendo destacado inclusive pelos autores que a maioria deles são comuns e essenciais, porém muitas vezes são ignorados pela empresa por:

a) Não perceber que a Segurança da Informação é uma responsabilidade corporativa;
b) Não perceber que a informação não é um problema técnico, mas sim de negócios;
c) Não perceber que a Segurança da Informação é um problema complexo.
d) Não perceber que a identificação dos riscos é a base para o Plano de Segurança da Informação;
e) Não perceber o papel das boas práticas aplicadas internacionalmente;
f) Não perceber a importância da existência da Política de Segurança da Informação;
g) Não perceber que o Monitoramento e a conformidade da Segurança da Informação é essencial;
h) Não perceber que uma estrutura de Governança da Segurança da Informação é importante;
i) Não perceber a importância de ter um Núcleo de conscientização de Segurança da Informação, para orientar os usuários;
j) Não fornecer infraestrutura, mecanismos de apoio e ferramentas para os gestores de segurança possam exercer o seu papel.

A ISO/IEC 27002 (2005) traz como conceito de Segurança da Informação, a proteção da informação, para minimizar os danos, a fim de garantir a continuidade dos negócios e o retorno de investimentos. A Segurança da Informação é alcançada a partir da adoção de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais ou ainda funções de *software* (ABRAHÃO, 2003). Estes controles, segundo o mesmo autor, precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

Eles podem ser estabelecidos utilizando alguns conceitos de boas práticas e também com a utilização de normas oficiais para embasar e ter um bom resultado. Um dos exemplos de normatização de Segurança da Informação é o que traz a série de normas da ISO/IEC 27000, que definem quais são os enfoques que devem ser levados em consideração no momento da elaboração das políticas de Segurança da Informação, já que elas são dedicadas a isso.

As normas que mais de destacam é a norma ISO/IEC 27001:2006 e a norma ISO/IEC 27002:2005, já citada anteriormente, que respectivamente tratam dos requisitos para a gestão da Segurança da Informação e segunda trata das práticas de sistemas de gestão da Segurança da Informação, na qual busca melhorar essa gestão através do estabelecimento de diretrizes e princípios para iniciar, programar, manter e aperfeiçoar a gestão da informação nas organizações.

De acordo com Luciano e Klein (2014), a Segurança da Informação possui três abordagens que atuam em conjunto visando à proteção da informação, que é a abordagem técnica, a abordagem normativa e a abordagem comportamental, que respectivamente representam medidas de proteção com h*ardware* e s*oftware*, aderência a normas e regulamentos e o fator comportamental do usuário.

A confidencialidade, a integridade e a disponibilidade são aspectos importantes que fazem parte do contexto acerca da Segurança da Informação (SÊMOLA, 2003; ISO/IEC 27001, 2006), que são detalhadas no Quadro 2.

Esses conceitos trazidos no Quadro 2 foram evoluindo com as pesquisas, sendo acrescentados novos requisitos para a informação segura.

Quadro 2: Elementos da Segurança da Informação

Disponibilidade	É o acesso à informação, no momento que necessário, às pessoas autorizadas, garantindo a disponibilidade caso esteja devidamente habilitado.
Confidencialidade	É a proteção da informação de acordo com o grau de sigilo, com a garantia de acesso somente às pessoas autorizadas.
Integridade	É a proteção contra alterações indevidas, sendo conservada na mesma condição que foi originada, isso em todo o processo que a informação percorre.

Fonte: Elaborado a partir de Sêmola (2003); ISO/IEC 27001 (2006).

Luciano e Klein (2014) apresentam um conceito da informação, a fim de que ela tenha utilidade. Para isso precisa atender algumas condições e não somente estar disponível para a organização. De acordo com os autores, a informação, desde a sua criação até o seu descarte precisa atender sete requisitos conforme são apresentados no Quadro 3.

Quadro 3: Requisitos da Informação Segura

Requisitos	Contextualização
Confidencialidade	A informação deve ser protegida contra a sua divulgação não autorizada de acordo com o grau de sigilo do seu conteúdo
Integridade	É a validade da informação de acordo com os valores de negócios e expectativas, bem como a exatidão e a completude dos ativos de informações
Disponibilidade	É a garantia da disponibilidade da informação no momento em que se faz necessário
Autenticidade	É o dever de assegurar que a informação é autêntica
Confiabilidade	É a garantia da autoria dos dados
Conformidade	A informação deve ser mantida em conformidade com o ato regulatório da qual foi criada, por exemplo, a política de Segurança da Informação
Irrefutabilidade	É a garantia da impossibilidade de negar a autoria da informação

Fonte: Elaborado a partir de Luciano e Klein (2014)

O caminho a ser adotado pelas instituições de saúde é reduzir ao máximo quaisquer riscos às informações e manter a integridade e a disponibilidade dos Sistemas de Informação. E para isso é importante fazer uma boa análise de riscos, definindo uma política de segurança dentro e fora da organização (internet, intranet e extranet), buscando como base documentos que possam auxiliar nessa tarefa.

2.4 DOCUMENTOS REGULATÓRIOS E NORMATIVOS DE PRIVACIDADE EM HOSPITAIS

Diversos documentos contêm informações ou servem como base de consulta de profissionais de saúde a respeito de privacidade de informações. Nesse item do referencial teórico, serão descritos alguns deles, os quais serão utilizados com mais detalhes no capítulo de resultados.

Um dos documentos muito utilizado, principalmente nos Estados Unidos é a HIPAA (*health insurance portability and accountability act*), na qual o principal objetivo é a proteção dos dados de saúde e também da utilização abusiva das informações sobre a saúde do paciente. As informações médicas do paciente devem estar contidas em tecnologias a fim de protegê-las.

As informações que devem ser protegidas, de acordo com o documento, são todas aquelas relacionadas ao atendimento e aos medicamentos, como notas de visitas dos médicos, resultados e diagnósticos médicos e informações sobre a saúde. Além da proteção dos registros informatizados ela recomenda a proteção da comunicação oral e também a troca de informação por computador e armazenamento eletrônico.

A lei HIPAA exige que as informações sejam acessadas com usuário e senha individuais aos sistemas, a fim de auditar as alterações realizadas pelo usuário no Prontuário Médico do paciente. A exigência também ocorre nas ferramentas da Tecnologia da Informação, exigindo que os computadores tenham senha de acesso, limitando somente aos usuários liberados, tratando também especificamente de recomendações em relação à privacidade de certas informações de saúde.

O governo dos Estados Unidos, segundo Baumer (2000), padronizou os regulamentos que tratam do controle e registro de informações médicas, devido à preocupação da proteção da informação pessoal e isso aconteceu, devido a aprovação da HIPAA.

No Brasil, a agência a Agência Nacional de Saúde Suplementar (ANS), foi criada através da Lei 9.961 de janeiro de 2000, com a atribuição de regulamentar o setor de saúde. Segundo o próprio site da Instituição:

> A finalidade institucional é promover a defesa do interesse público na assistência suplementar à saúde, regular as operadoras setoriais - inclusive quanto às suas relações com prestadores e consumidores - e contribuir para o desenvolvimento das ações de saúde no País, e, além disso, uma de suas competências é a de proceder à integração de informações com os bancos de dados do Sistema Único de Saúde (ANS, 2013).

O relacionamento entre os Hospitais ou instituições de saúde e as operadoras de planos de saúde, ocorre constantemente através do intercâmbio de informações, por isso a ANS criou uma norma em nível nacional intitulada TISS (Troca de Informação em Saúde Suplementar), com a intenção de que a integração ocorra de uma maneira padronizada.

O padrão TISS teve como base além de algumas normas internacionais e nacionais a estrutura da HIPAA, tornando-se uma referência (MENDES, 2009).

A criação do TISS visa trazer muitos benefícios às instituições de Saúde, de acordo com o seu portal de internet, como:

a) Diminuir a burocracia entre as entidades envolvidas diretamente no mercado de saúde suplementar, como por exemplo, hospitais e planos de saúde;

b) Melhorar a comunicação entre os atores da cadeia;

c) Reduzir a utilização do papel, agilizando o acesso do beneficiário aos serviços médico-hospitalares;

d) Facilitar a obtenção de informações para estudos epidemiológicos e definição de novas políticas de saúde;

e) Favorecer a realização de análise de custos e benefícios de investimentos na área de saúde;

f) Diminuir os formulários e consequentemente as falhas no seu preenchimento, reduzindo os custos administrativos;

g) Melhorar a qualidade da assistência à saúde;

h) Possibilitar comparações e análises de desempenho institucional implicando a otimização de recursos e aumento da qualidade de gestão.

Os padrões utilizados em outros países foram aplicados gerando categorias únicas da área de informática em saúde, utilizadas para a troca de informações entre os prestadores de serviço e hospitais. Esses padrões criados são:

a) Padrão de Comunicação – Foi definida a linguagem de marcação XML/Schema;

b) Padrão de Vocabulário – Padrão de nomes de procedimentos médicos.

c) Padrão de conteúdo e estrutura – Padrões de guias e demonstrativos;

d) Padrão de Privacidade, confidencialidade e segurança - Foram adotadas as normas editadas pelo Conselho Federal de Medicina.

Outro documento que possui algum tipo de informação a respeito de privacidade de informações é o Código de Ética Médica. Consta no artigo 11 a imposição do segredo como um princípio fundamental para o exercício da medicina. Já no Capítulo IX estão as obrigações com o segredo profissional, com orientação ao médico a respeito de seus auxiliares para zelar pelo segredo profissional. Consta também orientações aos médicos para não mostrarem e nem facilitarem o acesso de pessoas não profissionais da saúde ao prontuário do paciente.

Para auxiliar na tarefa, os sistemas devem adotar mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade das informações de saúde. A certificação digital é a tecnologia que melhor provê estes mecanismos (CAMPARA et al., 2013) . Segundo o Instituto Nacional de Tecnologia da Informação (ITI), o certificado digital é um documento eletrônico com a identificação de uma pessoa ou organização, no qual contêm além de outros dados, o nome e um número exclusivo chamado de chave pública, com a finalidade de validar a assinatura em documentos eletrônicos. Em 2001 foi criada uma medida provisória que instituiu a estrutura de Chaves Públicas Brasileiras, o ICP-BRASIL, cuja finalidade é garantir a integridade, autenticidade e validade dos documentos eletrônicos no âmbito jurídico e a realização de transações eletrônicas seguras. No ambiente hospitalar, significa que o profissional pode assinar digitalmente o prontuário eletrônico do paciente, não necessitando fazer a impressão do documento.

Um documento que não se pode chamar nem de normativo e nem de regulatório, mas sim de consultivo e tem grande importância para os hospitais é o Manual de Acreditação, e o processo de acreditação segundo a ONA (2014) é um processo periódico e voluntário que visa garantir a qualidade da assistência de saúde através de padrões definidos. Com isso, o hospital passa a adotar normas,

rotinas, guias e descrição de processos e consequentemente contribui para a padronização da assistência e a melhoria da qualidade (ALONSO et al., 2014).

Quando acreditada, a instituição é reconhecida interna e externamente pelo padrão de qualidade alcançado, por receber uma qualificação comprovada, pois alcançou um padrão de negócios e assistência externamente reconhecido (EMIDIO, 2013). O manual da JCI (2014) complementa que a acreditação possibilita melhorar a qualidade do cuidado ao paciente por trabalhar continuamente para reduzir os riscos para os profissionais e pacientes através da garantia de um ambiente seguro. Porém, segundo Emídio et al. (2013), a acreditação não é apenas um processo de gestão da qualidade, mas ela busca beneficiar os usuários, os trabalhadores e o próprio hospital, pois podem servir de modelo para outras instituições, por buscar um compromisso com a ética profissional, com a segurança e com procedimentos de qualidade no atendimento da população.

Segundo Campos (2008), a acreditação é o meio mais eficaz e mais conhecido internacionalmente de avaliação externa. A implantação de uma acreditação num ambiente hospitalar, segundo o mesmo autor, passa pela estruturação de três ações, quais sejam: a gestão da segurança, a organização de processos e a gestão do resultado, ou seja, todo o processo de acreditação ocorre inicialmente avaliando os padrões que são previamente estabelecidos e é realizada uma comparação com o que o hospital executa na prática nos aspectos relacionais à segurança (estrutura), organização (processos) e práticas de gestão e qualidade (resultados) (ALONSO et al., 2014).

Para Emídio et al. (2013), os benefícios vindos da acreditação são o reconhecimento por parte da comunidade, dos planos de saúde, dos funcionários e dos médicos, pois respectivamente são reconhecidos pela garantia da assistência, pela melhor remuneração dos serviços prestados, pelo orgulho dos funcionários em trabalharem num hospital acreditado e o aumento da complexidade dos procedimentos médicos devido a rigidez da segurança.

3 MÉTODO DE PESQUISA

Neste capítulo será apresentado o método utilizado para a execução da pesquisa, com a descrição das principais fases e técnicas para a realização da coleta e análise dos dados, assim como é apresentado o desenho de pesquisa.

O Quadro 4 apresenta um resumo da abordagem metodológica que foi utilizada para se chegar ao resultado da pesquisa, atendendo os objetivos.

Quadro 4: Objetivos x método

Objetivos	Abordagem Metodológica	Técnica de coleta de dados/Objetivo
Objetivo Específico: Identificar e classificar as práticas de privacidade das informações dos casos estudados	Estudo de Caso	Entrevista Semiestruturada, Análise de Documentos internos e observações, visando verificar como é o processo utilizado para proteger a informação
Objetivo Específico: Identificar os documentos Regulatórios e Normativos que possam conter mecanismos de privacidade das informações	Análise de Documentos Regulatórios e Normativos	Verificar Documentos Regulatórios e Normativos, com o objetivo de encontrar informações a respeito de práticas, sugestões e recomendações de privacidade da informação
Objetivo Específico: Classificar os mecanismos identificados nos Documentos Regulatórios e Normativos e os mecanismos encontrados nos Estudos de Caso	Estudo de Caso + Análise de Documentos Regulatórios e Normativos	Comparar e analisar os mecanismos encontrados em cada abordagem, classificando por tipo mecanismo (estrutura, processo ou relacionamento)
Objetivo Geral: Identificar os mecanismos que podem contribuir para preservar a privacidade das informações registradas no prontuário eletrônico do paciente	Estudo de Caso + Análise de Documentos Regulatórios e Normativos	Agrupamento de todos os mecanismos identificados, qualificando por contexto e contribuição

Fonte: Elaborado pelo autor

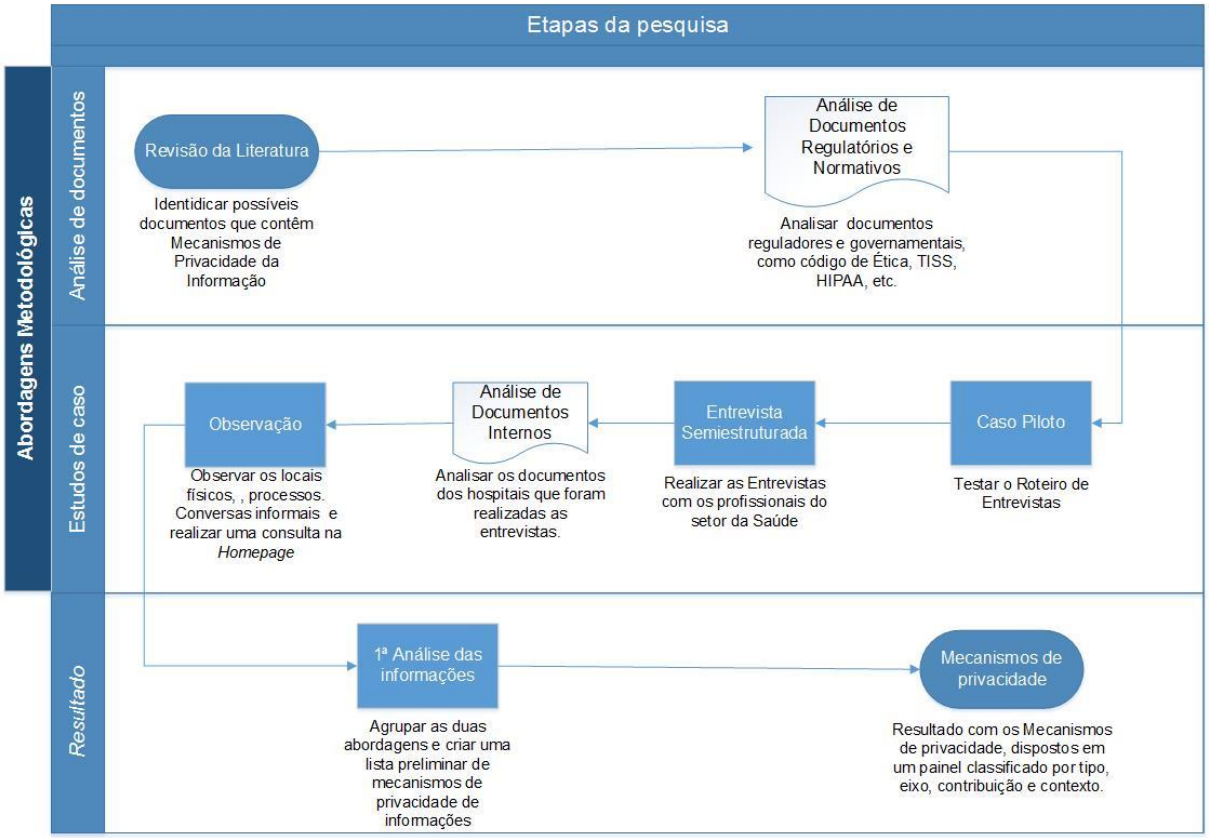
A pesquisa tem uma abordagem exploratória-descritiva, utilizando dados qualitativos. Segundo Malhotra (2001), um estudo exploratório pode ter como um dos objetivos possibilitar uma maior aproximação e entendimento do problema ao pesquisador, para que se consiga construir hipóteses mais adequadas ou tornar um problema complexo mais usual. Para Mattar (1999), a finalidade de uma pesquisa descritiva é descobrir e observar fenômenos, para posteriormente descrever, classificar e interpretar, sem modificá-lo ou interferir no mesmo.

A pesquisa foi realizada utilizando dados qualitativos, pois segundo Sampieri, Collado e Lucio (2006), a abordagem qualitativa está baseada em métodos de coleta de dados sem medição numérica, como as descrições e as observações. Seu propósito consiste em reconstruir a realidade, tal como é observada pelos atores de um sistema social predefinido.

Ela seguirá esses métodos, pois o objetivo da pesquisa é exatamente identificar os mecanismos utilizados pelos hospitais na prática, possibilitando uma verificação de todo o processo relacionado com a Segurança da Informação, desde a sua criação, manutenção e utilização, confrontando esses fatores com o que está descrito na literatura.

As técnicas de coleta de dados foram a Análise de Documentos e o Estudo de Caso. Na Figura 1 são descritos os procedimentos em cada uma das abordagens.

Figura 1: Desenho de Pesquisa



Fonte: Elaborado pelo autor

Nos itens a seguir serão detalhas as técnicas de coletas de dados, assim como os passos realizados para a análise dos dados.

3.1 TÉCNICAS DE COLETA DE DADOS

Este item do trabalho está voltado a apresentar e descrever detalhadamente as técnicas utilizadas para a coleta dos dados, dentro de cada abordagem metodológica, sendo cada uma delas realizada em uma etapa da pesquisa, conforme se detalha a seguir.

3.1.1 Análise de Documentos Regulatórios e Normativos

A primeira abordagem utilizada foi a Análise de Documentos Regulatórios e Normativos. A Análise de Documentos pode ser considerada uma rica fonte de dados, já que neles podem ser encontradas informações a respeito de práticas, sugestões e recomendações de privacidade da informação, porém, não necessariamente diretamente ligadas ao paciente e ao prontuário eletrônico. Foram analisadas 17 referências bibliográficas pertinentes ao assunto da dissertação (Apêndice D). Através delas foi possível identificar 20 possíveis documentos regulatórios que possam ter algum mecanismo de proteção de privacidade da informação. A relação dos documentos analisados consta no Quadro 5.

Quadro 5: Documentos Regulatórios e Normativos

Código	Tipo de Documento
DE1	Norma ABNT NBR ISO/IEC 27001
DE2	TISS - Troca de Informação em Saúde Suplementar
DE3	Resolução CFM Nº 1.821
DE4	Código de Ética Médica - Brasil
DE5	Código de Ética dos Profissionais de Enfermagem
DE6	Constituição Federal
DE7	Código Civil (lei 10.406)
DE8	Código de Defesa do Consumidor (lei 8.078)
DE9	Código Penal (lei nº 2.848)
DE10	Código de Ética da IMIA[1] para Profissionais de Informática em Saúde
DE11	Lei de Acesso à informação (lei nº 12.527)
DE12	Política Nacional de Informação e Informática em Saúde (PNIIS)
DE13	HIPAA - *Health Insurance Portability and Accountability Act*
DE14	ISO / TC 215
DE15	NBR ISO/IEC 27002
DE16	Marco Civil da internet
DE17	A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2
DE18	Manual de Acreditação da ONA
DE19	Manual de Acreditação da *Joint Commission International* (JCI)
DE20	PIPEDA- "*Personal Information Protection and Electronic Documents Act*"

Fonte: Elaborado pelo autor

A pesquisa documental, de acordo com Godoy (1995), pode trazer contribuições importantes para alguns estudos, e no caso desse estudo, a

[1] International Medical Informatics Association

importância se deu porque foi através deles que foram avaliados quais tipos de recomendações existem a respeito de privacidade de informação do paciente, caso as tenha. Porém, a sua utilização, segundo Yin (1989), deve ser muito cuidadosa e planejada para que eles sirvam para aumentar as evidências de outras fontes.

Esses documentos foram selecionados e analisados, pois são a base de informações que deveriam servir de roteiro no tratamento de privacidade de informação para os usuários mais comuns da área da saúde. Conforme Godoy (1995), nesse tipo de abordagem três fatores devem ser observados, que é a escolha dos documentos, o acesso a eles e a sua análise. Quanto ao acesso dos documentos, os mesmos estão disponíveis em sites de internet de cada órgão institucional ou governamental.

A finalidade principal dessa análise de documentos foi descobrir e selecionar quais são as boas práticas que tratam de privacidade da informação do paciente no prontuário eletrônico.

3.1.2 Estudos de Caso

A segunda abordagem metodológica realizada foi o Estudo de Caso. Segundo Yin (1989), ele tem a característica e a capacidade de trabalhar com várias evidências, como documentos, artefatos, entrevistas e observações e é adequado quando se estuda situações onde os comportamentos não podem ser manipulados, mas que seja possível fazer entrevistas sistemáticas, de preferência de eventos contemporâneos.

A realização do Estudo de Caso tem extrema importância para os propósitos deste estudo, pois através deles foi possível identificar processos informais que estão inseridos no cotidiano dos hospitais, porém não de menor importância, pois afetam diretamente a Segurança da Informação. Essas informações foram surgindo no decorrer das entrevistas e também no processo de observação.

Os Estudos de Caso foram realizados em dois hospitais, um deles localizado na cidade de São Paulo e outro localizado na cidade de Porto Alegre, e por questão de sigilo, serão utilizados codinomes, neste trabalho serão chamados respectivamente de Hospital Beta e Hospital Gama.

O Hospital Gama foi selecionado por ter um departamento de TI atuante e ganhador de vários prêmios com projetos inovadores na área de Tecnologia da Informação, voltado ao bem estar do paciente. É um hospital Público e possui mais de 800 leitos e no decorrer do ano de 2013 teve mais de 32.000 internações, cerca de 600.000 consultas e mais de 3.000.000 exames realizados, contando com aproximadamente 6.000 colaboradores distribuídos nos diversos setores, o que o torna um dos maiores hospitais do Brasil.

O Hospital Beta é um hospital privado, sem fins lucrativos e foi criado a mais de 90 anos, é referência Nacional em diversas Especialidades Médicas, sendo considerado um dos mais importantes centros médicos do Brasil e também da América Latina. De acordo com os dados de 2014, possui aproximadamente 450 leitos e após seu plano de expansão, contará com mais de 700 leitos. Tem cerca de cinco mil colaboradores e atende mais de 120 mil pacientes por ano. É pioneiro na incorporação de tecnologias e conhecido por suas práticas de vanguarda e excelência no atendimento.

Para se realizar esse Estudo de Caso, primeiramente foi aplicada uma entrevista semiestruturada, pois de acordo com Flick (2004), com ela é mais provável que sejam coletados os pontos de vista dos entrevistados, do que seria em uma entrevista padronizada ou num questionário.

Ela foi realizada com pessoas de TI que possuem contato com a informação do paciente no prontuário eletrônico. A entrevista semiestruturada, para Manzini (1990), pode fazer com que surjam informações de forma mais livre, não tendo um padrão de alternativas para as respostas fornecidas pelos entrevistados. A entrevista semiestruturada “[...] favorece não só a descrição dos fenômenos sociais, mas também sua explicação e a compreensão de sua totalidade [...] (TRIVIÑOS, 1987).

As entrevistas foram realizadas presencialmente, sendo gravadas em áudio e posteriormente transcritas. Foram quatro pessoas no hospital Gama e cinco pessoas no Hospital Beta, sem se preocupar com a quantidade ou com a generalização, mas sim com um aprofundamento e abrangência da compreensão, seguindo o recomendado por Minayo (1999). Dentre essas pessoas, foram o gerente responsável pela área de TI ou de Segurança da Informação, pessoas que trabalham com a interface TI/usuário final e pessoas que contribuem para a

formação das políticas de Segurança da Informação. As caracterizações detalhadas dos entrevistados de cada hospital estão descritas no capítulo de resultados.

Para a realização das entrevistas, foi elaborado um roteiro, com uma primeira parte voltada à identificação de cada um dos entrevistados, contendo alguns dados pessoais para melhor identificar e posteriormente utilizar na análise dos resultados. Foi solicitado o nome, idade, gênero, escolaridade, área de formação e experiência profissional.

A segunda parte foi criada para servir como um guia para o entrevistador não deixar de perguntar algo relevante, assim como não se desviar do assunto, perdendo tempo com questões que não fazem parte do contexto do trabalho. O roteiro foi criado com base na literatura existente sobre segurança e Privacidade da Informação. Primeiramente foram analisadas quais as variáveis que deveriam fazer parte do instrumento de pesquisa, tendo em vista o cumprimento dos objetivos. Após essa análise na literatura, chegou-se inicialmente a oito variáveis, conforme mostra o Quadro 6.

Quadro 6: Variáveis do Roteiro de Entrevistas

Variável	Objetivo	Fonte
Políticas de Segurança	Verificar se existe uma Política de Segurança da Informação. Como são criadas, divulgadas e atualizadas	FURNELL e RAJENDRAN, 2012
Regras	Quais são as regras formais e informais que o hospital estabelece para maximizar a Segurança da Informação	HERATH e RAO, 2009
Pressões no trabalho	Se existe algum tipo de pressão de cumprimento das regras, por parte do hospital e principalmente se tem algum efeito relacionado com a Segurança da Informação	HERATH e RAO, 2007
Procedimento disciplinar	Verificar quais são os procedimentos disciplinares quanto a quebra das regras de segurança	HERATH e RAO, 2007
Práticas de Segurança da Informação	Como são realizadas as tarefas cotidianas em relação às boas práticas de segurança, as proteções de equipamentos. E se existem orientações e treinamentos para as pessoas	NG et al. (2009) HERATH e RAO, 2007 BAUMER, EARP e PAYTON, 2000
Benefícios pessoais	Verificar se existe algum tipo de benefício para os que cumprem as regras e se isso tem relação com as melhores práticas de segurança	FURNELL e RAJENDRAN, 2012
Satisfação	Se os colaboradores estão satisfeitos com as atuais regras de segurança e também com o hospital, e se essa satisfação pode afetar ou não a segurança	KRAEMER e CARAYON, 2005
Comportamento pela segurança	Verificar o comportamento dos colegas perante o cumprimento das normas de segurança	HERATH e RAO, 2007

Fonte: Elaborado pelo autor com base nos autores supracitados

Posteriormente foram elaboradas as perguntas utilizando-se como base as variáveis já pesquisadas, totalizando 22 perguntas, não necessariamente com a mesma quantidade de perguntas para cada uma das variáveis, conforme descrito no Quadro 7.

