UNIVERSIDADE FEDERAL DO PARANÁ

SUELEN CRISTINA MIRA ROSA

PROPOSTA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA UTILIZAÇÃO DE PRONTUÁRIOS MÉDICOS PARA O HOSPITAL DO TRABALHADOR DA CIDADE DE CURITIBA

CURITIBA
2008

SUELEN CRISTINA MIRA ROSA

PROPOSTA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA UTILIZAÇÃO DE PRONTUÁRIOS MÉDICOS PARA O HOSPITAL DO TRABALHADOR DA CIDADE DE CURITIBA

Trabalho de conclusão de curso apresentado ao Curso de Bacharelado em Gestão da Informação do Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná.

Orientador: Prof. Dr. Mauro José Belli

CURITIBA
2008

TERMO DE APROVAÇÃO

SUELEN CRISTINA MIRA ROSA

PROPOSTA DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NA UTILIZAÇÃO DE PRONTUÁRIOS MÉDICOS PARA O HOSPITAL DO TRABALHADOR DA CIDADE DE CURITIBA

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do grau de Bacharel no Curso de Bacharelado em Gestão da Informação, Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Orientador: Prof. Dr. Mauro José Belli
Departamento de Ciência e Gestão da Informação

Profa. Dra. Denise Fukumi Tsunoda
Departamento de Ciência e Gestão da Informação

Prof. Dra. Helena de Fátima Nunes Silva
Departamento de Ciência e Gestão da Informação

Curitiba, 03 de dezembro de 2008.

Dedico a Deus pela vida, sabedoria e amor,
ao meu marido Ademilson,
minha mãe Maria de Lourdes,
meu pai Claudenir e meu irmão Victor Hugo,
os grandes incentivadores dessa conquista.

AGRADECIMENTOS

A Deus pelo amor e permissão,
a minha família por me apoiar e incentivar,
aos mestres pela dedicação no ensino,
aos amigos pelo companheirismo,
ao Hospital do Trabalhador por abrir as portas e
especialmente a Jurandir Luiz Freire por estar
no meu caminho no dia em que quase perdi a prova do vestibular.

“Águas profundas são as palavras da boca do homem, e ribeiro transbordante é a fonte da sabedoria...”

Provérbios 18:4

RESUMO

Apresenta estudo desenvolvido no Hospital do Trabalhador de Curitiba quanto à segurança das informações contidas nos prontuários médicos por eles utilizados, através do qual objetivou-se o desenvolvimento de uma proposta de políticas de gestão de segurança da informação, tendo como alvo os prontuários médicos. Trata a segurança da informação como um requisito fundamental para garantir a qualidade da informação e, consequentemente, atribuir a ela integridade, disponibilidade e confiabilidade. Descreve a segurança da informação como uma área do conhecimento dedicada à proteção dos ativos de informação, sendo as políticas um conjunto de normas, métodos e procedimentos que formalizam as preocupações com segurança. Define a estrutura e diretrizes que formam o Hospital do Trabalhador, bem como sua estrutura física e organizacional, no que diz respeito ao objeto de estudo. Apresenta a fundamentação teórica tomada por base; a metodologia de pesquisa, que se utilizou de observação e entrevista para obter as informações que deram origem aos fluxogramas desenvolvidos; a explicação do objeto de estudo e a descrição da política de segurança. Propõe diretrizes básicas para a implantação e manutenção da política, de modo que sua cultura organizacional não sofra impactos negativos, e também valida a política por meio de formulário de validação, respondido por funcionários do Hospital do Trabalhador, ativo mais afetado com a implantação de uma política. Expõe, ao fim, os fluxogramas base para a construção da política de segurança e a política na íntegra, bem como sua estrutura, abordagem, implicações, aprovações e diretrizes. Conclui que por meio da implantação de políticas de segurança da informação é possível administrar melhor os recursos informacionais.

Palavras-chave: Informação. Segurança da informação. Qualidade da informação. Políticas de segurança da informação.

LISTA DE FIGURAS, GRÁFICOS E QUADROS

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Diante da tendência de uso da informação, segurança tem se tornado cada vez mais motivo de preocupação para os usuários. Afinal, quando se fala em informação percebe-se que essa é cada dia mais utilizada e está permeando todas as áreas do conhecimento.

A gestão da segurança da informação é uma forma de gerenciar a informação de modo a garantir sua qualidade e assim manter sua confidencialidade, integridade e disponibilidade. A maior problemática desta atividade é a conciliação entre os diversos envolvidos no processo: os recursos humanos, tecnológicos e informacionais. Diante dessas dificuldades, foram criadas normas internacionais, tecnologias e processos que visam garantir o sentimento de segurança dos proprietários da informação, entendendo-se por proprietário o indivíduo responsável pela geração e manutenção da informação.

Na área de ciências da saúde a informação não se comporta de forma diferente, e dentre todas as fontes de informação destacam-se, para fins desse estudo, os prontuários médicos. Esses são importantes fontes que contém os mais variados dados para a medicina. Diante disso, a proteção desse recurso é uma forma de gerenciar informações críticas, que podem afetar a organização, tanto em sua imagem, integridade, recursos financeiros, recursos humanos, quanto nos demais envolvidos. E para que se possa garantir essa proteção, uma boa ação é o desenvolvimento de políticas específicas para essa necessidade.

Mostrando-se preocupado com essas iniciativas é que o Hospital do Trabalhador, da cidade de Curitiba, situado à Avenida República Argentina, nº 4406, cedeu espaço para que tal gestão fosse criada em suas dependências. Foi fundado em 1947, sob a denominação de “Sanatório Médico – Cirúrgico do Portão”. Veio a receber seu nome atual somente em 1997, após inúmeras mudanças de estrutura e diversas ampliações e implementações. Atua no atendimento ao trauma e emergências com as seguintes especialidades: cirurgia geral, ortopedia e traumatologia, neurocirurgia, clínica médica, pediatria, anestesiologia, cirurgia de mão, cirurgia vascular, microcirurgia, urologia, cirurgia buxo-maxilo-facial, cirurgia plástica, cirurgia pediatria, cirurgia torácica, otorrinolaringologia, terapia intensiva, obstetrícia, neonatologia, infectologia, medicina do trabalhador, patologia clínica,

anatomia patológica, radiologia, ultrassonografia, endoscopia digestiva, endoscopia respiratória e pneumologia.

Nesse cenário se configuram grandes preocupações, compondo a base do problema inicialmente detectado para esse trabalho. Tais preocupações são: como a informação contida nos prontuários médicos é utilizada dentro da organização? Qual é o impacto da má utilização desse instrumento? Quais são as preocupações adotadas com relação ao cuidado com as informações? Qual o impacto da má utilização dos procedimentos adotados pela organização? Quais os problemas derivam da ausência de controle adequado sobre os prontuários médicos?

Com base em todos esses questionamentos fundamentou-se a construção da proposta de segurança da informação que será apresentada ao final desse trabalho.

1.1 JUSTIFICATIVA

Nos hospitais e clínicas os prontuários médicos se comportam como importantes instrumentos de informação, que possuem regulamentações e práticas específicas. De tal forma, as informações contidas nesse meio, se mal utilizadas, podem acarretar sérios riscos à organização, como prejuízos da sua imagem junto à sociedade, sanções legais, pois é a organização a responsável em prestar esclarecimento caso algo de errado aconteça e até mesmo conseqüências financeiras, tanto pelo extravio de informações quanto por imposições de multas da justiça.

Além dessas implicações, a utilização inadequada desse recurso pode comprometer a padronização dos procedimentos dificultando a utilização e manutenção das informações, e assim, comprometendo a segurança da informação.

No que diz respeito ao prontuário como instrumento de responsabilidade médica, as questões éticas e morais podem implicar nas informações descritas. A falta desses preceitos acarreta uma séria fonte de riscos e perdas.

A função principal do prontuário como fonte de informação, também é fortemente prejudicada devido à insuficiente qualidade dos registros de dados. Esse problema configura-se frequentemente nas pesquisas, pois muitos estudos são inviabilizados pela falta de dados e descrições. Com isso, a informação presente nesse documento é invalidada, tornando-se recorrente nos casos em que o

procedimento realizado é semelhante, pois nessas ocasiões não são abordados detalhes que poderiam conduzir a um maior conhecimento e definição da situação clínica do paciente.

Mas de todas as implicações possíveis, a mais relevante é a vida do ser humano. Afinal, no momento em que se encontra em tratamento hospitalar o requisito básico é a manutenção da vida, que pode ser facilmente afetada caso procedimentos inadequados sejam descritos em seu prontuário médico.

1.2 OBJETIVOS

Com o intuito de desenvolver o estudo sobre a gestão e as políticas de segurança da informação, têm-se os seguintes objetivos:

1.2.1 Objetivo geral

Propor políticas de segurança da informação para o Hospital do Trabalhador de Curitiba como forma de garantir a qualidade das informações utilizadas nos prontuários médicos.

1.2.2 Objetivos específicos

A fim de alcançar o objetivo geral da presente pesquisa, apresentam-se os seguintes objetivos específicos:

- identificar a composição das informações de um prontuário médico;
- observar o ciclo que a informação percorre nos prontuários médicos;
- identificar os elementos geradores de informação na instituição;
- identificar os proprietários da informação, bem como seus níveis de acesso;
- criar proposta de políticas de segurança da informação;
- descrever os requisitos necessários para a implantação e a manutenção das políticas de segurança da informação;
- validar as políticas de segurança da informação propostas.

2 FUNDAMENTAÇÃO TEÓRICA

No que se refere à gestão da segurança da informação, percebe-se que esse é um assunto complexo e que envolve diversos fatores críticos. Para possibilitar a compreensão do tema e das questões que serão abordadas, de maneira a tratar todos esses fatores, permitindo uma compreensão mais elaborada sobre essa área apresenta-se os capítulos que seguem.

2.1 DADO, INFORMAÇÃO E CONHECIMENTO

Para dar início ao estudo da segurança da informação é preciso compreender a origem da informação e sua transformação até se tornar conhecimento.

Nesse momento é fundamental perceber as diferenças entre o que vem a ser dado, informação e conhecimento de forma a dominar os conceitos e aplicabilidades de cada um desses termos.

Dados podem ser considerados como um “conjunto de fatos, feitos, cenas, eventos e situações que possuam significado ou valor definido” (FELIX, 2003, p. 25).

De acordo com Felix (2003, p. 26), dados passam a ser informação quando existe processamento, relacionamento e transformação, de maneira que o que entra ganha um novo significado dentro do processo.

Esse mesmo autor ainda define como conhecimento a “seqüência de etapas, regras e diretrizes a serem utilizadas para transformar um conjunto de dados em uma informação pré-selecionada” (FELIX, 2003, p. 28).

Ao dar início ao processo de construção do termo informação, é importante destacar, como afirma Robredo (2003, p.1), que a informação tem se espalhado e sido amplamente utilizada, tanto para a comunicação através da fala quanto no vocabulário técnico-científico. Entretanto, apesar das variáveis, em linhas gerais o termo pode ser compreendido da mesma forma.

Para McGarry (1999, p. 4), a informação é composta por diferentes atributos, dentre eles se destaca a matéria-prima da qual é possível extrair o conhecimento, aquilo que recebemos e trocamos com o mundo e aquilo que é capaz de reduzir a incerteza em determinadas situações.

Explicando a informação, é inevitável ter de apresentar o termo do qual se tem origem, o dado. Dado pode ser compreendido como um elemento em sua forma bruta e que por sua essência não conduz a compreensão de um evento ou momento. Já a sua evolução, é o que se caracteriza como informação, podendo ser entendida de maneira geral como o resultado do processo de transformação dos dados, de forma que conduza a compreensão e que possa ser comunicada/transmitida para gerar conhecimento (ROBREDO, 2003, p.2-4).

O inegável é perceber que a informação está permeando todas as áreas de conhecimento da sociedade, independente do segmento no qual se atua. Para Sêmola (2003, p.1-2), a informação é um fator que influência todas as fases de existência de uma empresa, entre elas a melhor produtividade, a redução dos custos, o aumento da competitividade e o apoio à tomada de decisão.

Além de permear áreas, a informação também pode ser considerada como uma importante fonte responsável pelo que é comumente denominado nas organizações de "*empowerment*", e assim permite o controle e a administração de povos e civilizações. Mas com o passar dos anos, ela foi evoluindo até chegar à modernidade, na qual integra o contexto empresarial, permitindo que o poder seja utilizado para o setor competitivo, estratégico e até mesmo de sobrevivência para muitas organizações (FELIX, 2003, p. 14-15).

Felix (2003, p. 17) defende ainda que a informação historicamente tem sido a base para o desenvolvimento econômico, social e cultural da humanidade e a partir de seu entendimento, como fator decisivo para o progresso da humanidade, concretizou-se como recurso valioso.

Ainda de acordo com Sêmola (2005, p.286) a informação passou por um processo de descentralização e tornou-se mais automatizada, com isso a informação passou a ser compartilhada e a gestão busca mais agilidade no desenvolvimento de suas ações.

A informação não se restringe a essas definições, ela caracteriza-se também como um termo qualitativo. De acordo com Wilden *apud*. Robredo (2003, p.4), a informação se apresenta em estruturas, formas, figuras, modelos, configurações, idéias, ideais, signos, sinais, gestos e outros, com o objetivo de se organizar em sua própria variedade.

Com tantas visões e percepções não é de se negar que se tem a impressão de que a informação está em todo lugar e que tudo pode, de alguma forma, se

relacionar com a informação (ROBREDO, 2003, p.5). A partir dessas declarações, fica evidente o imenso universo que proporciona a aquisição de informação para a transformação em conhecimento.

O termo conhecimento, assim como a informação, possui diversos significados. Uma dessas definições é feita por Boisot *apud*. Robredo (2003, p.16) que afirma que se pode definir como “a aplicação e uso produtivo da informação. O conhecimento é mais que a informação, pois implica uma consciência do entendimento adquirido”.

Fazendo um paralelo entre informação e conhecimento, Nonaka e Takeuchi (1998, p.63) afirmam que o conhecimento é formado pelas crenças, compromissos e ações, diferentemente da informação. No entanto também relatam que ambas estão no viés do significado, sendo específicas em seu contexto relacional ou não.

Sabendo que os prontuários médicos estão baseados em dados que geram informações e através de estudos se tornam conhecimentos, percebe-se o quanto a segurança é uma ação necessária nesse processo em que diversas pessoas estão diariamente envolvidas.

2.2 GESTÃO E POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

A gestão da segurança da informação revela a grande preocupação que se deve ter com o atributo informação. Para Ferreira e Araújo (2006, p.9) a segurança da informação é a formação de um conjunto de normas, métodos e procedimentos que são utilizados para a manutenção da informação, que precisa manter-se constantemente formalizado e divulgado entre os usuários que estão envolvidos nos diversos processos em que a segurança é exigida.

De acordo com Sêmola (2003, p.43) segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Sabendo-se que a informação está em suportes variados, garantir a sua integridade depende de protegê-la de vários tipos de ameaças, de forma que proporcione a garantia do negócio, se minimize os riscos e se maximizem as oportunidades de negócio.

Para defender a informação é importante entender que, de acordo com Laudon e Laudon (2001, p.340), “a segurança se refere a políticas, procedimentos e medidas técnicas usadas para prevenir acessos não autorizados e atualizações, roubo e danos físicos a informação”. Ainda de acordo com eles, essa segurança pode ser garantida por meio de técnicas e ferramentas que salvaguardam hardware, software, redes de comunicação e dados.

Percebe-se assim que a gestão da segurança da informação é uma forma de gerenciar os ativos de informação contra aquilo que se considera indesejado para os processos de garantia de qualidade da informação.

A segurança da informação é um requisito fundamental para conferir à organização competitividade no universo corporativo, no fluxo de caixa, na lucratividade, no atendimento aos requisitos legais e na imagem da organização junto ao mercado e à sociedade. De tal forma a segurança precisa ser alcançada por meios técnicos e ser apoiada por uma gestão e procedimentos apropriados, permitindo que se alcance segurança. No entanto além dos requisitos já abordados, é indispensável a participação de todos os envolvidos na organização e nos processos relacionados ao que se deseja assegurar (ABNT NBR ISO/IEC 17799, 2005, p.ix).