Quadro 7: Variáveis e perguntas do roteiro de entrevistas

Variáveis	Aspectos a explorar	Referências
Políticas de Segurança	Como o estabelecimento trata com a questão de privacidade do paciente, existem regras ou esforços formais ou informais? O Hospital tem algum documento regulador de políticas de Segurança da Informação? Como você tem acesso a ele? Você o conhece?	FURNELL e RAJENDRAN, 2012 ABRAHÃO, 2003; FERREIRA e ARAÚJO, 2008
Regras	Você acredita que os seus colegas de trabalho cumprem as normas de segurança devido à certeza de detecção e a certeza de punição? Você acredita que essa punição é ocorre com agilidade?	HERATH e RAO, 2009
Pressões no trabalho	Porque minha atividade exige responsabilidade no cumprimento das políticas de Segurança da Informação e privacidade? Você acredita que o grande volume de tarefas ou atividades no trabalho faz com que se descuide de processos de Segurança da Informação? Tem algum exemplo?	HERATH e RAO, 2007
	O hospital me pressiona pelo cumprimento das regras presentes nas políticas de segurança nas atividades de trabalho, como ocorre?	HERATH e RAO, 2007
Procedi-mento disciplinar	Que medidas disciplinares a instituição adota para quem não cumpre com as Políticas de segurança.	HERATH e RAO, 2007
	Você acha que os procedimentos disciplinares são importantes para que as Políticas de segurança sejam cumpridas? Por quê?	HERATH e RAO, 2007
Práticas de Segurança da Informação	As práticas de segurança (treinamentos, troca de senha, controle de acesso físico e lógico, criação de normas, etc) existem no hospital? Como foram surgindo essas práticas? A quem se aplica? Elas são formais (descritas em um documento) ou são informais (apenas cumpridas por parte dos colaboradores)?	FURNELL e RAJENDRAN, 2012; CERT.BR 2012; LEMOS, 2001; NG et al. (2009)
	O Hospital é proativo em relação ao cumprimento das Políticas de Segurança da Informação, por quê? Com quais procedimentos?	FURNELL e RAJENDRAN, 2012
	O Hospital oferece informações para conscientizar sobre a necessidade de cumprir às regras das Políticas de privacidade? De que maneira?	FURNELL e RAJENDRAN, 2012
	O Hospital considera importante que cumpra com as regras de segurança? Como deixa isso claro?	FURNELL e RAJENDRAN, 2012
	O hospital exige algum conhecimento e cumprimentos das normas de segurança de documentos reguladores externos, como Código de ética profissional, SOX, HIPAA, ISO 27000. Como fazem essa cobrança?	HERATH e RAO, 2007
	Os dados são criptografados (codificados), quando se faz necessário a transmissão para ambientes externos. (ANS, Planos de saúde, etc)? Os computadores são protegidos por senha? Você pode acessar todos os pacientes que estão no hospital e verificar todos os dados deles? (Quais e o que pode acessar). Quais são as orientações para proteger as informações dos pacientes via comunicação oral entre os colaboradores. Os seus colegas comentam ou facilitam o acesso a informações e documentos para pessoas que não estão diretamente envolvidas	Código de Ética dos Profissionais de Enfermagem BAUMER, EARP e PAYTON, 2000 Código de Ética Médica

Variáveis	Aspectos a explorar	Referências
	na prestação da assistência, mesmo que seja apenas por curiosidade.	
	Você acha que o tipo de atividade exercida pela Instituição exige que sejam estabelecidas e cumpridas as políticas de privacidade? Por quê?	FURNELL e RAJENDRAN, 2012
Benefícios pessoais	Você acredita que o seu comportamento em relação ao cumprimento das políticas de segurança e privacidade o fazem ser positivamente reconhecido pelo Hospital, por quê?	FURNELL e RAJENDRAN, 2012
	Você se sente valorizado pelo hospital pelo cumprimento das regras presentes na política de segurança, como?	FURNELL e RAJENDRAN, 2012
Satisfação	O que lhe deixa satisfeito em relação às atividades de trabalho no hospital.	KRAEMER e CARAYON, 2005
	De que maneira as atuais regras de Segurança da Informação me deixam satisfeito ou insatisfeito.	KRAEMER e CARAYON, 2005
Compor-tamento pela segurança	Os seus colegas cumprem com as Políticas de Segurança que o Hospital propõe. (De que maneira?)	HERATH e RAO, 2007
	Que tipo de comportamento dos meus colegas que contribuem que para que as Políticas de Segurança sejam cumpridas. (interno e externo à instituição)	HERATH e RAO, 2007

Fonte: Elaborado pelo autor com base nos autores supracitados

Após a conclusão das perguntas e o agrupamento delas de acordo com as suas características de variações, elas foram agrupadas dentro de três grandes dimensões: Características documentais e regras de privacidade; Características organizacionais e Características comportamentais, conforme demonstra o Apêndice A.

Com o roteiro pronto, foi realizado um Caso Piloto em um Hospital de médio porte, descrito com mais detalhes no capítulo de resultados, com o propósito de adequar e melhorar o roteiro, como também verificar as dificuldades com vocabulários e questões mal formuladas.

Após a aplicação do piloto, verificou-se a necessidade de alteração de algumas questões, retiradas de outras e adequações dentro das variáveis. Também se verificou a necessidade de criar dois roteiros, pois existem alguns termos técnicos que os profissionais que não são da área de TI não sabiam o significado e também desconheciam a sua utilização. Todas as alterações estão detalhadas na descrição do Caso Piloto, no capítulo de resultados.

Com isso, foi criado um roteiro específico para os profissionais de TI (APÊNDICE B) e outro roteiro para os profissionais de outras áreas (APÊNDICE C).

Ao término das entrevistas foi realizada uma segunda técnica dentro do Estudo de Caso, qual seja, uma análise de documentos internos e observações do

estabelecimento de saúde. No Hospital Beta o Documento foi a “Política de Segurança da Informação”, já no Hospital Gama os documentos disponibilizados pelo setor de TI foram as “Diretrizes para o uso seguro das redes sociais” e a “Utilização de ativos de Tecnologia da Informação (TI)”, que são dois dos três documentos mais importantes que contemplam o conjunto de Segurança da Informação do Hospital. A finalidade dessa análise é de identificar possíveis mecanismos de privacidade e verificar a disponibilidade dessas informações às pessoas que têm acesso às informações do paciente no prontuário eletrônico.

A terceira técnica utilizada foi a observação realizada durante visitas aos Hospitais, consultas no site da instituição e conversas informais com colaboradores e clientes/pacientes. Assim como a observação em um documento do Hospital Gama que contem as regras de perfis de acesso para cada tipo de cargo/setor, com a descrição do que é permitido em cada *software.*

O objetivo do Estudo de Caso foi de coletar informações dos indivíduos a respeito da privacidade das informações e como são conhecidas, divulgadas e colocadas em prática pelas pessoas (através das entrevistas) e pela organização (análise de documentos internos e observações).

Ao término da primeira e segunda abordagem metodológica, foi criada uma lista de mecanismos de privacidade de informações dos pacientes.

3.2 TÉCNICAS DE ANÁLISE DE DADOS

A análise de conteúdo é um conjunto de técnicas por procedimentos de maneira sistemática e objetiva que tem a finalidade de obter indicadores (BARDIN, 1977), buscando organizar os dados com o intuito de fornecer respostas ao problema proposto na pesquisa (GIL, 1999), ou seja, “a análise de dados consiste em examinar, categorizar, classificar em tabelas, testar ou, do contrário, recombinar as evidências quantitativas e qualitativas para tratar as proposições iniciais de um estudo” (YIN, 2005, p.137).

Para a análise dos dados foi utilizada a metodologia de Bardin (1977), pela qual primeiramente foram agrupados os dados transcritos das entrevistas para facilitar e melhorar os recursos durante a análise, mesmo que segundo Gibbs (2009) essa transcrição não seja obrigatória em estudos qualitativos.

Após a seleção dos Documentos Regulatórios e Normativos, foi realizada uma análise de todos eles na íntegra, buscando identificar os possíveis mecanismos de proteção da privacidade. No capítulo de resultados, estão descritos cada um dos 20 Documentos Regulatórios e Normativos, inicialmente dispostos em forma de resumo em um quadro, constando os seus objetivos, a sua data de criação e a quem se aplica. Posteriormente foi analisado cada um deles, explicando a sua função e trechos que contenham algum conteúdo a respeito de privacidade e Segurança da Informação. Após ler o conteúdo de cada documento, o critério utilizado para a seleção dos trechos foi o de conter alguma descrição acerca de privacidade e Segurança da Informação, mesmo que indiretamente.

Após essa análise, os mecanismos encontrados foram agrupados e identificando em qual documento ele se encontra, posteriormente sendo cadastrados em uma tabela específica.

Ao término dessa primeira análise foram realizadas as entrevistas e as suas respectivas transcrições e analisadas cada uma das falas, reunindo por categorias os mecanismos, utilizando como base os mecanismos já encontrados na Análise dos Documentos Regulatórios e Normativos, acrescentando os novos mecanismos citados apenas nas entrevistas, criando uma nova tabela para cada Estudo de Caso.

Com essa tabela de mecanismos das entrevistas, foi criada uma nova tabela por Estudo de Caso, acrescentado os mecanismos encontrados na Análise dos documentos internos e nas observações, agrupando os que se identificavam e criando novos para que ainda não houvessem sido citados, tanto na análise de Documentos Regulatórios e Normativos assim como nas entrevistas, gerando assim três tabelas e quadros diferentes que foram:

a) Agrupamento da análise dos Documentos Regulatórios e Normativos;

b) Agrupamento das Entrevistas (uma tabela para cada Estudo de Caso);

c) Agrupamento do Estudo de caso, considerando as entrevista e, Análise de Documentos Internos e Observações (um Quadro para cada Estudo de Caso).

Após a análise de cada Estudo de Caso, foram unificados os Mecanismos citados individualmente em cada Estudo, gerando uma tabela única. Com esse resultado, foi desenvolvida uma nova tabela comparando a tabela de Mecanismos

dos Documentos Regulatórios e Normativos com a tabela de mecanismos unificados dos Estudos de Caso, dando origem um quadro final.

Com a intenção de melhorar a escrita os mecanismos, os mesmos foram renomeados e tiveram os seus códigos alterados, conforme demonstra o Apêndice F.

A partir desse quadro final e da reclassificação dos nomes e códigos, foram criados três outros quadros com todos os mecanismos identificados nas abordagens e técnicas utilizadas, acrescidos de informações qualitativas descritas a seguir.

A criação dos três quadros finais ocorreu considerando a classificação e a adequação de cada um dos mecanismos por tipo, ou seja, agrupando os Mecanismos de Estrutura em um quadro, os Mecanismos de Processo em outro quadro e os Mecanismos de Relacionamento num terceiro quadro.

Também foi realizada uma classificação dos mecanismos, conforme o seu eixo de ação, ou seja, vulnerabilidade, salvaguarda, detecção, punição e conscientização.

Para finalizar, foram classificados os mecanismos de acordo com o seu requisito de Segurança, considerando: Confidencialidade, Integridade, Disponibilidade, Autenticidade, Confiabilidade, Conformidade e Irrefutabilidade.

4 RESULTADOS

Neste capítulo serão apresentados os resultados e as analises realizadas na pesquisa.

4.1 DOCUMENTOS REGULATÓRIOS E NORMATIVOS

O Quadro 8 mostra o conjunto dos Documentos Regulatórios e Normativos analisados, apresentando a sua data de criação, os seus principais objetivos e a quem se aplica.

Quadro 8: Identificação dos Documentos Regulatórios e Normativos

Cód	Tipo de Documento	Data de criação	A quem se aplica	Objetivos
DE1	Norma ABNT NBR ISO/IEC 27001	10/2005	Todos os tipos de organizações	Específica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes
DE2	TISS (Troca de Informação em Saúde Suplementar).	10/2005	Operadoras de planos privados de assistência à saúde e os prestadores de serviços	O principal objetivo do padrão TISS é estimular a adoção de normas nacionais de informação, a terminologia única e identificadores unívocos, a fim de permitir a interoperabilidade entre diferentes Sistemas de Informação
DE3	Resolução CFM Nº 1.821	07/2007	Médicos, hospitais e empresas desenvolvedoras de sistemas	Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes
DE4	Código de Ética Médica – Brasil	01/1988	Profissionais médicos	Contém as normas éticas que devem ser seguidas pelos médicos no exercício da profissão, independentemente da função ou cargo que ocupem
DE5	Código de Ética dos Profissionais de Enfermagem	02/2007	Profissionais de enfermagem	Descreve os princípios, direitos, responsabilidades, deveres e proibições pertinentes à conduta ética dos Profissionais de Enfermagem
DE6	Constituição Federal	10/1988	Todos os cidadãos Brasileiros	Assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça
DE7	Código Civil (lei 10.406)	01/2002	Todos os cidadãos Brasileiros	A consolidação de assuntos e negócios mais comuns, vinculados à esfera das relações jurídicas privadas
DE8	Código de Defesa do Consumidor (lei 8.078)	09/1990	Todos os cidadãos Brasileiros	Apresentar um conjunto de normas que visam a proteção aos direitos do consumidor
DE9	Código Penal (lei 2.848)	12/1940	Todos os cidadãos Brasileiros	O objetivo é penalizar as condutas ilícitas

Cód	Tipo de Documento	Data de criação	A quem se aplica	Objetivos
DE10	Código de Ética da IMIA[2] para Profissionais de Informática em Saúde	10/2002	Profissionais de Informática em Saúde	Prover condutas éticas para os profissionais de TI em saúde e fornecer um conjunto de princípios
DE11	Lei de Acesso à informação (lei 12.527)	11/2011	Todos os órgãos públicos ou instituições particulares que recebem recursos financeiros públicos	Mostra os procedimentos a serem observados pelos órgãos Públicos, com a finalidade de garantir o acesso às informações
DE12	Política Nacional de Informação e Informática em Saúde (PNIIS)	04/2013	Usuários do sistema SUS e população em geral	Promover o uso inovador, criativo e transformador da Tecnologia da Informação contribuindo para a melhoria da atenção à saúde da população. Também visa uma melhor governança no uso da informação em saúde e dos recursos de informática, Integrando-se ao conceito de Governo Eletrônico
DE13	HIPAA	08/1996	Planos de saúde e Prestador de cuidados de saúde dos EUA	Descrever formas de proteção contra a utilização abusiva de informações sobre a saúde do Paciente e a proteção dos dados de saúde do Paciente
DE14	ISO / TC 215	1998	Todos os tipos de instituições de saúde e profissionais da saúde	Padronizar a informação na área da saúde; Garantir a compatibilidade de dados para fins de análise estatística, reduzindo redundâncias e duplicação de esforços
DE15	NBR ISO/IEC 27002	07/2007	Todas as empresas	Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de Segurança da Informação em uma organização
DE16	Marco Civil da Internet	04/2014	Todos os usuários de internet e provedores	Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.
DE17	A Infraestrutura de Chaves Públicas ICP-Brasil	08/2001	Todos os Cidadãos Brasileiros	O objetivo é viabilizar a emissão de certificados digitais para identificação virtual do cidadão
DE18	Manual de Acreditação da ONA	1998	Hospitais que desejam buscar acreditação	Dispõe um conjunto de processos, estruturas e entidades com a finalidade de fomentar e viabilizar a acreditação
DE19	Manual de Acreditação da Joint Commission International (JCI)	1998	Hospitais que desejam buscar acreditação	Descrever os padrões de Aceitação Hospitalar, pois contém todos os padrões, propósitos, elementos de mensuração dos padrões, políticas e procedimentos de acreditação
DE20	PIPEDA	04/2000	Cidadãos Canadenses	Fornecer o direito de privacidade da informação

Fonte: Elaborado pelo autor

[2] International Medical Informatics Association

A seguir estão detalhados os documentos, principalmente com o intuito de explicar o que é o Documento ou a Norma, assim como citar os principais pontos a respeito da segurança e da privacidade da informação.

4.1.1 Análise dos Documentos Regulatórios e Normativos

As descrições foram extraídas dos próprios documentos e tem relação direta e/ou indireta com a Segurança da Informação.

DE1) Norma ABNT NBR ISO/IEC 27001

A Norma ABNT NBR ISO/IEC 27001:2006 tem um caráter normativo que pode ser utilizado como base do processo de origem, aplicação, funcionamento, monitoramento, revisão, manutenção e melhoria do Sistema de Gestão da Segurança da Informação. A norma traz na sua introdução:

> Esta Norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados, tamanho e estrutura da organização. É esperado que este e os sistemas de apoio mudem com o passar do tempo. É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples. Esta Norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas (ABNT NBR ISO/IEC 27001:2006– Introdução: 0.1 – Geral).

DE2) TISS (Troca de Informação em Saúde Suplementar).

O Padrão TISS é um componente obrigatório a todas as instituições de saúde que atendem as operadoras de planos, pois toda a comunicação realizada entre os dois deve seguir as suas normas. Ele está organizado em cinco componentes: Organizacional; Conteúdo e estrutura; Representação de Conceitos em Saúde; Segurança e Privacidade e Comunicação.

A análise foi realizada no componente que traz os requisitos a respeito da segurança e privacidade, o qual estabelece requisitos de proteção dos dados de atendimento ao paciente, visando garantir o direito individual ao sigilo, à privacidade e à confidencialidade dos dados de atenção à saúde. Esta sessão é composta de 31 descrições, sendo distribuídas conforme a Tabela 1.

Tabela 1: Descrição dos requisitos de segurança e privacidade do TISS

Condição de Utilização	Quantidade	Porcentagem
Obrigatório	21	67,7%
Opcional	6	19,3%
Recomendado	4	13,0%
TOTAL	31	100%

Elaborado a partir de: ANS, 2013

Dentre as 31 descrições há 21 itens que são obrigatórios destacando-se: a identificação e autenticação do usuário em arquivos, portais e *webservices*[3]. A determinação da qualidade de senha e o período máximo de obrigatoriedade de troca da mesma, assim como o seu armazenamento por algoritmo de segurança e o bloqueio por muitas tentativas. Outro assunto tratado é a utilização de certificado digital (Chave pública para autenticação) assim como a sua estrutura e armazenamento para acessos remotos de dados, destacando-se finalmente:

> As operadoras de planos privados de assistência à saúde devem constituir proteções administrativas, técnicas e físicas para impedir o acesso eletrônico ou manual impróprio à informação de saúde, em especial à toda informação identificada individualmente (ANS, 2013).

DE3) RESOLUÇÃO CFM Nº 1.821

Esta resolução tem a função de aprovar normas técnicas referentes à digitalização e utilização dos sistemas informatizados para o armazenamento e manuseio dos prontuários dos pacientes, autorizando a eliminação de papel. Os arquivos digitalizados dos prontuários necessitarão ser controlados por um sistema especializado em GED, exigindo a utilização de assinatura digital. Sendo controlados por uma Comissão de Revisão de Prontuários. Ela considera também:

> [...] que os dados ali contidos pertencem ao paciente e só podem ser divulgados com sua autorização ou a de seu responsável, ou por dever legal ou justa causa; [...] que o sigilo profissional, que visa preservar a privacidade do indivíduo, deve estar sujeito às normas estabelecidas na legislação e no Código de Ética Médica, independente do meio utilizado para o armazenamento dos dados no prontuário, quer eletrônico quer em papel (RESOLUÇÃO CFM Nº 1.821).

DE4) Código de Ética Médica - Brasil

O Código de ética médica traz em seu artigo 11º:

[3] *Webservice* é uma solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes

> O médico deve manter sigilo quanto às informações confidenciais de que tiver conhecimento no desempenho de suas funções. O mesmo se aplica ao trabalho em empresas, exceto nos casos em que seu silêncio prejudique ou ponha em risco a saúde do trabalhador ou da comunidade (CÓDIGO DE ÉTICA MÉDICA).

E também traz um capítulo praticamente dedicado ao sigilo das informações, sendo este o IX, destinados às descrições de Segredos Médicos sendo oito artigos, isto é: do 102º ao 109º, destacando-se principalmente a privacidade das informações, nos artigos:

> Art. 104 - Fazer referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais ou na divulgação de assuntos médicos em programas de rádio, televisão ou cinema, e em artigos, entrevistas ou reportagens em jornais, revistas ou outras publicações legais.
>
> Art. 105 - Revelar informações confidenciais obtidas quando do exame médico de trabalhadores inclusive por exigência dos dirigentes de empresas ou instituições, salvo se o silêncio puser em risco a saúde dos empregados ou da comunidade.
>
> Art. 108 - Facilitar manuseio e conhecimento dos prontuários, papeletas e demais folhas de observações médicas sujeitas ao segredo profissional, por pessoas não obrigadas ao mesmo compromisso (CÓDIGO DE ÉTICA MÉDICA).

DE5) Código de Ética dos Profissionais de Enfermagem

O Código de Ética dos Profissionais de Enfermagem conta com um capítulo voltado ao sigilo profissional de uma maneira geral, contemplando os art. 81 a 85, sendo o primeiro versando a respeito do direito de não relevar as informações pertinentes à sua profissão, porém destacando-se principalmente o artigo de responsabilidades de deveres:

> Art. 82 - Manter segredo sobre fato sigiloso de que tenha conhecimento em razão de sua atividade profissional, exceto casos previstos em lei, ordem judicial, ou com o consentimento escrito da pessoa envolvida ou de seu representante legal (CÓDIGO DE ÉTICA DOS PROFISSIONAIS DE ENFERMAGEM).

E os art. 84 e 85 que tratam a respeito das proibições:

> Art. 84 - Franquear o acesso a informações e documentos para pessoas que não estão diretamente envolvidas na prestação da assistência, exceto nos casos previstos na legislação vigente ou por ordem judicial.
>
> Art. 85 - Divulgar ou fazer referência a casos, situações ou fatos de forma que os envolvidos possam ser identificados (CÓDIGO DE ÉTICA DOS PROFISSIONAIS DE ENFERMAGEM).

DE6) Constituição Federal

Na Constituição Federal Brasileira em seu Artigo 5º, inciso X, traz:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (CONSTIUIÇÃO FEDERAL, Artigo 5º, inciso X).

DE7) Código Civil (lei 10.406)

O Código Civil Brasileiro traz regras e princípios que regulam as relações jurídicas, entre as pessoas, e por isso incluem-se os colaboradores de hospitais. Dentro do código, se destacam os seguintes artigos a respeito da privacidade:

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.
>
> Art. 229. Ninguém pode ser obrigado a depor sobre fato:
>
> I - a cujo respeito, por estado ou profissão, deva guardar segredo (CÓDIGO CIVIL (LEI 10.406/2002)).

DE8) Código de Defesa do Consumidor (lei 8.078)

Como todo o paciente é um cliente, pois está utilizando serviços hospitalares, o hospital tem o dever de cumprir o que rege o código de Defesa do Consumidor, no qual dispõe à respeito da informação.

> Art. 34. O fornecedor do produto ou serviço é solidariamente responsável pelos atos de seus prepostos ou representantes autônomos (CÓDIGO DE DEFESA DO CONSUMIDOR (LEI 8.078/1990)).

Essa responsabilidade disposta acima no art. 34, se aplica também sobre médicos e enfermeiros, e sob todo o corpo clínico e de atendimento do paciente, decorrendo inclusive penas ao:

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros: Pena - Detenção de seis meses a um ano ou multa.
>
> Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata (CÓDIGO DE DEFESA DO CONSUMIDOR (LEI 8.078/1990)).

DE9) Código Penal (lei 2.848)

O código que rege as penalidades por atos ilegais realizados pelos cidadãos Brasileiros, como a divulgação ilícita e invasão de sistemas de computadores, é o código Penal, o qual é válido para todos os colaboradores dos hospitais, principalmente os que têm acesso a sistemas e prontuários dos pacientes, conforme descrito abaixo.

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
> § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos Sistemas de Informação ou banco de dados da Administração Pública.
> Art. 154 - Divulgação de informações obtidas no exercício de atividade profissional, incluindo entre os tipos penais a revelação, sem justa causa, de segredo do qual se teve conhecimento em razão de função, ministério, ofício ou profissão, e cuja revelação possa causar dano a alguém.
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012)
> Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação" (CÓDIGO PENAL (LEI 2848)).

DE10) Código de Ética da IMIA para Profissionais de Informática em Saúde

A IMIA (*International Medical Informatics Association*), é um órgão internacional, não governamental que tem o papel de aplicar a Tecnologia da Informação nas áreas da saúde e da pesquisa em medicina, representando a Informática na Medicina em nível mundial, servindo de integrador entre os países. Atendendo o seu objetivo ela criou um código de ética para profissionais de informática na saúde.

O código foi desenvolvido para ser aplicado nas práticas relativas a questões éticas dos profissionais de informática na saúde (PIS) e principalmente com a relação entre o profissional e os *stakeholders* que participam do processo, como; médicos, enfermeiros, pacientes, instituições de saúde, planos de saúde, etc.

A criação do código se deu devido à especificidade do PIS em relação a outros profissionais de informática de outros tipos de empresas, pois os primeiros tem o contato com o prontuário eletrônico e com informações do paciente ao qual ele pertence e eles podem influenciar na construção, manutenção, armazenamento, acesso e manipulação desses documentos.

> O PEP não apenas revela muitos dados privativos dos pacientes que devem ser mantidos em sigilo, mas principalmente é a base de decisões que terão um profundo impacto no seu bem-estar (IMIA, 2014).

O Código de Ética foi divido em duas partes: a primeira parte descreve um conjunto de princípios éticos fundamentais que encontraram aceitação internacional. Já na segunda parte ele traz um detalhamento de regras éticas para guiar os Profissionais de informática em saúde, sendo essas regras bem mais específicas e com diretrizes direcionadas em relação aos princípios éticos gerais da informática. Pode-se destacar entre várias regras, a que está contida no item de obrigações referentes ao indivíduo:

> Os profissionais de informática em saúde têm o dever de assegurar que medidas apropriadas estejam disponíveis e possam ser razoavelmente esperadas para garantir: a segurança dos prontuários ou registros eletrônicos; a integridade destes; sua qualidade material; suas condições de uso; sua acessibilidade.
>
> O direito fundamental de controle sobre a coleta, armazenagem, acesso, uso, comunicação, manipulação e disposição de dados pessoais é condicionado somente pelas necessidades legítimas, apropriadas e relevantes de acesso a esses dados por uma sociedade livre, responsável e democrática, e pelos direitos iguais e concorrentes de outras pessoas (IMIA, 2014).

E também a regra que está contida nas obrigações para com o hospital e com a sociedade.

> Os profissionais de informática em saúde têm o dever de assegurar, até o máximo de sua capacidade, que existam estruturas apropriadas para avaliar se a coleta, armazenagem, recuperação, processamento, acesso, comunicação e utilização de dados são feitos de forma aceitável, sob os pontos-de-vista técnico, legal e ético, nas instalações onde desempenham suas funções ou às quais se afiliam (IMIA, 2014).
>
> Os PIS têm a obrigação de garantir que: somente dados relevantes para necessidades legítimas de planejamento sejam coletados; sempre que possível, a identificação pessoal dos dados coletados seja removida, ou estes sejam tornados anônimos, de acordo com os objetivos legítimos da coleta de dados; a interligação de bases de dados possa ocorrer somente por outras razões que sejam legítimas e defensáveis, e que não violem os direitos fundamentais dos indivíduos aos quais os dados se referem; somente pessoas devidamente autorizadas tenham acesso aos dados relevantes (IMIA, 2014).

DE11) Lei de Acesso à informação (lei 12.527)

A Lei 12.527/2011 traz novas regras referentes à classificação da informação. Como princípio geral, estabelece que uma informação pública somente pode ser classificada como sigilosa quando considerada imprescindível à segurança da sociedade (à vida, segurança ou saúde da população) ou do Estado (soberania nacional, relações internacionais, atividades de inteligência).

A informação sob a guarda do Estado é sempre pública, devendo o acesso a ela ser restringido apenas em casos específicos. Isto significa que a informação produzida, guardada, organizada e gerenciada pelo Estado em nome da sociedade é um bem público. Porém as informações dos pacientes de um hospital público ou não, são restritas somente ao paciente e/ou algum responsável legal.

DE12) Política Nacional de Informação e Informática em Saúde (PNIIS)

A Política Nacional de Informação e Informática na Saúde, busca contribuir para a melhora da atenção à saúde da população e também um melhor controle da informação, para isso tem os seguintes princípios:

> A informação em saúde deve ter sua autenticidade e integridade preservadas [...] Informação de saúde pessoal é toda aquela atinente à gestão, à vigilância e à atenção à saúde individualmente identificada ou identificável, garantida ao indivíduo a sua confidencialidade, sigilo e privacidade de dados [...] A informação de saúde que identifica a pessoa, gerada em qualquer evento de atenção à saúde, é de interesse do indivíduo, e seu uso somente pode ser autorizado pelo indivíduo ou por seu responsável legal, salvo disposição legal (PNIIS, 2013).

DE13) HIPAA - *Health Insurance Portability and Accountability Act*

A HIPAA é uma lei Americana, que entrou em vigor em 1996 e tem como principal objetivo a redução de fraudes e manutenção da privacidade das informações médicas.

O Brasil não precisa obrigatoriamente se adequar às leis da HIPAA, como nos Estados Unidos, porém é uma normativa que auxilia muito nos processos e segurança, pois um dos principais objetivos é assegurar que as informações de saúde dos pacientes são de fato protegidas seja pelo hospital ou por um terceiro que presta serviço de qualquer tipo de meio de comunicação, meio eletrônico, papel ou oral. A HIPAA busca regulamentar em quais situações podem ser divulgadas as

informações dos pacientes, como por exemplo, a prevenção de doença de saúde pública e a exposição à doença contagiosa quando autorizada por lei.

A HIPAA traz várias recomendações, como por exemplo, o cuidado para não se posicionar computadores próximos a corredores. Outra recomendação é a de que Médicos e Enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas. Outra recomendação importante é a que todos os colaboradores devem participar de treinamentos constantes a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho, bem como receber sanções adequadas para os que violam suas Políticas de Privacidade.

A conformidade com a HIPAA exige também que o órgão de saúde tenha um plano de recuperação para desastres que possam vir a ocorrer com as informações dos pacientes. Armazenando os dados de uma maneira segura, tanto técnicas como físicas, para se evitar a utilização intencional ou não. Também exige uma rotina estruturada de b*ackup* das informações, assim como proteções internas para a conexão de um novo *hardware* ou *software* na rede, contanto também com uma proteção de *firewall* nos servidores.

Quando a instituição de saúde tiver a necessidade de fazer troca de informações com empresas externas, a HIPAA exige que esse tráfego seja criptografado. E no ambiente interno é obrigatória a autenticação por parte de todos os colaboradores, com os perfis definidos com acesso às informações dos pacientes somente para aqueles que devem ter acesso, inclusive com *logs* de acesso e *logs* de alterações realizadas no prontuário do Paciente.

Nos processos internos do hospital, a lei recomenda que se tenham avisos, com editais, orientando como o hospital pode divulgar informações e também como ele protege as informações através de práticas descritas e procedimentos realizados, contanto também com a criação e a implantação de uma política de privacidade para divulgar internamente aos colaboradores. E para controlar e executar e fornecer informações a respeito de práticas de privacidade, o hospital precisa ter uma pessoa responsável, para também receber denúncias internas ou externas de quebra de sigilo de privacidade da informação.

O hospital precisa manter os documentos de Políticas de Privacidade e procedimentos, suas boas práticas, avisos, ou qualquer tipo de ações por até seis

anos após a última data de criação ou de vigência, pois eles precisam ser documentados.

E para finalizar, a HIPAA impõe penalidades ao hospital, como por exemplo, uma multa da importância de U$ 100 pelo não cumprimento de uma regra de privacidade. E também uma penalidade de até U$ 250.000 e dez anos de prisão se a conduta envolver a intenção de transferir, vender ou utilizar as informações de saúde para fins comerciais, ganho pessoal ou dano malicioso.

DE14) ISO / TC 215

A ISO é uma Organização Internacional, originada nos Estados Unidos, que cria normas para garantir que os produtos e serviços sejam seguros, confiáveis e de boa qualidade. Dentre os vários comitês que a ISO possui, um deles é destinado à Informática na Saúde, que é o Comitê Técnico ISO TC 215, criado em 1998, com a função de tratar da normalização no domínio da informática em saúde, a fim de facilitar o intercâmbio e utilização de dados relacionados com a saúde, informação e conhecimento coerente e consistente para apoiar e permitir que todos os aspectos do sistema de saúde.

O Comitê da ISO TC 215 possui as seguintes características conforme a Tabela 2.

Tabela 2: Características técnicas do Comitê ISO TC 215

Dados	Quantidade
Publicações e Atualizações	136
Países Participantes	33
Países observadores	26
Grupos de Trabalhos	8

Fonte: ISO TC 215

A seguir há uma descrição dos grupos de trabalho conforme apresenta o Quadro 9. Dentre os oito grupos, destaca-se um, com especial relação com esta pesquisa, o qual foi analisado com maior ênfase, que é o ISO/TC 215/WG 4, que trata da questão da privacidade e segurança e traz as definições dos padrões e metodologias para proteger e melhorar a confidencialidade, disponibilidade, e integridade da informação em saúde, bem como as boas práticas para o gerenciamento seguro da informação em saúde.

Quadro 9: Grupos de Trabalho do Comitê ISO TC 215

Grupo de trabalho	Função
ISO/TC 215/CAG 1	Conselho Executivo, harmonização e operações
ISO/TC 215/WG 1	Arquitetura, *Frameworks* e Modelos
ISO/TC 215/JWG 1	Medicina Tradicional Chinesa (Informática)
ISO/TC 215/WG 2	Sistemas e interoperabilidade de dispositivos
ISO/TC 215/WG 3	Conteúdo semântico
ISO/TC 215/WG 4	Segurança e Privacidade
ISO/TC 215/WG 6	Negócios de farmácia e medicamentos
ISO/TC 215/JWG 7	Aplicação da gestão de risco a redes na Tecnologia da Informação.

Fonte: ISO TC 215

Das 136 publicações e atualizações, 28 delas referem-se ao Grupo de Trabalho 4, e, portanto, tratam de segurança e privacidade, conforme informados no Quadro 10.

Quadro 10: Publicações da ISO TC 215 referentes à segurança e privacidade

	Código	Descrição	Número de Pág.	Estágio de implantação*
1	ISO 10159:2011	Mensagens e comunicação - Manifesto de referência para acesso *Web*	9	NPI
2	ISO/HL7 10781:2009	Registro Eletrônico de Saúde – Modelo de Sistema Funcional	213	PIR
3	ISO/IEEE 11073-10201:2004	Comunicação e dispositivo médico no ponto de atendimento	167	PIC
4	ISO/TR 11633-1:2009	A gestão da Segurança da Informação para manutenção remota de dispositivos médicos e Sistemas de Informação Médicas	17	NPI
5	ISO/TR 11633-2:2009	A Gestão da Segurança da Informação para manutenção remota de dispositivos médicos e Sistemas de Informação Médica - Parte 2: Implementação de um Sistema de Gestão de Segurança da Informação	66	NPI
6	ISO/TR 11636:2009	Dinâmica de infraestrutura rede privada virtual	70	NPI
7	ISO/TS 13131:2014	Serviços de Telessaúde - Diretrizes de planejamento da Qualidade	32	NPI
8	ISO/TS 13582:2013	Compartilhamento de informações dos Registros	28	NPI
9	ISO/TS 14441:2013	Requisitos de segurança e privacidade dos sistemas de Registros Eletrônicos para uso na avaliação da conformidade	112	NPI
10	ISO 17090-1:2013	Infraestrutura de Chave Pública - Parte 1: Visão geral de serviços de Certificação Digital	39	NPI
11	ISO 17090-2:2008	Infraestrutura de Chave Pública Parte 2: Perfil de Certificado	27	PIR
12	ISO 17090-3:2008	Infraestrutura de Chave Pública -- Parte 3: Gerenciamento de políticas de autoridade de certificação	36	PIC
13	ISO/TR 17791:2013	Orientação sobre normas para a habilitação de segurança em *software* de saúde	47	NPI
14	ISO/TR 21089:2004	Confiabilidade no processo de fluxos de informação	47	PIR
15	ISO 21091:2013	Os serviços de diretório para os prestadores de saúde, pessoas ligadas à saúde e prestadoras de	46	NPI

	Código	Descrição	Número de Pág.	Estágio de implantação*
		serviços		
16	ISO/TS 21547:2010	Requisitos de segurança para o arquivamento de registos de saúde eletrônicos - Princípios	77	PA
17	ISO/TR 21548:2010	Requisitos de segurança para o arquivamento de registos de saúde eletrônicos - Orientações	30	NPI
18	ISO/HL7 21731:2014	HL7 - Referência modelo de informação	47	NPI
19	ISO/TR 22221:2006	Os bons princípios e práticas para um D*atawarehouse* de dados clínicos	42	NPI
20	ISO 22600-1:2014	Gerenciamento de privilégios e de controle de acesso - Parte 1: Visão geral e gestão da política	27	NPI
21	ISO 22600-2:2014	Gerenciamento de privilégios e de controle de acesso - Parte 2: Os modelos formais	26	NPI
22	ISO 22600-3:2014	Informática em saúde - gerenciamento de privilégios e de controle de acesso - Parte 2: Implementações	67	NPI
23	ISO 22857:2013	Orientações sobre a proteção de dados para facilitar os fluxos externos de dados pessoais de saúde	56	NPI
24	ISO/TS 25238:2007	Classificação dos riscos de segurança de *software* de saúde	24	PA
25	ISO 27799:2008	Informática em saúde - A Gestão da Segurança da Informação na saúde utilizando a norma ISO / IEC 27002	58	PIR
26	ISO/TR 27809:2007	Medidas para garantir a segurança do paciente em um *software* de saúde	38	NPI
27	ISO/HL7 27931:2009	Norma de troca de dados - Um protocolo de pedido de intercâmbio eletrônico de dados em ambientes de saúde	185	PA
28	IEC 80001-1:2010	Aplicação da gestão de risco de TI. Redes com dispositivos médicos - Parte 1: Funções, responsabilidades e atividades	70	NPI

*Legenda: NPI - Norma publicada internacionalmente ; PIC - Padrão Internacional confirmado ; PIR - Padrão internacional para ser revisado ; PA - Próximo de avaliação.

Elaborado a partir de: ISO TC 215

Devido ao alto custo para a aquisição de cada uma das 28 normas (em torno de R$ 500,00 cada uma, totalizando aproximadamente R$ 14.000,00), a análise foi realizada utilizando-se o escopo e a introdução que estão com acesso liberado ao documento no site da própria ISO. Porém, mesmo com essa análise não sendo tão aprofundada quanto se pretendia, foi possível identificar diversos mecanismos de proteção da privacidade, conforme serão apresentados nos Quadros 13 e 14.

DE15) NBR ISO/IEC 27002

A norma NBR ISO/IEC 27002, foi resumida em 11 seções que correspondem a controles de Segurança da Informação, conforme apresenta o Quadro 11.

Quadro 11: Controles de Segurança da Informação da NBR ISO/IEC 27002

Nome/Seção	Resumo
Política de Segurança da Informação (5)	A empresa deve criar um documento com a Política de Segurança da Informação, onde deveria conter normas e requisitos de Segurança da Informação, controles, avaliação e gerenciamento de riscos, conceitos de Segurança da Informação, entre outros. Devendo ser revisada regularmente e comunicada a todos
Organizando a Segurança da Informação (6)	Criar uma estrutura de gerenciamento da Segurança da informação, tendo a participação de diversos colaboradores com funções relevantes, para que se definam as responsabilidades pela Segurança da Informação, com acordos de confidencialidade para a proteção da informação sigilosa, seja de acesso interno ou externo
Gestão de Ativos (7)	A empresa deve identificar os ativos para formar um inventário estruturado, para posteriormente ser mantidos, documentados com regras que definam como fazer uso do ativo e classificados de acordo com a característica de nível de proteção de cada um. Uma vez que o ativo “é qualquer coisa que tenha valor para a organização”
Segurança em Recursos Humanos (8)	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa. Ao se candidatar a pessoa deve entender as responsabilidades do cargo, que precisam estar descritos pela empresa. Depois de estar exercendo as funções, o empregado deve ser treinado quanto aos procedimentos de Segurança da Informação e também da forma correta de utilizar os recursos da informação, para que sempre fique bem claro às ameaças relativas à Segurança da Informação. E no momento da demissão, imediatamente deve-se tirar todos os tipos de acessos
Segurança Física e do Ambiente (9)	Deve haver proteção para as instalações físicas, assim como para os equipamentos , com controles de acesso, onde são armazenadas as informações criticas da instituição
Gestão das Operações e Comunicações (10)	A empresa deve planejar os seus recursos para evitar falhas ou sobrecargas, deve ter ferramentas para se proteger de invasões ou códigos maliciosos, avisando os funcionários sobre isso. Realizar cópias de segurança e gerenciamento da rede. Inclusive com políticas definidas para transmissão externa de informações para terceiros. Outro fator importante é o monitoramento de atividades não autorizadas de processamento da informação, registrando os acessos. A divisão de função quando se tratar de sistemas, para que a mesma pessoa não realize todas as operações do processo, com a intenção reduzir o risco de mau uso ou uso indevido dos sistemas
Controle de Acesso (11)	Deve-se definir as autorizações de acesso de acordo com cada função na empresa, estando isso claro para o colaborador, para se evitar o acesso não autorizado aos sistemas
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (12)	As informações devem ser protegidas com criptografia. E os meios de Segurança de Sistemas de Informação devem ser conhecidos antes do desenvolvimento ou implementação
Gestão de Incidentes de Segurança da Informação (13)	É importante estabelecer procedimentos formais, para informar os funcionários e usuários a respeito de eventos da Segurança da Informação para que se tome uma decisão rápida a fim de resolver a falha
Gestão da Continuidade do Negócio (14)	A continuidade do negócio deve ser garantida ou minimizada contra falhas ou desastres, almejando que as principais operações sejam recuperadas rapidamente e para isso deve ter planos formais para identificar e reduzir riscos
Conformidade (15)	Deve-se verificar regularmente e analisar a Segurança dos Sistemas de Informação, para evitar a violação de alguma lei ou contratos com terceiros

Fonte: ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão de Segurança da Informação. ABNT, 2005

DE16) Marco Civil da Internet

Muitas instituições de saúde disponibilizam resultados de exames para pacientes via internet e principalmente disponibilizam os dados dos pacientes para consultas por parte dos médicos. Com isso os hospitais entram na mesma regra de qualquer outro provedor de internet e conforme descreve o marco Civil da internet.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (LEI Nº 12.965, 2014).

DE17) A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2

A certificação digital, de acordo com o órgão que o regulamenta é uma das ferramentas mais modernas de segurança para proteção pessoal e da empresa.

> Assinatura Digital: É o processo eletrônico de assinatura através de senha pessoal, baseado em sistema criptográfico assimétrico que permite aferir com segurança a origem e integridade de seu conteúdo. Tendo garantia de que somente o titular do certificado digital poderia ter realizado determinada operação (ICP-BRASIL, 2001).

A ICP-Brasil faz a geração e o gerenciamento das chaves criptográficas; para validar assinatura digital garantindo a autoria de um documento eletrônico, tornando-o juridicamente válido. Com essa assinatura digital válida, não é mais necessário a impressão do prontuário eletrônico. Outro exemplo é a TISS, que exige que seja utilizada essa ferramenta para validar e garantir a autenticidade das informações.

DE18) Manual de acreditação da ONA

A ONA – Organização Nacional de Acreditação é uma entidade não governamental e sem fins lucrativos que tem a função de realizar certificações de

qualidade, chamadas de Acreditação, em serviços de saúde no Brasil, com o foco na segurança do paciente. A “acreditação é um método de avaliação voluntário, periódico e reservado, que busca garantir a qualidade da assistência por meio de padrões previamente definidos. Constitui, essencialmente, um programa de educação continuada e, jamais, uma forma de fiscalização”(ONA, 2014 pág. 13).

No manual, que deve ser seguido pelo hospital que almeja conseguir a acreditação, existem cinco seções. A que será analisada é a de número quatro, a qual descreve sobre a gestão da informação do paciente/cliente. Nesta seção são apresentados alguns requisitos que devem ser cumpridos pelo hospital, e eles são descritos em forma de perguntas, que são:

> Profissionais dimensionados de acordo com a realidade da organização? [...] Planeja as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura? [...] Define planos de contingência que assegurem o acesso e integridade das informações? [...] Organiza e integra as informações dos pacientes? [...] Estabelece mecanismos que assegurem a qualidade e a integridade dos registros e informações dos pacientes? [...] Identifica os perigos dos processos relacionados a gestão da informação do paciente e desenvolve ações para conte-los? [...] Estuda as ações implementadas para minimizar os perigos, os resultados obtidos e define melhorias. [...] Acompanha e avalia o desempenho do processo, promovendo ações de melhorias (MANUAL DE ACREDITAÇÃO DA ONA, 2014).

DE19) Manual de Acreditação da *Joint Commission International* (JCI)

A JCI - *Joint Commission International*, fundada em 1994, é uma organização sem fins lucrativos, que fornece à hospitais do mundo todo, treinamentos, certificações e acreditações. Acreditou hospitais em mais de 90 países e está presente nos cinco continentes. A missão da JCI é melhorar a qualidade da assistência à saúde na comunidade internacional, fornecendo serviços de acreditação no mundo. O propósito dessa iniciativa é oferecer à comunidade internacional um processo objetivo, baseado em padrões, para avaliar as instituições de saúde. A meta do programa é estimular a melhoria contínua e sustentada em instituições de saúde ao aplicar padrões e indicadores de consenso internacional.

O documento é dividido em 12 unidades e cada uma delas traz um determinado assunto. Para a dissertação foi analisada a unidade 12, que é o gerenciamento de informação. A metodologia do documento é sempre apresentar a recomendação em formato de perguntas ao hospital, para verificar se existe ou não

o processo e também em qual nível de gerenciamento e controle será acreditado, como pode ser visto abaixo.

> A instituição tem um plano para atender às necessidades de informação. O plano inclui como será garantida a confidencialidade, a segurança e a integridade de dados e informações? [...] Os profissionais da instituição têm acesso ao nível de informação relativo às suas necessidades e responsabilidades de trabalho? [...] Os prontuários e as informações são protegidos contra perda, destruição, adulterações e acesso ou não autorizado? [...] Os tomadores de decisão e outros profissionais da instituição são educados e treinados sobre os princípios de gerenciamento de informação? (JCI, 2014).

Os processos que a acreditação propõe aos hospitais sempre buscam a plena segurança do paciente, e como consequência os processos que estão relacionados acabam tendo uma melhora, e um deles é exatamente a segurança das informações.

> [...] A instituição mantém a confidencialidade e a segurança dos dados e informações e é especialmente cuidadosa com a preservação da confidencialidade de dados e informações sensíveis. O equilíbrio entre o compartilhamento e a confidencialidade dos dados é definido. A instituição determina os níveis de segurança e confidencialidade mantidos para diferentes categorias de informação (por exemplo, o prontuário do paciente, dados de pesquisa). O acesso a cada categoria de informação baseia-se na necessidade e está definido por cargo e função, incluindo os estudantes em ambientes acadêmicos? [...] Existe um processo para assegurar que apenas pessoas autorizadas façam anotações nos prontuários e que cada anotação identifique a autoria e a data do registro? (JCI, 2014).

Praticamente todas as pessoas que trabalham no ambiente hospitalar são envolvidas nos processos de acreditação, pois de uma forma ou outra podem ter acesso a algum departamento que presta atendimento ao paciente. Um exemplo é o acesso dos colaboradores da limpeza aos sistemas de gerenciamento de informações, liberando ou bloqueando o quarto para a limpeza. E por esse acesso de tantas pessoas, a acreditação se preocupa.

> [...] Uma vez concluído e aprovado como necessário, o plano de gerenciamento de informação da instituição é implementado. A instituição fornece pessoal, tecnologia e outros recursos necessários para implementar o plano e atender às necessidades de informação dos profissionais, dirigentes e outros? [...] Os profissionais da instituição têm acesso ao nível de informação relativo às suas necessidades e responsabilidades de trabalho? [...] Deve ser garantido aos profissionais da instituição o acesso aos dados e informações através de senhas, chaves para áreas de armazenamento de dados, crachás ou outros meios? [...] Os prontuários e as informações são protegidos contra perda, destruição, adulterações e acesso ou uso não autorizado? [...] Os profissionais da instituição que geram, coletam, analisam e utilizam dados e informações são educados e treinados para participar efetivamente do gerenciamento de informação? (JCI, 2014).

No Brasil, segundo a JCI (2014) existem 27 hospitais acreditados pela JCI - *Joint Commission International*, localizadas em 5 cidades, assim distribuídas: 16 hospitais em São Paulo, cinco no Rio de Janeiro, três em Porto Alegre, dois em Recife e um em Joinville.

DE20) PIPEDA- "*Personal Information Protection and Electronic Documents Act*"

A PIPEDA - "Personal Information Protection and Electronic Documents Act" é uma lei canadense que regula a privacidade da informação. Ela entrou em pleno vigor no ano de 2004, quando contemplou a participação de todos os tipos de empresas do país. Ela estabelece 10 princípios de práticas de informação e obrigações de privacidade básicas que são resumidas no Quadro 12.

Quadro 12: Os 10 princípios da PIPEDA

Princípios	Descrição
Responsabilidade	As informações a respeito das políticas de privacidade devem ser disponibilizadas aos clientes, por algum meio, porém é necessário ter uma pessoa responsável pela privacidade e Segurança da Informação na organização
Finalidades de identificação	O recolhimento das informações dos clientes por parte das empresas deve ser justificada e identificada as razões
Consentimento	O cliente deve ser informado como será a utilização e o recolhimento das informações
Limitando a coleta	Somente recolher as informações dos clientes que são de extrema necessidade, tentando limitar ao máximo
Limitação de utilização, divulgação e retenção	A utilização das informações pessoais deve ser apenas para a finalidade na qual foram coletadas e a empresa deve manter essas informações apenas o tempo necessário
Precisão	A informação do cliente deve ser mantida pela empresa sempre completas e atualizadas caso seja necessário
Proteção	Proteção da informação pessoal contra roubo ou perda através da utilização de medidas adequadas
Abertura	As políticas de Segurança da Informação devem ser de fácil compreensão e disponíveis facilmente
Acesso Individual	O indivíduo tem o direto de ter acesso à sua informação pessoal que a empresa possui dele, salvo em algumas exceções
Contato e/ou contestação da conformidade	O contato para reclamações sobre relatos de preocupação com a Segurança da Informação deve ser desenvolvido pela empresa

Fonte: Elaborado a partir de PIPEDA (2014)

A primeira função da PIPEDA, quando criada em abril de 2000 era a de promover a confiança dos consumidores de comércio eletrônico. Com o passar dos anos ela foi se alterando e tornou-se válida para todos no Canadá, regulamentando a utilização da informação no País, inclusive com disposições para facilitar o uso de documentos eletrônicos.

4.1.2 Identificação dos mecanismos provenientes dos Documentos

Ao término da análise dos 20 Documentos Regulatórios e Normativos, chegou-se a 37 mecanismos, conforme demonstra o Quadro 13. Em dois deles não foi possível identificar nenhum mecanismo (DE11 e DE12). Em alguns deles foi possível identificar apenas um, porém em outros foi possível a identificação de diversos mecanismos. Foi criado um código para identificar o mecanismo com as iniciais (MDE) e uma ordem sequencial da quantidade localizada. Também encontra-se no Quadro 13, o nome, a justificativa e na última coluna estão dispostos os documentos nos quais foram encontrados os mecanismos.

Quadro 13: Mecanismos encontrados nas análises dos Documentos Regulatórios e Normativos

Código	Mecanismos	Justificativa/Objetivo	Regulatório/Normativo
MDE1	Implantar e manter um Sistema de Gestão da Segurança da Informação	Para garantir a permanecia e cumprimento das políticas	DE1 – DE13 – DE14 - DE15 -DE19 – DE20
MDE2	Ter uma pessoa responsável pela Política de Segurança da Informação	Para garantir a permanecia e cumprimento das políticas	DE13 – DE14- DE18 – DE19 – DE20
MDE3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	Para garantir que somente a pessoa autorizada tenha acesso à informação	DE2 –DE10 – DE13 – DE14 - DE18 – DE19 -
MDE4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	Para dificultar a quebra de senha e acessos indevidos	DE2
MDE5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	Garantir a autenticidade da informação	DE2 – DE3 – DE14 - DE17- DE18
MDE6	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED	Para facilitar a recuperação das informações	DE3
MDE7	Possuir uma Comissão de Revisão de Prontuários	Para melhorar os processos de segurança.	DE3
MDE8	Instruir o Médico e Enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	Evitar o vazamento da informação	DE4 – DE5 – DE9
MDE9	Prevenir para que Médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	Evitar o vazamento da informação	DE13
MDE10	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	Para evitar a divulgação de informações	DE3 - DE4 - DE5- DE6- DE7- DE9 – DE13 - DE15
MDE11	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	No sentido também da ética	DE3 – DE4 – DE5 - DE13 – DE14 -DE15 – DE18 – DE19
MDE12	Instalar Antivírus,VPN e *firewall*	Para evitar invasão por pessoas não autorizadas, sejam elas internas ou externas	DE2 - DE9 -DE13 – DE14 - DE15 - DE19 - DE20
MDE13	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	Para se evitar muitos acessos, por muitas pessoas, aumentando assim o risco de vazamento de informação	DE10 – DE13 – DE14 - DE15 – DE19
MDE14	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	Para garantir os serviços	DE1 -DE2 - DE10 – DE14 -DE15 – DE16 – DE19 –DE20

Código	Mecanismos	Justificativa/Objetivo	Regulatório/Normativo
MDE15	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura	Para garantir os serviços	DE14 -DE18 – DE19
MDE16	Coletar somente dados relevantes dos clientes/pacientes	Para diminuir a possibilidade de vazamento da informação	DE10 – DE20
MDE17	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	Evitar muitos acessos à informação	DE10 – DE14 -DE19
MDE18	Evitar posicionar computadores próximos a corredores	Evita-se o acesso indevido	DE13
MDE19	Impor sanções adequadas para os que violam as políticas de privacidade	Impor punições para que diminua as ações	DE4 – DE5 – DE7 – DE8 – DE9 - DE13
MDE20	Penalidade com multa em dinheiro	Para evitar a ocorrência	DE13
MDE21	Ter um plano de recuperação ou contingência para desastres com informações	Caso tenha alguma intercorrência	DE13 – DE14 - DE15 – DE19 – DE20
MDE22	Ter um *backup* estruturado das informações	Para recuperar o dado caso seja perdido	DE13 – DE15 – DE18 – DE19 – DE20
MDE23	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede	Evitando a propagação de algum vírus ou espionagem	DE13 – DE20
MDE24	Ter um *software* de HIS – adequado e de boa qualidade	Para o cadastro e gerenciamento dos dados	DE14
MDE25	Criptografar o tráfego externo de informações	Dificulta a coleta indevida de dados	DE2 -DE13 – DE15
MDE26	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do Paciente	Caso seja necessário a verificação futura	DE9 -DE13 – DE14 - DE19
MDE27	Criar e divulgar aos colaboradores uma política de privacidade	Para que todos tenham conhecimento das regras	DE13 – DE14 -DE15 – DE18 - DE19 – DE20
MDE28	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa	Verificam-se maus comportamentos anteriores	DE15
MDE29	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo	Evita-se a coleta indevida de dados	DE15
MDE30	Definir regras para transmissão externa de informações para terceiros	Evita-se a coleta indevida de dados	DE14 -DE15 –DE19
MDE31	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação	A fim de detectar acessos indevidos	DE14 -DE15
MDE32	Dividir as funções dos colaboradores nos sistemas	Para que a mesma pessoa não realize todas as operações do processo, com a intenção reduzir o risco de mau uso ou uso indevido dos sistemas	DE15
MDE33	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação	Caso se verifique uma alteração terá tempo hábil	DE15 – DE19
MDE34	Analisar regularmente a Segurança dos Sistemas de Informação	Evitar a violação de alguma lei ou contratos com terceiros	DE14 -DE15 – DE18
MDE35	Ter a quantidade de Profissionais dimensionados de acordo com a realidade da organização ou departamento	Para evitar sobrecarga de trabalho	DE18
MDE36	Disponibilizar as políticas de Segurança da Informação aos clientes	Para que os clientes tenham ciência de seus direitos	DE20
MDE37	Manter as informações dos clientes apenas o tempo necessário por lei	Para diminuir o risco de vazamento	DE14- DE20

Fonte: Elaborado pelo autor

O Quadro 14 mostra a análise cruzada entre os Mecanismos identificados que estão dispostos na vertical (colunas) e os Documentos Regulatórios e Normativos

que estão na Horizontal (linhas). A última linha (TOTAL), do quadro representa o total de mecanismos que foram encontrados em cada um dos documentos analisados, sendo estes identificados individualmente através de um (x) no decorrer da coluna. Já a coluna total representa a quantidade de documentos em que consta o Mecanismo, identificando em cada uma das linhas, os documentos individualmente marcados com um (x). As legendas com os nomes dos Mecanismos estão descritas no Quadro 13.

Quadro 14: Mecanismos identificados (M) x Documentos Regulatórios e Normativos (D)

M \ D	DE1	DE2	DE3	DE4	DE5	DE6	DE7	DE8	DE9	DE10	DE11	DE12	DE13	DE14	DE15	DE16	DE17	DE18	DE19	DE20	TOTAL
MDE1	x												x	x	x				x	x	6
MDE2													x	x				x	x	x	5
MDE3		x								x			x	x				x	x		6
MDE4		x																			1
MDE5		x	x											x			x	x			5
MDE6			x																		1
MDE7			x																		1
MDE8				x	x				x												3
MDE9													x								1
MDE10			x	x	x	x	x		x				x		x						8
MDE11			x	x	x								x	x	x			x	x		8
MDE12		x							x				x	x	x				x	x	7
MDE13										x			x	x	x				x		5
MDE14	x	x								x				x	x	x			x	x	8
MDE15														x				x	x		3
MDE16										x										x	2
MDE17										x				x					x		3
MDE18													x								1
MDE19				x	x		x	x	x				x								6
MDE20													x								1
MDE21													x	x	x				x	x	5
MDE22													x		x			x	x	x	5
MDE23													x							x	2
MDE24														x							1
MDE25		x											x		x						3
MDE26									x				x	x					x		4
MDE27													x	x	x			x	x	x	6
MDE28															x						1
MDE29															x						1
MDE30														x	x				x		3
MDE31														x	x						2
MDE32															x						1
MDE33															x				x		2
MDE34														x	x			x			3
MDE35																		x			1
MDE36																				x	1
MDE37														x						x	2
TOTAL	2	6	5	4	4	1	2	1	5	5	0	0	17	18	17	1	1	9	15	11	

Legenda (D): **DE1** -Norma ABNT NBR ISO/IEC 27001; **DE2** - TISS (Troca de Informação em Saúde Suplementar); **DE3**-Resolução CFM Nº 1.821; **DE4**- Código de Ética Médica - Brasil; **DE5** -Código de Ética dos Profissionais de Enfermagem; **DE6**-Constituição Federal; **DE7** -Código Civil (lei 10.406); **DE8**-Código de Defesa do Consumidor (lei 8.078); **DE9**-Código Penal (lei nº 2.848); **DE10**-Código de Ética da IMIA para Profissionais de Informática em Saúde; **DE11**-Lei de Acesso à informação (lei nº 12.527); **DE12**- Política Nacional de Informação e Informática em Saúde (PNIIS); **DE13**-HIPAA (*Health Insurance Portability and Accountability Act)*; **DE14**-ISO / TC 215; **DE15**-NBR ISO/IEC 27002; **DE16**-Marco Civil da internet; **DE17**-A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2; **DE18**-Manual de Acreditação da ONA; **DE19** -Manual de Acreditação da *Joint Commission International* (JCI); **DE20**- PIPEDA (*Personal Information Protection and Electronic Documents Act*).
Fonte: Elaborado pelo Autor com base na análise de documentos supracitados

Após a descrição qualitativa dos mecanismos encontrados e dispostos no Quadro 13, e também de forma resumida no Quadro 14, é possível verificar alguns pontos importantes. O comitê da ISO/TC 215 (DE14) foi o documento com o maior número de mecanismos identificados, com 18 no total, logo em seguida aparecem a HIPAA (DE13) e a NBR ISO/IEC 27002 (DE15) com 17 mecanismos em cada um deles. No Manual de Acreditação da *Joint Commission International* (JCI) (DE19) tiveram 15 mecanismos localizados.

Mesmo não sendo possível a análise na íntegra, mas sim através dos resumos dos 28 documentos contidos na ISO/TC 215 (DE14), ele foi o que apresentou o maior número de mecanismos. Esse fato o faz ser um dos documentos de maior importância quando se trata de Segurança da Informação e privacidade na saúde.

Dos cinco Documentos Regulatórios e Normativos mais citados, três deles são específicos da Saúde, ou seja, a HIPAA, o manual de acreditação da JCI e considerando que foram selecionados somente os regulamentos dedicados a saúde, a ISO/TC 215.

Exceto os cinco documentos mais citados (DE14, DE13, DE15, DE19 e DE20) e também o Manual de Acreditação da ONA (DE18), com nove mecanismos, o restante deles tiverem individualmente um número pequeno de mecanismos localizados, por serem documentos muito específicos na grande maioria dos casos, como por exemplo, o Código de Ética Médica – Brasil (DE4).

Já a Lei de Acesso à informação (DE11) e a Política Nacional de Informação e Informática em Saúde (DE12), não tiveram nenhum mecanismo localizado, mesmo sendo importantes para a área da saúde. São documentos mais voltados ao Setor público e principalmente dispondo sobre o dever e meios de divulgação das informações administrativas.

O que se pode destacar é que os documentos que os hospitais mais devem ter atenção, segundo o resultado são: ISO/TC 215 (DE14), HIPAA (DE13), NBR ISO/IEC 27002 (DE15), Manual de Acreditação da JCI (DE19), PIPEDA (DE20) e Manual de Acreditação da ONA (DE18), mesmo que nenhum deles seja de uso obrigatório no Brasil. Outro destaque é que poucos documentos possuem um grande número de mecanismos.