É possível identificar outros pensadores que entendem a segurança da informação de modo semelhante. Para a Fundação Nacional da Qualidade – FNQ (2007, p.14-15) “a gestão da segurança da informação abrange os aspectos necessários para garantir a atualização e preservação da confidencialidade, integridade e disponibilidade das informações”.

O maior problema de não se adotar uma medida de gestão de segurança da informação é assumir os riscos a qual a organização fica exposta. A FNQ (2007, p.14-15), ainda discute as implicações a que essa falta pode expor a organização, são elas:

a) a criação de gargalos ou problemas operacionais para clientes e outras partes interessadas em razão de descompassos nas atualizações de informação;
b) perdas de competitividade e ativos resultantes de roubos, fraudes e produção inadequada em relação à confidencialidade;
c) descontinuidade operacional causada por perdas irreversíveis em conseqüência de desastres; e

d) interrupções nos acessos às informações por falhas de infra-estrutura, geração e comunicação de dados.

A política de segurança da informação pode ser percebida por alguns autores de forma muito semelhante à gestão da segurança da informação, no entanto os padrões que as diferencia poderão ser compreendidos e discutidos.

Por política de segurança da informação entende-se o conjunto de normas, métodos e procedimentos do qual se faz uso durante a manutenção da informação, de forma que esses procedimentos sejam formalizados e divulgados a todos que fazem uso dos ativos de informação que estão em risco (FERREIRA e ARAÚJO, 2006, p. 9).

De acordo com a NBR ISO/IEC 17799 (2005, p. 8), a política de segurança da informação tem o objetivo de "prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes".

Três critérios, também relevantes para a gestão da segurança da informação, são de extrema importância para a composição de uma política na qual a informação apresente qualidade, esses critérios são, conforme expresso por Ferreira e Araújo (2006, p.17):

a) confidencialidade – garantia de que a informação é acessível somente para pessoas autorizadas a terem acesso;
b) integridade – salvaguarda da exatidão da informação e dos métodos de processamento;
c) disponibilidade – garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

É possível se aprofundar no entendimento desses itens na seção 2.2.1 dessa pesquisa, especifica de qualidade da informação.

Durante a construção de uma política de segurança é importante destacar os cuidados no seu desenvolvimento e elaboração, pois de acordo com Ferreira e Araújo (2006, p.10) eles precisam ser metódicos, criteriosos e adotar técnicas que permitam alterações nos equipamentos, tecnologias, responsabilidades, e por fim no perfil da empresa e dos negócios.

Outros aspectos também são evidenciados durante o processo de construção de uma política de segurança, conforme citam Ferreira e Araújo (2006, p.10), são eles: a) estabelecimento do conceito de que a informação é um ativo importante para

a organização; b) envolvimento da alta administração com relação à segurança da informação; c) responsabilidade formal dos colaboradores da empresa sobre a salvaguarda dos recursos da informação, definindo o conceito de irrevogabilidade; e d) estabelecimento de padrões para a manutenção da segurança da informação.

Não basta para o desenvolvimento das políticas que todos os colaboradores e a alta gerência estejam comprometidos. É fundamental que as políticas, normas e procedimentos de segurança da informação sejam simples, escritas de maneira clara e concisa, homologadas e assinadas pela alta administração, estruturadas de forma a permitir que sua implementação seja realizada em etapas, estejam alinhadas com as estratégias da organização, oriente para os possíveis riscos, serem flexíveis a ponto de se enquadrarem aos possíveis novos requerimentos de tecnologia, negócios e outros, priorizar as informações de maior valor e importância e serem positivas e não proibitivas e punitivas, de modo que possam cativar os envolvidos (FERREIRA e ARAÚJO, 2006, p.11-12).

Ao desenvolver uma política, alguns fatores são fundamentais para se obter sucesso, entre eles Ferreira e Araújo (2006, p.17) destacam:

a) formalização dos processos e instruções de trabalho;
b) utilização de tecnologias capazes de prover segurança;
c) atribuição formal das responsabilidades e das respectivas penalidades;
d) classificação das informações;
e) treinamento e conscientizações constantes.

Além disso, algumas características são indispensáveis de acordo com Ferreira e Araújo (2006, p.18-19), são elas: a) ser verdadeira, exprimir a realidade da empresa sendo coerente com as ações e ser possível de cumprir; b) ser complementada com a disponibilidade de recursos, liberação de recursos financeiros e de pessoal para que as diretrizes criadas sejam implementadas com o passar do tempo; c) ser válida para todos, ou seja, ser cumprida por todos que utilizam o ativo informação, sendo aplicada desde o presidente até o estagiário recém-contratado; d) ser simples, escrita com linguagem de fácil leitura e compreensão evitando termos técnicos e difíceis; e) comprometimento da alta administração da organização, a política deve ser assinada, explicitada e demonstrar total apoio da alta administração à política.

Muitos são os benefícios que a implantação de políticas de segurança da informação podem proporcionar à organização, desde que tenham sido criadas

adequadamente. Entre elas Ferreira e Araújo (2006, p.19-20) citam algumas relevantes, de acordo com o Quadro 1 abaixo.

Prazo	Benefício	Resumo
Curto prazo	Formalização	Formalização e documentação dos procedimentos de segurança adotados pela empresa.
	Controle de procedimentos	Implementação de novos procedimentos e controles.
	Acessos	Prevenção de acessos não autorizados, danos ou interferência no andamento dos negócios, mesmo nos casos de falhas ou desastres.
	Segurança no negócio	Maior segurança nos processos de negócios.
Médio Prazo	Padronização	Padronização dos procedimentos de segurança incorporados na rotina da empresa.
	Adaptação do negócio	Adaptação segura de novos processos do negócio.
	Qualificação em caso de incidentes	Qualificação e quantificação dos sistemas de respostas a incidentes.
	Conformidade	Conformidade com padrões de segurança, como a NBR/ISSO IEC 17799.
Longo Prazo	Retorno sobre investimento	Retorno sobre o investimento realizado, por meio da redução da incidência de problemas relacionados à segurança.
	Consolidação da imagem organizacional	Consolidação da imagem associada à segurança da informação.

QUADRO 1: BENEFÍCIOS GERADOS PELA IMPLANTAÇÃO DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DE ACORDO COM O PRAZO
FONTE: ADAPTADO DE FERREIRA E ARAÚJO (2006, p. 19-20).

A intenção de uma gestão através de políticas de segurança da informação é uma realidade, que comprovada pela literatura e pelos casos apresentados torna-se uma solução viável para os problemas apresentados pelo Hospital do Trabalhador.

2.2.1 Qualidade da informação

A segurança da informação objetiva assegurar a qualidade da informação nos atributos que se considera de extrema importância: confidencialidade, integridade e responsabilidade.

Entretanto, a qualidade é um conceito subjetivo e sujeito a múltiplas interpretações. Para Felix (2003, p. 38), “uma informação é considerada de qualidade quando os dados são completos (princípio da completeza) e quando o processo utilizado para transformar esses dados em informação é eficiente”. Comprova-se então, que a informação de qualidade requer o envolvimento de outros atributos, sendo que esses precisam atuar em perfeita sincronia para que não se desvirtue o princípio da qualidade.

As questões relacionadas à qualidade da informação tornaram-se primordiais no contexto das organizações, pois se tratam de um recurso que consiste em gerar e divulgar somente informações confiáveis. O fato de que alguma coisa possui qualidade permite a ela se destacar em meio às atividades similares (FELIX, 2003, p. 30-31).

Os atributos de qualidade podem ser definidos de diversas maneiras. Conforme descrito por Sêmola (2003, p.45) tem-se que confidencialidade trata da informação a ser protegida de acordo com o grau de sigilo exigido pelo seu conteúdo; integridade trata da necessidade de manter a informação com a mesma condição em que foi disponibilizada pelo seu proprietário, preservando o documento contra alterações; e disponibilidade diz respeito à necessidade de manter toda informação gerada ou adquirida, disponível para seus usuários no momento em que eles necessitarem e independente da finalidade.

A Fundação Nacional da Qualidade - FNQ (2007, p.17-18) descreve os itens que compõe a qualidade das informações de forma mais detalhada, embora similar. Para eles a confidencialidade das informações abrange o estabelecimento de políticas contra acessos não autorizados, feitos por meio de senhas, dispositivos de reconhecimento do usuário e ferramentas que tenham a mesma finalidade, sendo que a classificação é feita por meio de regras de classificação através das quais os usuários são distribuídos conforme o seu nível de permissão. Já a integridade se relaciona com o uso de informações corretas e confiáveis que buscam a exatidão e integridade das informações e dos métodos de processamento. Isso é feito por meio

de verificação de autenticidade, consistência e exatidão dos dados, controle de arquivos e modificações e inspeção de qualidade nos suportes que contém informação. A disponibilidade procura garantir que aqueles que têm acesso a informação sempre a tenham quando necessitarem. Esse acesso pode ser garantido através de sistemas on-line, canais de acesso via internet, disponibilização de computadores e dispositivos de acesso remoto e mecanismos de pronto restabelecimento de acesso em caso de descontinuidades.

Para garantir que a informação possua a qualidade desejada, é fundamental compreender os processos no seu ciclo de vida. Para Sêmola (2003, p.9) é durante esse ciclo que a informação é colocada em risco, pois é nesse momento que os ativos físicos, tecnológicos e humanos fazem uso da informação.

O mesmo autor ainda define quatro momentos em que é necessário aplicar qualidade para garantir a segurança, são eles: a) Manuseio – momento no qual a informação é criada e manipulada; b) Armazenamento – momento no qual a informação é armazenada, independente do suporte; c) Transporte – momento no qual existe a transferência das informações independente do meio de envio; e d) Descarte – momentos no qual se elimina a informação que não é mais desejada.

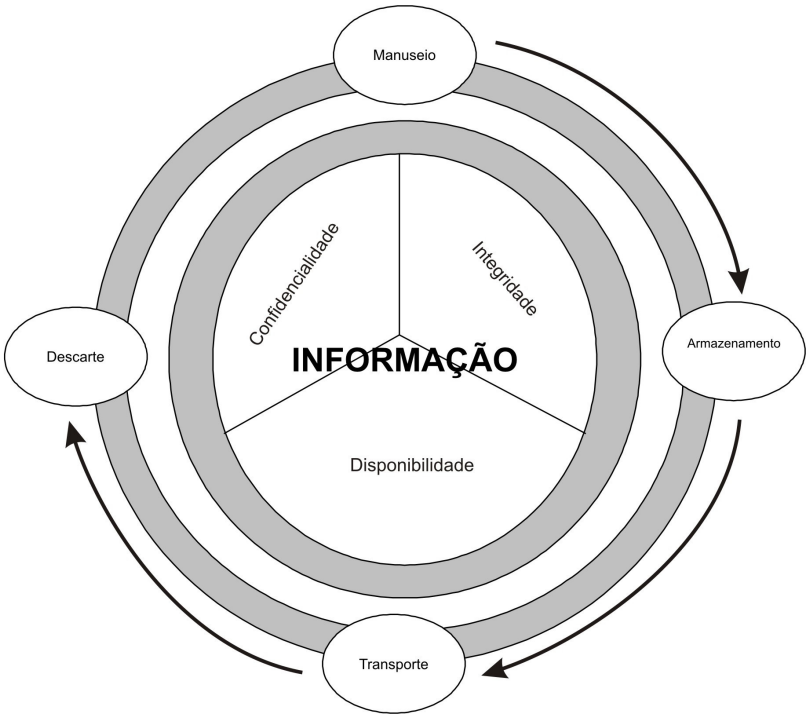


FIGURA 1: QUATRO MOMENTOS DO CICLO DE VIDA DA INFORMAÇÃO, CONSIDERANDO OS CONCEITOS BÁSICOS E OS ASPECTOS COMPLEMENTARES
FONTE: SÊMOLA (2003, p.11)

Além de garantir que durante o ciclo de vida da informação ele sempre atinja a qualidade, também é importante destacar que existem outros atributos que cooperam para que a tão desejada qualidade não se perca no caminho e/ou seja, encontrada insatisfatoriamente. A seguir será representado um quadro que aborda outras três dimensões da qualidade da informação, tempo, conteúdo e forma.

Dimensão	Atributo	Resumo
Tempo	Prontidão	A informação deve ser fornecida quando necessária.
	Aceitação	A informação deve estar atualizada quando for fornecida
	Freqüência	A informação deve ser fornecida todas as vezes que forem necessárias.
	Período	A informação pode ser sobre períodos e instantes do presente, passado ou futuro.
Conteúdo	Precisão	A informação deve estar isenta de erros.
	Relevância	A informação deve estar relacionada às necessidades do seu receptor específico, para uma situação específica.
	Integridade	Toda a informação que for necessária deve ser fornecida.
	Concisão	Apenas a informação que for necessária deve ser fornecida.
	Amplitude	A informação pode ter um alcance amplo ou reduzido, um foco externo ou interno.
	Desempenho	A informação pode revelar desempenho pela mensuração das atividades concluídas, dos progressos realizados ou dos cursos acumulados.
Forma	Clareza	A informação deve ser fornecida de uma forma fácil de ser compreendida.
	Detalhe	A informação deve ser fornecida na forma normal, detalhada ou resumida.
	Ordem	A informação deve ser organizada em uma seqüência predeterminada.
	Apresentação	A informação deve ser apresentada na forma narrativa, numérica, gráfica ou outras.
	Mídia	A informação deve ser fornecida na forma de documentos em papel impresso, monitores de vídeo ou outras.

QUADRO 2: DIMENSÕES DA QUALIDADE DA INFORMAÇÃO
FONTE: FELIX (2003, p. 37-38)

Em se tratando da gestão da segurança da informação, a preocupação mais recorrente é a qualidade da mesma, que é indispensável nos prontuários médicos e relevante para destacar o prejuízo que sua falta pode causar, por exemplo, a vida.

2.3 PRONTUÁRIO MÉDICO

O prontuário médico é a ferramenta principal do presente estudo. Para isso é de fundamental importância compreender seu significado, como é composto e as preocupações com relação à sua utilização.

Para Houaiss e Villar (2004, p.601), prontuário pode ser definido como “manual de informações úteis ou ficha com dados de alguém”.

Apesar da imprecisão da definição desse conceito, pode-se entendê-lo como o conjunto de documentos padronizados e ordenados, no qual são registrados os cuidados profissionais prestados aos pacientes. É também o meio que atesta a assistência médica prestada, seja particular ou de uma instituição, considerado repositório do segredo médico do paciente (CONSELHO REGIONAL DE MEDICINA DE SANTA CATARINA, 2000).

Pela Resolução n.º 1.638/02 do Conselho Federal de Medicina, prontuário pode ser definido como “documento único, constituído de um conjunto de informações, sinais e imagens registrados, gerados a partir de fatores, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilitam a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo”.

Além da sua característica como documento legal, o prontuário serve a outras áreas para diversas atividades, tais como: consulta, avaliação, ensino, pesquisa, auditoria, estatística médico-hospitalar, sindicâncias, investigações epidemiológicas, processos éticos e legais, defesa e acusação, entre outros (CONSELHO REGIONAL DE MEDICINA DO DISTRITO FEDERAL, 2006, p. 11). Todas essas atividades são constituídas com base em prontuários de qualidade, pois aqueles que não apresentam essa característica não são úteis em casos, como por exemplo, pesquisas científicas, por não fornecerem os dados mínimos necessários. Assim, manter a segurança das informações em todas essas fases é uma preocupação, pois sem isso é impossível assegurar a veracidade de seus conteúdos.

Prontuários médicos devidamente criados e utilizados proporcionam benefícios para todos os envolvidos: a) para o paciente, ao possibilitar atendimento e tratamento mais eficiente, já que seus históricos de atendimento estão registrados; b) para o médico, ao proporcionar melhor qualidade no atendimento, e além de

prova documental em caso de tramitações nos conselhos de classe e tribunais de justiça; c) para a instituição assistencial e os poderes públicos, pois constitui defesa legal e demonstra a qualidade do atendimento que está sendo oferecido; d) para o ensino e a pesquisa é a possibilidade de revisão dos casos, facilitando estudos e diagnósticos; e e) para a equipe assistencial permite mais interação entre os profissionais que estão acompanhando o paciente em seu tratamento diário e como instrumento de comunicação (CONSELHO REGIONAL DE MEDICINA DO DISTRITO FEDERAL, 2006, p. 11-12).