Analisando o Quadro 14 pelo ângulo dos mecanismos encontrados, verifica-se que o MDE10, MDE11 e MDE14, tiveram oito aparições, ou seja, cada mecanismo foi citado por oito documentos diferentes dos 20 que foram analisados.

Dentre os três que mais aparecerem dois deles são voltados a ações para os colaboradores: “Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações” (MDE10) e “Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho” (MDE11). O terceiro mecanismo que mais apareceu, está relacionado ao hospital, que é “Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações” (MDE14).

O que se observa é que vários mecanismos foram encontrados em vários documentos, exceto 12 deles que foram citados em apenas um documento. Com isso chega-se à conclusão de que o número de Mecanismos encontrados em relação aos Documentos Regulatórios e Normativos analisados está bem distribuído, porém o número de Documentos Regulatórios e Normativos com vários mecanismos é bem restrito.

4.2 ESTUDOS DE CASO

O primeiro Estudo de Caso foi realizado em um hospital de médio porte na cidade de Cascavel no estado do Paraná, onde trabalham aproximadamente 500 pessoas, sendo atendidos cerca de 8.000 pacientes por mês. Esse piloto teve a intenção de testar o instrumento de pesquisa, ou seja, o roteiro de entrevistas, para verificar possíveis equívocos com o vocabulário, mau formação da pergunta, entre outros.

Nesse estudo não foi considerado o resultado das entrevistas para questões de análise e também não foi realizado essa análise separadamente. Simplesmente as respostas das entrevistas foram descartadas. As considerações realizadas pelos entrevistados e as adequações necessárias, estão descritas detalhadamente no próximo item denominado de Caso Piloto.

4.2.1 Caso Piloto

De acordo com Marconi e Lakatos (2003), todo o instrumento de pesquisa deve passar por um pré-teste, para se verificar a fidedignidade a validade e a operatividade, ou se seja, se é possível obter os mesmos resultados, independente da aplicação, verificar se nenhum dado ficou de fora ou se todos que têm, são mesmo necessários e se o vocabulário e a questão estão claros. Também de acordo com Chagas (2000) é importante a aplicação do teste piloto, uma vez que é possível se verificar problemas e dúvidas que não foram detectadas durante a elaboração. E completa que, sem a sua aplicação pode haver perca de dinheiro, tempo e principalmente credibilidade caso tenha alguma falha grave no questionário.

Com isso o caso piloto foi realizado com quatro colaboradores do Hospital São Lucas de Cascavel no Paraná, conforme características individuais descritas no Quadro 15.

Quadro 15: Caracterização dos participantes do caso piloto

Cargo/função	Área de formação	Grau de formação	Tempo de experiência profissional	Sexo	Idade
Auxiliar de TI - Assistencial	Enfermagem	Especialista	5 anos	Feminino	28 anos
Direção Administrativa	Medicina	Especialista	25 anos	Masculino	52 anos
Administrador de Sistemas	Informática	Graduação	4 anos	Masculino	21 anos
Auxiliar de TI	Informática	Ensino Médio	5 anos	Masculino	21 anos

Fonte: Elaborado pelo autor

O caso piloto foi realizado com uma amostra reduzida, porém os entrevistados como coloca Gil (2002) foram muito similares com as que foram realizadas na pesquisa final e os seus resultados de acordo com Marconi e Lakatos (2003), não fizeram parte da amostra final da pesquisa.

A média de tempo por entrevista do caso piloto foi em torno de 15 minutos. Além de garantir que as perguntas e observações realizadas sejam objetivas no sentido de medir as variáveis que se pretende o intuito do teste conforme afirma Gil (2002) é desenvolver as habilidades e processos de aplicação.

Após a utilização do roteiro para o caso piloto, verificou-se a necessidade de algumas adequações, conforme descritas abaixo:

a) A divisão do roteiro inicial em outros dois roteiros, pois existem alguns termos técnicos que os profissionais que não são da área de TI não sabiam o significado e também desconheciam a sua utilização. Com isso, foi criado um roteiro específico para os profissionais de TI (APÊNDICE B) e outro roteiro para os profissionais de outras áreas (APÊNDICE C);
b) Outra alteração necessária foi a identificação de cada uma das perguntas, enumerando-as e também as dividindo em quadros para melhorar a estética e principalmente a organização para o entrevistador ter melhor visão e não se confundir no momento da entrevista. O roteiro de entrevistas dos profissionais de TI (Apêndice B) ficou com 19 perguntas e o roteiro para os profissionais de outras áreas (Apêndice C) ficou com 17 perguntas;
c) Nesses novos roteiros foi retirada uma das variáveis que era originalmente a de “comportamento pela segurança”, pois se entendeu que, tanto as duas perguntas quanto a variável já estavam contidas na variável de “prática de Segurança da Informação”;
d) A questão 1 (APÊNDICES B e C) foi restruturada, melhorando a compreensão;
e) A questão 1 teve a sua pergunta inicial dividida em sub perguntas, pois as respostas do roteiro inicial não foram completas.
f) A questão 2 dos dois novos roteiros também foi melhorada a escrita sem alterar o seu significado;
g) Na variável “Regras” foram reformuladas totalmente as perguntas 3 e 4, pois não houve uma compreensão por parte dos respondentes, gerando uma resposta inesperada em todos os testes realizados;
h) A questão 5 teve uma pequena alteração de palavras, principalmente trocando de primeira pessoa para “você”;
i) A questão 6 foi reformulada para o entrevistado descrever melhor a sua opinião, pois na pergunta antiga a resposta era muito objetiva;
j) A questão “O Hospital é proativo em relação ao cumprimento das Políticas de Segurança da Informação, por quê? Com quais procedimentos?” Essa pergunta foi retirada, pois a mesma já fora respondida pelas perguntas da variável “Políticas de Segurança”;

k) A questão “Você acha que o tipo de atividade exercida pela instituição exige que sejam estabelecidas e compridas as políticas de privacidade? Por quê?” foi retirada, pois a resposta era óbvia que sim, devido à natureza do serviço.

Estas pequenas alterações foram realizadas melhorando assim o roteiro de entrevistas para a aplicação nos demais Estudos de Caso.

A seguir serão apresentadas as análises e resultados dos Estudos de Caso realizados, cada um deles foi analisado em um item diferente, sendo chamado de Estudo de Caso do Hospital Beta e Estudo de Caso do Hospital Gama. Nos Estudos de Caso foram realizadas entrevistas (E), análise de documentações internas (D) e também observações (O).

4.2.2 Estudos de Caso no Hospital Beta

A primeira técnica utilizada no Estudo de Caso foi a entrevista. No Hospital Beta, localizado na cidade de São Paulo, foram realizadas cinco entrevistas, com pessoas de cargos diferenciados. As características de cada entrevistado contam no Quadro 16.

Quadro 16: Caracterização dos entrevistados Hospital Beta

Código	Gênero	Idade	Escolaridade	Área de Formação	Cargo	Experiência profissional/Anos de empresa
EB1	F	41	Especialização	Informática	Administrador de Projetos na área de Inovação	21/6
EB2	M	37	Especialização	Informática	Gerente de Infraestrutura	18/1
EB3	M	29	Especialização	Informática	Analista de Negócios	11/11
EB4	M	31	Especialização	Informática	Administrador de Projetos	10/8
EB5	M	36	Graduação	Informática	Analista de suporte técnico Pleno	18/7

Fonte: Elaborado pelo autor

Através das entrevistas realizadas foi possível verificar as práticas que são utilizadas pelo Hospital Beta, no que tange à privacidade da informação. Quando indagados pela pergunta de como o estabelecimento trata a questão de privacidade do paciente e principalmente quais os esforços realizados foram bem enfáticos nas respostas:

> Nós temos regras formais, para combater a questão da privacidade. Nós temos uma área que esta disponível para consulta via Intranet, onde estão todas as normas e regulamentações da instituição (EB1).
>
> O nível de incidentes que a gente tem é muito baixo, não é 100%, pois sempre tem alguns incidentes que nos trazem um pouco de preocupação (EB2).
>
> O colaborador assina um termo de conduta e se ele descumprir vai sofrer as medidas cabíveis. Ele sabe que isso pode acontecer, ou seja, se ele descumprir poderá ser punido (EB2).

Um dos assuntos que foi mais discutido e tratado durante a entrevista, sempre reaparecendo em muitas respostas de forma indireta, principalmente nos exemplos, é o treinamento e os processos utilizados pelo hospital:

> [...] O pessoal da área assistencial, por exemplo, não entra direto para trabalhar na assistência, ele passa por um período de educação continuada, não sei te especificar exatamente o quanto, mas é mais de um mês, um período longo que eles passam desde as orientações assistenciais, como e o cuidado do paciente pelo hospital até essa questão da política de informação, nas outras áreas eles tem uma orientação mínima e específica para colaboradores daquela área (EB1).
>
> [...] Não é uma pressão na realidade, uma coisa coerciva. Existe uma educação continuada. O tema esta sempre vindo e indo de diversas maneiras, principalmente por conta das certificações que a gente passa periodicamente (EB2).
>
> [...] Deixa claro relembrando estas questões periodicamente nos treinamentos *online* e com ações rotineiras, como a exigência de renovação de senhas de acesso aos sistemas, por exemplo (EB4).
>
> As regras de Segurança da Informação tornam-se empecilhos apenas quando os processos da instituição não estão bem definidos, situação que obriga o colaborador a buscar atalhos para execução de suas atividades. Atualmente, minha rotina de trabalho está adequada às normas da instituição, portanto, não tenho queixas sobre nenhuma delas (EB4).

Todos os usuários do Hospital Beta, inclusive visitantes e acompanhantes de pacientes possuem uma senha de acesso com a liberação adequada, pois o hospital tem um cuidado muito grande com isso.

> Nós temos uma política até da formação da senha. Tem que ter uma máscara, com maiúscula, e para resolver também um pouco na área assistencial, nós temos o leitor biométrico, para autenticação via biometria para o prontuário eletrônico (EB1).
>
> Todos os computadores são protegidos por senhas (EB3).

Além da política de formação de senha há um incentivo muito grande nas conversas informais e atuação dos colaboradores.

> No manual de normas e condutas que a gente tem existe essa orientação clara e específica em relação a comunicação oral. Não somente aos acessos que você tem no sistema, mas a forma de se comunicar, então eles colocam as situações, desde você ser abordado por uma pessoa que pergunta a respeito de um paciente, ate que você não deve comentar nada

> do que acontece no hospital, até com os seus familiares a gente tem essa orientação, não comente nem com a sua família se uma determinada pessoa esta internada ou não no hospital. Porque essa situação acaba se propagando. Você comenta somente com o seu marido, mas ele vai comentar com alguém. Então existe essa orientação e está no manual de conduta. E em relação as redes sociais também, jamais publique alguma informação que possa expor o paciente e nem publique fotos tiradas dentro do hospital, dentro da instituição (EB1).
>
> Atuamos com descrição, cuidado e seriedade, pois seguimos regras institucionais registradas e documentadas que determinam quais são os deveres e cuidados para que a informação do paciente seja sempre preservada (EB5).
>
> Apesar do cumprimento de uma política de segurança exigir colaboração e disciplina das pessoas, não existe uma pressão sobre o assunto. O hospital procura orientar o indivíduo e cercar, através de ferramentas de segurança, qualquer possibilidade de infração (EB4).

A atualização das normas ocorre de maneira constante. Uma questão que ficou muito clara nas entrevistas, foi a “obrigatoriedade” do Hospital se adaptar e se adequar as regras das Instituições de Certificação Hospitalar, como a Organização Nacional de Acreditação (ONA) e a *Joint Commission International* (JCI), entre outras.

> Se tem um fato que gera um risco e pode ser recorrente, geralmente nós temos duas linhas de atuações, que é periodicamente revisar as normas e se necessário acrescentar alguma coisa específica para esse risco para tentar divulgar uma boa prática ou delimitar que esteja relacionado a esse risco. Para evitar que aconteça novamente e também implementar controles sistêmicos, alguma ferramenta ou customizações dentro do nosso sistema de gestão ou o sistema que eventualmente tenha esse risco (EB2).
>
> Acho importante dizer que nós somos um hospital acreditado pela *Joint Commission* há vários anos e por conta disso, tem toda uma estrutura que existe dentro do hospital... onde esses assuntos são discutidos e esses riscos são avaliados e onde ocorrem as decisões desses riscos entrarem como novas normas ou não, então a gente tem uma área específica de gerência de riscos, um comitê de prontuário, que avalia uma comissão de prontuário de paciente (EB1).
>
> As novas regras surgem muito por conta das certificações devido a novas normas, por exemplo (EB2).
>
> Eu acho que a cobrança das normas existe e ela é constante até por conta das certificações nas quais a gente passa, então, por conta da *Joint Commission* a gente passa por vários treinamentos ao longo do ano e esse assunto, sempre é abordado na Segurança da Informação (EB1).

Como não se tem uma legislação específica no Brasil sobre privacidade, principalmente na saúde, percebe-se conforme Kameda e Pazello (2013) a necessidade de uma regulamentação para se garantir a proteção da privacidade, no qual trata os limites para a utilização de dados pessoais, inclusive para as

informações pessoais sensíveis e de saúde, e os direitos do fornecedor desses dados. E esse assunto também é citado por um dos entrevistados.

> Eu gostaria que tivesse uma política como HIPAA, uma política nacional onde essa norma ficasse mais clara para que a privacidade do paciente não ficasse só garantida aqui na nossa instituição, mas como um todo, porque como eu vejo por exemplo, durante a copa o pessoal estar fotografando o Neymar, aquilo me incomodou muito porque como eu tenho esse conceito tão embutido dentro de mim (EB1).

E ao término da entrevista foi citado um sentimento bastante presente em todas elas, que é o comprometimento por parte dos colaboradores no sentido de cumprir as normas de segurança.

> Ao fazer isso a gente sente que esta ajudando a pessoa (paciente). Ela já não esta numa situação boa. Trabalhamos numa área que a informação é muito sensível (EB2).
>
> Acredito que o reconhecimento é consequência do seu trabalho, se você é um profissional que segue as normas determinadas pela instituição o reconhecimento é natural (EB5).
>
> A satisfação vem quando você tem seu trabalho reconhecido, e isso só chega através do seu próprio esforço, o que vem adiante é sempre consequência disso (EB5).
>
> A possibilidade de oferecer facilidades e melhorias na rotina de colaboradores e pacientes trás satisfação ao meu trabalho (EB4).
>
> As regras de Segurança da Informação são de grande satisfação, pois funcionam de forma imperceptível como agregador de funcionamento do processo (EB3).
>
> Pessoalmente eu fico satisfeita em acompanhar a evolução das pessoas, de como essas normas vem sendo construídas e o quanto elas foram sendo entendidas pelas pessoas em todos os níveis no hospital. É um processo evolutivo que não tem fim, ele vai sempre melhorando (EB1).

Após as transcrições e análises das entrevistas, foram identificados 32 mecanismos que são possíveis de utilização para prevenir e melhorar a privacidade da informação, conforme demonstra a Quadro 17. Nele é descrito o mecanismo identificado por um código específico das entrevistas do hospital beta, criado para facilitar a rastreabilidade durante todo o decorrer da análise. Em cada um dos mecanismos marcados com um (X) representa qual o entrevistado que o citou durante as entrevistas, sendo estes representados pelos entrevistados (EB1, EB2...), podendo observar as suas características pessoais no Quadro 16.

Quadro 17: Mecanismos identificados nas entrevistas: Hospital Beta

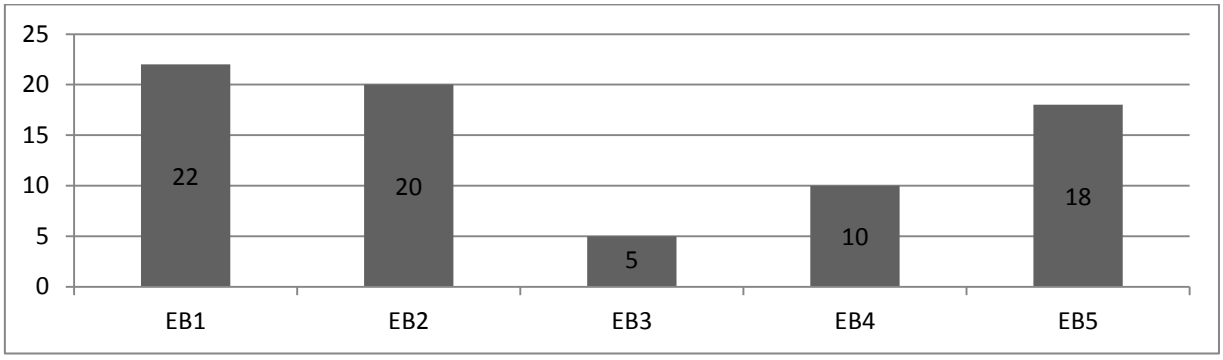
Código	Mecanismos	EB1	EB2	EB3	EB4	EB5
MEB1	Implantar e manter um Sistema de Gestão da Segurança da Informação	X	X			
MEB2	Ter uma pessoa responsável pela Política de Segurança da Informação	X	X			
MEB3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	X	X	X	X	X
MEB4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	X	X		X	X
MEB5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos		X			
MEB6	Possuir uma Comissão de Revisão de Prontuários	X				
MEB7	Instruir o médico e enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	X	X			
MEB8	Prevenir para que médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	X				
MEB9	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	X	X			
MEB10	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	X	X		X	X
MEB11	Instalar Antivírus, VPN e *firewall*				X	X
MEB12	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	X	X		X	X
MEB13	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	X	X			X
MEB14	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	X	X	X		X
MEB15	Impor sanções adequadas para os que violam as políticas de privacidade	X	X	X	X	X
MEB16	Ter um plano de recuperação ou contingência para desastres com informações					X
MEB17	Ter um *backup* estruturado das informações					X
MEB18	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede					X
MEB19	Ter um *software* de HIS – adequado e de boa qualidade	X				
MEB20	Criptografar o tráfego externo de informações		X		X	X
MEB21	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do paciente					X
MEB22	Criar e divulgar aos colaboradores uma política de privacidade	X	X	X	X	X
MEB23	Dividir as funções dos colaboradores nos sistemas		X			
MEB24	Analisar regularmente a Segurança dos Sistemas de Informação		X			
MEB25	Ter a quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento	X			X	X
MEB26	Criar uma intranet para deixar os documentos disponíveis	X		X	X	X
MEB27	Ter uma área de qualidade para controlar os documentos	X				
MEB28	Não utilizar celular no local de trabalho, principalmente no beira leito	X	X			
MEB29	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento	X				X
MEB30	Valorizar e até premiar em dinheiro a boa prática de Segurança da Informação	X	X			X
MEB31	Ter uma política pública específica para a privacidade da informação no Brasil	X	X			
MEB32	Assinatura de um termo de conduta no momento da contratação, com sanções		X			

Fonte: Elaborado pelo autor

Através das entrevistas foi possível identificar que, dos 32 mecanismos apenas três deles foram citados pelos cinco entrevistados, e isso pode ocorrido devido ao fato de todos terem cargo/função diferenciados. Porém, o que chamou mais a atenção foi o fato de que os entrevistados que mais citaram mecanismos foram exatamente aqueles que possuem maior experiência de anos de trabalho.

Na Figura 2, é demonstrado um resumo do total de mecanismos que cada um dos entrevistados contribuiu. Destacando-se o entrevistado EB1, com o maior número de mecanismos citados durante a sua entrevista. E também o entrevistado EB2 com um número expressivo de citações. Esses dois entrevistados são os que têm o maior nível hierárquico de cargo, entre os entrevistados do Hospital Beta.

Figura 2: Total de mecanismos identificados a partir das falas de cada entrevistado–Hospital Beta



Fonte: Elaborado pelo autor

A seguir serão apresentados os mecanismos agrupados pelo tipo de abordagem no qual foram descobertos, ou seja, se foi através das Entrevistas (E), Documentos Internos (D) ou Observação (O), do Estudo de Caso do Hospital Beta.

Na linha de cada mecanismo identificado, esta mostrando quantas citações ele teve durante as Entrevistas (E), ou seja, quantas pessoas citaram determinado mecanismo, considerando que o número de entrevistados do Hospital Beta eram cinco. Na coluna de (D) Documentos Internos, foi analisado um documento e nas observações (O), apesar de serem feitas visitas às instalações, consultas no Site institucional e também conversas informais, foi considerado somente como uma citação. Totalizando assim sete possíveis meios de citação de mecanismos, sendo cinco das entrevistas, uma dos documentos internos e uma das observações, conforme mostra o Quadro 18.

Quadro 18: Mecanismos identificados no Estudo de Caso Beta

Código	Mecanismos – Estudo de Caso – Hospital Beta	E	D	O
MECB1	Implantar e manter um Sistema de Gestão da Segurança da Informação	2		1
MECB2	Ter uma pessoa responsável pela Política de Segurança da Informação	2		
MECB3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	5	1	1
MECB4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	4	1	
MECB5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	1		1
MECB6	Possuir uma Comissão de Revisão de Prontuários	1		
MECB7	Instruir o médico e enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	2		1
MECB8	Prevenir para que médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	1		1
MECB9	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações.	2		1
MECB10	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	4	1	
MECB11	Instalar Antivírus, VPN e *firewall*	2	1	
MECB12	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	4		1
MECB13	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	3	1	1
MECB14	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura		1	
MECB15	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	4		1
MECB16	Impor sanções adequadas para os que violam as políticas de privacidade	5	1	1
MECB17	Ter um plano de recuperação ou contingência para desastres com informações	1	1	
MECB18	Ter um backup estruturado das informações	1		
MECB19	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede	1	1	1
MECB20	Ter um *software* de HIS – adequado e de boa qualidade	1		1
MECB21	Criptografar o tráfego externo de informações	3	1	
MECB22	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do paciente	1	1	
MECB23	Criar e divulgar aos colaboradores uma política de privacidade	5		
MECB24	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa			1
MECB25	Definir regras para transmissão externa de informações para terceiros		1	
MECB26	Dividir as funções dos colaboradores nos sistemas	1		
MECB27	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação		1	
MECB28	Analisar regularmente a Segurança dos Sistemas de Informação	1	1	
MECB29	Ter a quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento	3		1
MECB30	Criar uma intranet para deixar os documentos disponíveis	4		1
MECB31	Ter uma área de qualidade para controlar os documentos	1		1
MECB32	Não utilizar celular no local de trabalho, principalmente no beira leito	2		
MECB33	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento	2		
MECB34	Valorizar e até premiar em dinheiro a boa prática de Segurança da Informação	3		1
MECB35	Ter uma política pública específica para a privacidade da informação no Brasil	2		
MECB36	Assinatura de um termo de conduta no momento da contratação, com sanções	1		
TOTAL		32	14	17

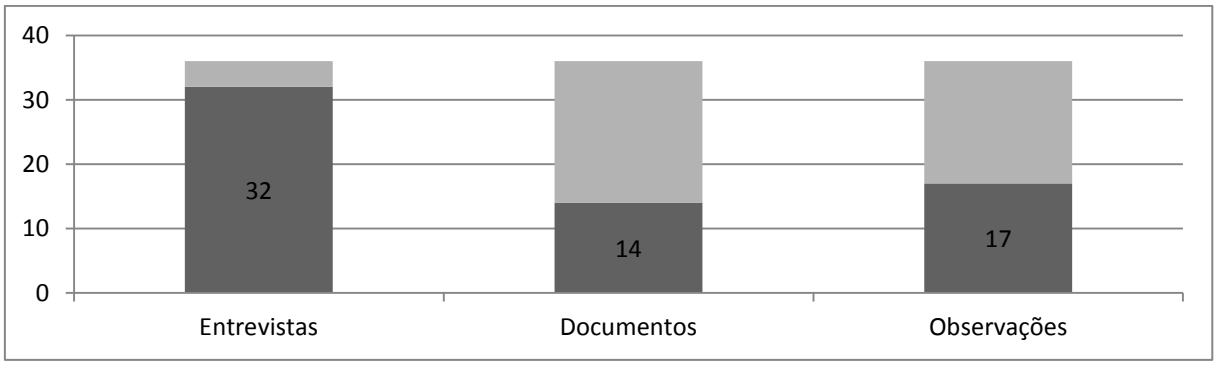
Legenda: E - Entrevistas; D - Documentos Internos; O - Observações

Fonte: Elaborado pelo autor

A Figura 3 demonstra um resumo do Quadro 18, ou seja, a totalização das técnicas nas quais foram identificados os 36 mecanismos no Estudo de Caso Beta, representados no gráfico pela cor cinza claro. A cor cinza escuro do gráfico

representa a quantidade de mecanismos encontrados em cada uma das técnicas, ou seja, dos 36 mecanismos encontrados considerando todas as técnicas utilizadas no Estudo de Caso Beta, 32 deles foram citados nas entrevistas, 14 foram identificados nos Documentos Internos e 17 nas observações. Do total de 36 mecanismos, quatro deles foram identificados igualmente nas três técnicas. No Quadro 18, é possível verificar quais mecanismos foram identificados em quais técnicas.

Figura 3: Total de mecanismos por técnica de coleta de dados–Estudo de Caso Beta



Fonte: Elaborado pelo autor

A Figura 3 demonstra que as entrevistas tiveram um grande número de mecanismos identificados em relação ao total, verificando-se uma grande eficiência da técnica utilizada.

4.2.3 Estudos de Caso no Hospital Gama

No Hospital Gama foram realizadas quatro entrevistas, todas com colaboradores do setor de TI, conforme características dos entrevistados demonstradas no Quadro 19.

Quadro 19: Caracterização dos entrevistados do Hospital Gama

Código	Gênero	Idade	Escolaridade	Área de Formação	Cargo	Experiência profissional/Anos de empresa
EG1	M	38	Especialização	Administração	Coordenador de TI	10/10
EG2	F	43	Especialização	Administração – Ênfase em Análise	Chefe do setor de Segurança da Informação	17/15
EG3	F	49	Graduação	Administração – Ênfase em Análise	Chefe do Setor de Sistemas Assistenciais	23/23
EG4	M	25	Graduação	Informática	Analista de TI	5/5

Fonte: Elaborado pelo autor

Durante as entrevistas foi possível observar a grande preocupação com a Segurança da Informação, iniciando no momento da contratação do funcionário:

> Hoje qualquer profissional, não somente o médico, quando ele é cadastrado, lá na área de recursos humanos, o sistema automaticamente já dá o perfil de acesso ao sistema de acordo com as atribuições e capacitações que ele tem (EG1).
>
> Quando ele recebe o usuário e senha, o usuário ainda é bloqueado, então automaticamente para ele usar qualquer sistema, ele recebe uma folha do RH com o usuário e o e-mail, mas com a senha bloqueada, ele tem que ir num computador qualquer do hospital para desbloquear e nesse momento o sistema apresenta a política de segurança para ele ler e aceitar (EG1).
>
> [...] nós temos um processo de *login* e senha unificados, a mesma senha vale para tudo, para acessar a rede, o e-mail o contracheque, para acessar as informações financeiras da pessoa. Então esse tipo de coisa, se eu fornecer a minha senha para a outra pessoa, ele pode ver outras coisas, como pode mandar um e-mail no meu nome (EG2).
>
> [...] tem um controle de acesso para tudo. Temos uma burocracia bem grande para alterar perfis de acessos. Não é para qualquer pessoa que é liberado (EG4).

Outro indicativo de preocupação é pela divisão dos setores, no qual tem um setor específico para tratar da Segurança da Informação conforme enfatizado nas entrevistas:

> O hospital sempre foi preocupado com as questões da segurança e temos um inter-relacionamento muito grande e a comissão de prontuário sempre foi cuidadosa com os acessos aos prontuários (EG1).
>
> Eu, na prática como atuo diretamente com esse processo. Eu atuo diretamente com incidentes de segurança, a punição e a cobrança, seja só um e-mail cobrando e dizendo que aquilo não deve ser feito ou em casos mais graves como suspensão e casos de demissão. Eu acredito que ela dá um bom efeito (EG2).
>
> Eu investigo os erros por *log*. Em ultimo caso eu acesso com o meu *login*. Até eu, que sou a responsável pelo serviço, tenho cuidados de não acessar o prontuário com a minha senha (EG3).

Além da comissão de prontuários, conforme citado pelo entrevistado (EG1), há também outras comissões, comprovando que é um hospital muito bem estruturado e preocupado com a Segurança da Informação.

> A comissão de prontuário é extremamente atuante, e eles têm um painel que eles conseguem ver, quem está acessando os prontuários, por exemplo, se aparece para eles que um analista de TI esta acessando o prontuário, eles vem aqui e batem na nossa porta (EG1).
>
> Além da comissão de prontuário que fez todas essas regras de acesso, também tem uma comissão de ética. E também a gente faz cursos EAD, que todos os funcionários são obrigados a participar. Um deles é sobre ética, no qual fala do acesso ao prontuário,, inclusive para nós da CGTI, todos os funcionários do hospital fazem esses cursos (EG3).

Os processos de divulgação das políticas de segurança e das boas práticas, assim como avisos importantes, são bem diversificados e eficientes.

> A gente faz cartaz e comunicado, quando atualizamos a norma fazemos uma ação de divulgação muito grande. Hoje em dia temos outras mídias como e-mail, intranet, pois está mais consolidada (EG1).
>
> O que está documentado que são as decisões que estão na intranet para a divulgação e acesso a todo o momento (EG2).
>
> Nós temos na entrada do sistema uma caixa postal, que deixa recados e avisos. Ela é utilizada para recados importantes do uso do sistema também (EG1).

Os treinamentos são realizados constantemente para todos os colaboradores, alguns de forma voluntária, porém outros de forma obrigatória, esses treinamentos são diversificados, abrangendo diversos assuntos e dentre eles a segurança e a privacidade da informação.

> O hospital é acreditado pela *Joint Comission*, e ela é extremamente rigorosa. Inclusive essa questão dos treinamentos é uma exigência de que todos os funcionários passam por treinamentos (EG1).
>
> Para mim os cursos de EAD surtem um resultado muito bom, porque é obrigatório (EG2).
>
> Então você tem acesso, e você tem um perfil que permite acessar o prontuário on-line e você conhece o paciente que está internado, você não vai sair comentando, sobre isso. E isso a gente a aprende no EAD (EG3).

Ao término das entrevistas, foi possível identificar 41 mecanismos. Alguns deles foram citados por todos os participantes, conforme demonstra o Quadro 20. Nele é descrito o mecanismo identificado por um código específico das entrevistas do Hospital Gama. Em cada um dos mecanismos marcados com um (X) representa qual o entrevistado que citou determinado mecanismo durante as entrevistas, sendo estes representados por (EG1, EG2...).

Quadro 20: Mecanismos identificados nas entrevistas: Hospital Gama

Código	Mecanismos	EG1	EG2	EG3	EG4
MEG1	Implantar e manter um Sistema de Gestão da Segurança da Informação	X			X
MEG2	Ter uma pessoa responsável pela Política de Segurança da Informação	X	X		
MEG3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	X	X		X
MEG4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	X	X		
MEG5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	X			X
MEG6	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED	X		X	
MEG7	Possuir uma Comissão de Revisão de Prontuários	X	X	X	
MEG8	Instruir o médico e enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	X	X	X	
MEG9	Prevenir para que médicos e enfermeiros não conversem com pacientes		X	X	

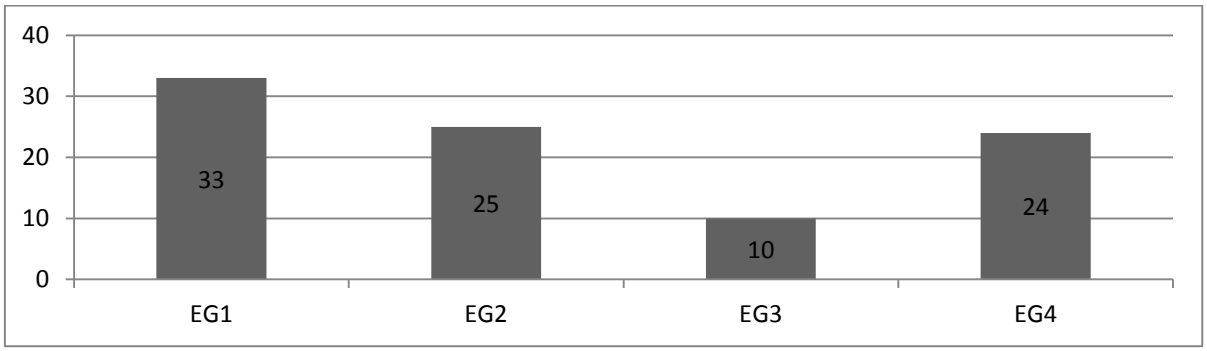
Código	Mecanismos	EG1	EG2	EG3	EG4
	a respeito de diagnósticos em áreas públicas				
MEG10	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	X	X		
MEG11	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	X	X		
MEG12	Instalar Antivírus, VPN e *firewall*				X
MEG13	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	X	X		X
MEG14	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	X			X
MEG15	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura	X	X		X
MEG16	Coletar somente dados relevantes dos clientes/pacientes		X		
MEG17	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	X	X	X	
MEG18	Impor sanções adequadas para os que violam as políticas de privacidade	X	X		
MEG19	Ter um plano de recuperação ou contingência para desastres com informações				X
MEG20	Ter um *backup* estruturado das informações				X
MEG21	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede				X
MEG22	Ter um *software* de HIS – adequado e de boa qualidade	X	X		X
MEG23	Criptografar o tráfego externo de informações	X			X
MEG24	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do Paciente	X	X		X
MEG25	Criar e divulgar aos colaboradores uma política de privacidade	X			
MEG26	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo	X	X		X
MEG27	Definir regras para transmissão externa de informações para terceiros	X			X
MEG28	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação	X	X	X	
MEG29	Dividir as funções dos colaboradores nos sistemas	X			
MEG30	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação				X
MEG31	Analisar regularmente a Segurança dos Sistemas de Informação	X	X		
MEG32	Ter a quantidade de Profissionais dimensionados de acordo com a realidade da organização ou departamento	X			X
MEG33	Manter as informações dos clientes apenas o tempo necessário por lei		X		
MEG34	Criar uma intranet para deixar os documentos disponíveis	X	X		X
MEG35	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento	X	X	X	
MEG36	Assinatura de um termo de conduta no momento da contratação, com sanções	X	X		X
MEG37	Criar uma integração de *login* e senha válido para todos os sistemas	X			X
MEG38	Desconectar o sistema por tempo de inatividade	X		X	X
MEG39	Utilizar nomes fictícios nas bases de testes e homologações	X	X	X	X
MEG40	Acesso do prontuário somente no momento que o paciente esta internado	X	X	X	X
MEG41	Dar ciência da leitura dos termos de Segurança da Informação no momento da troca da senha	X	X		X

Fonte: Elaborado pelo autor

A Figura 4 faz um balanço resumido do Quadro 20, para facilitar a visualização, demonstrando o total de mecanismos que cada entrevistado contribuiu. O que se pode perceber é que o entrevistado EG1 que é o coordenador de TI teve o

maior número de mecanismos citados e o entrevistado EG4 trouxe em suas falas, mecanismos mais voltados à parte técnica, por ser graduado na área de informática. A entrevistada EG3 foi a que menos contribuiu com mecanismos, pois é a que tem uma função mais específica em relação aos demais entrevistados, uma vez que ela trabalha diretamente com a área assistencial, fazendo a *interface* entre a TI e a assistência ao Paciente.

Figura 4: Total de mecanismos identificados a partir das falas de cada entrevistado–Hospital Gama



Fonte: Elaborado pelo autor

Ao término da análise das entrevistas, que resultou em 41 mecanismos de privacidade do Hospital Gama, foram analisados os documentos internos. Na etapa de observação foram analisados os processos internos, através de visitas às instalações e também conversas informais com colaboradores e clientes, além da descrição que há no *site* da instituição.

O Quadro 21 representa o resultado dos mecanismos localizados no Estudo de Caso do Hospital Gama, com a quantidade de entrevistados que citaram o mecanismo nas entrevistas (E), a quantidade de documentos que trazem o mecanismo na análise dos Documentos Internos (D) e nas observações realizadas (O). Levando em consideração que o número total das entrevistas são quatro, a coluna (E) do Quadro 21 traz a quantidade de entrevistados que citaram o mecanismo, a coluna (D) traz o número total de documentos que citaram o mecanismo e a coluna (O) as observações possível de classificar como mecanismo. Totalizando assim sete possíveis citações, originadas de quatro entrevistas, dois documentos internos e uma observação.

Quadro 21: Mecanismos identificados no Estudo de Caso Gama

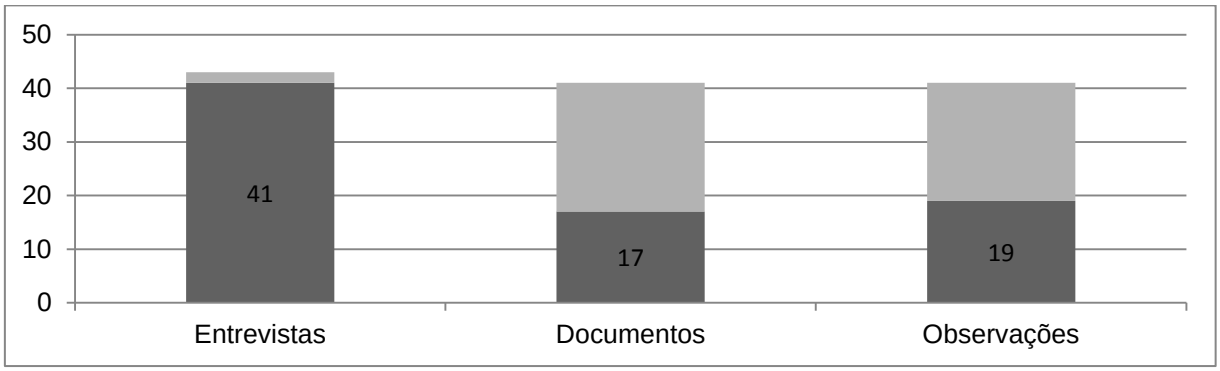
Código	Mecanismos – Estudo de Caso – Hospital Gama	E	D	O
MECG1	Implantar e manter um Sistema de Gestão da Segurança da Informação	2	1	1
MECG2	Ter uma pessoa responsável pela Política de Segurança da Informação	2		1
MECG3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	3	2	1
MECG4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	2	2	1
MECG5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	2		1
MECG6	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED	2		
MECG7	Possuir uma Comissão de Revisão de Prontuários	3		1
MECG8	Instruir o Médico e Enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	3		
MECG9	Prevenir para que Médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	2		1
MECG10	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	2		1
MECG11	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	2	1	
MECG12	Instalar Antivírus, VPN e *firewall*	1	1	
MECG13	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	3		
MECG14	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	2	1	1
MECG15	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura	3	1	
MECG16	Coletar somente dados relevantes dos clientes/pacientes	1		
MECG17	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	3	1	
MECG18	Evitar posicionar computadores próximos a corredores			1
MECG19	Impor sanções adequadas para os que violam as políticas de privacidade	2	1	
MECG20	Ter um plano de recuperação ou contingência para desastres com informações	1	1	
MECG21	Ter um b*ackup* estruturado das informações	1	1	
MECG22	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede	1	1	1
MECG23	Ter um *software* de HIS – adequado e de boa qualidade	3		1
MECG24	Criptografar o tráfego externo de informações	2	1	
MECG25	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do Paciente	3		
MECG26	Criar e divulgar aos colaboradores uma política de privacidade	1	1	1
MECG27	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo	3		
MECG28	Definir regras para transmissão externa de informações para terceiros	2	1	
MECG29	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação	3	1	1
MECG30	Dividir as funções dos colaboradores nos sistemas	1		1
MECG31	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação	1		
MECG32	Analisar regularmente a Segurança dos Sistemas de Informação	2		
MECG33	Ter a quantidade de Profissionais dimensionados de acordo com a realidade da organização ou departamento	2		1
MECG34	Manter as informações dos clientes apenas o tempo necessário por lei	2		
MECG35	Criar uma intranet para deixar os documentos disponíveis	3		1
MECG36	Cursos e treinamentos a distância obrigatórios com provas e avaliações de	3		

Código	Mecanismos – Estudo de Caso – Hospital Gama	E	D	O
	teste de conhecimento			
MECG37	Assinatura de um termo de conduta no momento da contratação, com sanções	3		1
MECG38	Criar uma integração de *login* e senha válidos para todos os sistemas	2		
MECG39	Desconectar o sistema por tempo de inatividade	3		1
MECG40	Utilizar nomes fictícios nas bases de testes e homologações	4		
MECG41	Acesso do prontuário somente no momento que o paciente esta internado	4		
MECG42	Dar ciência da leitura dos termos de Segurança da Informação no momento da troca da senha	3		
MECG43	Bloquear a utilização de mídias de gravação (pendrive) internos assim como acesso a repositórios na internet e e-mail externo		1	
TOTAL		41	17	19

Legenda: E - Entrevistas; D - Documentos Internos; O - Observações
Fonte: Elaborado pelo autor

A Figura 5 traz um resumo dos mecanismos identificados por tipo de técnica utilizada para coletá-los.

Figura 5: Total de mecanismos por técnica de coleta de dados–Estudo de Caso Gama



Fonte: Elaborado pelo autor

A figura mostra na sua parte cinza claro o total de mecanismos encontrados considerando as três técnicas, ou seja, 43 no total. É possível verificar na parte cinza escuro, o total de mecanismos identificados em cada uma das técnicas. Por exemplo, 19 mecanismos foram identificados pela técnica de observações de um total de 43 mecanismos. Deve se observar que a soma das três colunas em cinza escuro, ultrapassa a quantidade de mecanismos identificados, porém isso ocorre porque vários mecanismos estão contidos nas diferentes técnicas, ou seja, eles se repetem, conforme demonstra o Quadro 21. Pode-se verificar que do total de mecanismos identificados no Estudo de Caso Gama, sete deles aparecem igualmente nas três técnicas e 16 deles foram citados em apenas uma das técnicas.

A coluna referente às entrevistas teve quase a totalidade dos mecanismos citados, isto é, apenas dois mecanismos dos 43 totais não foram identificados nas entrevistas.

No Estudo de caso Gama, a entrevista foi a técnica mais eficiente na identificação dos mecanismos de privacidade da informação, com um número de mecanismos localizados maior que o dobro localizado em outra técnica.

4.3 CONSOLIDAÇÃO DOS RESULTADOS DOS ESTUDOS DE CASO

Na Tabela 3 é apresentado o resultado com as informações agrupadas do Estudo de Caso do Hospital Beta e do Estudo de Caso do Hospital Gama. São identificados os mecanismos encontrados tanto na etapa das entrevistas (E), como na análise dos documentos internos (D), assim como nas observações (O) realizadas.

Tabela 3: Mecanismos identificados nos Estudos de Caso Beta e Gama

Código	Mecanismos	BETA				GAMA				TG
		E	D	O	T	E	D	O	T	
MEC1	Implantar e manter um Sistema de Gestão da Segurança da Informação	2		1	3	2	1	1	4	**7**
MEC2	Ter uma pessoa responsável pela Política de Segurança da Informação	2			2	2		1	3	**5**
MEC3	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	5	1	1	7	3	2	1	6	**13**
MEC4	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	4	1		5	2	2	1	5	**10**
MEC5	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	1		1	2	2		1	3	**5**
MEC6	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED				0	2			2	**2**
MEC7	Possuir uma Comissão de Revisão de Prontuários	1			1	3		1	4	**5**
MEC8	Instruir o médico e enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	2		1	3	3			3	**6**
MEC9	Prevenir para que médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	1		1	2	2		1	3	**5**
MEC10	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	2		1	3	2		1	3	**6**
MEC11	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	4	1		5	2	1		3	**8**
MEC12	Instalar Antivírus, VPN e *firewall*	2	1		3	1	1		2	**5**
MEC13	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	4		1	5	3			3	**8**
MEC14	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	3	1	1	5	2	1	1	4	**9**
MEC15	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura		1		1	3	1		4	**5**
MEC16	Coletar somente dados relevantes dos clientes/pacientes				0	1			1	**1**
MEC17	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	4		1	5	3	1		4	**9**
MEC18	Evitar posicionar computadores próximos a corredores				0			1	1	**1**
MEC19	Impor sanções adequadas para os que violam as políticas de privacidade	5	1	1	7	2	1		3	**10**
MEC20	Ter um plano de recuperação ou contingência para desastres com informações	1	1		2	1	1		2	**4**
MEC21	Ter um *backup* estruturado das informações	1			1	1	1		2	**3**
MEC22	Ter proteções internas para a conexão de um novo *hardware* ou	1	1	1	3	1	1	1	3	**6**

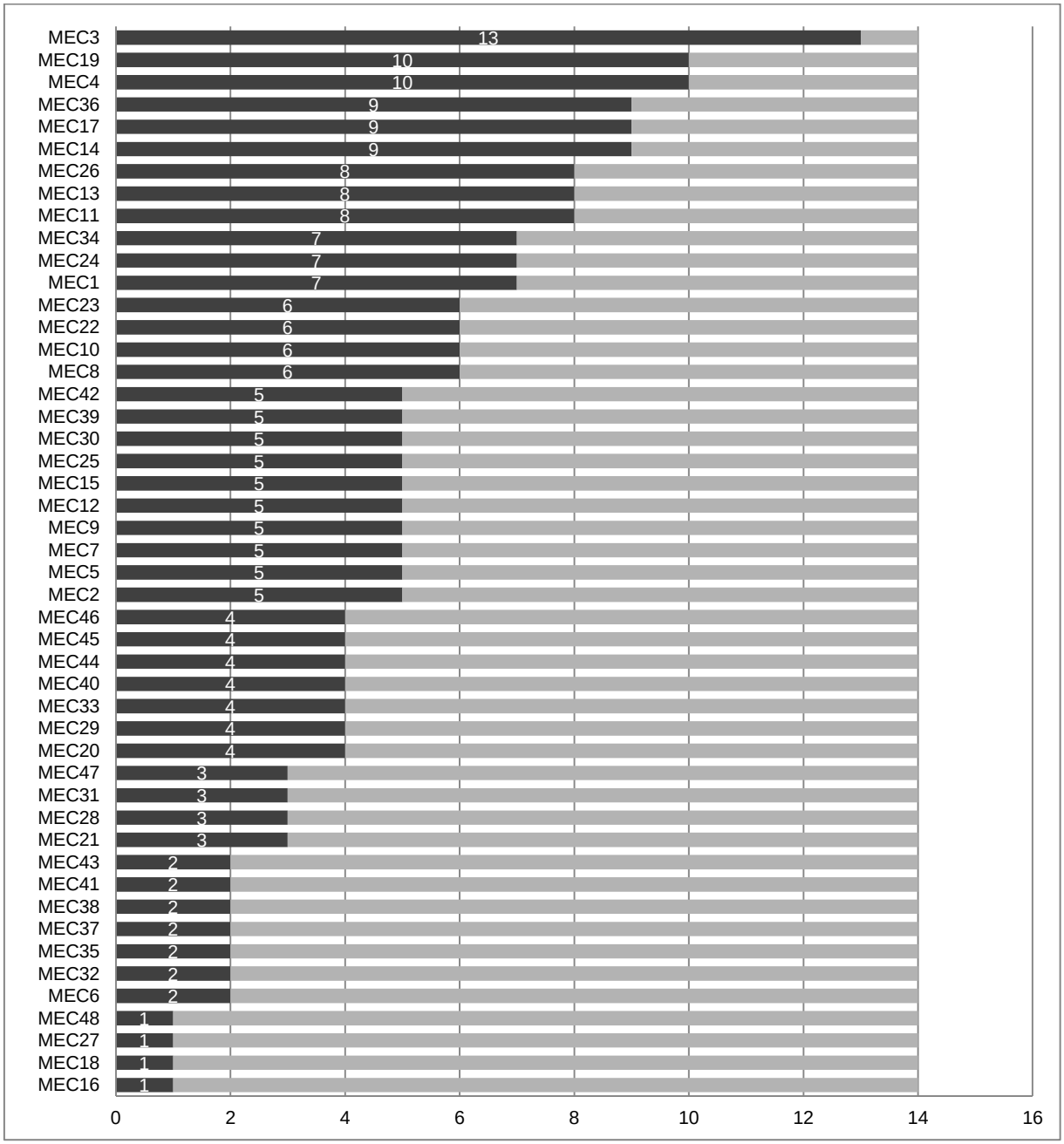
Código	Mecanismos	BETA				GAMA				TG
		E	D	O	T	E	D	O	T	
	software na rede									
MEC23	Ter um *software* de HIS – adequado e de boa qualidade	1		1	2	3		1	4	**6**
MEC24	Criptografar o tráfego externo de informações	3	1		4	2	1		3	**7**
MEC25	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do paciente	1	1		2	3			3	**5**
MEC26	Criar e divulgar aos colaboradores uma política de privacidade	5			5	1	1	1	3	**8**
MEC27	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa			1	1				0	**1**
MEC28	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo				0	3			3	**3**
MEC29	Definir regras para transmissão externa de informações para terceiros		1		1	2	1		3	**4**
MEC30	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação				0	3	1	1	5	**5**
MEC31	Dividir as funções dos colaboradores nos sistemas	1			1	1		1	2	**3**
MEC32	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação.		1		1	1			1	**2**
MEC33	Analisar regularmente a Segurança dos Sistemas de Informação	1	1		2	2			2	**4**
MEC34	Ter a quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento	3		1	4	2		1	3	**7**
MEC35	Manter as informações dos clientes apenas o tempo necessário por lei				0	2			2	**2**
MEC36	Criar uma intranet para deixar os documentos disponíveis	4		1	5	3		1	4	**9**
MEC37	Ter uma área de qualidade para controlar os documentos	1		1	2				0	**2**
MEC38	Não utilizar celular no local de trabalho, principalmente no beira leito	2			2				0	**2**
MEC39	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento	2			2	3			3	**5**
MEC40	Valorizar e até premiar em dinheiro a boa prática de Segurança da Informação	3		1	4				0	**4**
MEC41	Ter uma política pública específica para a privacidade da informação no Brasil	2			2				0	**2**
MEC42	Assinatura de um termo de conduta no momento da contratação, com sanções	1			1	3		1	4	**5**
MEC43	Criar uma integração de *login* e senha válido para todos os sistemas				0	2			2	**2**
MEC44	Desconectar o sistema por tempo de inatividade				0	3		1	4	**4**
MEC45	Utilizar nomes fictícios nas bases de testes e homologações				0	4			4	**4**
MEC46	Acesso do prontuário somente no momento que o paciente esta internado				0	4			4	**4**
MEC47	Dar ciência da leitura dos termos de Segurança da Informação no momento da troca da senha				0	3			3	**3**
MEC48	Bloquear a utilização de mídias de gravação (*pendrive*) internos assim como acesso a repositórios na internet e e-mail externo				0		1		1	**1**

Legenda: E - Entrevistas; D - Documentos Internos; O – Observações; T - Total individual por Hospital; TG – Total Geral
Fonte: Elaborado pelo autor

A Tabela mostra o total de mecanismos localizados nos dois Estudos de Caso, agrupando os que são iguais e criando um código para cada um dos 48 mecanismos, iniciando com (MEC...). Em cada um deles é possível verificar a sua origem, ou seja, Estudo de Caso Beta (BETA) ou Estudo de Caso Gama (GAMA).

A Figura 6, traz o total de Mecanismos identificados e ordenados do maior para o menor número de citações.

Figura 6: Total de citação para cada mecanismo nos Estudos de Caso



Fonte: Elaborado pelo autor

Dentro de cada um dos Estudos de Caso, é possível identificar em quais técnicas que foram citados os mecanismos. A coluna chamada de (T) dentro de cada estudo, representa o total de mecanismos citados, considerando cada uma das técnicas. Lembrando que a possibilidade de citações era de sete em cada um dos Estudos de Caso. O total Geral é a soma de todas as citações de mecanismos considerando as três técnicas de coletas de dados de cada Estudo de Caso, chegando num total máximo de 14 citações.

Do total de 48 mecanismos apenas dois deles são citados em todas as técnicas dos dois Estudos de Caso e 17 mecanismos foram identificados em apenas um dos Estudos de Caso. E nenhum mecanismo teve a totalidade de citações que seria de 14.

O mecanismo mais citado nos Estudos de Caso, foi o “Identificar e autenticar o usuário em sistemas, arquivos, portais ou webservices” (MEC3), das 14 possibilidade de citações do mecanismo, ele apenas não foi mencionado por um dos entrevistados do Hospital Gama, tendo com isso 13 citações no total.

Os mecanismos que menos apareceram nos Estudos de Caso são o MEC16, o MEC18, o MEC27 e o MEC48, com apenas uma citação dentre todas as possíveis. A questão de coletar somente os dados relevantes dos pacientes, que é um desses mecanismos, primeiramente deve ser avaliada, pois cada profissional médico coleta as informações que achar necessário para constar no histórico do paciente, a fim de auxiliar no diagnóstico, e por isso não pode ser contestado por profissionais de Segurança da Informação. Outro mecanismo que apareceu somente uma vez, mas não deixa de ser importante é o de evitar o posicionamento de computadores próximos a corredores, principalmente se houver fluxo de pessoas que não são colaboradores do hospital. Essa atitude simples pode evitar que pessoas curiosas olhem as informações nos monitores, seja esta simplesmente um nome, como também dados relevantes e confidenciais do paciente.

4.4 CONSOLIDAÇÃO DOS RESULTADOS DOS CASOS E DOS DOCUMENTOS

Primeiramente foram organizados os mecanismos referentes aos documentos Regulatórios e Normativos, numa segunda etapa, foram identificados e organizados os mecanismos referentes aos Estudos de Caso, resultados indicados nas análises anteriores. No Quadro 22, estão agrupados os mecanismos, unificando o código e mostrando de qual abordagem é a sua origem. Da análise dos Documentos Regulatórios e Normativos (MDE...) ou dos Estudos de Caso (MEC...), ou ambos.

Neste Quadro, o código (M1...M2) foi criado apenas para identificar o mecanismo na sequência da análise. Ele traz também a abordagem metodológica de origem do mecanismo, com a quantidade de vezes que esse mecanismo foi citado. Utilizando como base a totalização conforme o Quadro 13 e a Tabela 3 e levando em consideração que na abordagem de Análise dos Documentos

Regulatórios e Normativos tem-se 20 citações possíveis e na Análise dos Estudos de Caso tem-se 14 citações possíveis, o número total é de 34 citações possíveis que o mecanismo pode ter.

A quantidade de mecanismos de privacidade que foram identificados foi de 50, estando dispostos no Quadro 22, juntamente com a quantidade de citações, estando esta ordenada do maior para o menor número de citações.

Quadro 22: Mecanismos identificados: Documentos Regulatórios e Normativos x Estudos de Caso

Cód	Mecanismo	Documentos Regulatórios /Normativos	Estudos de Caso	Total
M1	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	MDE3	MEC3	**19**
M2	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	MDE14	MEC14	**17**
M3	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	MDE11	MEC11	**16**
M4	Impor sanções adequadas para os que violam as políticas de privacidade	MDE19	MEC19	**16**
M5	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	MDE10	MEC10	**14**
M6	Criar e divulgar aos colaboradores uma política de privacidade	MDE27	MEC26	**14**
M7	Implantar e manter um Sistema de Gestão da Segurança da Informação	MDE1	MEC1	**13**
M8	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	MDE13	MEC13	**13**
M9	Instalar Antivírus, VPN e *firewall*	MDE12	MEC12	**12**
M10	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	MDE17	MEC17	**12**
M11	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	MDE4	MEC4	**11**
M12	Ter uma pessoa responsável pela Política de Segurança da Informação	MDE2	MEC2	**10**
M13	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	MDE5	MEC5	**10**
M14	Criptografar o tráfego externo de informações	MDE25	MEC24	**10**
M15	Instruir o médico e enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	MDE8	MEC8	**9**
M16	Ter um plano de recuperação ou contingência para desastres com informações	MDE21	MEC20	**9**
M17	Armazenar *logs* de acesso e *logs* de alterações realizadas no prontuário do paciente	MDE26	MEC25	**9**
M18	Criar uma intranet para deixar os documentos disponíveis		MEC36	**9**
M19	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura	MDE15	MEC15	**8**
M20	Ter um *backup* estruturado das informações	MDE22	MEC21	**8**
M21	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede	MDE23	MEC22	**8**
M22	Ter a quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento	MDE35	MEC34	**8**
M23	Ter um *software* de HIS – adequado e de boa qualidade	MDE24	MEC23	**7**
M24	Definir regras para transmissão externa de informações para terceiros	MDE30	MEC29	**7**
M25	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação	MDE31	MEC30	**7**

Cód	Mecanismo	Documentos Regulatórios /Normativos	Estudos de Caso	Total
M26	Analisar regularmente a Segurança dos Sistemas de Informação	MDE34	MEC33	**7**
M27	Possuir uma Comissão de Revisão de Prontuários	MDE7	MEC7	**6**
M28	Prevenir para que médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	MDE9	MEC9	**6**
M29	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento		MEC39	**5**
M30	Assinatura de um termo de conduta no momento da contratação, com sanções		MEC42	**5**
M31	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo	MDE29	MEC28	**4**
M32	Dividir as funções dos colaboradores nos sistemas	MDE32	MEC31	**4**
M33	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação	MDE33	MEC32	**4**
M34	Manter as informações dos clientes apenas o tempo necessário por lei	MDE37	MEC35	**4**
M35	Valorizar e até premiar em dinheiro a boa prática de Segurança da Informação		MEC40	**4**
M36	Desconectar o sistema por tempo de inatividade		MEC44	**4**
M37	Utilizar nomes fictícios nas bases de testes e homologações		MEC45	**4**
M38	Acesso do prontuário somente no momento que o paciente esta internado		MEC46	**4**
M39	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED	MDE6	MEC6	**3**
M40	Coletar somente dados relevantes dos clientes/pacientes	MDE16	MEC16	**3**
M41	Dar ciência da leitura dos termos de Segurança da Informação no momento da troca da senha		MEC47	**3**
M42	Evitar posicionar computadores próximos a corredores	MDE18	MEC18	**2**
M43	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa	MDE28	MEC27	**2**
M44	Ter uma área de qualidade para controlar os documentos		MEC37	**2**
M45	Não utilizar celular no local de trabalho, principalmente no beira leito		MEC38	**2**
M46	Ter uma política pública específica para a privacidade da informação no Brasil		MEC41	**2**
M47	Criar uma integração de *login* e senha válido para todos os sistemas		MEC43	**2**
M48	Penalidade com multa em dinheiro	MDE20		**1**
M49	Disponibilizar as políticas de Segurança da Informação aos clientes	MDE36		**1**
M50	Bloquear a utilização de mídias de gravação (*pendrive*) internos assim como acesso a repositórios na internet e e-mail externo		MEC48	**1**

Fonte: Elaborado pelo autor

Dos três mecanismos que tiveram somente uma citação, um deles chama bastante à atenção, pois deveria ter aparecido mais vezes. O mecanismo em questão é o “M50 - Bloquear a utilização de mídias de gravação (*pendrive*) internos, assim como acesso a repositórios na internet e e-mail externos”. O *pendrive* e o e-mail, respectivamente, podem ser, devido a facilidade de seu uso, um caminho para o vazamento de informações. Já os outros dois mecanismos que tiveram apenas uma citação, foram encontrados apenas em Documentos Regulatórios e Normativos e não foram encontrados nos Estudos de Caso, pois de fato, não são práticas realizadas nos hospitais.

O que se percebe na relação dos 50 mecanismos encontrados, é uma grande semelhança entre alguns deles, e também uma granularidade. Mas para esta dissertação, não foram agrupados os mecanismos semelhantes, para não se perder a essência da pesquisa e principalmente cumprimento dos objetivos do trabalho. Por exemplo: os mecanismos, “M1-Identificar e autenticar o usuário em sistemas, arquivos, portais ou webservices”; “M10-Liberar acesso aos dados relevantes somente para pessoas, devidamente autorizadas” e o “M47-Criar uma integração de *login* e senha, válidos para todos os sistemas”, poderiam ser agrupados, pois todos eles tratam de autenticação e autorização.