A segurança da informação se torna um fator de preocupação ainda mais relevante quando afeta o caráter sigiloso concedido ao prontuário por lei. Por meio do Código de Ética Médica, criado pela Resolução n.º 1.246/88, é possível verificar no artigo 11 que cabe ao médico manter o sigilo das informações sobre o paciente que tiver conhecimento durante o desenvolvimento de sua profissão.

Dessa forma, é possível perceber que tanto o médico como os que têm acesso são responsáveis por manter a qualidade das informações constantes nos prontuários médicos, e que cabe aos mesmos desenvolver critérios que mantenham essas informações seguras.

Um prontuário médico é composto por um conjunto de documentos. Conforme o Conselho Regional de Medicina do Distrito Federal (2006, p.24-26), compõem os prontuários os seguintes elementos:

a) capa ou envelope do prontuário;
b) ficha de identificação do paciente;
c) formulário ou pauta de diagnósticos;
d) folha de anamnese e exame físico;
e) ficha de pronto-socorro;
f) formulário de internação e alta;
g) ficha obstétrica;
h) ficha de recém-nascido;
i) ficha de odontologia;
j) folhas de evolução do paciente;
k) folhas de pedidos de parecer;
l) guias e relatórios de encaminhamentos;
m) laudos de exames complementares;

n) folhas especiais de procedimentos terapêuticos (ficha de desenvolvimento e crescimento, ficha de hemodiálise, relatório de quimioterapia, relatório de radioterapia, ficha de diálise peritoneal, ficha de nutrição parenteral);
o) ficha de descrições cirúrgicas;
p) ficha anestésica;
q) folhas de prescrição;
r) relatório de enfermagem, folhas de prescrição e de informações de enfermagem e folhas de dados vitais (temperatura, pulso e respiração), balanço hídrico, eliminações;
s) relatório de profissionais não-médicos (assistente social, farmacêutico, estomatorapeuta, fisioterapeuta, fonoaudiólogo, nutricionista, ortoptista, ortesista, pedagogo, psicólogo, terapeuta ocupacional);
t) atas de esterilização (vasectomia e ligadura tubária);
u) folhas de resumo de alta, de óbito ou de transferência;
v) relatório de necropsia e cópia da declaração de óbito;
w) ficha de controle de infecção hospitalar;
x) folha de termo de consentimento livre e esclarecido.

2.4 CULTURA ORGANIZACIONAL

A cultura organizacional é algo criado de forma intrínseca pela própria organização durante o seu desenvolvimento. De maneira geral, Medeiros Filho (1992, p.25) define que se trata de uma combinação dos elementos que compõe a organização: filosofias, valores, processos, usos, costumes e comportamentos, formais ou não, que distingue a organização de qualquer outra, tornando-a única.

De acordo com Houaiss e Villar (2004, p.204) cultura pode ser entendida como um “conjunto de padrões de comportamento, crenças, costumes, atividades, etc. de um grupo social”, de forma que se pode realmente perceber esses hábitos dentro das empresas.

Pensando em cultura sob o ponto de vista antropológico, Freitas (1991, p.3) afirma que se trata de “um sistema de cognições compartilhadas” e que “a mente humana gera cultura pelo significado de um número finito de regras”.

Organicamente, a cultura pode ser entendida como uma variável interna, já que as organizações são instrumentos que produzem tanto bens, serviços e produtos como artefatos culturais distintos, caracterizados como rituais, lendas e cerimônias (FREITAS, 1991, p.5).

Schein *apud* Freitas (1991, p.7) define a cultura organizacional como um modelo de pressupostos inventados ou descobertos por determinado grupo durante o seu processo de aprendizagem e que tem a finalidade de permitir a adaptação a problemas externos e integração interna. Os demais membros que passem a incorporar esse grupo são ensinados a agir segundo tal pressuposto, tendo em vista que ele foi validado pelos primeiros.

A cultura organizacional pode ser encarada por diferentes visões, no entanto todas convergem, pois a consideram como um conjunto de determinadas características. De modo similar pode-se perceber que a cultura organizacional é formada por uma base de padrões e premissas que determinado grupo inventou, descobriu ou desenvolveu durante seu processo de aprendizagem de resolução de problemas e adaptações, sendo que o que foi considerado satisfatório é ensinado a novos membros desse processo, fazendo com que todo o grupo perceba, pense e sinta de forma similar em relação a determinada situação (SCHEIN *apud*. ZAVAREZE, 2008, p. 2).

A cultura organizacional é formada por três subdivisões, são elas: 1) artefatos e criações, modelos de comportamento visíveis e audíveis aos membros do grupo; 2) valores, que o grupo possui, compartilha entre si e considera como de alto grau; 3) pressupostos básicos e crenças, elementos próprios da atividade humana que são invisíveis ao grupo, mas que anteriormente já os era consciente, ou sinônimos daquilo que é tido como verdadeiro dentro da organização (SCHEIN *apud*. FREITAS, 1991, p.8-20).

O processo de criação da cultura de uma organização tem início, na maioria dos casos, com o fundador da mesma, já que é ele quem exerce maior influência durante esse processo inicial. É ele também que constitui a base, a partir da qual a empresa enfrentará as primeiras dificuldades e aprenderá com o seu êxito, aceitando instintivamente suas decisões como adequadas. Já a manutenção da cultura de uma organização centraliza-se nas áreas de recursos humanos, pois consistem em canais que materializam a consciência interna da cultura (ANZIZU *apud*. FREITAS, 1991, p.86-92).

No entanto, essa mesma cultura é o que dificulta, e às vezes até impede, o desenvolvimento da organização, pois quando a cultura já está estabelecida cria-se uma política de estabilidade. De acordo com Medeiros Filho (1992, p.23) independente da mudança que venha a ser proposta, estrutural, gerencial ou de processos operacionais, normalmente a receptividade não acontece, pois se tratam de pessoas com dificuldade para aceitar inovações e criatividades e que preferem se manter acomodadas.

Mas, para que a política de segurança seja aplicável é importante pensar no processo de implantação, que pode mudar radicalmente os procedimentos até então adotados e, consequentemente, a cultura da organização.

Freitas (1991, p.115) define mudança de cultura como “um outro rumo, uma nova maneira de fazer as coisas, alicerçada em novos valores, símbolos e rituais”.

A mudança de cultura dentro de qualquer instituição é um processo que requer planejamento, e para que isso ocorra é importante observar a necessidade de um consenso entre os envolvidos, pois é um processo que não é simples e nem barato e que sempre deixa alguns traumas como conseqüências. Ainda é necessário perceber que a mudança de cultura implica em diversos outros fatores, tais como estratégia, estrutura, habilidades e principalmente procedimentos. Sabe-se também que não é toda alteração de comportamento que implica em mudança de cultura organizacional (FREITAS, 1991, p. 115).

Para que o resultado desejado seja alcançado durante um processo de transformação de cultura é necessário que alguns cuidados básicos sejam adotados, assim como descreve Freitas (1991, p.117):

a) reconhecer a necessidade de um consenso entre os envolvidos e que as pessoas são resistentes à mudança por gerar ruptura nos seus padrões, mas que são essas que exercem a maior influência durante a construção do consenso;
b) exprimir e enfatizar a confiança (de mão dupla) em todos os assuntos relacionados com a mudança;
c) pensar na mudança como a construção de habilidades e concentrar no treinamento uma parte importante do processo;
d) dar tempo para que as pessoas se acostumem e consolidem a mudança;
e) encorajar as pessoas a se adaptarem à idéia básica de que a mudança se ajusta ao mundo real que as rodeia.

Mas para que a mudança de cultura seja um fato real dentro dar organizações e produza a transformação desejada é preciso que as justificativas de comportamento sejam ajustadas e bem fundamentadas, caso contrário as pessoas continuarão apegadas aos padrões e crenças anteriores (FREITAS, 1991, p.117).

3 METODOLOGIA

A pesquisa foi realizada por meio do método dedutivo, pois, de acordo com Lakatos (1992, p.106), esse é um método que parte de teorias e leis e recorre a fenômenos particulares, encaixando-se com a proposta da pesquisa, que é por meio do conhecimento da teoria estudar uma área específica de segurança da informação aplicada a um setor específico.

Para a utilização de tal método foi aplicada uma técnica de forma a alcançar o resultado pretendido. A técnica foi a de observação direta intensiva, que compreende a observação dos procedimentos utilizados no dia a dia e a entrevista das pessoas envolvidas com esses procedimentos para compreender a utilização das informações (LAKATOS, 1992, p. 107).

A fim de alcançar o objetivo principal desse trabalho as atividades foram divididas em alguns tópicos.

O início das atividades de compreensão do campo escolhido para estudo se deu com a revisão de material bibliográfico e apontamentos das informações relevantes. Nesse processo foi realizada uma intensa pesquisa, tanto em suportes físicos quanto na internet para levantar todo o material que se caracteriza relevante para a fundamentação teórica da pesquisa. Durante essas atividades é que o campo de pesquisa foi delimitado, mediante verificação das potencialidades de pesquisa.

Após as leituras procedeu-se a identificação do foco de estudo. Isso foi possível por meio de leituras e conversas com profissionais mais experientes. Conversar e pesquisar foi fundamental para alinhar o pensamento inicial de desenvolvimento do projeto com a realidade. Tais pensamentos e arguições foram relevantes para entender o que significa estudar uma grande área como a de saúde, e que pode se tornar inviável em alguma parte do processo. Demonstrando a necessidade de recorte no trabalho, voltando-se a pesquisa para pequena faixa que compõe esta área de conhecimento. Após a definição da área de conhecimento do estudo, um complicador foi delimitar exatamente como a pesquisa seria realizada, já que outros campos de pesquisa estavam disponíveis. Nesse momento decidiu-se pelo estudo das áreas mais próximas aos prontuários médicos, por ser esse o momento no qual ocorrem os maiores incidentes de segurança da informação.

Para a criação de políticas de segurança da informação é necessário conhecer o modelo a se adotar e saber como cada uma das metodologias pode ser

aplicada nos diversos campos de atuação. Pensando nisso, é que se procedeu a identificação do possível modelo de política de segurança da informação a ser utilizado para o caso específico de estudo. A identificação foi realizada por meio da verificação dos diversos modelos existentes. A partir disso e da observação do ambiente, constatou-se a necessidade de uma política de segurança da informação clara e consistente, entendendo quais os melhores modelos para o caso de estudo.

Para fazer a coleta de informações no ambiente de estudo foram dedicadas várias manhãs de observação junto às pessoas responsáveis pelos setores estudados, sendo eles maternidade, ambulatório, faturamento, serviço de prontuário do paciente, pronto socorro e postos de internação. Como resultado, foram produzidos fluxogramas contendo todas as descrições das atividades realizadas pela organização quanto à utilização dos prontuários médicos, sendo que esses tiveram apenas a função de retratar os procedimentos adotados atualmente no ambiente, não sendo adotado para tanto uma metodologia específica e não recebendo ênfase por não se tratar do objetivo da pesquisa. Após a confecção, todos os fluxos foram aprovados pelas pessoas que forneceram as informações, dando credibilidade às informações coletadas. Apenas no fluxo que se refere aos postos de internação é que as informações foram generalizadas para todos os postos no qual pode ocorrer internação, isso se deve ao fato de que não foi permitido o acesso a todos eles para verificação de suas peculiaridades, mas de acordo com informações recebidas todos os postos procuram seguir a mesma linha de atuação.

Após a obtenção de todas as informações no ambiente de estudo, iniciou-se a construção das políticas de segurança da informação. Nesse processo foi preciso analisar detalhadamente os fluxos, pois além de propor novas políticas também foi necessário descrever os cuidados já existentes na organização que não estavam registrados em nenhum documento formalizado.

Optou-se pelo desenvolvimento de uma política baseada no modelo disponibilizado por Ferreira e Araújo (2003, p. 57-113) e na NBR ISO/IEC 17799:2005, abordando os tópicos que foram julgados necessários para atender as peculiaridades percebidas e os objetivos propostos. Para compor o corpo da política, foram escolhidos os tópicos que mais se aplicam ao ambiente de estudo, assim elencou-se como essencial apresentar introdução, criação e atuação de um Comitê de Segurança, utilização dos recursos de tecnologia da informação, utilização dos

recursos de informação, controle de acesso físico, gerenciamento de incidentes de segurança, manutenção da política e aprovação da alta gerencia.

Para que a política seja viável e implantada, os passos necessários para a implantação foram contemplados em um capítulo específico, sendo que essa ficaria a cargo do Comitê de Segurança e para isso seriam adotados o treinamento e a divulgação como pontos chave. Embora não seja necessário empenhar esforços inexistentes, a implantação precisa seguir alguns passos simples e a partir disso será possível garantir que sempre que for adequadamente utilizada a política poderá gerar benefícios à instituição.

Quanto às preocupações com a manutenção da política, foi importante pensar no quanto as informações se transformam, bem como os modos de utilização, criação e disseminação da informação são modificados e o intuito de garantir que as políticas estejam sempre atuando em sincronia com as mudanças. Assim, a qualquer tempo ou em tempo determinado a política poderá ser alterada para atender às necessidades da organização.

Para dar credibilidade a política de segurança da informação desenvolvida foi necessário colher a opinião dos que estão atuando naquele local. Optou-se por incluir as pessoas que contribuíram no processo inicial de coleta de dados, por já estarem interadas na pesquisa e por se tratarem de pessoas estratégicas para a efetiva implantação das políticas. Também foram escolhidos esses profissionais em virtude de serem eles os mais atingidos com a criação de uma política e a alteração dos procedimentos de trabalho. Foram analisadas as respostas de cinco pessoas responsáveis por fornecer as informações de seus setores autorizadas por suas gerências a participar desse processo. Embora de grande importância a avaliação da diretoria não pôde ser realizada por falta de possibilidades para explicação da política, da pesquisa e de contato pessoal. Entretanto, as respostas dadas foram julgadas suficientes pela autora para a validação das políticas, tendo em vista que todas as pessoas que forneceram as informações responderam ao formulário.

Com o intuito de validar as políticas propostas, as pessoas que forneceram as informações responderam um Formulário de Validação da Política de Segurança da Informação (Apêndice I). Tal formulário foi elaborado com seis afirmações fechadas e uma aberta, às fechadas foram atribuídos pontos conforme a resposta dada, ficando da seguinte forma:

(1) Discordo totalmente

(2) Discordo parcialmente

(3) Indiferente

(4) Concordo parcialmente

(5) Concordo totalmente

Cada questionário poderia atingir até 30 pontos, sendo que o total de pontos foi calculado fazendo o somatório das respostas dadas.

A questão aberta teve a função de se tornar uma pequena declaração da pessoa com relação à política de segurança, criando uma espécie de breve depoimento de cada uma das pessoas.

Com o desenvolvimento de todas essas etapas foi possível elaborar uma política possível de ser implementada e que procurou preencher todas as lacunas existentes no ambiente de estudo, quanto à garantia de qualidade da informação e das políticas de segurança da informação.

4 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

As políticas de segurança da informação precisam ser compostas de acordo com as especificidades do ambiente e com padrões específicos, sendo de tal forma um documento de valor para a organização no qual estará inserido. Dessa forma, a seguir será apresentado o ambiente de estudo, como ocorre a utilização dos prontuários médicos nesse ambiente, identificando-se os proprietários da informação e suas interações com esse documento.

4.1 AMBIENTE DE ESTUDO

A aplicação do estudo relacionado às políticas de segurança da informação foi realizada no Hospital do Trabalhador de Curitiba, que se situa a Avenida Republica Argentina, nº 4406, no bairro Novo Mundo.

De acordo com o divulgado em seu portal, o Hospital do Trabalhador (HT) tem a missão de “Contribuir para a qualidade de vida do cidadão e da comunidade, desenvolvendo, em nível de excelência, ações de saúde voltadas a prevenção, assistência, reabilitação, ensino e pesquisa, nas áreas de trauma e emergência, saúde do trabalhador, materno-infantil e infectologia”, e apresenta como filosofia a prática de assistência de qualidade a seus pacientes, aliada as propostas de integração do ensino a estas ações.

Atualmente, apresenta uma estrutura organizacional, conforme apresentado no seu organograma (Figura 2), composta pela direção geral, direção técnica, direção acadêmica, direção administrativa, chefe do corpo médico, núcleo de informações e análise de situações e núcleo de epidemiologia e controle de infecção hospitalar. Outros órgãos estão ligados a cada uma das diretorias: diretoria administrativa, seções de recursos financeiros, gestão de pessoas, material e patrimônio, infra-estrutura operacional e apoio administrativo; diretoria acadêmica, centros de estudos, pesquisa e desenvolvimentos; diretoria técnica, seções de hotelaria hospitalar, serviço de enfermagem e técnica assistencial.

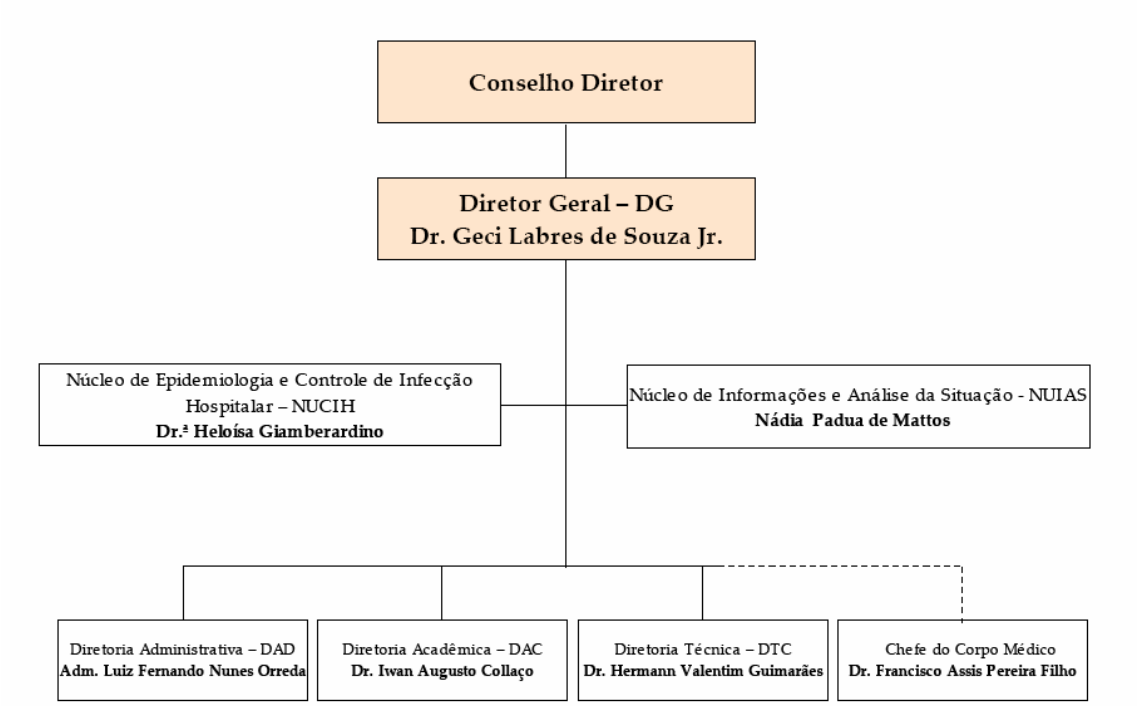


FIGURA 2: ORGANOGRAMA DO HOSPITAL DO TRABALHADOR
FONTE: HOSPITAL DO TRABALHADOR: RELATÓRIO DE ATIVIDADES 2007

Essa composição geral é subordinada ao Conselho Diretor, sendo esse último o responsável pela avaliação e autorização das diretrizes administrativas. É composto por 5 conselheiros, sendo dois representantes da Secretaria de Saúde do Estado do Paraná e Instituto de Saúde do Paraná (SESA/ISEP), um da Universidade Federal do Paraná (UFPR), um da Fundação da Universidade Federal do Paraná para o Desenvolvimento da Ciência, da Tecnologia e da Cultura (FUNPAR) e um da Secretaria Municipal de Saúde, com seus respectivos suplentes.

No entanto a composição do conselho só foi possível após a fixação dos convênios celebrados entre: o Governo do Estado do Paraná, a Prefeitura de Curitiba, a UFPR e a FUNPAR.

Por meio dessas parcerias foi possível dar um salto nos quesitos produtividade e qualidade dos serviços prestados, possibilitando ao Hospital do Trabalhador transformar-se em um Centro de Excelência no Atendimento aos Acidentados em geral. Também graças aos convênios ocorreu a implantação do Pronto-Socorro de Trauma.

Com o desenvolvimento das parcerias, aumentou-se o número de pesquisas na instituição. Para administrar essas pesquisas e principalmente os estágios

curriculares e extracurriculares é que em 1999 foi criado o Centro de Estudos, Pesquisa e Desenvolvimento Humano. Por meio dessa iniciativa o Hospital do Trabalhador passou a ser reconhecido pelo Ministério da Educação e da Cultura e pelo Ministério da Saúde como “Hospital Auxiliar de Ensino”.

Os convênios firmados não visavam apenas a concessão de títulos e reconhecimentos, mas também importante fonte para captação de recursos adicionais, evolução com os conhecimentos científicos e técnicos, flexibilidade na aquisição de pessoas, insumos e equipamentos e melhorias na estrutura física. No ano de 2007 a receita mensal média foi de R$ 4.382.944,40, sendo totalmente investida internamente.

Atualmente, o HT possui em seu quadro funcional aproximadamente 1500 funcionários, sendo que desses 286 são médicos e mais de 360 compõe o corpo de enfermagem. Tem capacidade instalada de 190 leitos para internação, divididos conforme o Quadro 3.

Trauma	64
Maternidade	35
Pediatria	30
Infectologia	16
UCIN*	10
UTI** Adulto	10
UTI** Neo	08
UTI** Pediátrica	02
Hospital Dia ***	15
Total	***190***

* Unidade de Cuidados Intermediários Neonatais
** Unidade de Terapia Intensiva
*** Unidade Inaugurada em Julho de 2007

QUADRO 3: DIVISÃO DOS LEITOS DE INTERNAÇÃO
FONTE: HOSPITAL DO TRABALHADOR: RELATÓRIO DE ATIVIDADES 2007

Atua no atendimento à Assistência de Saúde do Trabalhador e nas diversas áreas relacionadas ao Trauma e Emergência, com as seguintes especialidades: cirurgia geral, ortopedia e traumatologia, neurocirurgia, clínica médica, pediatria, anestesiologia, cirurgia de mão, cirurgia vascular, microcirurgia, urologia, cirurgia buxo-maxilo-facial, cirurgia plástica, cirurgia pediatria, cirurgia torácica,

otorrinolaringologia, terapia intensiva, obstetrícia, neonatologia, infectologia, medicina do trabalhador, patologia clínica, anatomia patológica, radiologia, ultrassonografia, endoscopia digestiva, endoscopia respiratória e pneumologia.

A história do HT foi iniciada em 1947 e até a atualidade vem sofrendo alterações em sua essência e em sua estrutura física, que constantemente é ampliada para atender a demanda. No Quadro 4 é possível acompanhar o seu desenvolvimento histórico, fornecido em uma linha do tempo.

ANO	ACONTECIMENTO
1947	Fundado o "Sanatório Médico-Cirúrgico do Portão" para atendimento a pacientes com tuberculose e doenças torácicas.
1980	Transformou-se em Hospital Geral do Portão e tornou-se referência no atendimento em infectologia e SIDA.
1994	Tornou-se o Hospital Geral Mauro Senna Goulart ao concluírem-se as obras de reforma e ampliação de capacidade instalada, iniciada 15 anos antes. São adquiridos diversos equipamentos para a sua ativação completa.
1995	Implantou-se o Serviço de Maternidade, recebendo em 15 de Fevereiro, o 1º bebê recém-nascido, iniciando o processo de reativação do hospital.
1996	Iniciaram-se as cirurgias de correção de defeitos congênitos da face em parceria com o Centro de Atendimento Integral ao Fissurado Lábio-Palatal/SESA/ISEP.
1997	Recebe a denominação de "Hospital do Trabalhador" com o estabelecimento da nova missão através do convênio celebrado em 17 de Agosto com o Governo do Estado do Paraná/Secretaria do Estado de Saúde, Prefeitura Municipal de Curitiba/Secretaria Municipal de Saúde, Universidade Federal do Paraná e Fundação da Universidade Federal do Paraná para o Desenvolvimento da Ciência, Tecnologia e Cultura. Estabeleceu-se o efetivo controle social através da instalação do "Conselho Deliberativo". Iniciou-se o Serviço de Cirurgia de Mão.
1998	Inaugurou-se o "Serviço de Trauma e Emergência" com o início do funcionamento do Pronto Socorro, das 4 salas do Centro Cirúrgico, da UTI de trauma adulto, das unidades de internamento adulto e infantil para o trauma, do ambulatório e do serviço de reabilitação de membros superiores.
1999	Foi cadastrado como Hospital de referência da "Rede Estadual de Urgência e Emergência do Paraná".
2000	Tornou-se "Hospital Amigo da Criança", título concedido pela UNICEF e Ministério da Saúde/BR. "Centro Colaborador do Ministério da Saúde para a Qualidade da Gestão e Assistência Hospitalar". "Hospital Auxiliar de Ensino" passando a receber os recursos do FIDEPS.
2001	Implantou-se a UTI Neonatal e Pediátrica. O hospital foi inserido no cadastro em Alta Complexidade de Neurocirurgia Nível II/SUS/MS. Passou a atuar como sede da base da Rede Paraná Urgência (UTI Móvel).
2002	Recebeu licença sanitária dentro do Programa PASES/Secretaria Municipal de Saúde. Recertificação como "Centro colaborador do Ministério da Saúde para a Qualidade da Gestão e Assistência Hospitalar". Cadastro em Alta Complexidade de Ortopedia e Traumatologia. Certificação do "Programa de Humanização Hospitalar" do Ministério da Saúde. Iniciou-se o atendimento das doenças ocupacionais.
2003	Recebeu a licença ambiental.
2005	Hospital do Trabalhador recebe a Certificação como Hospital de Ensino através da Portaria Interministerial n. 862/ Ministério da Saúde e da Educação, publicada no Diário Oficial da União, Seção 1, n.109 / 09 de Junho de 2005.

QUADRO 4: LINHA DO TEMPO HISTÓRICA DO HOSPITAL DO TRABALHADOR
FONTE: ADAPTADO DO PORTAL DO HOSPITAL DO TRABALHADOR

Sabe-se que o número de atendimentos do hospital aumentou com o passar dos anos, e que demandou ampliação da estrutura para atendimento (Gráfico 1). Em paralelo, houve aumento no número de cirurgias (Gráfico 2). Segundo o próprio hospital, o crescimento foi devido às parcerias e aos investimentos realizados.

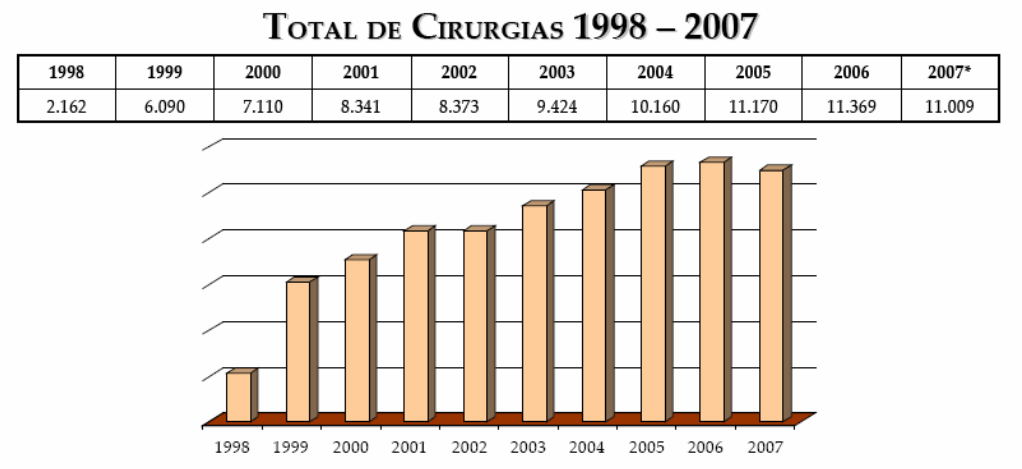


GRÁFICO 1: EVOLUÇÃO DOS ATENDIMENTOS
FONTE: HOSPITAL DO TRABALHADOR: RELATÓRIO DE ATIVIDADES 2007

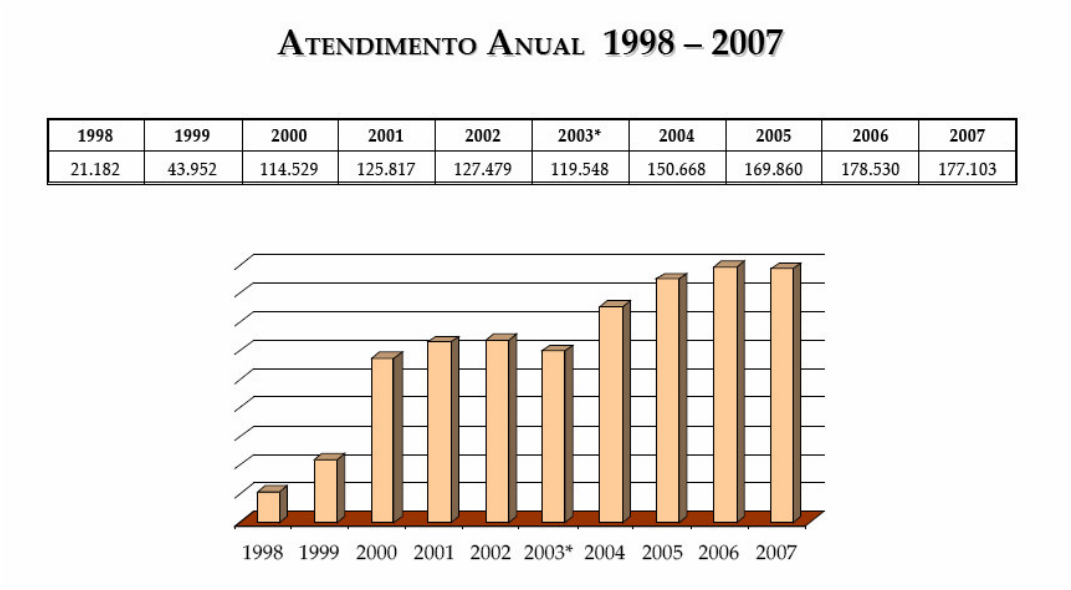


GRÁFICO 2: EVOLUÇÃO DAS CIRURGIAS
FONTE: HOSPITAL DO TRABALHADOR: RELATÓRIO DE ATIVIDADES 2007

Para garantir que o atendimento seja fornecido ao paciente com melhor qualidade e para continuar sendo reconhecido no meio em que atua é que o Hospital do Trabalhador implantou a Comissão de Controle de Infecção Hospitalar/Serviço de Controle de Infecção. Esse setor tem a função de desenvolver ações deliberadas e sistemáticas para a redução mínima possível da incidência das infecções hospitalares.

A Comissão de Controle de Infecção Hospitalar do Hospital do Trabalhador tem atuado em várias frentes a fim de envolver todos os profissionais na conscientização sobre a importância desse controle para o aprimoramento da qualidade assistencial. Em média são realizadas 250 avaliações mensais por esta equipe nos pacientes hospitalizados e 10 treinamentos e atendimentos de avaliações em geral.

4.2 UTILIZAÇÃO DO PRONTUÁRIO MÉDICO NO AMBIENTE DE ESTUDO

O Hospital do Trabalhador, como uma instituição de saúde pública, atua dentro dos padrões pré-estabelecidos pela legislação e com comandos rígidos quanto à atuação com seus prontuários médicos. Entretanto, suas informações ainda permanecem expostas a erros constantes.