Esse agrupamento não foi realizado, porque o mecanismo “M1” é uma prática que quase todos os hospitais fazem, pois é simples. O “M10” somente alguns fazem, pois a carga de trabalho aumenta e é necessário ter uma equipe, por isso, os hospitais pequenos não o fazem por completo. Já o “M47” só é criado e utilizado pelos hospitais com grande estrutura, por ser de difícil implantação, exigindo muito planejamento. Com isso os mecanismos ficaram mais genéricos, pois se agrupasse-os, por exemplo, ou todos os hospitais fariam ou quase nenhum utilizaria por ser muito específico.

Mas para melhorar o resultado final da dissertação, primeiramente os mecanismos foram reclassificados, criando um novo código e alterando o nome original, para deixar um nome mais sucinto. No Apêndice F, estão detalhadas as alterações realizadas no nome e no código. Após essa adequação dos códigos e nomes, os mecanismos foram agrupados em Mecanismos de Estrutura (Quadro 23), Mecanismos de Processo (Quadro 24) e Mecanismos de Relacionamento (Quadro 25), conforme conceito apresentado por Wiedenhoft (2013). Segundo Guldentops, Van Grembergen e De Haes (2004) os Mecanismos de Estrutura são responsáveis por criar regras e papéis, os Mecanismos de Processo gerenciam práticas voltadas a estratégia de TI e também tem a função de implementar os sistemas de tomadas de decisões e os Mecanismos de Relacionamento são responsáveis pelo entendimento dos objetivos entre TI e negócios.

Após a classificação pelo tipo de mecanismos, foi realizada uma classificação conforme o seu eixo de ação, ou seja, vulnerabilidade, salvaguarda, detecção, punição e conscientização, (ALBRECHTSEN E HOVDEN, 2009); (LIGINLAL ET AL.,

2009); (BULGURCU ET AL., 2010); (HERATH E RAO, 2009) E (D'ARCY E HOVAV, 2009), marcando com um (X) em qual dos eixos o mecanismo melhor se enquadra.

Os mecanismos finalmente foram classificados de acordo com o requisito de Segurança, considerando: Confidencialidade, Integridade, Disponibilidade, Autenticidade, Confiabilidade, Conformidade e Irrefutabilidade (LUCIANO e KLEIN, 2014), constando nos quadros com uma legenda.

Os resultados foram divididos em três quadros para facilitar a visualização. Dentro do Quadro 23, os mecanismos estão listados por uma ordem sequencial do código. Tanto o código quanto o nome foram readequados conforme consta no Apêndice F.

Quadro 23: Relação final dos Mecanismos de Estrutura para a proteção da privacidade do paciente

Mecanismos de Estrutura (Código/Nome/Quantidade de citações)		*Vulnerabilidade*	*Salvaguarda*	*Detecção*	*Punição*	*Conscientização*	Requisito*
1	Área de qualidade para controlar os documentos -2		X				CONFD
2	Comissão de Revisão de Prontuários - 6		X				CONFM
3	Controle e armazenamento dos prontuários eletrônicos em um sistema especializado em GED - 3	X					DISP
4	Estrutura física adequada para o gerenciamento do SI - 17		X				DISP
5	Implantação e manutenção do Sistema de Gestão da Segurança da Informação - 13		X				CONFD
6	Instalação de Antivírus, VPN e *firewall - 12*		X				CONFD
7	Pessoa responsável pela Política de Segurança da Informação - 10		X				CONFD
8	Proteções internas para a conexão de um novo *hardware* ou *software* na rede - 8		X				CONFD
9	Quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento - 8		X				DISP

*Legenda: CONFD–Confidencialidade; INT–Integridade; DISP–Disponibilidade; AUT-Autenticidade; CONFB – Confiabilidade; CONFM – Conformidade; IRR - Irrefutabilidade
Fonte: Fonte: Elaborado a partir de: Albrechtsen e Hovden (2009); Liginlal et al. (2009); Bulgurcu et al. (2010); Herath e Rao (2009); D'Arcy e Hovav (2009); Guldentops, Van Grembergen e De Haes (2004) e Luciano e Klein (2014)

No Quadro 24, constam os mecanismos de processo e estão listados por uma ordem sequencial do código. Tanto o código quanto o nome foram readequados conforme consta no Apêndice F.

Quadro 24: Relação final dos Mecanismos de Processo para a proteção da privacidade do paciente

Mecanismos de Processo (Código/Nome/Quantidade de citações)		*Vulnerabilidade*	*Salvaguarda*	*Detecção*	*Punição*	*Conscientização*	Requisito*
10	Acesso do prontuário somente no momento da internação - 4		X				CONFD
11	Acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes - 13		X				CONFD
12	Análise dos antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa - 2		X				INT
13	Análise regular da segurança dos Sistemas de Informação - 7		X				CONFD
14	Anulação imediata dos acessos do empregado demitido - 4		X				CONFD
15	Armazenamento de *logs* de acesso e *logs* de alterações realizadas no prontuário do paciente - 9		X				CONFM
16	*Backup* estruturado das informações - 8		X				DISP
17	Bloqueio de utilização de mídias de gravação (*pendrive*), acesso a repositórios na internet e e-mail externo - 1			X			INT
18	Ciência da leitura dos termos de Segurança da Informação -3		X				CONFD
19	Coleta somente dados relevantes dos clientes/pacientes - 3		X				INT
20	Criação de uma integração de *login* e senha válidos para todos os sistemas - 2		X				IRR
21	Criptografia para o tráfego externo de informações - 10		X				AUT
22	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento - 5		X				CONFD
23	Definição de regras para transmissão de dados externos - 7		X				INT
24	Determinação de máscara de senha e tempo máximo de troca de senha e bloqueio por muitas tentativas - 11		X				CONFD
25	Divisão das funções dos colaboradores nos sistemas - 4					X	INT
26	Identificação e autenticação dos usuários - 19	X					CONFB
27	Inativação do sistema por tempo ocioso - 4		X				CONFD
28	Liberação do acesso aos dados relevantes somente para pessoas devidamente autorizadas - 12		X				CONFD
29	Monitoramento constantemente das atividades incomuns de processamento da informação - 7		X				CONFM
30	Não utilização do celular, principalmente no beira leito -2		X				INT
31	Obrigatoriedade de assinatura do termo de conduta na contratação - 5		X				CONFB
32	Penalização com multa -1				X		CONFM
33	Planejamento das atividades, para executar as tarefas com segurança- 8		X				DISP
34	Plano de contingência para desastres com informações - 9		X				DISP
35	Política pública específica para a privacidade da informação no Brasil-2		X				INT
36	Prevenção no posicionamento de computadores próximos a corredores - 3		X				CONFD
37	Sanções adequadas para os que violam as políticas de privacidade-16				X		CONFM
38	*Software* de HIS adequado e de boa qualidade - 7		X				CONFD
39	Treinamento constante para os colaboradores - 16					X	CONFD
40	Utilização de nomes fictícios nas bases de testes e homologações - 4		X				INT
41	Utilização do certificado digital nos prontuários eletrônicos - 10		X				CONFB

*Legenda: CONFD–Confidencialidade; INT–Integridade; DISP–Disponibilidade; AUT-Autenticidade; CONFB – Confiabilidade; CONFM – Conformidade; IRR – Irrefutabilidade

Fonte: Fonte: Elaborado a partir de: Albrechtsen e Hovden (2009); Liginlal et al. (2009); Bulgurcu et al. (2010); Herath e Rao (2009); D'Arcy e Hovav (2009); Guldentops, Van Grembergen e De Haes (2004) e Luciano e Klein (2014)

No Quadro 25, constam os mecanismos de relacionamento e estão listados por uma ordem sequencial do código, identificados conforme consta no Apêndice F.

Quadro 25: Relação final dos Mecanismos de Relacionamento para a proteção da privacidade do paciente

	Mecanismos de Relacionamento (Código/Nome/Quantidade de citações)	*Vulnerabilidade*	*Salvaguarda*	*Detecção*	*Punição*	*Conscientização*	Requisito*
42	Criação e divulgação aos colaboradores da política de privacidade - 13					X	CONFM
43	Disponibilização das políticas de Segurança da Informação aos clientes -1		X				INT
44	Divulgação dos meios de segurança de SI antes da implantação - 4					X	INT
45	Envio de comunicados constantes aos colaboradores, orientando sobre a proteção da informação - 16					X	CONFM
46	Instrução informal de médicos e enfermeiros a não divulgar casos - 9		X				CONFM
47	Intranet para consulta dos documentos de políticas - 9	X					DISP
48	Manutenção das informações dos clientes apenas o tempo necessário por lei - 4		X				DISP
49	Prevenção para que os colaboradores não conversem com pacientes a respeito de diagnósticos em áreas públicas - 6					X	CONFM
50	Valorização e premiação pelo cumprimento da Segurança da Informação - 4		X				CONFD

*Legenda: CONFD–Confidencialidade; INT–Integridade; DISP–Disponibilidade; AUT-Autenticidade; CONFB – Confiabilidade; CONFM – Conformidade; IRR - Irrefutabilidade
Fonte: Fonte: Elaborado a partir de: Albrechtsen e Hovden (2009); Liginlal et al. (2009); Bulgurcu et al. (2010); Herath e Rao (2009); D'Arcy e Hovav (2009); Guldentops, Van Grembergen e De Haes (2004) e Luciano e Klein (2014)

Dos 50 mecanismos encontrados, nove são de estrutura, 32 de processo e nove de relacionamento. Destacando–se com uma quantidade bem elevada em relação aos demais, os Mecanismos de Processo conforme demonstra a Tabela 4.

Tabela 4: Resumo do resultado por tipo de mecanismo

Tipo de mecanismos[4]	Total	Citações	Requisitos[5]						
			CONFD	INT	DISP	AUT	CONFB	CONFM	IRR
Estrutura	9	79	5	0	3	0	0	1	0
Processo	32	217	12	8	3	1	3	4	1
Relacionamento	9	65	1	2	2	0	0	4	0
TOTAL	50	361	18	10	8	1	3	9	1

*Legenda: CONFD–Confidencialidade; INT–Integridade; DISP–Disponibilidade; AUT-Autenticidade; CONFB – Confiabilidade; CONFM – Conformidade; IRR - Irrefutabilidade
Fonte: Elaborado pelo autor

[4] De acordo com a classificação de Guldentops, Van Grembergen e De Haes (2004)
[5] De acordo com Luciano e Klein (2014)

Cada mecanismo foi classificado de acordo com o requisito acerca da Segurança da Informação, destacando-se conforme demonstra a Tabela 4. O número de citações que apresentam as Tabelas 4 e 5 é a quantidade de vezes em que cada mecanismo foi citado considerando os Documentos Regulatórios e Normativos e os Estudos de Caso conforme mostra na Tabela 3 e no Apêndice F, multiplicados pelo número de mecanismos no qual foi classificado, seja ele por tipo de mecanismo, eixo de ação ou requisito da informação. Já nas colunas que apresentam a quantidade dos requisitos da Tabela 4, é a contagem do número de mecanismos que se classificam em cada um dos requisitos.

Para a validade do resultado e principalmente para se evitar a arbitrariedade, foi requisitado o auxilio de dois *experts*, um deles em Segurança da Informação e o outro em Mecanismos, para realizar a classificação de cada um dos mecanismos conforme o seu tipo e também dentro do seu eixo de ação. Essa classificação realizada por cada um dos especialistas foi executada sem que eles tivessem conhecimento da classificação inicial, evitando a influência nas respostas. Após essa análise realizada pelos especialistas, foram discutidas as divergências, chegando-se a uma resposta em comum.

Durante todo o processo de Análise, os resultados obtidos foram codificados de acordo com a etapa, com o objetivo de facilitar as análises sequenciais, reduzir a quantidade de textos nas tabelas, quadros e figuras. Esses códigos têm principalmente o objetivo de manter a rastreabilidade de todo o resultado. Uma tabela foi criada no Apêndice E para facilitar a localização, a compreensão e a rastreabilidade de cada um dos códigos criados durante o processo de Análise dos Resultados.

O que se pode levar em consideração é um número muito elevado da confidencialidade com 217 citações, sendo elas cinco nos Mecanismos de Estrutura, 12 nos Mecanismos de Processos e uma nos Mecanismos de Relacionamento. Esse número elevado de mecanismos associados à Confidencialidade é um fator positivo, pois mostra que os hospitais se preocupam com a proteção da informação.

A confidencialidade que de acordo com a ISO/IEC 27001, é a garantia de que a informação é acessível somente para pessoas autorizadas, ou seja, a proteção contra a divulgação não autorizada da informação, se sobressaiu no resultado final, sendo de extrema importância para a proteção das informações, porém o que é

destacável é a relação desse requisito com o tipo de Mecanismo de Processo, ou seja, a grande maioria das ações relacionadas a privacidade e segurança das informações dos hospitais, são os processos criados para garantir a confidencialidade da informação.

Esse resultado se comprova, pois é exatamente a maior preocupação dos hospitais, ou seja, os processos realizados para garantir a preservação da informação do paciente, como por exemplo é colocado por um entrevistado do hospital Beta, que eles possuem até um política de formação de senha e também leitores biométricos para as áreas mais vulneráveis do hospital, para acessar os sistemas de gestão, pois de acordo com Sêmola (2003), as informações devem ser protegidas de acordo com o seu conteúdo e grau de sigilo.

A Tabela 5 faz um cruzamento do tipo de mecanismo em relação ao eixo de ação de cada um deles, destacando-se o eixo de ação de salvaguarda, sendo classificados 38 mecanismos nesse eixo, ou seja, 76% deles, mostrando que os documentos e as ações realizadas pelos hospitais pesquisados buscam se prevenir quanto a proteção da informação. Além disso, o que se observa é uma preocupação grande com a conscientização em relação aos treinamentos e instruções dos colaboradores, classificados no tipo de Mecanismo de Relacionamento. Esse resultado é de extrema importância, pois demonstra que os hospitais, além de manterem as suas Políticas de Privacidade e se preocuparem com a salvaguarda, trabalham com o ser humano, através dos treinamentos e instruções, no sentido de sempre prevenir e divulgar novos meios de segurança para evitar possíveis problemas relacionados à Segurança da Informação.

Tabela 5: Resumo do resultado por Eixo de Ação x Tipo do mecanismo

Eixo de Ação	Estrutura		Processo		Relacionamento		TOTAL	
	QTD*	CIT**	QTD	CIT	QTD	CIT	QTD	CIT
Vulnerabilidade	1	3	1	19	1	9	3	31
Salvaguarda	8	76	26	160	4	18	38	254
Detecção	0	0	1	1	0	0	1	1
Punição	0	0	2	17	0	0	2	17
Conscientização	0	0	2	20	4	38	6	58
TOTAL	9	79	32	217	9	65	50	361

Legenda: * QTD – Quantidade de mecanismos ; ** CIT – Total de Citações dos mecanismos
Fonte: Elaborado a partir de: Albrechtsen e Hovden (2009); Liginlal et al. (2009); Bulgurcu et al. (2010); Herath e Rao (2009); D'Arcy e Hovav (2009) e Guldentops, Van Grembergen e De Haes (2004)

A Tabela 6 mostra o cruzamento dos mecanismos classificados nos Quadros 23, 24 e 25, considerando os requisitos da informação em relação aos eixos de ação. Com essa Tabela se comprova que os mecanismos encontrados durante a pesquisa, são classificados em sua maioria no requisito de salvaguarda, que é o cuidado com o perigo e a confidencialidade que é exatamente a proteção da informação quanto da divulgação. Massad, Marin e Azevedo Neto (2003) que colocam que o próprio prontuário eletrônico é uma estrutura utilizada para a salvaguarda das informações, do histórico do paciente assim como também informações do seu estado de saúde.

O fato da grande maioria dos mecanismos estarem classificados no eixo de ação de Salvaguarda, deve ser levado em consideração, uma vez que esse fator não pode prejudicar o acesso à informação, principalmente pelo próprio paciente e também prejudicar o andamento do atendimento, devido a burocracias e ao grande número de mecanismos voltados a isso. Esse grande número de mecanismos causa preocupação exatamente neste sentido, de que a proteção é tão grande que acaba atrapalhando o andamento regular dos processos. Por isso, esses dois fatores devem ser dosados, ou seja, o de andamento dos processos e a salvaguarda da informação.

Esse eixo teve um destaque muito grande os resultados, mostrando que as ações dos hospitais não têm uma preocupação muito grande com detecção ou a punição, mas procuram conscientizar os colaboradores e principalmente proteger as suas informações. Porém essa conscientização teve um número muito baixo em relação a salvaguarda, e isso não é um fato bom, pois os hospitais tentam proteger as informações, mas esquecem que o fator humano pode influenciar a Segurança da Informação.

Tabela 6: Requisitos da informação x Eixo de ação

	Vulnerabilidade	Salvaguarda	Detecção	Punição	Conscientização	Total
Confidencialidade		17			1	18
Integridade		7	1		2	10
Disponibilidade	2	6				8
Autenticidade		1				1
Confiabilidade	1	2				3
Conformidade		4		2	3	9
Irrefutabilidade		1				1
TOTAL	3	38	1	2	6	50

Fonte: Elaborado a partir de Luciano e Klein (2014) e Ng, Kankanhalli, Xu (2009)

Após a análise dos mecanismos encontrados e classificados, uma questão que chamou a atenção é a de que, de uma maneira geral o eixo de punição, não teve um destaque, pois apresentou apenas dois mecanismos citados no todo. Mas o que se percebe é que a preocupação maior está nos processos e meios de instrução e treinamento para se evitar o vazamento das informações do prontuário eletrônico do paciente.

A punição por si só, pode não ter resultados efetivos, e pode no futuro trazer algum tipo de vingança por parte do infrator. Segundo Herath e Rao (2009) a severidade da punição pelo não cumprimento das normas de Segurança da Informação, são fatores relevantes sobre as intenções de comportamento na área de Segurança da Informação, porém para mesmos autores a existência e a visibilidade de outros mecanismos podem ser mais importantes que a severidade da sanção imposta. Com isso acredita-se que o mais correto é disponibilizar treinamentos e melhorias de processos, como já vem sendo feito pelos hospitais.

Essas ações que são realizadas, principalmente no sentido de salvaguarda, é exatamente evitar o vazamento de informações, pois o impacto é bastante grande, seja para o hospital, seja para os pacientes ou familiares e até mesmo para o convívio social.

5 CONSIDERAÇÕES FINAIS

Ao finalizar o trabalho, destaca-se o cumprimento do objetivo principal, que era o de identificar os mecanismos para preservar a privacidade das informações do paciente no prontuário eletrônico. Esses mecanismos foram encontrados, totalizando 50 que foram identificados nas diferentes abordagens metodológicas e técnicas de coleta de dados. Imagina-se, em virtude das diferentes fontes de dados que estes mecanismos possam ser aplicados em diferentes hospitais, porém, é necessário ressaltar que não necessariamente todos os mecanismos se apliquem a todos os contextos. Um exemplo disso é um mecanismo citado por alguns entrevistados do Hospital Beta quando perguntados se eles se sentiam valorizados pelo hospital pelo cumprimento das regras presentes na política de segurança. E a resposta de dois deles foi:

> Sim, inclusive com premiação (EB2).
>
> [...] a gente recebe um bônus vamos dizer assim, se a gente cumprir. Um pré-requisito, para receber esse bônus é ter feito algum desses treinamentos e alguns deles são obrigatórios [...] (EB1).

O primeiro objetivo específico, que era o de Identificar os documentos regulatórios e normativos que poderiam conter mecanismos de privacidade das informações foi atendido por meio da localização de 20 documentos com diversos mecanismos relacionados à Segurança da Informação, tendo como destaque a ISO/TC 215, a HIPAA, a NBR ISO/IEC 27002, o Manual de Acreditação da JCI, a PIPEDA e o Manual de Acreditação da ONA .

O segundo objetivo específico foi cumprido quando identificados nos hospitais durante todo o processo de coleta de dados nos Estudos de Caso, e pelo resultado das análises, as práticas realizadas para a prevenção da informação, pois verificou-se que o fato que mais ocorre e mais se objetiva, são as ações fragmentadas de treinamento formais, avisos e instruções, tanto em murais como em sistemas de gestão, para mostrar, instruir e conscientizar o colaborador a proteger as informações dos pacientes. O mecanismo “39 - Treinamento constante para os colaboradores” foi o terceiro mais citado, com 16 aparições e o mecanismo ”45 - Envio de comunicados constantes aos colaboradores”, orientando sobre a proteção da informação, o quinto que mais apareceu, com 14 citações.

O resultado do estudo considera que é importante ter um grande documento para validar as ações como mostra o mecanismo “42 - Criação e divulgação aos colaboradores da política de privacidade”, que é citado 14 vezes sendo o sexto maior e também considera importante a penalização de acordo como mecanismo “37- Sanções adequadas para os que violam as políticas de privacidade”. Porém na prática ocorrem ações fragmentadas por assuntos e por setores, para que o colaborador assimile melhor e tenha um resultado mais efetivo.

O fato que ficou muito claro durante o processo de coleta de dados dos Estudos de Caso é a grande influência que a acreditação tem em relação à privacidade da informação. A grande aplicação dos mecanismos ocorre principalmente a esse fato, isso porque a acreditação naturalmente obriga o hospital a documentar e a ter vários processos que criam mecanismos naturais de proteção. Ou seja, a acreditação da ONA e principalmente da *Joint Comission,* ou outra acreditação internacional, melhora consideravelmente a proteção das informações dos Pacientes. Isso se consolida com outro resultado, que foi a análise realizada na etapa da Pesquisa de Análise de Documentos Regulatórios e Normativos, na qual foram detectados 15 mecanismos, sendo o terceiro com maior número de mecanismos encontrados.

O terceiro objetivo específico foi atendido através da classificação dos mecanismos. Foi possível chegar a algumas conclusões, como por exemplo a associação da salvaguarda em relação aos processos de trabalho. Outra conclusão que se chega é que os Mecanismos de Estrutura e processos estão muito ligados ao eixo de ação de salvaguarda. E os Mecanismos de Relacionamento estão ligados à Conscientização.

Observa-se que dos 50 mecanismos identificados, 18 deles, isto é, 76% dos mecanismos estão associados à Confidencialidade, e desse total, 12 deles, foram classificados como Mecanismos de Processos. Ou seja, os mecanismos mais citados são os de processo em relação à salvaguarda e os mecanismos de relacionamento em relação a conscientização dos colaboradores.

Com isso, conclui-se que, apesar de ser possível a aplicação de todos os mecanismos em hospitais, provavelmente os hospitais pequenos terão muitas dificuldades em alguns mecanismos, pois requer um recurso financeiro, assim como uma boa estrutura física e pessoal. O que mais se destacou no resultado, foram os

mecanismos de processo, inclusive bem mais que os de estrutura, e isso mostra que os grandes hospitais têm a preocupação com processos internos seguros no manuseio do prontuário eletrônico, o que pode não acontecer com hospitais pequenos, devido a falta de estrutura necessária.

Os hospitais públicos brasileiros, que normalmente são hospitais que recebem um grande número de pacientes, como é o Hospital Gama, onde foi realizado um dos Estudos de Caso, atendem exclusivamente através do SUS. Para esse atendimento é utilizado o cartão SUS, que foi criado para agilizar e melhorar o processo, pois através dele o hospital pode verificar os registros dos pacientes, uma vez que os seus dados ficarão disponíveis no sistema informatizado, possibilitando que os profissionais de saúde busquem o histórico clinico do paciente. Porém, a utilização aumenta o risco de vazamento de informação, pois como atendimento ocorre a nível nacional, devem-se avaliar quais pessoas podem acessar a informação, como controlar esse acesso através de uma auditoria, como é o intercambio de dados, ou seja, uma maneira de garantir a integridade e a confidencialidade no tratamento dessas informações, através de mecanismos.

Uma crítica que convêm, é exatamente a de não ter uma legislação para se utilizarem de base obrigatória e regulamentar todos os hospitais do Brasil no âmbito da segurança da informação. O que se percebe com isso é que as acreditações procuram realizar esse papel, na tentativa de prevenir e assegurar a privacidade da informação dos pacientes. Alguns outros documentos regulatórios e normativos analisados, também buscam esse papel, porém, se concluiu que, poucos documentos possuem muitos mecanismos, mas, sempre um mecanismo citado em algum documento pode não estar no outro, e por isso esses documentos acabam se completando. Não existindo assim um documento completo que possa atender um hospital como um todo.

Mesmo com os vários mecanismos citados nos documentos regulatórios, constatou-se que com os Estudos de Casos, esses mecanismos foram reforçados e novos foram agregados sendo identificados no cotidiano e nas boas práticas escritas e que de fato ocorrem nos hospitais.

Um fator identificado na análise e que chama atenção negativamente é a grande quantidade de mecanismos concentrados no mesmo eixo de ação, no mesmo requisito e no mesmo tipo. Isso mostra que os hospitais estão se

preocupando apenas com algumas características, sendo elas principalmente de processos e deixado de lado outras, pois não se percebeu uma preocupação tão grande com a questão comportamental do individuo, por exemplo.

Mas o fator positivo é que de fato órgãos governamentais e não governamentais, conselhos de classe e principalmente as instituições de saúde têm buscado melhorar constantemente, mesmo que em passos lentos, principalmente no sentido de leis, a privacidade das informações dos pacientes no prontuário eletrônico, através da utilização de diversos mecanismos, que foram identificados nessa dissertação.

Uma das contribuições que o resultado da dissertação pode trazer às organizações de uma maneira geral é a identificação dos documentos Regulatórios e Normativos, com a quantidade de mecanismos encontrados em cada um deles, sendo possível filtrar de acordo com o objetivo. Principalmente se o documento ou norma se aplicam à organização para servir de base ou consulta de boas práticas de segurança e privacidade das informações em relação aos seus dados e aos dados dos seus clientes, bem como os documentos que trazem as penalidades pelo descumprimento da privacidade da informação.

Outra contribuição que a dissertação pode fornecer às organizações é a possibilidade da utilização da grande maioria dos mecanismos, adotando-os para se ter uma informação mais segura, inclusive na utilização da internet para a transmissão de dados.

A maior contribuição da dissertação é exatamente para os hospitais, independente do seu tamanho. A primeira contribuição é mostrar em quais documentos Regulatórios e Normativos os hospitais podem se basear, para ter um comportamento mais seguro em relação à Privacidade da Informação. A segunda contribuição é mostrar a relação de mecanismos descobertos no decorrer de todas as abordagens metodológicas e técnicas de coleta de dados, que podem auxiliar os gestores e os responsáveis pela Segurança da Informação dos hospitais à proteger os seus dados e principalmente proteger as informações dos pacientes no prontuário eletrônico. Deve-se levar em consideração que nem todos os mecanismos se aplicam a todos os hospitais, porém a adoção ou o cumprimento deles ajuda a tornar o hospital mais seguro.

Outra contribuição possível para os hospitais é verificar através da classificação dos mecanismos proposta por este trabalho, se as ações que estão realizando, ou seja, se os mecanismos que possuem não estão concentrados em uma única área, deixando outras de lado, por exemplo, se o hospital possui somente mecanismos relacionados à estrutura, deixando vulneráveis os processos e os relacionamentos. Ou possui muitos mecanismos punitivos e poucos voltados a conscientização dos colaboradores.

A contribuição da dissertação para a área acadêmica, foi a trazer a relação dos Documentos Regulatórios e Normativos que possam ser utilizados em outras pesquisas, e principalmente um conceito que é pouco explorado em pesquisas acadêmicas, que é o comitê da ISO/TC 215, e o grupo de trabalho responsável por desenvolver normas para a área da saúde, com muitos documentos publicados.

Outra contribuição acadêmica é o esclarecimento dos tipos de mecanismos e Documentos Regulatórios e Normativos que os contêm, possibilitando assim consultas para ter base para outras pesquisas.

Os principais limites da pesquisa, além daquelas que são inerentes as características de cada um dos métodos escolhidos, é o fato das entrevistas realizadas nos Estudos de Caso, ocorrerem somente com Pessoal de TI, embora não fosse o objetivo, foi o que acabou tendo acesso e se considerou que isso não afetaria os objetivos do estudo. Mesmo não tendo pessoas do corpo clínico, a pesquisa não perde a sua validade ou importância, uma vez que o trabalho não busca o seu resultado por percepção, mas por fatos que ocorrem no cotidiano do hospital. Outro fator que torna a pesquisa limitada é o Estudo realizado apenas em dois hospitais reduzindo assim o número de documentos internos e também as entrevistas.

Essa limitação dos Estudos de Caso se deu inclusive pelo custo que também teve uma consequência nas análises dos Documentos Regulatórios e Normativos, pois poderiam ser mais bem explorados, porém o valor de aquisição dos materiais limitou o estudo.

Essa pesquisa contribuiu no sentido de encontrar mecanismos de Segurança da Informação através de diferentes abordagens e fontes de dados. Com esse

resultado, ou utilizando-se dos mesmos princípios desse trabalho, propõem-se as seguintes pesquisas futuras:

a) Aprofundar o estudo, realizando uma comparação entre as práticas de prevenção da privacidade dos Hospitais dos Estados Unidos e do Brasil;

b) Identificar os fatores críticos de sucesso em cada mecanismo encontrado nesse trabalho;

c) Fazer uma pesquisa com novos hospitais. Para validar e classificar os mecanismos fazer um Grupo de Foco para identificar os mecanismos mais relevantes;

d) Realizar uma revisão com um grupo maior de especialistas dos mecanismos encontrados para qualificá-los e agrupar;

e) Analisar detalhadamente os documentos do comitê da ISO/TC 215, explorando formas de viabilizar a sua aquisição.

As contribuições e as sugestões de pesquisas futuras descritas neste trabalho, têm a intenção de contribuir no cotidiano e também nas pesquisas em relação à Privacidade da Informação, principalmente no ambiente hospitalar, pois se constatou que os hospitais possuem alguns mecanismos, mas isso ainda não é o suficiente, uma vez que existem ocorrências de incidentes com a informação e a privacidade do paciente.

REFERÊNCIAS

ABRAHÃO, M. S. A Segurança da Informação Digital na Saúde. Sociedade Beneficente Israelita Brasileira, 2003. Disponível em: <http://www.einstein.br/biblioteca/artigos/131%20132.pdf>. Acesso em: 30 Jun. 2014.

ABU-DALBOUH, H. A Proposed mHealth Model for Improving the Quality Care in Hospitals. **Research Journal of Applied Sciences, Engineering and Technology** 7(7): 1215-1219, 2014.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual decision making. IEEE Security & Privacy. IEEE Computer Society. v.3, n.1, p. 26-33, jan/fev 2005. Disponível em: < http://www.sims.berkeley.edu/~jensg/research/paper/Acquisti_Grossklags05.pdf>. Acesso em: 10 Maio 2014.