Tal afirmação se deve ao fato de que não existe dentro da instituição documentos oficiais que descrevam os procedimentos que devem ser adotados nas diversas áreas pelas quais ocorre a manipulação dos prontuários.

Informações obtidas junto aos funcionários nos permitem concluir que são recorrentes as descrições de que com frequência acontecem incidentes com os prontuários médicos e, consequentemente, com as informações. Foram observadas ocorrências de perdas de prontuários médicos por meio de empréstimos e retiradas sem autorização, perda de folhas importantes, o encontro de documentações de pacientes em setores mesmo depois de o paciente ter recebido alta, entre outros.

Além disso, também pode ser percebido que a falta de um documento formal insere barreiras ao desenvolvimento das atividades. Não há nenhuma ferramenta para treinamento, e todos os funcionários conhecem o funcionamento das atividades devido à cultura do “sempre fizemos assim”. Percebe-se também que no caso de um

eventual engano todo o processo pode ser comprometido, sendo que todos estão sujeitos a isso, principalmente novos colaboradores que ainda precisam se adaptar à cultura em que é inserido.

Por mais que a preocupação seja com a qualidade das informações e o perfeito manuseio dos prontuários esteja presente nos colaboradores, nenhum deles recebeu treinamento adequado sobre as restrições e as disposições com relação ao assunto.

Dentro da instituição o prontuário médico está presente em quase todos os setores, sendo em partes ou como um todo, exceto naqueles relacionados aos serviços gerais de suporte ao atendimento. Com isso, a possibilidade de novos incidentes fica ainda mais evidenciada.

Para fins desse estudo foram verificados os processos de utilização dos prontuários médicos nos Postos de Internação, entendendo-se por postos de internação todos os setores nos quais há alojamento de pacientes para tratamento, no Ambulatório, na Maternidade, no Pronto Socorro, no Faturamento e no Serviço de Prontuário do Paciente (SPP).

Foi possível identificar como proprietários da informação os médicos, os fisioterapeutas, a equipe de enfermagem e os colaboradores de nível administrativo do faturamento e do serviço de prontuário do paciente. Aos outros funcionários cabe apenas o “saber” das informações geradas por si mesmos.

Todos os proprietários da informação têm acesso ao prontuário para inserção e consulta de informações, no entanto a partir do momento em que o prontuário é encaminhado ao SPP somente pessoas autorizadas passam a ter acesso às informações, sendo as procuras submetidas a registro.

Quanto à utilização dos prontuários médicos nos serviços de emergência, Pronto Socorro e Maternidade, percebe-se que as informações são preenchidas corretamente e dentro dos padrões utilizados, não existindo erros graves, mas a preocupação consiste no fato de que a caligrafia utilizada, em alguns casos, não permite a compreensão dos dados ali depositados, de modo que se prejudica a qualidade das informações. Quando existe a necessidade de encaminhamento do paciente para outros setores de hospital não se verificou falhas, entretanto em alguns momentos o prontuário médico foi encaminhado incompleto ou não juntamente com o paciente.

No faturamento e no SPP os prontuários médicos são utilizados com seriedade e rigor, pois cabe a esses setores responder pelo extravio de algum documento que compõe o prontuário. Nesses identificou-se que esporadicamente acontecem incidentes, como a perda de um prontuário ou problemas no faturamento devido à falta de documentos, conforme relatado pelos funcionários. Os tipos de documentos que têm maior índice de extravio são os de exames e altas, documentos similares a formulários, pois apresentam dimensões pequenas e gramatura reduzida.

Já nas atividades do ambulatório, o maior incidente percebido foi a falta ou sobra de prontuários no momento dos atendimentos e a mistura de exames, pois em alguns casos eles estão anexados aos prontuários e em outros eles são levados pelos próprios pacientes. Quando da necessidade de internação do paciente que se dirige ao ambulatório, os procedimentos são realizados com falhas quase imperceptíveis. Normalmente, todos os documentos são encaminhados corretamente. As falhas percebidas foram a de falta de informações nas fichas de encaminhamento de pacientes e de erros quanto ao número do tipo de procedimento.

Quando os pacientes não necessitam de internação foram notados problemas como a falta de dados em documentos que compõe o prontuário ou a falta dos mesmos.

Dessa forma pode-se perceber que as informações são bem direcionadas dentro da instituição apontando como principal barreira a falta de normatização dos procedimentos.

4.3 DESCRIÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PROPOSTA

A política de segurança da informação proposta para o Hospital do Trabalhador (Apêndice G) foi desenvolvida visando atender a todas as falhas de segurança da informação percebidas naquele local. Também teve o objetivo de criar um documento formal com as políticas que já são adotadas pela instituição.

A base das políticas criadas se deu de acordo com as instruções disponibilizadas por Ferreira e Araújo (2006) através do livro Políticas de Segurança da Informação e também da norma da ABNT, a NBR ISO/IEC 17799:2005.

A política proposta procurou abordar outros itens além dos relacionados às informações do prontuário por considerar que são relevantes para a garantia da integridade das informações constantes nesse documento. Assim a política de segurança da informação é composta pelos seguintes capítulos:

1) Introdução – breve descrição do que se caracteriza como política de segurança da informação, sua abrangência, seu objetivo e o posicionamento da instituição quanto às informações;
2) Comitê de segurança – capítulo que descreve a importância da implantação de um comitê de segurança da informação, caracterizando sua composição, atribuições e atividades esperadas desse órgão;
3) Utilização dos recursos de tecnologia da informação – descreve as políticas adotadas pela organização quanto aos recursos disponibilizados para os colaboradores, abrange as restrições, as responsabilidades de cada um, as implicações e a utilização desse recurso para prevenir incidentes de segurança da informação;
4) Utilização dos recursos de informação – nesse capítulo foram descritas todas as políticas adotadas quanto à utilização dos prontuários médicos em todas as áreas analisadas. Foram descritos as restrições, os acessos, as consultas, as permissões, o manuseio e as ações a serem seguidas pelos setores envolvidos;
5) Controle de acesso físico – descrição de todos os cuidados necessários para o controle do acesso a organização, tanto para colaboradores da organização quanto para prestadores de serviços e visitantes;
6) Gerenciamento de incidentes de segurança – breve descrição das características de um incidente de segurança, bem como das atribuições dos colaboradores e do comitê frente a desrespeitos da política de segurança da informação. Aborda também as responsabilidades no julgamento de incidentes e as punições que podem ser aplicadas;
7) Manutenção da política – esse capítulo descreve todos os procedimentos necessários para que a política esteja sempre revista e em conformidade com

novas legislações e mudanças organizacionais, prevê períodos de atualização e as atividades ligadas a essa atualização;

8) Aprovação da alta gerência do Hospital do Trabalhador – descreve a ciência da organização quanto às políticas, sua vigência e seu apoio as mesmas.

Todos os capítulos criados abordaram conteúdos percebidos como críticos por meio da análise dos fluxogramas construídos (Apêndices A, B, C, D, E e F).

4.4 IMPLANTAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O processo de implantação das políticas de segurança da informação passa por diversos fatores que devem ser observados, dentre eles o impacto gerado na ruptura da cultura organizacional adotada até o momento.

Sugere-se designar ao Comitê de Segurança a ser criado, a responsabilidade pelos passos e decisões do processo de implementação das políticas de segurança da informação.

Para que seja possível implantar, é necessário que sejam feitas divulgações internas da nova política a ser adotada, treinando todas as chefias inicialmente, pois são elas que replicam as informações e cobram a efetiva utilização. Posteriormente os colaboradores, por serem os usuários diretos da informação e entenderem essa atitude como motivadora, transmitindo a importância da atuação conjunta. O treinamento deve ter um caráter de conscientização e se tornar de conhecimento de todos, fazendo com que exista uma disseminação formal das informações.

Para a divulgação formal deve ser elaborado um material promocional que seja replicado a toda a organização, permitindo que todos tenham conhecimento pleno das novas diretrizes. Esse material de divulgação deve ser disponibilizado na Intranet e em jornais e folhetos internos, e também se recomenda que nesses meios sejam divulgadas outras informações relacionadas à política de segurança da informação, mantendo o colaborador ciente dos acontecimentos quanto a esse tema.

Para que não exista indisponibilidade de informações por falta de acesso, a política de segurança da informação deve ser vinculada a um formato de manual

básico, compacto e com linguagem acessível, disponibilizado na Intranet da instituição e impresso.

Com esses cuidados básicos pode-se assegurar que não haverá rupturas intransponíveis na cultura organizacional, garantindo conforme relata Freitas (1991) a confiança, pois todos conhecerão e atuarão em conformidade com as atividades aprovadas; mudança, pois terão sido treinados e instruídos no novo processo, conscientizando-se de sua atuação nessas mudanças; tempo de adaptação, já que os colaboradores passarão por treinamento para então assimilar e consolidar em si as novas mudanças; e encorajamento, devido ao conhecimento e entendimento daquilo que se espera que realize e da importância que possui dentro do processo de adaptação do novo conceito a ser aplicado na instituição.

Executando-se todos os passos estabelecidos para a implantação das políticas de segurança da informação, é possível afirmar que as chances de sucesso são muito maiores. Mas, além disso, o processo de implantação também precisa estar aliado ao de manutenção, já que no momento em que se passa a colocar em prática as políticas algumas alterações podem ser realizadas, necessitando atuação conjunta.

Por fim, para se assegurar que a política foi compreendida e será utilizada por todos os envolvidos no processo de utilização dos prontuários médicos, é necessário que se aplique após o treinamento o Formulário de Validação das Políticas de Segurança da Informação (Apêndice H). De tal forma, por meio da análise das respostas é possível verificar a necessidade de qualquer modificação nas políticas, do entendimento e conscientização adquiridos, permitindo que após essa análise concluam-se as alterações necessárias e a organização como um todo passe a atuar de forma consciente e adequada à segurança de suas informações.

4.5 MANUTENÇÃO DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Para que a política de segurança da informação esteja sempre em conformidade com as atividades desenvolvidas e vividas pela organização em todos os momentos, é necessário que exista um processo contínuo de manutenção (adaptações, alterações, inclusões e exclusões).

De acordo com Ferreira e Araújo (2006, p.125) a manutenção periódica das políticas tem o objetivo de mantê-las atualizadas frente a novas tendências, tecnologias e acontecimentos.

De acordo com o que foi estabelecido na política (Apêndice G) o intervalo médio proposto para a realização da manutenção é de um ano. No entanto nada impede que em todos os momentos nos quais forem percebidos ou informados novos fatos que impactem a política, ocorram alterações. Recomenda-se que fatos esporádicos não prejudiquem a manutenção anual, pois anualmente são revistos todos os procedimentos e não apenas casos isolados.

A responsabilidade pela manutenção das políticas de segurança da informação é do Comitê de Segurança. Entretanto, todos os colaboradores envolvidos devem estar atentos, pois compõem o quadro dos proprietários da informação. Aos colaboradores, são disponibilizadas duas formas de intervir no processo de manutenção das políticas. Primeiramente o Formulário de Solicitação de Alteração da Política de Segurança da Informação (Apêndice I), em papel, que pode ser requisitado ao Comitê de Segurança e também em meio eletrônico via Intranet.

Sempre que a política de segurança da informação sofrer alterações, essas deverão ser avaliadas e autorizadas pela diretoria do hospital, demonstrando apoio e conhecimento, o que transmite aos colaboradores maior confiança e respeito frente à utilização das políticas.

Todas as alterações realizadas nas políticas de segurança da informação devem ser informadas a todos os colaboradores (administrativos, equipe médica, de enfermagem, terapêutica e de hospedagem hospitalar), de forma que todos atuem igualmente, não gerando novos fatos que prejudiquem a segurança das informações. A divulgação dessas políticas pode acontecer por meio de palestras, treinamentos, comunicados em murais de avisos ou outros meios que sejam propícios para essa divulgação. Compete ao Comitê de Segurança desenvolver os esforços necessários para que as mudanças sejam comunicadas a todos os envolvidos.

Ferreira e Araújo (2006, p.126) descrevem alguns itens relevantes que devem ser abordados no processo de revisão:

a) eventuais riscos identificados;
b) alterações na legislação do negócio;

c) incidentes de segurança;
d) vulnerabilidades encontradas;
e) alterações na estrutura organizacional; e
f) mercado.

Recomenda-se ao Comitê de Segurança que todos esses itens sejam abordados durante as revisões da política de segurança da informação, pois possibilitam uma abordagem de todos os fatores capazes de impactar a política de segurança da informação.

5 ANÁLISE E DISCUSSÃO DE RESULTADOS

O desenvolvimento de políticas de segurança da informação para as atividades relacionadas aos prontuários médicos é uma maneira eficaz de assegurar que as atividades desenvolvidas nesse âmbito sejam corretamente realizadas e. como conseqüência, que os processos sejam fortemente padronizados, minimizando os riscos quanto a incidentes de informação.

Por meio da realização de um estudo de observação, foi possível identificar falhas e inconsistências nos processos de manipulação dos prontuários médicos. Além disso, também foram percebidos realidades da cultura organizacional, “um faz e todos os outros fazem do mesmo jeito”, gerando um histórico de pessoas que procuram realizar as tarefas sempre do mesmo jeito por terem sido ensinadas de tal forma, sem que nunca os processos tenham sido documentados ou descritos em algum meio formal.

Com isso as possibilidades de falha se tornam ainda maiores, pois em determinados momentos cada um pode desejar agir conforme o seu entender, prejudicando o andamento rotineiro e causando entraves no processo.

Esses facilitadores de incidentes de informação são, em partes, reconhecidos pelos funcionários como deficiências da instituição. Outros itens, que também atuam como forma de garantir a qualidade e a segurança da informação, foram verificados e incorporados à política, os quais não haviam sido declarados inicialmente e também não foram percebidos como riscos às atividades relacionadas à segurança das informações.

As políticas de segurança da informação propostas para o Hospital do Trabalhador têm a função de colaborar para o funcionamento adequado das atividades relacionadas aos prontuários médicos, orientando todos os colaboradores da organização a atividades padronizadas e de acordo com critérios específicos.

Com essas políticas, visa-se garantir que os incidentes relacionados à informação sejam radicalmente minimizados, fazendo com que não mais sejam perdidos prontuários, documentos que os compõem e coibindo acessos não autorizados. Além disso, as políticas adotadas também cumprem o papel de regular “modos” de realizar as atividades que já eram adotadas pela instituição, mas que, até o momento não haviam sido normatizadas, conduzindo a organização à “boas

práticas” na gestão da informação, agregando qualidade nos processos médicos que têm por base os prontuários médicos.

Para que essa política possa ser implementada conforme os padrões adotados pela literatura, é fundamental que os processos de implantação e revisão (manutenção) sejam acompanhados de perto, seguindo as instruções fornecidas. Caso se opte por outras formas de implantação, o processo pode não ser adequadamente realizado, apresentado novas complicações no processo.

Os processos de implantação e manutenção das políticas precisam estar alinhados, pois no momento de implantação já podem ser verificadas necessidades de alteração das políticas. De tal forma que, sempre será possível manter uma política que atenda a instituição em sua forma de agir e que atue continuamente em conformidade com os padrões desejados pela organização.

No Ambulatório do Hospital, a pessoa responsável pela validação da política foi a enfermeira chefe de setor, Cristiane Serafim. Conforme identificado no formulário, foram atingidos 28 pontos, número que representa aproximadamente 93,5% de aceitação da política nesse setor. Em seu depoimento tem-se o seguinte:

> As informações contidas nos prontuários são muito importantes e devem ser manipuladas com muito cuidado, visto que poderão ser utilizadas em várias situações. É nosso dever criar meios de controlar possíveis danos e extravios e melhorar a qualidade do mesmo.

Por intermédio do mesmo formulário foi possível perceber que para as atividades relacionadas aos Postos de Internação e ao Pronto Socorro, foi obtido apoio total, o que corresponde a 30 pontos ou 100% de aceitação. A pessoa responsável por fornecer informações quanto a esses setores, Giovana de Paula Miecznirowski, afirmou que:

> No dia a dia estamos tão envolvidos com a assistência que não nos damos conta da importância em relação aos registros de informações, até mesmo para escrever rotinas pertinentes a esse assunto, é de fundamental importância se ter rotinas padronizadas para uniformizar as atividades dentro de um mesmo ambiente de trabalho.

No Faturamento, o formulário apontou que a política de segurança seria bem vista, no entanto com um índice pouco menor de aceitação, atingiu-se 25 pontos e o equivalente a aproximadamente 83,5% de aceitação. Nesse setor se percebeu certa restrição à implantação da política por gerar mudança nos processos e,

consequentemente, rupturas na cultura organizacional adotada até o momento. O item mais crítico foi a compreensão da política proposta, demonstrando restrições de compreensão da importância que o cuidado mais específico com a informação tem para a organização. A esse item se seguiu a descrença na melhoria do trabalho e a segurança quanto a implantação exprimir mais garantia as pessoas. A responsável por esse setor é Regiane Skroch, no entanto ela optou por não escrever uma declaração, mas em entrevista revelou saber da importância desse projeto e como a padronização é relevante para a atuação correta das atividades realizadas no faturamento.

Já no Serviço de Prontuário do Paciente (SPP) também se percebeu um índice similar ao do Faturamento, com pontuação em nível mais baixo e compreensão das políticas de forma geral. Nesse setor foram somados 26 pontos o que corresponde a aproximadamente 86,7% de aceitação. Foram pontuadas de forma inferior as questões correspondentes a compreensão da política de segurança da informação e de sua importância, a utilização das políticas mesmo com a aprovação da alta gerência, ao sentimento de segurança que tal ferramenta pode proporcionar ao desenvolvimento de suas atividades e a credibilidade conferida a melhoria dos processos a partir da gestão por políticas. Percebeu-se a falta de entendimento do que a implantação de uma política pode gerar para a organização, caracterizando-se em resistência a novos meios de fazer algo já consolidado pela cultura. A responsável por esse setor, Maria Barbosa, também optou por não dar seu depoimento, mas em entrevista pessoal revelou saber da importância dessas políticas.

Na Maternidade a política de segurança foi avaliada de forma positiva, tendo a pesquisa atingido 28 pontos, o que corresponde a 93,5%. Os itens em que a pontuação foi mais baixa referem-se a dúvida quanto a utilização das políticas mesmo que essas tenham aprovação dos órgãos superiores e por descrer da possibilidade de melhoria em todas as atividades relacionadas a prontuários médicos com a implantação das políticas. A entrevistada nesse setor foi a Sra. Sonia, ela forneceu o seguinte depoimento:

> Acredito que é extremamente necessária a implantação de políticas de segurança para facilitar e garantir o sigilo e o trabalho das pessoas envolvidas no processo. Iniciativas dessa natureza são muito bem vindas.

Conforme pode ser percebido na análise dos formulários de validação, em geral a aceitação as políticas de segurança da informação pode se configurar como um investimento de sucesso para a organização. Fato percebido pela pontuação média alcançada e pela porcentagem sempre mantida acima da linha dos 83%, índice considerado alto para a pesquisa.

Com todas as etapas desenvolvidas para a criação das políticas propostas, pode-se perceber que esse é um instrumento de grande importância para a organização, mas que ainda não tinha sido pensado e desenvolvido.

Ainda foi possível confirmar a relevância do prontuário médico para o hospital e para o paciente, reforçando a teoria inicial de que informações com qualidade baixa podem gerar diversos tipos de prejuízos, inclusive uma vida, e fortalecendo a necessidade de implantação de uma política de segurança da informação.

O desenvolvimento desse projeto e a validação realizada também confirmaram a necessidade eminente de gerir de forma adequada as questões relacionadas à cultura organizacional. Isso porque a cultura é composta de pessoas, e essas demonstraram para a pesquisa ser o ativo mais crítico no novo processo que se pretende implantar na organização. De tal forma, por mais que elas sejam favoráveis a mudanças, possivelmente também sejam a maior força de resistência.

O que mais se destacou em todo o processo de pesquisa foi perceber que as organizações ainda não se deram conta da necessidade de formalização de seus processos, gerindo incorretamente as suas informações.

6 CONSIDERAÇÕES FINAIS

O desenvolvimento de uma política de segurança da informação, independentemente do cliente final, é um processo dispendioso que exige conhecimento aprofundado da organização, da atividade realizada e de construção de políticas. Além disso, é uma atividade que precisa estar em conformidade com a realidade da organização e com o seu modo de administrar as informações, é propondo-se mudanças que adéquem as atividades ao utilizado pelo mercado.

Para as políticas de segurança da informação que foram desenvolvidas para o Hospital do Trabalhador, as preocupações não foram diferentes, afinal a proposta teve de se adequar as regras já existentes, as novas necessárias e a cultura de se fazer do mesmo jeito fortemente enraizada.

Apesar das dificuldades e oposições encontradas após a conclusão da criação das políticas, foi possível cumprir com o objetivo geral do trabalho, que era propor políticas que garantam a qualidade das informações utilizadas pela instituição.

Os objetivos específicos também foram cumpridos na íntegra. Foi possível conhecer: como se compõe um prontuário médico, bem como a importância que cada documento apresenta no contexto geral; observar e descrever por meio de fluxogramas, o ciclo que as informações percorrem dentro da instituição; saber por quem e como são geradas as informações que estão descritas nos prontuários; verificar os acessos que são concedidos aos proprietários da informação; descrever os procedimentos básicos para a implantação; a manutenção das políticas; e a validação das políticas por meio de um formulário específico. Ressaltando-se a implantação e a manutenção como ferramentas essenciais para o processo de implantação de políticas de segurança da informação.

Esta pesquisa não tem fim com a conclusão dessa etapa. É de conhecimento que uma política se compõe de políticas, normas e procedimentos, e que nessa fase apenas foram elaboradas as políticas. Entretanto, espera-se que a conclusão das etapas não realizadas sejam continuadas pelo Hospital do Trabalhador, ficando a cargo do Comitê de Segurança a ser implantado.

Acredita-se que essa pesquisa representa um marco inicial para a configuração de um ambiente muito mais seguro em relação às informações que estão disponíveis nos prontuários médicos. Entretanto, com o desenvolvimento dos

itens que complementam a política, o novo ambiente de informação do Hospital do Trabalhador provavelmente tornar-se-á mais adequado e ainda mais seguro, garantindo à instituição e aos pacientes um atendimento confiável e de qualidade, assegurando que todas as informações que circulam através dos prontuários sejam fidedignas.

REFERÊNCIAS

ABNT NBR ISO IEC 17799:2005. **Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2. ed., 2005. 120 p.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.246, de 1988. **Código de ética médica.** Disponível em:<http://www.portalmedico.org.br/novoportal/index5.asp>. Acesso em: 18 out. 2008.

CONSELHO FEDERAL DE MEDICINA. Resolução nº1.638, de 2002. **Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde.** Disponível em: <http://www.portalmedico.org.br/resolucoes/cfm/2002/1638_2002.htm>. Acesso em: 18 out. 2008.

CONSELHO REGIONAL DE MEDICINA DE SANTA CATARINA. **Manual de orientação ética e disciplinar**. 2. ed. rev. e atual. Florianópolis, v. 1, mar. 2000. Disponível em:
< http://www.portalmedico.org.br/Regional/crmsc/manual/parte3b.htm>. Acesso em: 14 abr. 2008.

CONSELHO REGIONAL DE MEDICINA DO DISTRITO FEDERAL. **Prontuário médico do paciente:** guia para uso prático. Brasília, 2006. 91p. Disponível em:<www.jovensmedicos.org.br/publicacoes/arquivos/CRMDF/prontuario_medico.pdf>. Acesso em: 10 set. 2008.

FELIX, Wellington. **Introdução a gestão da informação**. Campinas: Alínea, 2003. 96 p.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação**: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006. 188 p.

FREITAS, Maria Ester de. **Cultura organizacional:** formação, tipologias e impactos. São Paulo: Makron, 1991. 140 p.

FUNDAÇÃO NACIONAL DA QUALIDADE. **Cadernos de Excelência**: informações e conhecimento. n. 5. São Paulo: Fundação Nacional da Qualidade, 2007. 40 p..

HOSPITAL DO TRABALHADOR. **O hospital**. Disponível em: <http://200.189.113.52/ht/hospital.htm>. Acesso em: 14 jun. 2007.

HOSPITAL DO TRABALHADOR. **Hospital do Trabalhador:** relatório de atividades 2007. Curitiba, 2007. 71 p.

HOUAISS, Antônio; VILLAR, Mauro de Salles. **Minidicionário Houaiss da língua portuguesa**. Rio de Janeiro: Objetiva, 2004. 2. ed. rev. e aum. 907 p.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia do trabalho científico**. São Paulo: Atlas, 1992, 214 p.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Gerenciamento de sistemas de informação**. Rio de Janeiro: LTC, 2001. 3 ed. 433 p.

MCGARRY, Kevin. Sobre conhecimento e informação. In:_____. **O Contexto dinâmico da informação:** uma análise introdutória. Brasília: Briquet de Lemos, 1999, p. 1-34.

MEDEIROS FILHO, Benedito Cabral de. **Revolução na cultura organizacional**. São Paulo: STS, 1992. 142 p.

NONAKA, Ikugiro; TAKEUCHI, Hirotaka. **Criação de conhecimento na empresa**: como as empresas japonesas geram a dinâmica da inovação. Rio de Janeiro: Campus, 1998. 380 p.

ROBREDO, Jaime. **Da ciência da informação revisitada aos sistemas humanos de informação**. Brasília: Thesaurus, 2003. 243 p.

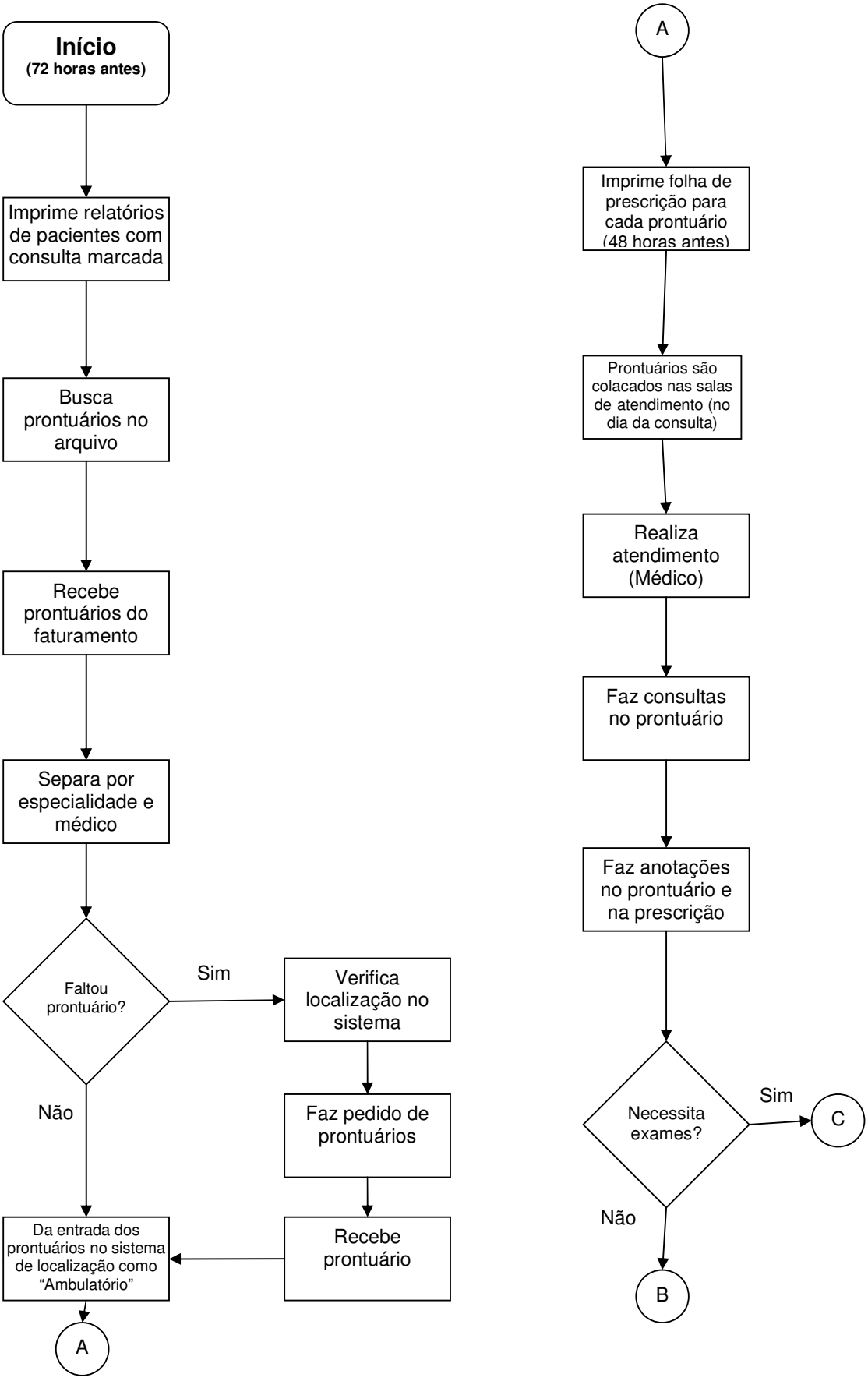
SÊMOLA, Marcos. Gestão da segurança da informação. In: STAREC, Claudio; GOMES, Elisabeth B. P.; CHAVES, Jorge B. L. (Org.). **Gestão estratégica da informação e inteligencia competitiva**. São Paulo: Saraiva, 2005, p. 285-305.

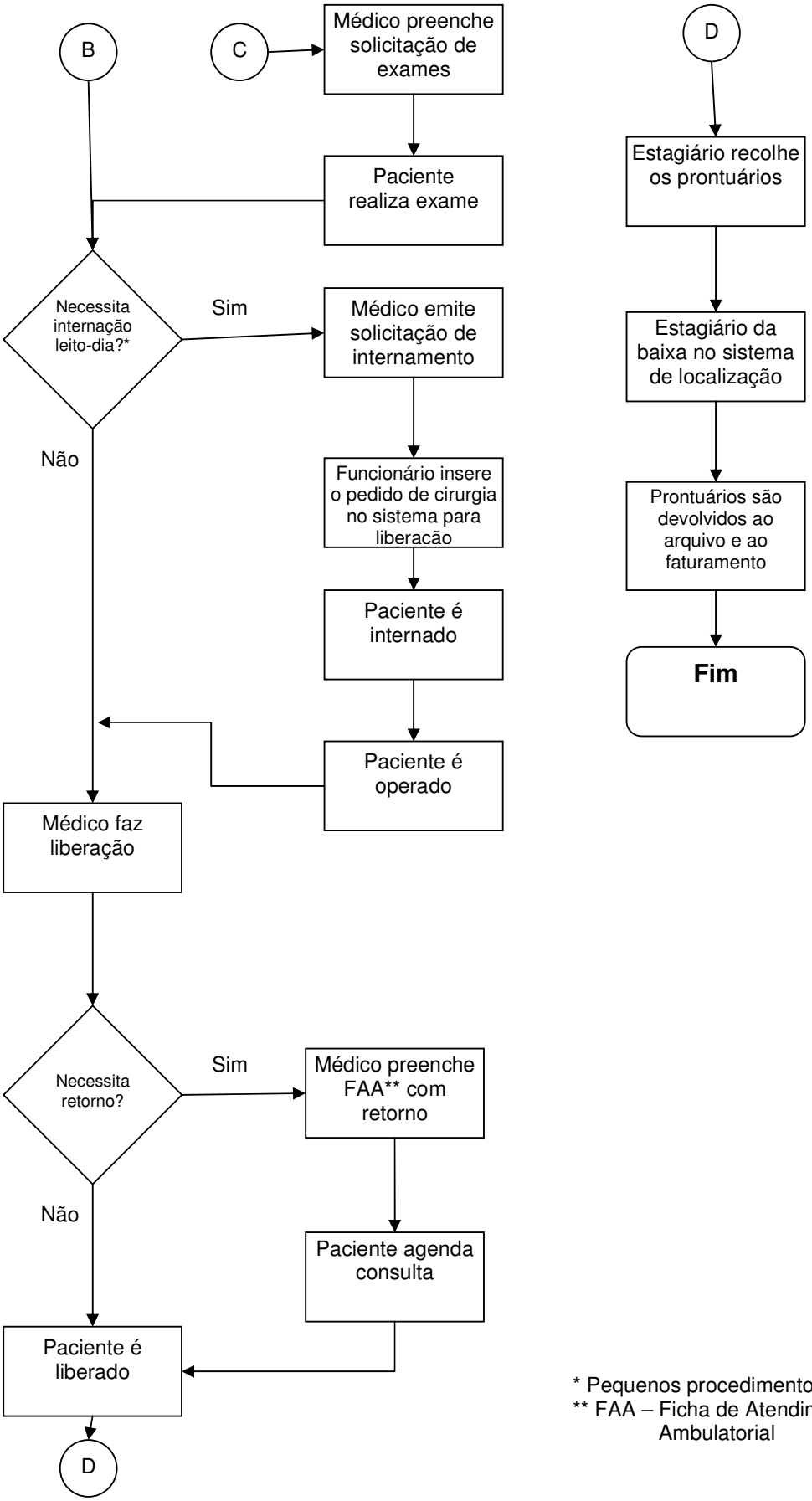
_____. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003, 156 p.