ALBRECHTSEN, E.; HOVDEN, J. The information security digital divide between information security managers and users. **Computers & Security**, v. 28, n. 6, p. 476-490, 2009.

ALDERMAN E., KENNEDY C.. **The Right to Privacy**. New York: Knopf ; 1995.

ALONSO, L. B. N.; DROVAL, C.; FERNEDA, E.; EMÍDIO, L.. Acreditação Hospitalar e a Gestão da Qualidade dos Processos Assistenciais. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n. 2, p. 34-49, jul./dez. 2014.

ALVES, E., SALVADOR, V. F. M – Vantagens e Desvantagens do Prontuário Eletrônico do Paciente. **Anais da VIII Jornada Científica**, Centro Universitário São Camilo, São Paulo, outubro de 2004.

ANDERSON, R., MOORE T.. The Economics of Information Security. Science 314 (5799), pp.610–613, October 27, 2006. Disponível em: <http://dx.doi.org/10.1126/science.1130992>. Acesso em: 20 Jun. 2014.

ANDERSON, J. M. Why we need a new definition of information security. **Computers & Security**, v. 22, n. 4, p. 308–313, May 2003.

ANS - AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. PADRÃO TISS. Segurança & privacidade novembro, 2013.

___ AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR. Disponível em: <http://www.ans.gov.br/>. Acesso em: 27 Jun. 2014.

APPARI. A.; JOHNSON, M. E. Information Security and Privacy in Healthcare: Current State of Research. Center for Digital Strategies Tuck School of Business. Dartmouth College, Hanover NH. August 2008

ARCE, I. The weakest link revisited. **IEEE Security & Privacy**, v. 1, n. 2, p. 72–76, Mar./Apr. 2003.

Aspectos Éticos e Prontuários Médicos. Disponível em: <http://www.virtual.epm.br/material/tis/currmed/temas/med5/med5t31999/etica/aspectos.htm>. Acesso em: 27 Jun. 2014.

BARDIN, L. Análise de conteúdo. Lisboa: Edições 70, 1977

BASTOS, C. R., Curso de direito constitucional. São Paulo: Saraiva, 1998.

BAUMER, D.; EARP, J.; PAYTON, F. **Privacy of Medical Records: IT implications of HIPAA**, New York: ACM Press, 2000.

BIBLIOMED Há um futuro promissor na história clínica eletrônica. Disponível em: <http://corporativo.bibliomed.com.br/lib/ShowDoc.cfm? LibDocID=177&ReturnCatID=9>. Acesso em: 27 Jun. 2014.

BOSS, S. R.; KIRSCH, L. J.; ANGERMEIER I.; Shingler R. A.; WAYNE R.. If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. **European Journal of Information Systems** (2009) 18,151–164

BRAGANÇA, C. E. B. A. Privacidade em informações de saúde: uma análise do comportamento percebido por profissionais de saúde de Instituições Hospitalares do Rio Grande do Sul. 30/08/2010. 124 f. Dissertação (Mestrado em Administração) - Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul, 2010.

BRAGANÇA, C. E. B. A; LUCIANO, E. M.; TESTA, M. G.. Segurança da Informação e privacidade de informações de pacientes de instituições de saúde: uma análise exploratória da privacidade percebida pelos profissionais. **EnANPAD**. Rio de Janeiro – 25 a 29 de setembro de 2010.

BRASIL, Decreto-Lei No 2.848, de 7 de Dezembro de 1940. Código Penal Presidência da República.

_____. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF, Senado, 1998.

_____, Decreto-Lei No 8.078, de 11 de Setembro de 1990. Código de Defesa do Consumidor. Presidência da República

_____, Lei No 10.406, de 10 de Janeiro de 2002. Institui o Código Civil. Presidência da República.

_____, Lei Nº 12.527, de 18 de novembro de 2011. Lei de Acesso à informação Regula o acesso a informações. Presidência da República. Congresso Nacional.

_____, Lei Nº 12.965, DE 23 Abril DE 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos.

_____, Política Nacional de Informação e Informática em Saúde (PNIIS). Ministério da Saúde, 2013.

BRETERNITZ, V. J.; SILVA, L. A.. *Big Data*: um novo conceito gerando oportunidades e desafios. **Revista RETC** – Edição 13ª, outubro de 2013, página 106.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I.. Information Security Policy: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly** Vol. 34 No. 3 pp. 523-548/Sepember 2010.

CAMPARA, M.; ALKIMIN, R. A.; MESQUITA, J. M. C; MUYLDER, C. F.; DIAS, A. T.; LA FALCE, J. Implantação do Prontuário Eletrônico de Paciente**, Revista de Administração Hospitala**r, v.10, n.3, pp. 61-74, setembro/dezembro, 2013.

CAMPOS, L. I. **Impacto da implantação do sistema de gestão da qualidade em hospitais acreditados com excelência pelo Sistema Brasileiro de Acreditação ONA.** Belo Horizonte: UFMG. 133 p. Dissertação (Mestrado em Ciências da Saúde - Infectologia e Medicina Tropical), Faculdade de Medicina, Universidade Federal de Minas Gerais, 2008.

CHAGAS, A. T. R. O Questionário na Pesquisa Científica. **Administração On Line. Prática - Pesquisa – Ensino**. Vol. 1 - Nº 1. Jan/Fev/Mar – 2000.

Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. **MIS Quaterly**, v. 34, n. 3, p. 523-548, 2010.

CONSELHO FEDERAL DE ENFERMAGEM. Código de Ética dos Profissionais de Enfermagem. Rio de Janeiro, 08 de fevereiro de 2007.

CONSELHO FEDERAL DE MEDICINA. Código de Ética Médica. Diário Oficial da União; Poder Executivo, Brasília, DF, de 26 jan. 1988. Seção 1, p. 1574-7.

CONSELHO FEDERAL DE MEDICINA. RESOLUÇÃO CFM Nº 1.821, DE 11 DE JULHO DE 2007. Diário Oficial da União; Poder Executivo, Brasília, DF, 23 nov. 2007. Seção I, p. 252

COSTA, C. G. A. Desenvolvimento e Avaliação Tecnológica de um Sistema de Prontuário Eletrônico do Paciente, Baseado nos Paradigmas da World Wide Web e da Engenhar ia de *Software*. Dissertação de Mestrado. Universidade Estadual de Campinas, 2001.

COSTA, C. G. A. Prontuário Eletrônico do Paciente: Legislação, Auditoria e Conectividade, - **8º Congresso Latino Americano de Serviços de Saúde**, 2003.

CURRAN, M.; CURRAN, K.. The ethics of informa-tion. **J Nur Administration** 1991;21(1):47-9.

D'ARCY, J.; HOVAV, A. Does one size fit all? Examining the differential effects of IS security countermeasures. **Journal of Business Ethics**, v. 89, p. 59-71, 2009.

DA VEIGA, A.; ELOFF, J. H. P. A framework and assessment instrument for information security culture. **Computers & Security**, v. 29, n. 2, p. 196-207, 2010.

DEGIRMENCI, K.; GUHR, N.; BREITNER, M. H..Mobile Applications And Access To Personal Information: A Discussion Of Users' Privacy Concerns. **Thirty Fourth International Conference on Information Systems**, Milan 2013.

DOURISH P., ANDERSON K.. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. **Human Computer Interaction**, 2006, Volume 21, pp. 319342

EMÍDIO, L.F.; ALONSO, L.B.N.; FERNEDA, E.; HEDLER, H.C.. Acreditação Hospitalar: Estudos de Caso no Brasil. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 3, n. 1, p. 98-113, jan./jun. 2013.

FABRI, M. Desafios para a Preservação da Privacidade no Contexto da Saúde. **Rev. Temas em Debate**, Rio de Janeiro, v.1, n.1, p.306-322, 2003.

FADEN R.R., BEAUCHAMP T.L.A history and theory of informed consent. New York: Oxford Univ, 1986.

FERNANDES, D. A.; ABREU, A. F. **Tecnologia da Informação aplicada a Sistemas de Informação empresariais** – O papel estratégico da Informação e dos Sistemas de Informação nas empresas, 3ª. ed., São Paulo: Atlas, 2003

FERREIRA, F. N. F.; ARAÚJO, M.T.. **"Políticas de Segurança da Informação - Guia prático para elaboração e implementação"**. Rio de Janeiro: Ciência Moderna, 2008.

FINNE, T. A Conceptual framework for information security management. **Computers & Security**, v. 16, n. 6, p. 303-307, 1998.

FLICK, Uwe. **Uma introdução à Pesquisa Qualitativa**, traduzido por Sandra Netz, Bookman, 2004

FONTES, E. **Segurança da Informação: o usuário faz a diferença**. Rio de Janeiro: Editora Saraiva, 2006.

FRANCISCONI, C. F., GOLDIM, J.R. Aspectos bioéticos da confidencialidade e privacidade. In: Costa SIF, Oselka G, Garrafa V, organizadores. Iniciação à Bioética. Brasília: Conselho Federal de Medicina, 1998: 269-84

FTC. 2009. "Beyond Voice: Mapping the Mobile Marketplace." Disponível em: <www.ftc.gov/opa/2009/04/mobilerpt.shtm > Acesso em: 29 Jun. 2014.

FURNELL, S; RAJENDRAN, A. Understanding the influences on information security behaviour. **Computer Fraud & Security**, v. 2012, n. 3, p. 12-15, 2012.

GAERTNER, A.; SILVA, H. P. Privacidade da Informação na Internet: Ausência de Normalização, Proceedings. **CINFORM - Encontro Nacional de Ciência da Informação VI**, Bahia, 2005

GIBBS, Graham. **Análise de dados qualitativos**. Porto Alegre: Artmed, 2009.

GIL, A. C. **Métodos e técnicas de pesquisa social.** São Paulo: Atlas, 1999.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GODOY A. S.. PESQUISA QUALITATIVA: TIPOS FUNDAMENTAIS. **RAE** • v. 35 • n. 3 • Mai./Jun. 1995, São Paulo, Brasil.

GOLDIM,J. R.; FRANCISCONI, X. **Bioética Clínica.** 2005**.** Disponível em: < http://www.pucrs.br/bioetica/cont/carlos/bioeticaclinica.pdf> Acesso em: 25 Jun. 2014.

GULDENTOPS, E., VAN-GREMBERGEN, W. e DE HAES, S. Control and governance maturity survey: establishing a reference benchmark and a self-assessment tool. **Information Systems Control Journal**, v6, p.32-35. 2004

GOLDSTEIN, M. M. Health Information Technology and the Idea of Informed. IN: **Journal of Law, Medicine & Ethics**. The effects of health information technology on the physician-patient relationship, pp. 27 – 35, spring 2010.

HAICAL, C. Controle de acesso físico. Disponível em: <http:\\www.modulo.com.br> Acesso em: 15 Ago. 2014.

HAMELINK, C. J.. The ethics of cyberspace. London: Sage Publications Ltd. 2000.

HERATH, Tejaswini; RAO, H. Raghav. Protection motivation and deterrence: a framework for security policy compliance in organizations**. European Journal of Information Systems**, v. 18, n. 2, p. 106-125, 2009.

HENDERSON S.C., SNYDER C.A., Personal information privacy: implications for MIS managers, **Information & Management**. 36(4), 1999, pp. 213–220.

HIPAA - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 - U.S. Department of Health & Human Services, AUG. 21, 1996.

IBGE, Assistência Médica Sanitária 2009. Rio de Janeiro: IBGE, 2010.

ICP Brasil – Medida Provisória Nº 2.200 de 28 de junho de 2001.

IMIA - Código de Ética da IMIA para Profissionais de Informática em Saúde. Disponível em< http://www.imia-medinfo.org/new2/>. Acesso em: 10 Dez. 2014.

IOM - INSTITUTE OF MEDICINE. The computer-based patient record: an essential technology for health care, revised edition, Division of Health Care Services, Institute of Medicine, National Academy of Science, Washington, D.C., USA, 1997

ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems – Requirements, 2013

ISO/IEC 27002, Information technology -- Security techniques -- Code of practice for information security controls, 2013

ISO/TC 215 - Health informatics – Disponível em: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=54960

ITGI. Cobit 4.1: Control Objectives Management Guidelines Maturity Models. Rolling Meadows/EUA: IT Governance Institute, 2007.

ITI - Instituto Nacional de Tecnologia da Informação. Disponível em < www.iti.gov.br>. Acesso em: 27 Jun. 2014.

JCI - *Joint Commission International Accreditation – Standards for Hospital* – Disponível em: http://www.jointcommissioninternational.org/: Acesso em: 10 dez. 2014

JUNIOR, A.E.A.; SANTOS, E.M.. A percepção da importância de Controles de Segurança da Informação em hospitais públicos brasileiros**. RECIIS – R. Eletr. de Com. Inf. Inov. Saúde.** Rio de Janeiro, v.7, n.2, Jun., 2013. Disponível em: http://www.reciis.icict.fiocruz.br/index.php/reciis/article/viewArticle/688/1565. Acesso em 10 jan 2015.

KALORAMA Information (a division of MarketResearch.com). Wireless Opportunities in Healthcare. 2007

KAMEDA, K.; PAZELLO M. E-Saúde e desafios à proteção da privacidade no Brasil. Instituo Nupef, Outubro 2013. Disponível em http://www.nupef.org.br/. Acesso em 15 dez 2014.

KLEIN, R. H.. Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à Segurança da Informação. 24/03/214. 100 f. Dissertação (Mestrado em Administração) - Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul, 2014.

KOBAYASHI, L. O. M.; FURUIE, S.S. **Segurança em Imagens Médicas: Uma Revisão**. São Paulo: USP, 2006.

KRAEMER, S.; CARAYON, P.. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. **Applied Ergonomics** 38 (2007) 143–154. 2005.

LEIKO-LILLPI H. et al. Privacy: a review of the titerature. **Intern Jour of Nursing Studies.** 2001;38(6):663-671.

LEINO-KILPI H., et.al. Privacy: a review of the literature. **International Journal of Nursing Studies** 38 (2001) 663–671.

LEMOS, Aline Morais. Política de Segurança da Informação, Universidade Estácio de Sá, Rio de Janeiro, 2001.

LI, Y.. Theories in online information privacy research: A critical review and an integrated framework. **Decision Support Systems** 54 (2012) 471–481

LIGINLAL, D.; SIM, I.; KHANSA, L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. **Computers & Security**.v.28, p.215-228, 2009.

LOCH, J.A.. Confidencialidade: natureza, características e limitações no contexto da relação clínica. 2003. PUCRS. Disponível em: http://www.pucrs.br/bioetica/cont/jussara/confidencialidad.pdf: Acesso em: 10 de mar 2015

LOHR, S. The Age of Big Data. In: The New York Times, New York, 11 fev. 2012. Sunday Review. Disponível em: < http :// www . nytimes . com /2012/02/12/ sunday - review / big - datas - impact - in - the - world . html ?_ r =2& ref = technology > . Acesso em: 28 Jun. 2014.

LOUREIRO, S.C. Segurança da Informação: Preservação das Informações Estratégicas com Foco em sua Segurança. 12/2008.66 p. Monografia de Conclusão de Curso (Especialização) Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.

LUCIANO, E. M.; BRAGANÇA, C. E. B. de A.; TESTA, M. G. Privacidade de informações de pacientes de instituições de saúde: a percepção de profissionais da área de saúde. **Reuna** (Belo Horizonte), v. 16, p. 89-102, 2011.

LUCIANO, E. M.; MAÇADA, A. C. G.; MAHMOOD, M. A.. " The influence of human factors on vulnerability to information security breaches" (2010**). AMCIS 2010 Proceedings. Paper** 351.

LUCIANO, E. M.; KLEIN, R. H. – In. PRADO, E.P.V.; SOUZA C.A. (Orgs) Fundamentos de Sistemas de Informação, 1 ed. Rio de Janeiro: Elsevier, 2014, cap. 6, p. 93-110.

MAANEN, J. V.. Reclaiming qualitative methods for organizational research: a preface, **In Administrative Science Quarterly**, vol. 24, no. 4, December 1979 a, pp 520-526.

MALHOTRA, N.K. **Pesquisa de marketing: uma orientação aplicada**. 3.ed. Porto Alegre: Bookman, 2001.

MANNING, P. K., Metaphors of the field: varieties of organizational discourse, **In Administrative Science Quarterly**, vol. 24, no. 4, December 1979, pp. 660-671.

MANZINI, E. J. A entrevista na pesquisa social. Didática, São Paulo, v. 26/27, p. 149-158, 1990.

MARCIANO, J.L.P.. Segurança da Informação - uma abordagem social – Brasília, 2006.

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MARINHO, Z. P. Security Officer: quem é esse profissional e quais suas funções? Disponível em <http:\\www.modulo.com.br> Acesso em: 08 Ago. 2014.

MARQUES , E. P. et al. Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES). SBIS. 22/10/2013. 91p.

MASSAD, E., MARIN, H.F., AZEVEDO, R. S. O Prontuário do Paciente na Assistência, Informação e Conhecimento Médico. São Paulo. USP, 2003.

MASON, R. O. Four ethical issues of the information age.**MIS Quart**.10(1) 4–12. 1986

MATTAR, F. N. **Pesquisa de marketing: metodologia e planejamento**. 5. ed. São Paulo: Atlas, 1999.

MENDES, S. F. et al.. Uma análise da implantação do padrão de troca de informação em saúde suplementar no Brasil. **J. Health Inform**. 2009 Out-Dez; 1(2): 61-7

MERCURI, R.T. The HIPAA - potamus in Health Care Data Security. **Communications of the ACM,** vol.47, no.7.pp. 25-28, 2004.

MINAYO, M. C. S. (org). **Pesquisa social: teoria, método e criatividade**. Petrópolis/RJ: Vozes, 2001.

MITNICK, K. D.; SIMON, W.. L. **A arte de Enganar**. São Paulo. Person Education do Brasil Ltda, 2003.

MITTAL, N.; NAULT, B. R. Investments in Information Technology: Indirect Effects and Information Technology Intensity. **Information Systems Research**. V. 20, Issue 1, P.:140-154: Mar, 2009.

MOREIRA, N. S. S**egurança Mínima: Uma visão corporativa da Segurança da Informação**, Rio de Janeiro: Axcel Books, 2001.

MOTTA, G. H. M. B. Um Modelo de Autorização Contextual para o Controle de Acesso ao Prontuário Eletrônico do Paciente em Ambientes Abertos e Distribuídos.05/02/2004. 213 f. Tese (Escola Politécnica). USP, 2003.

NG, B.; KANKANHALLI, A.; XU, Y. Studying users' computer security behavior: A health belief perspective. **Decision Support Systems**, v. 46, n. 4, p. 815, 2009.

NOVAES, M.A.; BELIAN, R.B.. Pontos estratégicos para especificação de um prontuário eletrônico do paciente como instrumento de cooperação clínica na web: Sociedade Brasileira de Informática em Saúde. **Anais do IX Congresso Brasileiro de Informática em Saúde**; 2004 nov 7-10; Ribeirão Preto, SP. Brasil; 2004.[4 p.].

NRC National Research Council. For the Record: Protecting Electronic Health Information. 1997.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. Disponível em: <http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp>. Acesso em: 30 Jun. 2014.

OLIVEIRA, J. F. Gestão de Tecnologias da Informação e da Comunicação na Saúde: uma análise sobre o uso do prontuário eletrônico. **Interface** – Natal/RN – v.9 – n.1 – jan/jun 2012

ONA – ORGANIZAÇÃO NACIONAL DE ACREDITAÇÃO. Manual das Organizações Prestadoras de Serviço de Saúde, Brasília, 2014.

PATRÍCIO, C. M. *et al*. O prontuário eletrônico do paciente no sistema de saúde brasileiro: uma realidade para os médicos? ***Scientia Medica****,* Porto Alegre, v. 21, n. 3, p. 121-131, 2011. Disponível em: <http://revistaseletronicas .pucrs.br/ojs/index.php/scientiamedica/article/viewFile/8723/6722>. Acesso em: 23 dez. 2014.

PELISSARI, F. A. B. Segurança de redes e análise sobre a conscientização das empresas da cidade de Bauru (SP) quanto ao problema. Tese (Especialização) – Faculdade de Ciências – UNESP, Bauru, 2002.

PERONDI, M.B.M.; SAKAN, T.M.S.; SCHVARTSMAN, C.. The use of an electronic medical system in a pediatric emergency department with a clinical score triage system. Einstein. 2008.

PETRISON, L. A.; WANG, P. Exploring the dimensions of consumer privacy: An analysis of coverage in british and american media. **Journal of Direct Marketing**, 9(4), 19-37. 1995.

PIPEDA - The *Personal Information Protection and Electronic Documents Act* . OFFICE OF THE PRIVACY COMMISSIONER OF CANADA. Disponivel em https://www.priv.gc.ca/leg_c/r_o_p_e.asp. Acesso em: 15 dez. 2014.

Privacy Legislation in Canada – Disponível em: <http://www.privcom.gc.ca/fs-fi/02_05_d_15_e.asp> Acesso em: 28 Jun. 2014.

PUPULIM, J. S. L.; SAWADA, N. O. O cuidado de enfermagem e a invasão de privacidade do doente: uma questão ético-moral. **Revista Latino-americana de Enfermagem**. V. 10, 3, p. 483-488, 2002.

RAMAN, A. Enforcing Privacy through Security in Remote Patient Monitoring Ecosystems, **6th International Special Topic Conference on Information Technology Applications in Biomedicine**. 2007

RFC 2828. Request for comments: internet security glossary. Disponível em:<http:\\www.faqs.org/rfcs/rfc2828.html> Acesso em: 08 Ago. 2014.

ROSE, E. A. An examination of the concern for information privacy in the New Zealand regulatory context. **Information & Management**, v. 43, 3, p. 322-335, 2006.

SALVADOR, V.F.M.; ALMEIDA, F.V.. Aspectos éticos e de segurança do prontuário eletrônico do paciente. In: **Anais da II Jornada do Conhecimento e da Tecnologia.** Marília SP. Brasil. 2005. Disponível em: http://www.uel.br/projetos/oicr/pages/ arquivos/Valeria_Farinazzo_aspecto_etico.pdf. Acesso em 05 de dez 2014.

SAMPIERI, Roberto H.; COLLADO, Carlos F.; LUCIO, Pilar B. **Metodologia de Pesquisa**. 3. Ed, São Paulo: McGraw Hill, 2006.

SÊMOLA, M. **Gestão de Segurança da Informação – uma visão executiva**. 8ª. Ed, Rio de Janeiro: Elsevier, 2003.

SILVA, D. R. P.; STEIN L.M. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição 2007**; Vol 10: 46-53. Disponível em: <http://www.cienciasecognicao.org.br>. Acesso em: 06 Set. 2014.

SIMIONATO, A. C.; SANT'ANA, R. C. G.; SANTOS, P. L. V. A. C.. Privacidade e os Simulacros Digitais Gerados Pelos Dados Pessoais. **Encontro Internacional Dados, Tecnologia e Informação**, 2013, Marília. São Paulo.

SIPONEN, M. A conceptual foundation for organizational information security awareness, **Information Management & Computer Security**, 8, 1, 31-41. 2000.

SMITH, M.. Data protection, health care and the new European directive. **British Medical Journal** 312, 197–198. 1996.

SZUBA, T. Safeguarding your technology – pratical guidelines for eletronic education Information Security. São Paulo: U.S Department of Education. National Center for Education Statistics, 1998

TRCEK, D., TROBEC, R., PAVESIC, N., TASIC, J. F. (2007) Information systems security and human behavior, **Behavior & Information Technology**, 26, 2, 113–118.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação.** São Paulo: Atlas, 1987.

VANCE, A.; SIPONEN, M.; PAHNILA, S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. **Information & Management**, 2012.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management, Computers & Security, vol. 23, issue 5, pp. 371-376: 2004.

XU, H., et. al. Measuring mobile users' concerns for information privacy. **Thirty Third International Conference on Information Systems**, Orlando 2012.

WAINER, J. Princípios que devem reger um prontuário único do paciente. **Revista Textos de La Ciber Sociedad**; 2008. Disponível em: http://www.cibersociedad.net/textos/articulo.php?art=193. Acesso em: 10 jan 2015.

WESTIN, A. F. **Privacy and Freedom**. New York: Atheneum, 1967.

WIEDENHÖFT, G.C.. Identificação de critérios para monitorar a efetividade dos Mecanismos de Governança de Tecnologia da Informação. 27/03/2013. 117 f. Dissertação (Mestrado em Administração) - Faculdade de Administração,

Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul, 2013.

Win, K.T., Susilo, W., and Mu, Y. Personal Health Record Systems and Their Privacy Protection. **Journal of Medical Systems**, vol.30, pp 309 – 315. 2006.

YIN, R. K ..Case Study Research - Design and Methods. **Sage Publications Inc** ., USA, 1989.

YIN, R. K. **Estudo de Caso – planejamento e métodos.** (2Ed.). Porto Alegre: Bookman. 2001.

_____. **Estudo de Caso: planejamento e métodos**. Porto Alegre: Bookman, 2005.

ZANDIEH, S.O.; KAHYUN, Y.F.; KUPERMAN, G.J.; et al. Challenges to EHR implementation in electronic versus paper-based office practices. J Gen Intern Med. 2008; 23:755-61.

ZIKOPOULOS, P; DE ROOS, D; PARASURAMAN, K; DEUTSCH, T; GILES, J; CORRIGAN, D. Harness the power of Big Data- The IBM Big Data Platform. Emeryville: McGraw-Hill Osborne Media, 2012.

APÊNDICE A – ROTEIRO DE ENTREVISTA ORIGINAL

Este roteiro de entrevista é parte integrante da pesquisa acadêmica realizada por Odirlei Antonio Magnagnagno (odirlei@fag.edu.br), no âmbito do Programa de Mestrado Acadêmico da PUCRS, sob a orientação da Profa. Drª Edimara Mezzomo Luciano (eluciano@pucrs.br).
Os dados serão usados apenas de forma consolidada, não permitindo a identificação uma vez que as respostas serão divulgadas sempre de maneira agrupada, impossibilitando a identificação. Não existem respostas certas ou erradas, o que se busca é a percepção do respondente a acerca dos assuntos abordados nesta entrevista. Suas respostas são muito importantes para a área de Segurança da Informação e contribuirão para um ambiente mais seguro através da divulgação dos resultados.

Estabelecimento:

Nome:

Gênero: ⭘ Feminino. ⭘ Masculino.

Qual a sua idade?_____ anos.

Qual das opções abaixo melhor representa seu nível de escolaridade:

- ⭘ Ensino fundamental (1º grau)
- ⭘ Ensino médio (2º grau)
- ⭘ Ensino superior
- ⭘ Especialização/MBA,
- ⭘ Mestrado/Doutorado.

Qual das opções abaixo melhor representa sua área de formação:

- ⭘ Administração.
- ⭘ Informática.
- ⭘ Medicina
- ⭘ Enfermagem
- ⭘ Outra: _____.

Qual o seu cargo/função atual?_____.

Quantos anos de experiência profissional você tem (total de anos)? ___ anos.

Há quantos anos trabalha neste estabelecimento? ___ anos.

Trabalha somente neste estabelecimento de saúde ou trabalha em outros também.

Dimensões	Variáveis	Aspectos a explorar	Referências
Caracterís-ticas documentais e regras de privacidade	Políticas de Segurança	Como o estabelecimento trata com a questão de privacidade do paciente, existem regras ou esforços formais ou informais? O Hospital tem algum documento regulador de políticas de Segurança da Informação? Como você tem acesso a ele? Você o conhece?	FURNELL e RAJENDRAN, 2012 ABRAHÃO, 2003; FERREIRA e ARAÚJO, 2008
	Regras	Você acredita que os seus colegas de trabalho cumprem as normas de segurança devido à certeza de detecção e a certeza de punição? Você acredita que essa punição é ocorre com agilidade?	HERATH e RAO, 2009
Caracterís-ticas organiza-cionais	Pressões no trabalho	Porque minha atividade exige responsabilidade no cumprimento das políticas de Segurança da Informação e privacidade? Você acredita que o grande volume de tarefas ou atividades no trabalho faz com que se descuide de processos de Segurança da Informação? Tem algum exemplo?	HERATH e RAO, 2007
		O hospital me pressiona pelo cumprimento das regras presentes nas políticas de segurança nas atividades de trabalho, como ocorre?	HERATH e RAO, 2007
	Procedi-mento disciplinar	Que medidas disciplinares a instituição adota para quem não cumpre com as Políticas de segurança.	HERATH e RAO, 2007
		Você acha que os procedimentos disciplinares são importantes para que as Políticas de segurança sejam cumpridas? Por quê?	HERATH e RAO, 2007
	Práticas de Segurança da Informação	As práticas de segurança (treinamentos, troca de senha, controle de acesso físico e lógico, criação de normas, etc) existem no hospital? Como foram surgindo essas práticas? A quem se aplica? Elas são formais (descritas em um documento) ou são informais (apenas cumpridas por parte dos colaboradores)?	FURNELL e RAJENDRAN, 2012; CERT.BR 2012; LEMOS, 2001; NG et al. (2009)
		O Hospital é proativo em relação ao cumprimento das Políticas de Segurança da Informação, por quê? Com quais procedimentos?	FURNELL e RAJENDRAN, 2012
		O Hospital oferece informações para conscientizar sobre a necessidade de cumprir às regras das Políticas de privacidade? De que maneira?	FURNELL e RAJENDRAN, 2012
		O Hospital considera importante que cumpra com as regras de segurança? Como deixa isso claro?	FURNELL e RAJENDRAN, 2012
		O hospital exige algum conhecimento e cumprimentos das normas de segurança de documentos reguladores externos, como Código de ética profissional, SOX, HIPAA, ISO 27000. Como fazem essa cobrança?	HERATH e RAO, 2007
		Os dados são criptografados (codificados), quando se faz necessário a transmissão para ambientes externos. (ANS, Planos de saúde, etc)? Os computadores são protegidos por senha? Você pode acessar todos os pacientes que estão no hospital e verificar todos os dados deles? (Quais e o que pode acessar). Quais são as orientações para proteger as informações dos pacientes via comunicação oral entre os colaboradores. Os seus colegas comentam ou facilitam o acesso a informações e documentos para pessoas que não estão diretamente envolvidas na prestação da assistência, mesmo que seja apenas por curiosidade.	Código de Ética dos Profissionais de Enfermagem BAUMER, EARP e PAYTON, 2000 Código de Ética Médica
		Você acha que o tipo de atividade exercida pela Instituição exige que sejam estabelecidas e cumpridas	FURNELL e RAJENDRAN, 2012

Dimensões	Variáveis	Aspectos a explorar	Referências
		as políticas de privacidade? Por quê?	
Caracterís-ticas comporta-mentais	Benefícios pessoais	Você acredita que o seu comportamento em relação ao cumprimento das políticas de segurança e privacidade o fazem ser positivamente reconhecido pelo Hospital, por quê?	FURNELL e RAJENDRAN, 2012
		Você se sente valorizado pelo hospital pelo cumprimento das regras presentes na política de segurança, como?	FURNELL e RAJENDRAN, 2012
	Satisfação	O que lhe deixa satisfeito em relação às atividades de trabalho no hospital.	KRAEMER e CARAYON, 2005
		De que maneira as atuais regras de Segurança da Informação me deixam satisfeito ou insatisfeito	KRAEMER e CARAYON, 2005
	Comporta-mento pela segurança	Os seus colegas cumprem com as Políticas de Segurança que o Hospital propõe. (De que maneira?)	HERATH e RAO, 2007
		Que tipo de comportamento dos meus colegas que contribuem que para que as Políticas de Segurança sejam cumpridas. (interno e externo à instituição)	HERATH e RAO, 2007

APÊNDICE B – INSTRUMENTO PARA ENTREVISTAS COM PROFISSIONAIS DE TECNOLOGIA DA INFORMAÇÃO.