ZAVAREZE, Tais Evangelho. **Cultura organizacional**: uma revisão de literatura. 2008. Disponível em: <http://www.psicologia.com.pt/artigos/textos/A0441.pdf>. Acesso em: 29 set. 2008.

APÊNDICE A – Fluxograma do ambulatório

PROCEDIMENTO PARA UTILIZAÇÃO DO PRONTUÁRIO NO ATENDIMENTO AMBULATORIAL

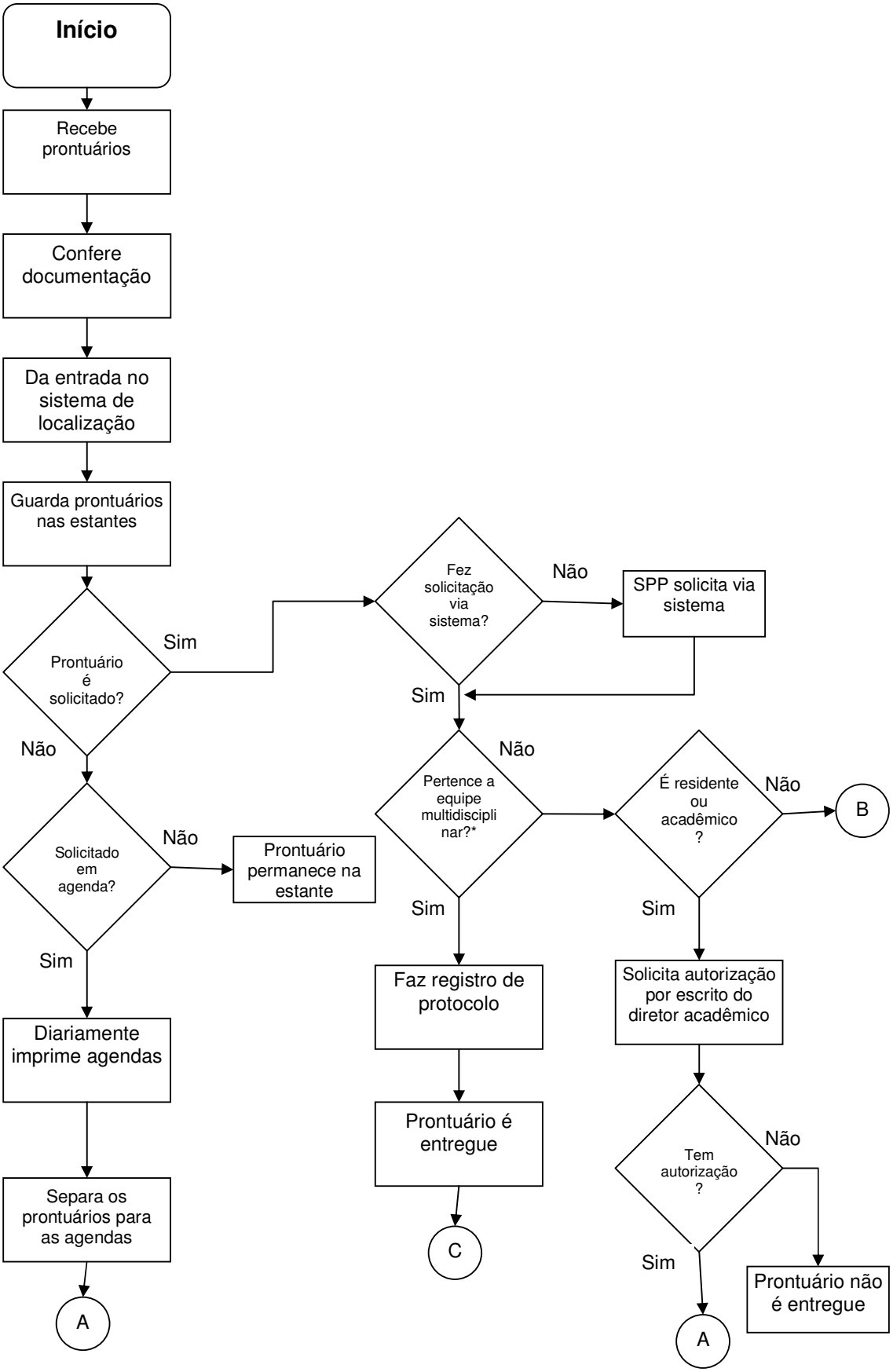


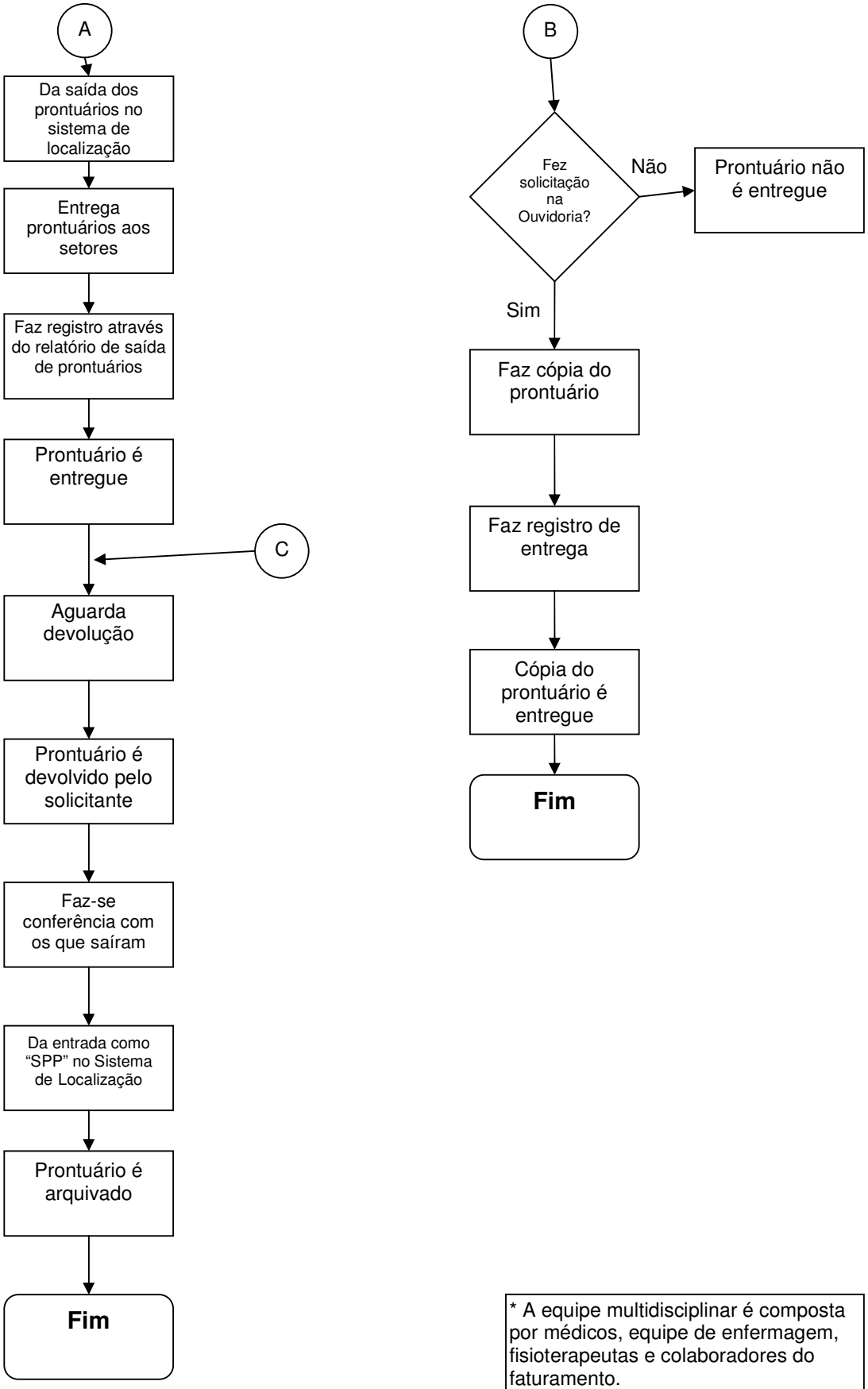


* Pequenos procedimento cirúrgicos.
** FAA – Ficha de Atendimento Ambulatorial

APÊNDICE B – Fluxograma do Serviço de Prontuário do Paciente

PROCEDIMENTOS BÁSICOS DE UTILIZAÇÃO DO PRONTUÁRIO MÉDICO NO SERVIÇO DE PRONTUÁRIO DO PACIENTE (SPP OU ARQUIVO)

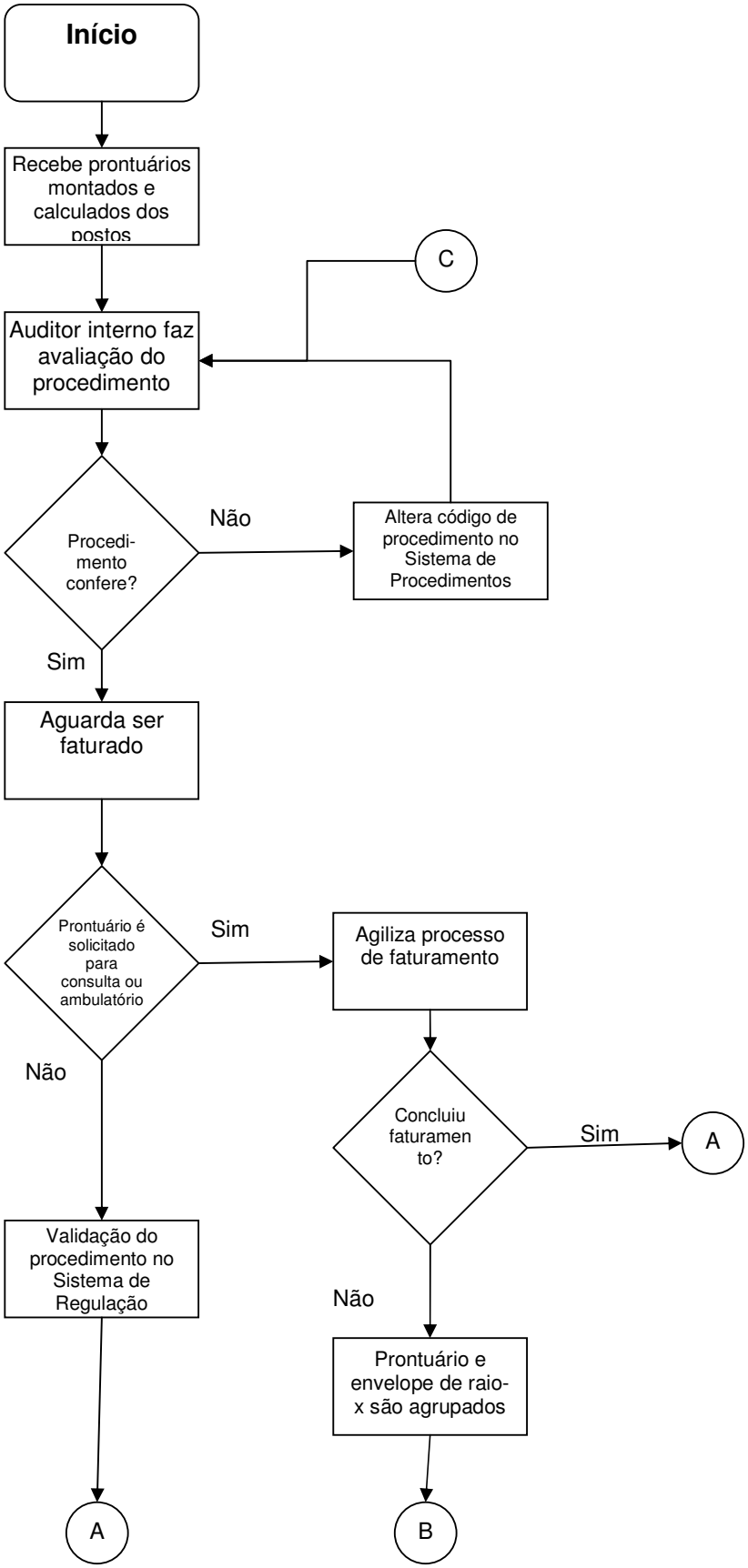


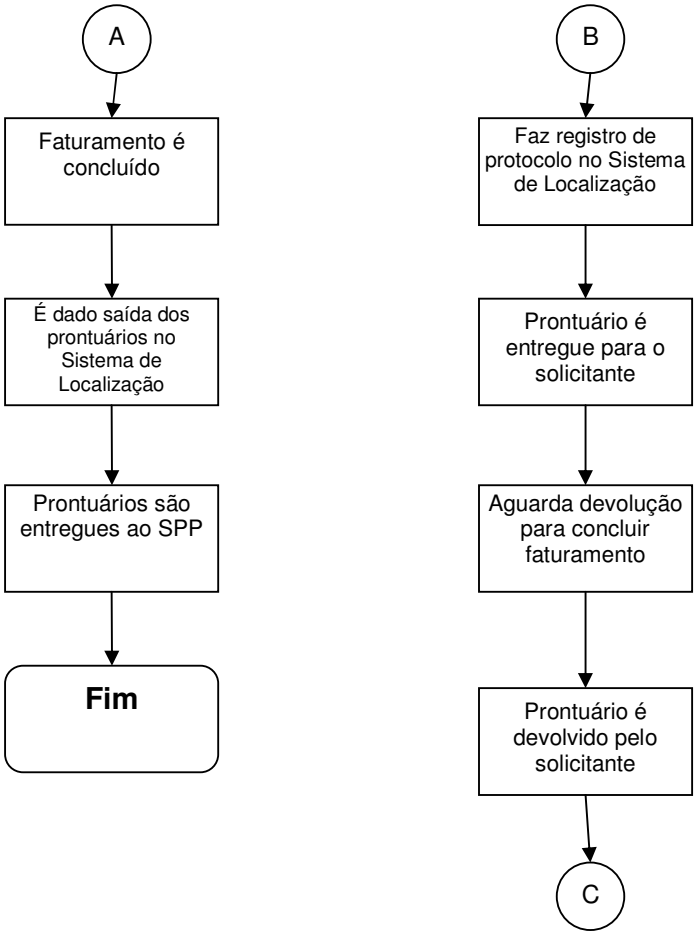


* A equipe multidisciplinar é composta por médicos, equipe de enfermagem, fisioterapeutas e colaboradores do faturamento.