Roteiro de Entrevista

Este roteiro de entrevista é parte integrante da pesquisa acadêmica realizada por Odirlei Antonio Magnagnagno (odirlei@fag.edu.br), no âmbito do Programa de Mestrado Acadêmico da PUCRS, sob a orientação da Profª. Drª Edimara Mezzomo Luciano (eluciano@pucrs.br).
Os dados serão usados apenas de forma consolidada, não permitindo a identificação do respondente, uma vez que as respostas serão divulgadas sempre de maneira agrupada, impossibilitando a identificação. Não existem respostas certas ou erradas, o que se busca é a percepção do respondente acerca dos assuntos abordados nesta entrevista. Suas respostas são muito importantes para a área de Segurança da Informação em prontuários eletrônicos e contribuirão para um ambiente mais seguro em instituições de saúde, através da divulgação dos resultados.

Identificação dos processos de trabalho relativos a privacidade da informação do paciente em Instituições de Saúde.

Estabelecimento:_____

Nome:_____

Gênero: O Feminino. O Masculino.

Qual a sua idade?_____ anos.

Qual das opções abaixo melhor representa seu nível de escolaridade:

- O Ensino fundamental (1º grau)
- O Ensino médio (2º grau)
- O Ensino superior
- O Especialização/MBA,
- O Mestrado/Doutorado.

Qual das opções abaixo melhor representa sua área de formação:

- O Administração.
- O Informática.
- O Medicina
- O Enfermagem
- O Outra: _____.

Qual o seu cargo/função atual?_____.

Quantos anos de experiência profissional você tem (total de anos)? ___ anos.

Há quantos anos trabalha neste estabelecimento? ___ anos.

Você Trabalha somente neste estabelecimento de saúde ou trabalha em outros também, quais? _____

Dimensões	Variáveis	Aspectos a explorar	Referências
Caracterís-ticas documentais e regras de privacidade	Políticas de Segurança	1) Como o estabelecimento trata a questão de privacidade do paciente? Existem regras ou esforços neste sentido? Eles são formais ou informais?	FURNELL e RAJENDRAN, 2012 ABRAHÃO, 2003; FERREIRA e ARAÚJO, 2008
		2) O Hospital tem algum documento regulador de políticas de Segurança da Informação? Você o conhece? Como você tem acesso a ele?	ABRAHÃO, 2003; FERREIRA e ARAÚJO, 2008
	Regras	3) Você acredita que os seus colegas de trabalho cumprem as normas de Segurança da Informação?	HERATH e RAO, 2009
		4) Qual é a relação que você vê quanto à certeza de detecção e a certeza de punição, com o cumprimento das normas de Segurança da Informação?	HERATH e RAO, 2009
Caracterís-ticas organiza-cionais	Pressões no trabalho	5) Você acredita que a sua atividade exige responsabilidade no cumprimento das políticas de Segurança da Informação e privacidade, porque?	HERATH e RAO, 2007
		6) Como você vê a relação entre um grande volume de tarefas ou atividades no trabalho e a qualidade e o cumprimento das regras Segurança da Informação?	HERATH e RAO, 2007
		7) O hospital pressiona você a cumprir as regras presentes nas políticas de segurança nas atividades de trabalho, como ocorre?	HERATH e RAO, 2007
	Procedi-mento disciplinar	8) Que medidas disciplinares a instituição adota para quem não cumpre com as Políticas de segurança?	HERATH e RAO, 2007
		9) Você acha que os procedimentos disciplinares são importantes para que as Políticas de segurança sejam cumpridas? Por quê?	HERATH e RAO, 2007
	Práticas de Segurança da Informação	10) As práticas de segurança (treinamentos, troca de senha, controle de acesso físico e lógico, criação de normas, etc) existem no hospital? Como foram surgindo essas práticas? A quem se aplica? Elas são formais (descritas em um documento) ou são informais (apenas cumpridas por parte dos colaboradores)?	FURNELL e RAJENDRAN, 2012; CERT.BR 2012; LEMOS, 2001; NG et al. (2009)
		11) O Hospital oferece informações para conscientizar sobre a necessidade de cumprir as regras das Políticas de privacidade? De que maneira?	FURNELL e RAJENDRAN, 2012
		12) O Hospital considera importante que cumpra com as regras de segurança? Como deixa isso claro?	FURNELL e RAJENDRAN, 2012
		13) O hospital exige algum conhecimento e cumprimentos das normas de segurança de documentos reguladores externos, como Código de ética profissional, SOX, HIPAA, ISO 27000. Como fazem essa cobrança?	HERATH e RAO, 2007
		14) Os dados são criptografados (codificados), quando se faz necessário a transmissão para ambientes externos. (ANS, Planos de saúde, etc)?	BAUMER, EARP e PAYTON, 2000
		15) Os computadores são protegidos por senha? Você pode acessar todos os pacientes que estão no hospital e verificar todos os dados deles? (Quais e o que pode acessar).	Código de Ética Médica Código de Ética dos Profissionais de

Dimensões	Variáveis	Aspectos a explorar	Referências
		Quais são as orientações para proteger as informações dos pacientes via comunicação oral entre os colaboradores? Os seus colegas comentam ou facilitam o acesso a informações e documentos para pessoas que não estão diretamente envolvidas na prestação da assistência, mesmo que seja apenas por curiosidade.	Enfermagem
Caracterís-ticas comporta-mentais	Benefícios pessoais	16) Você acredita que o seu comportamento em relação ao cumprimento das políticas de segurança e privacidade o fazem ser positivamente reconhecido pelo Hospital, por quê?	FURNELL e RAJENDRAN, 2012
		17) Você se sente valorizado pelo hospital pelo cumprimento das regras presentes na política de segurança, como?	FURNELL e RAJENDRAN, 2012
	Satisfação	18) O que lhe deixa satisfeito em relação às atividades de trabalho no hospital	KRAEMER e CARAYON, 2005
		19) De que maneira as atuais regras de Segurança da Informação lhe deixam satisfeito ou insatisfeito	KRAEMER e CARAYON, 2005

APÊNDICE C – INSTRUMENTO PARA ENTREVISTAS COM PROFISSIONAIS DE ASSISTÊNCIA MULTIDISCIPLINAR

Roteiro de Entrevista

Este roteiro de entrevista é parte integrante da pesquisa acadêmica realizada por Odirlei Antonio Magnagnagno (odirlei@fag.edu.br), no âmbito do Programa de Mestrado Acadêmico da PUCRS, sob a orientação da Profª. Drª Edimara Mezzomo Luciano (eluciano@pucrs.br).
Os dados serão usados apenas de forma consolidada, não permitindo a identificação do respondente, uma vez que as respostas serão divulgadas sempre de maneira agrupada, impossibilitando a identificação. Não existem respostas certas ou erradas, o que se busca é a percepção do respondente acerca dos assuntos abordados nesta entrevista. Suas respostas são muito importantes para a área de Segurança da Informação em prontuários eletrônicos e contribuirão para um ambiente mais seguro em instituições de saúde, através da divulgação dos resultados.

Identificação dos processos de trabalho relativos a privacidade da informação do paciente em Instituições de Saúde.

Estabelecimento:_____

Nome:_____

Gênero: ⭘ Feminino. ⭘ Masculino.

Qual a sua idade?_____ anos.

Qual das opções abaixo melhor representa seu nível de escolaridade:

⭘ Ensino fundamental (1º grau)
⭘ Ensino médio (2º grau)
⭘ Ensino superior
⭘ Especialização/MBA,
⭘ Mestrado/Doutorado.

Qual das opções abaixo melhor representa sua área de formação:

⭘ Administração.
⭘ Informática.
⭘ Medicina
⭘ Enfermagem
⭘ Outra: _____.

Qual o seu cargo/função atual?_____.

Quantos anos de experiência profissional você tem (total de anos)? ___ anos.

Há quantos anos trabalha neste estabelecimento? ___ anos.

Você Trabalha somente neste estabelecimento de saúde ou trabalha em outros também, quais? _____

Dimensões	Variáveis	Aspectos a explorar	Referências
Caracterís-ticas documentais e regras de privacidade	Políticas de Segurança	1) Como o estabelecimento trata a questão de privacidade do paciente? Existem regras ou esforços neste sentido? Eles são formais ou informais?	FURNELL e RAJENDRAN, 2012 ABRAHÃO, 2003; FERREIRA e ARAÚJO, 2008
		2) O Hospital tem algum documento regulador de políticas de Segurança da Informação? Você o conhece? Como você tem acesso a ele?	ABRAHÃO, 2003; FERREIRA e ARAÚJO, 2008
	Regras	3) Você acredita que os seus colegas de trabalho cumprem as normas de Segurança da Informação?	HERATH e RAO, 2009
		4) Qual é a relação que você vê quanto à certeza de detecção e a certeza de punição, com o cumprimento das normas de Segurança da Informação?	HERATH e RAO, 2009
Caracterís-ticas organiza-cionais	Pressões no trabalho	5) Você acredita que a sua atividade exige responsabilidade no cumprimento das políticas de Segurança da Informação e privacidade, porque?	HERATH e RAO, 2007
		6) Como você vê a relação entre um grande volume de tarefas ou atividades no trabalho e a qualidade e o cumprimento das regras Segurança da Informação?	HERATH e RAO, 2007
		7) O hospital pressiona você a cumprir as regras presentes nas políticas de segurança nas atividades de trabalho, como ocorre?	HERATH e RAO, 2007
	Procedimento disciplinar	8) Que medidas disciplinares a instituição adota para quem não cumpre com as Políticas de segurança?	HERATH e RAO, 2007
		9) Você acha que os procedimentos disciplinares são importantes para que as Políticas de segurança sejam cumpridas? Por quê?	HERATH e RAO, 2007
	Prática de Segurança da Informação	10) As práticas de segurança (treinamentos, troca de senha, controle de acesso físico e lógico, criação de normas, etc) existem no hospital? Como foram surgindo essas práticas? A quem se aplica? Elas são formais (descritas em um documento) ou são informais (apenas cumpridas por parte dos colaboradores)?	FURNELL e RAJENDRAN, 2012; CERT.BR 2012; LEMOS, 2001; NG et al. (2009)
		11) O Hospital oferece informações para conscientizar sobre a necessidade de cumprir as regras das Políticas de privacidade? De que maneira?	FURNELL e RAJENDRAN, 2012
		12) O Hospital considera importante que cumpra com as regras de segurança? Como deixa isso claro?	FURNELL e RAJENDRAN, 2012
		13) Os computadores são protegidos por senha? Você pode acessar todos os pacientes que estão no hospital e verificar todos os dados deles? (Quais e o que pode acessar). Quais são as orientações para proteger as informações dos pacientes via comunicação oral entre os colaboradores? Os seus colegas comentam ou facilitam o acesso a informações e documentos para pessoas que não estão diretamente envolvidas na prestação da assistência, mesmo que seja apenas por curiosidade	Código de Ética Médica Código de Ética dos Profissionais de Enfermagem
	Benefícios pessoais	14) Você acredita que o seu comportamento em relação ao cumprimento das políticas de segurança e	FURNELL e RAJENDRAN,

Dimensões	Variáveis	Aspectos a explorar	Referências
Caracterís-ticas comporta-mentais		privacidade o fazem ser positivamente reconhecido pelo Hospital, por quê?	2012
		15) Você se sente valorizado pelo hospital pelo cumprimento das regras presentes na política de segurança, como?	FURNELL e RAJENDRAN, 2012
	Satisfação	16) O que lhe deixa satisfeito em relação às atividades de trabalho no hospital	KRAEMER e CARAYON, 2005
		17) De que maneira as atuais regras de Segurança da Informação lhe deixam satisfeito ou insatisfeito	KRAEMER e CARAYON, 2005

APÊNDICE D – REFERÊNCIAS BIBLIOGRÁFICAS QUE CITAM OS DOCUMENTOS REGULATÓRIOS E NORMATIVOS

Bibliografia	CÓD	Nome
SIMIONATO, A. C.; SANT'ANA, R. C. G.; SANTOS, P. L. V. A. C.. Privacidade e os Simulacros Digitais Gerados Pelos Dados Pessoais. **Encontro Internacional Dados, Tecnologia e Informação**, 2013, Marília. São Paulo.	DE9	Código Penal (lei nº 2.848)
	DE16	Marco Civil da internet
MENDES, S. F. et al.. Uma análise da implantação do padrão de troca de informação em saúde suplementar no Brasil. **J. Health Inform**. 2009 Out-Dez; 1(2): 61-7	DE2	TISS (Troca de Informação em Saúde Suplementar)
SALVADOR, V.F.M.; ALMEIDA, F.V.. Aspectos éticos e de segurança do prontuário eletrônico do paciente. In: **Anais da II Jornada do Conhecimento e da Tecnologia.** Marília SP. Brasil. 2005. Disponível em: http://www.uel.br/projetos/oicr/pages/arquivos/Valeria_Farinazzo_aspecto_etico.pdf. Acesso em 05 de dez 2014.	DE3	Resolução CFM Nº 1.821
	DE4	Código de Ética Médica – Brasil
	DE5	Código de Ética dos Profissionais de Enfermagem
	DE6	Constituição Federal
	DE7	Código Civil (lei 10.406)
	DE9	Código Penal (lei nº 2.848)
	DE17	A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2
OLIVEIRA, J. F. Gestão de Tecnologias da Informação e da Comunicação na Saúde: uma análise sobre o uso do prontuário eletrônico. **Interface** – Natal/RN – v.9 – n.1 – jan/jun 2012	DE3	Resolução CFM Nº 1.821
	DE4	Código de Ética Médica – Brasil
	DE5	Código de Ética dos Profissionais de Enfermagem
	DE6	Constituição Federal
	DE17	A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2
FABRI, M. Desafios para a Preservação da Privacidade no Contexto da Saúde. **Rev. Temas em Debate**, Rio de Janeiro, v.1, n.1, p.306-322, 2003.	DE4	Código de Ética Médica – Brasil
	DE5	Código de Ética dos Profissionais de Enfermagem
	DE6	Constituição Federal
PATRÍCIO, C. M. *et al*. O prontuário eletrônico do paciente no sistema de saúde brasileiro: uma realidade para os médicos? ***Scientia Medica****,* Porto Alegre, v. 21, n. 3, p. 121-131, 2011. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/scientiamedica/article/viewFile/8723/6722>. Acesso em: 23 dez. 2014.	DE3	Resolução CFM Nº 1.821
	DE4	Código de Ética Médica – Brasil
	DE5	Código de Ética dos Profissionais de Enfermagem
	DE6	Constituição Federal
	DE7	Código Civil (lei 10.406)
	DE9	Código Penal (lei nº 2.848)
GAERTNER, A.; SILVA, H. P. Privacidade da Informação na Internet: Ausência de Normalização, Proceedings. **CINFORM - Encontro Nacional de Ciência da Informação VI**, Bahia, 2005	DE6	Constituição Federal
	DE8	Código de Defesa do Consumidor (lei 8.078)
	DE20	PIPEDA- "*Personal Information Protection and Electronic Documents Act*"

Bibliografia	CÓD	Nome
ALONSO, L. B. N.; DROVAL, C.; FERNEDA, E.; EMÍDIO, L.. Acreditação Hospitalar e a Gestão da Qualidade dos Processos Assistenciais. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n. 2, p. 34-49, jul./dez. 2014.	DE18	Manual de Acreditação da ONA
	DE19	Manual de Acreditação da *Joint Commission International* (JCI)
JUNIOR, A.E.A.; SANTOS, E.M.. A percepção da importância de Controles de Segurança da Informação em hospitais públicos brasileiros. RECIIS – R. Eletr. de Com. Inf. Inov. Saúde. Rio de Janeiro, v.7, n.2, Jun., 2013. Disponível em http://www.reciis.icict.fiocruz.br/index.php/reciis/article/viewArticle/688/1565. Acesso em 10 jan 2015.	DE6	Constituição Federal
	DE11	Lei de Acesso à informação (lei nº 12.527)
	DE15	NBR ISO/IEC 27002
BRAGANÇA, C. E. B. A; LUCIANO, E. M.; TESTA, M. G.. Segurança da Informação e privacidade de informações de pacientes de instituições de saúde: uma análise exploratória da privacidade percebida pelos profissionais. **EnANPAD**. Rio de Janeiro – 25 a 29 de setembro de 2010.	DE3	Resolução CFM Nº 1.821
	DE13	HIPAA - *Health Insurance Portability and Accountability Act*
KLEIN, R. H.. Ameaças, controle, esforço e descontentamento do usuário no comportamento seguro em relação à Segurança da Informação. 24/03/214. 100 f. Dissertação (Mestrado em Administração) - Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul, 2014.	DE1	Norma ABNT NBR ISO/IEC 27001
	DE11	Lei de Acesso à informação (lei nº 12.527)
	DE15	NBR ISO/IEC 27002
APPARI. A.; JOHNSON, M. E. Information Security and Privacy in Healthcare: Current State of Research. Center for Digital Strategies Tuck School of Business. Dartmouth College, Hanover NH. August 2008	DE13	HIPAA - *Health Insurance Portability and Accountability Act*
KAMEDA, K.; PAZELLO M. E-Saúde e desafios à proteção da privacidade no Brasil. Instituo Nupef, Outubro 2013. Disponível em http://www.nupef.org.br/. Acesso em 15 dez 2014.	DE2	TISS (Troca de Informação em Saúde Suplementar)
	DE4	Código de Ética Médica – Brasil
	DE6	Constituição Federal
	DE7	Código Civil (lei 10.406)
	DE8	Código de Defesa do Consumidor (lei 8.078)
	DE9	Código Penal (lei nº 2.848)
	DE12	Política Nacional de Informação e Informática em Saúde (PNIIS)
BRAGANÇA, C. E. B. A. Privacidade em informações de saúde: uma análise do comportamento percebido por profissionais de saúde de Instituições Hospitalares do Rio Grande do Sul. 30/08/2010. 124 f. Dissertação (Mestrado em Administração) - Faculdade de Administração, Contabilidade e Economia. Pontifícia Universidade Católica do Rio Grande do Sul, 2010.	DE1	Norma ABNT NBR ISO/IEC 27001
	DE2	TISS (Troca de Informação em Saúde Suplementar)
	DE4	Código de Ética Médica – Brasil
	DE6	Constituição Federal
	DE7	Código Civil (lei 10.406)
	DE9	Código Penal (lei nº 2.848)
	DE12	Política Nacional de Informação e Informática em Saúde (PNIIS)
	DE13	HIPAA - *Health Insurance Portability and Accountability Act*
	DE15	NBR ISO/IEC 27002
	DE18	Manual de Acreditação da

Bibliografia	CÓD	Nome
		ONA
	DE20	PIPEDA- "*Personal Information Protection and Electronic Documents Act*"
LOUREIRO, S.C. Segurança da Informação: Preservação das Informações Estratégicas com Foco em sua Segurança.12/2008.66 p. Monografia de Conclusão de Curso (Especialização) Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.	DE1	Norma ABNT NBR ISO/IEC 27001
	DE9	Código Penal (lei nº 2.848)
	DE15	NBR ISO/IEC 27002
	DE17	A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2
MARQUES , E. P. et al. Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES). SBIS. 22/10/2013. 91p.	DE1	Norma ABNT NBR ISO/IEC 27001
	DE2	TISS (Troca de Informação em Saúde Suplementar)
	DE3	Resolução CFM Nº 1.821
	DE14	ISO / TC 215
	DE15	NBR ISO/IEC 27002
	DE17	A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2
WAINER, J. Princípios que devem reger um prontuário único do paciente. **Revista Textos de La Ciber Sociedad**; 2008. Disponível em: http://www.cibersociedad.net/textos /articulo.php?art=193. Acesso em: 10 jan 2015.	DE10	Código de Ética da IMIA[6] para Profissionais de Informática em Saúde
	DE13	HIPAA - *Health Insurance Portability and Accountability Act*
KOBAYASHI, L. O. M.; FURUIE, S.S. **Segurança em Imagens Médicas: Uma Revisão**. São Paulo: USP, 2006.	DE10	Código de Ética da IMIA para Profissionais de Informática em Saúde

[6] International Medical Informatics Association

APÊNDICE E – IDENTIFICAÇÃO E RASTREABILIDADE DOS CÓDIGOS UTILIZADOS NA ANÁLISE DOS DADOS.

Códigos	Descrição	Localização
DE1...DE20	Documentos Regulatórios e Normativos	Quadro 5
		Quadro 8
		Quadro 13
MDE1...MDE37	Mecanismos dos Documentos Regulatórios e Normativos	Quadro 13
		Quadro 14
		Quadro 22
EB1...EB5	Entrevistados Hospital Beta	Quadro 16
		Figura 2
MEB1...MEB32	Mecanismos das Entrevistas do Hospital Beta	Quadro 17
MECB1...MECB36	Mecanismos do Estudo de Caso do Hospital Beta	Quadro 18
EG1...EG4	Entrevistados Hospital Gama	Quadro 19
		Figura 4
MEG1...MEG41	Mecanismos das Entrevistas do Hospital Gama	Tabela 20
MECG1...MECG43	Mecanismos do Estudo de Caso do Hospital Gama	Quadro 21
MEC1...MEC48	Mecanismos unificados dos Estudos de Caso Beta e Gama	Tabela 3
M1...M50	Mecanismos unificados dos Documentos Regulatórios e Normativos e dos Estudos de Caso	Quadro 22
1...50	Mecanismos Finais	Apêndice F

APÊNDICE F – READEQUAÇÃO DOS NOMES E CÓDIGOS DOS MECANISMOS

Código Final	Nome do mecanismo final	Código original	Nome do mecanismo Original	Total de Citações
1	Área de qualidade para controlar os documentos	M44	Ter uma área de qualidade para controlar os documentos	2
2	Comissão de Revisão de Prontuários	M27	Possuir uma Comissão de Revisão de Prontuários	6
3	Controle e armazenamento dos prontuários eletrônicos em um sistema especializado em GED	M39	Controlar e armazenar os prontuários eletrônicos num sistema especializado em GED	3
4	Estrutura física adequada para o gerenciamento do SI	M2	Ter estrutura física apropriada para a coleta, armazenagem, recuperação, processamento e acesso das informações	17
5	Implantação e manutenção do Sistema de Gestão da Segurança da Informação	M7	Implantar e manter um Sistema de Gestão da Segurança da Informação	13
6	Instalação de Antivírus, VPN e *firewall*	M9	Instalar Antivírus, VPN e *firewall*	12
7	Pessoa responsável pela Política de Segurança da Informação	M12	Ter uma pessoa responsável pela Política de Segurança da Informação	10
8	Proteções internas para a conexão de um novo *hardware* ou *software* na rede	M21	Ter proteções internas para a conexão de um novo *hardware* ou *software* na rede	8
9	Quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento	M22	Ter a quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento	8
10	Acesso do prontuário somente no momento da internação	M38	Acesso do prontuário somente no momento que o paciente esta internado	4
11	Acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	M8	Liberar acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes	13
12	Análise dos antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa	M43	O departamento de RH deve analisar os antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa	2
13	Análise regular da Segurança dos Sistemas de Informação	M26	Analisar regularmente a Segurança dos Sistemas de Informação	7
14	Anulação imediata dos acessos do empregado demitido	M31	Desabilitar todos os tipos de acessos do empregado no momento da demissão do mesmo	4
15	Armazenamento de *logs* de acesso e *logs* de alterações realizadas no prontuário do paciente	M17	Armazenar *log* de acesso e *logs* de alterações realizadas no prontuário do paciente	9
16	*Backup* estruturado das informações	M20	Ter um *backup* estruturado das informações	8
17	Bloqueio de utilização de mídias de	M50	Bloquear a utilização de mídias	1

Código Final	Nome do mecanismo final	Código original	Nome do mecanismo Original	Total de Citações
	gravação (*pendrive*), acesso a repositórios na internet e e-mail externo		de gravação (*pendrive*) internos assim como acesso a repositórios na internet e e-mail externo	
18	Ciência da leitura dos termos de Segurança da Informação	M41	Dar ciência da leitura dos termos de Segurança da Informação no momento da troca da senha	3
19	Coleta somente dados relevantes dos clientes/pacientes	M40	Coletar somente dados relevantes dos clientes/pacientes	3
20	Criação de uma integração de *login* e senha válidos para todos os sistemas	M47	Criar uma integração de *login* e senha válido para todos os sistemas	2
21	Criptografia para o tráfego externo de informações	M14	Criptografar o tráfego externo de informações	10
22	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento	M29	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento	5
23	Definição de regras para transmissão de dados externos	M24	Definir regras para transmissão externa de informações para terceiros	7
24	Determinação de máscara de senha e tempo máximo de troca de senha e bloqueio por muitas tentativas	M11	Determinar a qualidade da senha e o período máximo de obrigatoriedade de troca da mesma e o bloqueio por muitas tentativas	11
25	Divisão das funções dos colaboradores nos sistemas	M32	Dividir as funções dos colaboradores nos sistemas	4
26	Identificação e autenticação dos usuários	M1	Identificar e autenticar o usuário em sistemas, arquivos, portais ou *webservices*	19
27	Inativação do sistema por tempo ocioso	M36	Desconectar o sistema por tempo de inatividade	4
28	Liberação do acesso aos dados relevantes somente para pessoas devidamente autorizadas	M10	Liberar acesso aos dados relevantes somente para pessoas devidamente autorizadas	12
29	Monitoramento constantemente das atividades incomuns de processamento da informação	M25	Monitorar constantemente as atividades não autorizadas ou incomuns de processamento da informação	7
30	Não utilização do celular, principalmente no beira leito	M45	Não utilizar celular no local de trabalho, principalmente no beira leito	2
31	Obrigatoriedade de assinatura do termo de conduta no momento da contratação.	M30	Obrigatoriedade de assinatura do termo de conduta na contratação	5
32	Penalização com multa	M48	Penalidade com multa em dinheiro	1
33	Planejamento das atividades, para executar as tarefas de forma segura	M19	Planejar as atividades, avaliando as condições operacionais e infraestrutura, para executar as tarefas de forma segura	8
34	Plano de contingência para desastres com informações	M16	Ter um plano de recuperação ou contingência para desastres com informações	9
35	Política pública específica para a	M46	Ter uma política pública	2

Código Final	Nome do mecanismo final	Código original	Nome do mecanismo Original	Total de Citações
	privacidade da informação no Brasil		específica para a privacidade da informação no Brasil	
36	Prevenção no posicionamento de computadores próximos a corredores	M42	Evitar posicionar computadores próximos a corredores	2
37	Sanções adequadas para os que violam as políticas de privacidade	M4	Impor sanções adequadas para os que violam as políticas de privacidade	16
38	*Software* de HIS adequado e de boa qualidade	M23	Ter um *software* de HIS – adequado e de boa qualidade	7
39	Treinamento constante para os colaboradores	M3	Treinar constantemente os colaboradores a respeito de políticas e procedimentos de acordo com a sua atuação no trabalho	16
40	Utilização de nomes fictícios nas bases de testes e homologações	M37	Utilizar nomes fictícios nas bases de testes e homologações	4
41	Utilização do certificado digital nos prontuários eletrônicos	M13	Utilizar o certificado digital (Chave pública para autenticação) para prontuários eletrônicos	10
42	Criação e divulgação aos colaboradores da política de privacidade	M6	Criar e divulgar aos colaboradores uma política de privacidade	14
43	Disponibilização das políticas de Segurança da Informação aos clientes	M49	Disponibilizar as políticas de Segurança da Informação aos clientes	1
44	Divulgação dos meios de segurança de SI antes da implantação	M33	Divulgar os meios de Segurança de Sistemas de Informação antes do desenvolvimento ou implantação	4
45	Envio de comunicados constantes aos colaboradores, orientando sobre a proteção da informação	M5	Enviar comunicados constantemente aos colaboradores, orientando como o hospital pode divulgar informações e também como ele protege as informações	14
46	Instrução informal de médicos e enfermeiros a não divulgar casos	M15	Instruir o médico e enfermeiro a não divulgar casos de exemplos que possam ser identificados, mesmo informalmente	9
47	Intranet para consulta dos documentos de políticas	M18	Criar uma intranet para deixar os documentos disponíveis	9
48	Manutenção das informações dos clientes apenas o tempo necessário por lei	M34	Manter as informações dos clientes apenas o tempo necessário por lei	4
49	Prevenção para que os colaboradores não conversem com pacientes a respeito de diagnósticos em áreas públicas	M28	Prevenir para que médicos e enfermeiros não conversem com pacientes a respeito de diagnósticos em áreas públicas	6
50	Valorização e premiação pelo cumprimento da Segurança da Informação	M35	Valorizar e até premiar em dinheiro a boa prática de Segurança da Informação	4