APÊNDICE C – Fluxograma do Faturamento

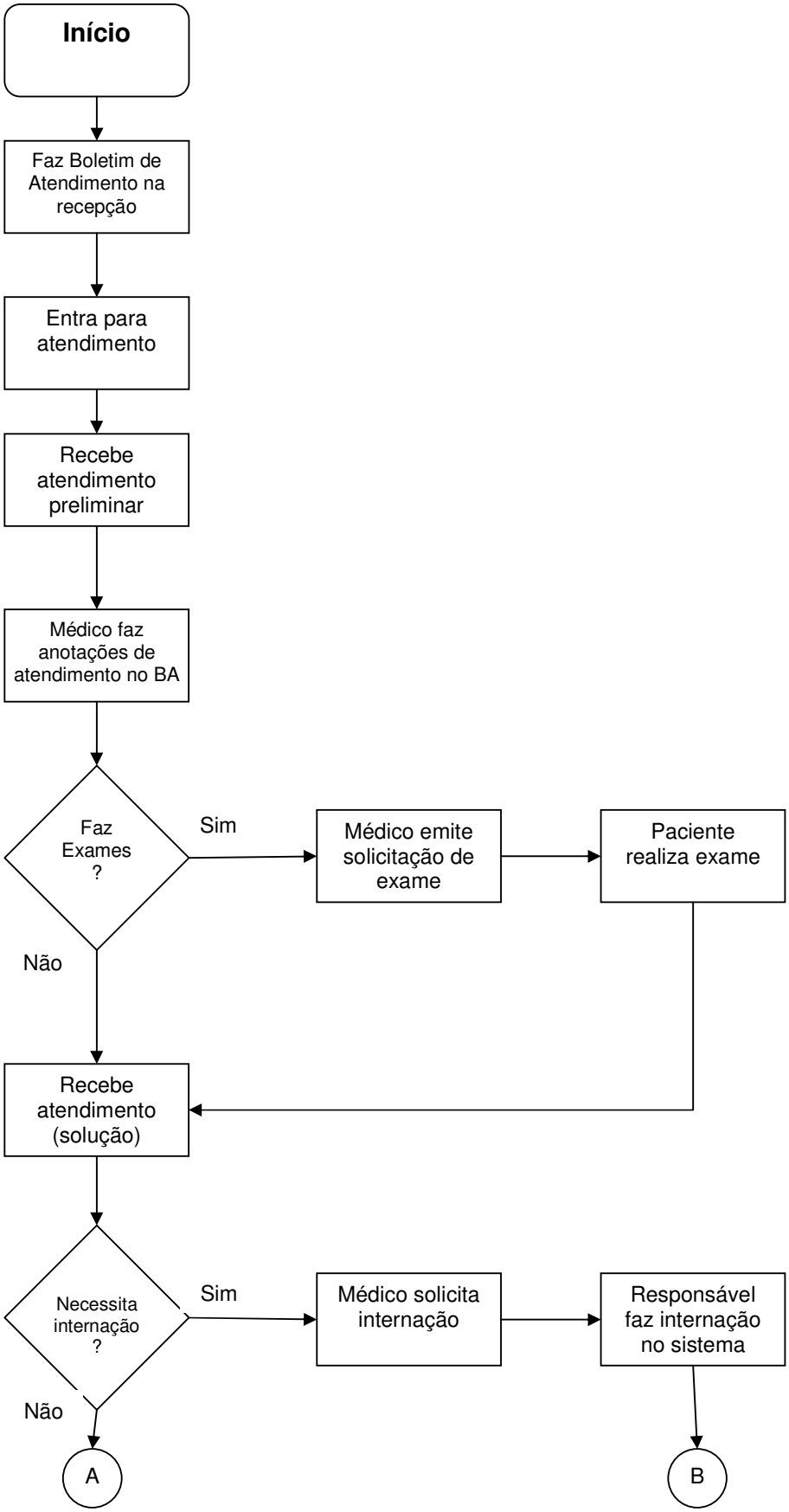
PROCEDIMENTOS BÁSICOS DE UTILIZAÇÃO DO PRONTUÁRIO MÉDICO NO FATURAMENTO

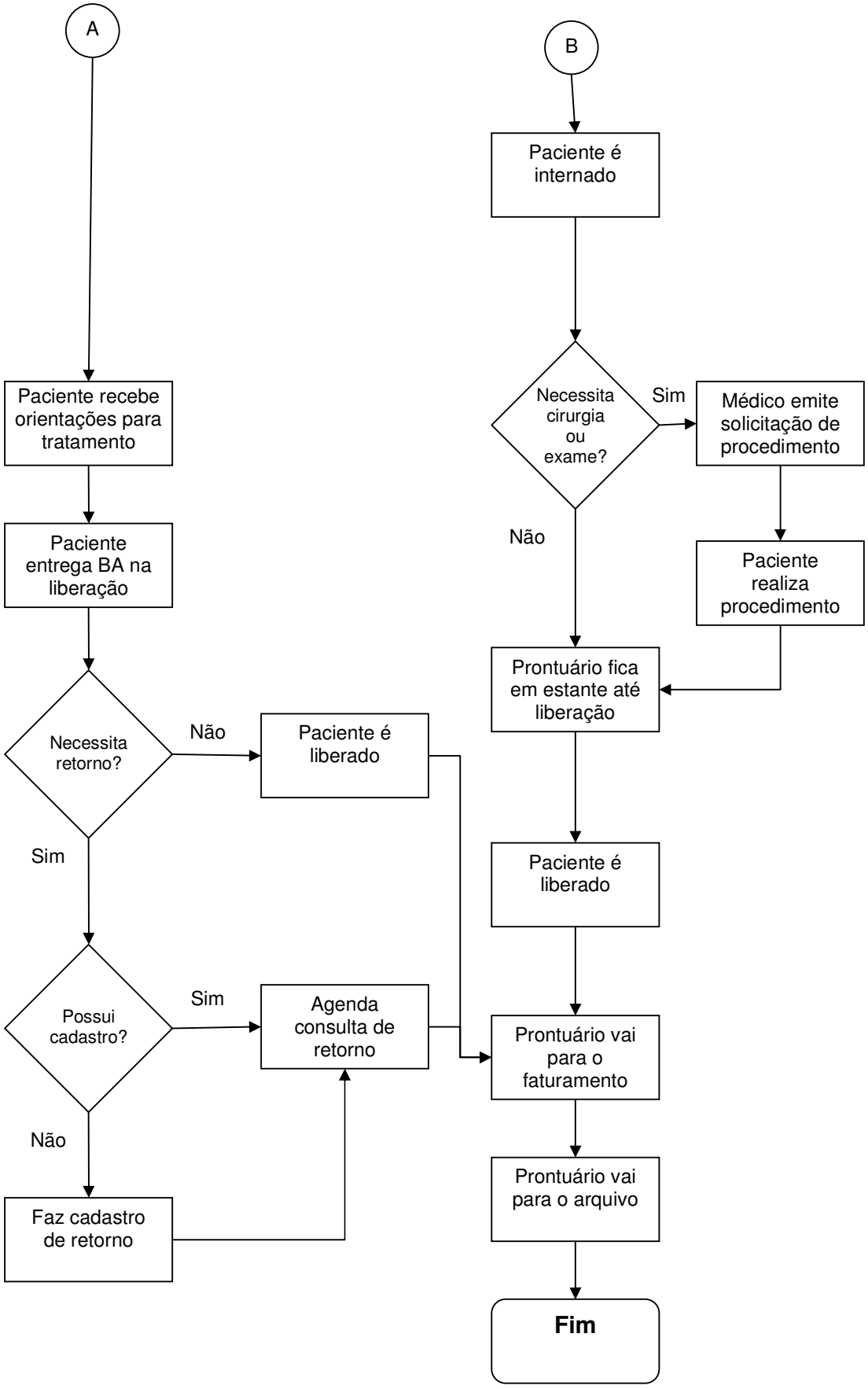



A
Faturamento é concluído
É dado saída dos prontuários no Sistema de Localização
Prontuários são entregues ao SPP
Fim
B
Faz registro de protocolo no Sistema de Localização
Prontuário é entregue para o solicitante
Aguarda devolução para concluir faturamento
Prontuário é devolvido pelo solicitante
C

APÊNDICE D – Fluxograma da Maternidade

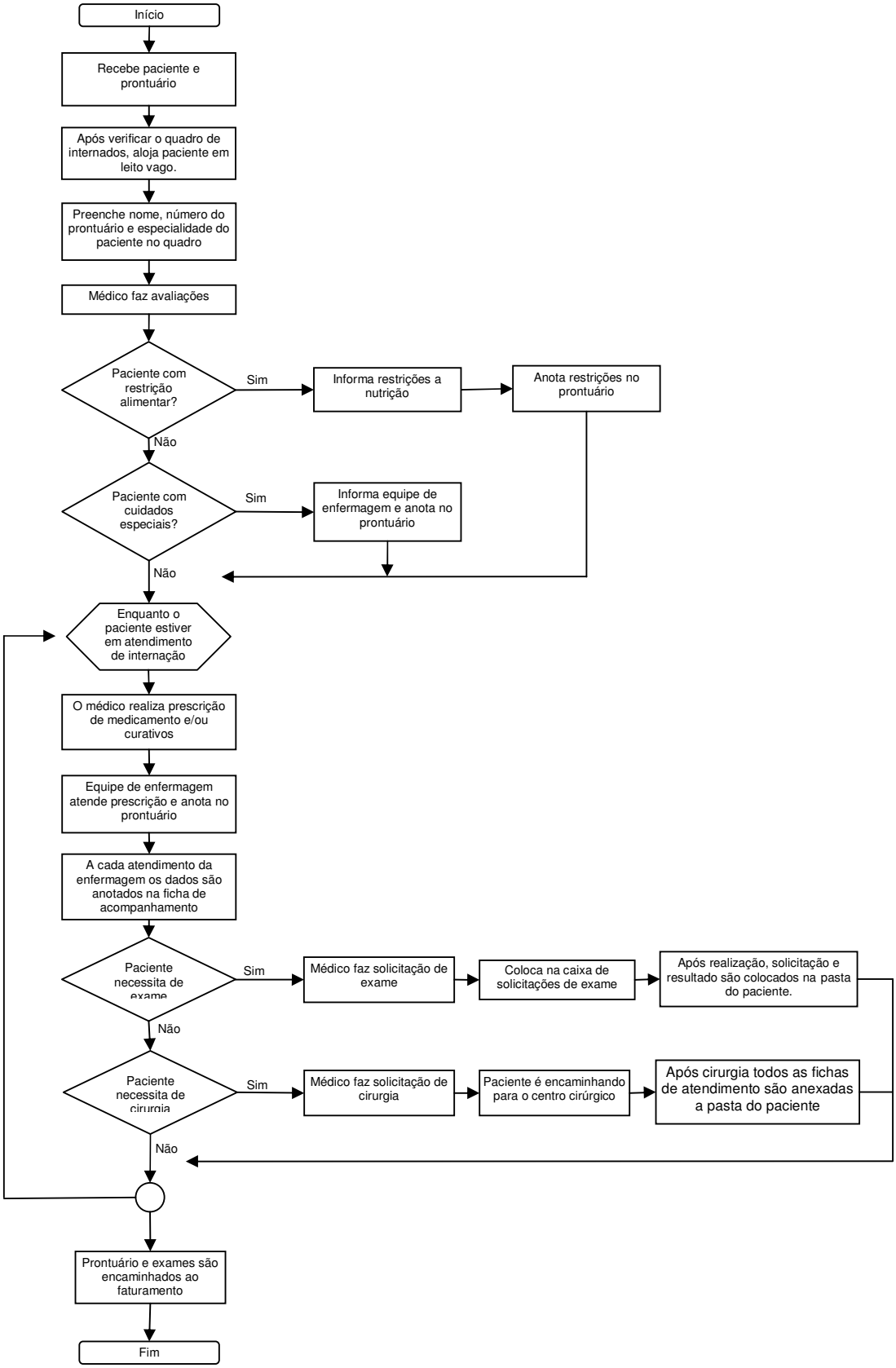
PROCEDIMENTO DE INICIALIZAÇÃO DO PRONTUÁRIO MÉDICO ATRAVÉS DE ENTRADA PELA MATERNIDADE




A
B
Paciente é internado
Paciente recebe orientações para tratamento
Necessita cirurgia ou exame?
Sim
Médico emite solicitação de procedimento
Não
Paciente realiza procedimento
Paciente entrega BA na liberação
Prontuário fica em estante até liberação
Necessita retorno?
Não
Paciente é liberado
Sim
Paciente é liberado
Possui cadastro?
Sim
Agenda consulta de retorno
Prontuário vai para o faturamento
Não
Prontuário vai para o arquivo
Faz cadastro de retorno
Fim

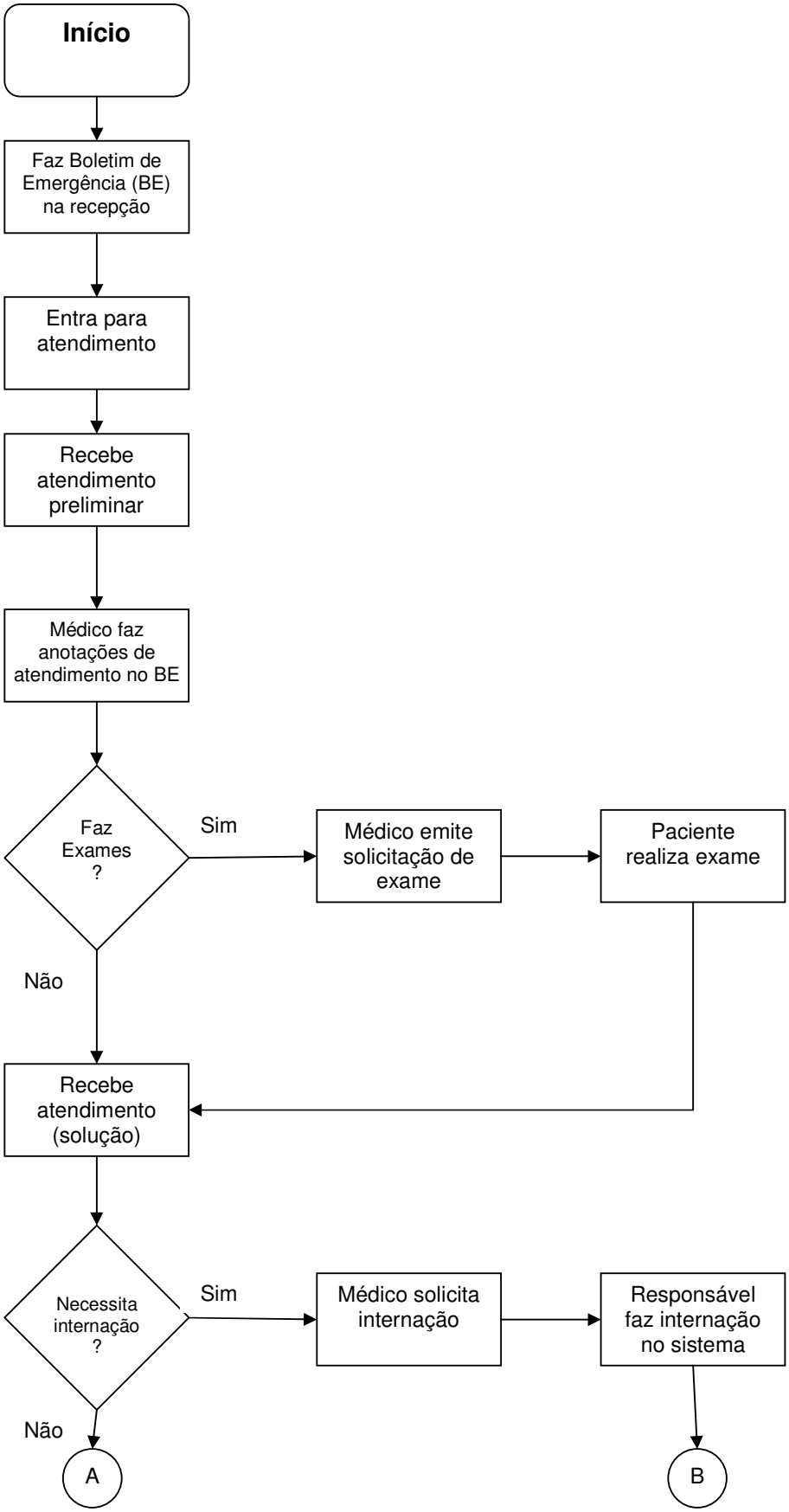
APÊNDICE E – Fluxograma dos pontos de internação

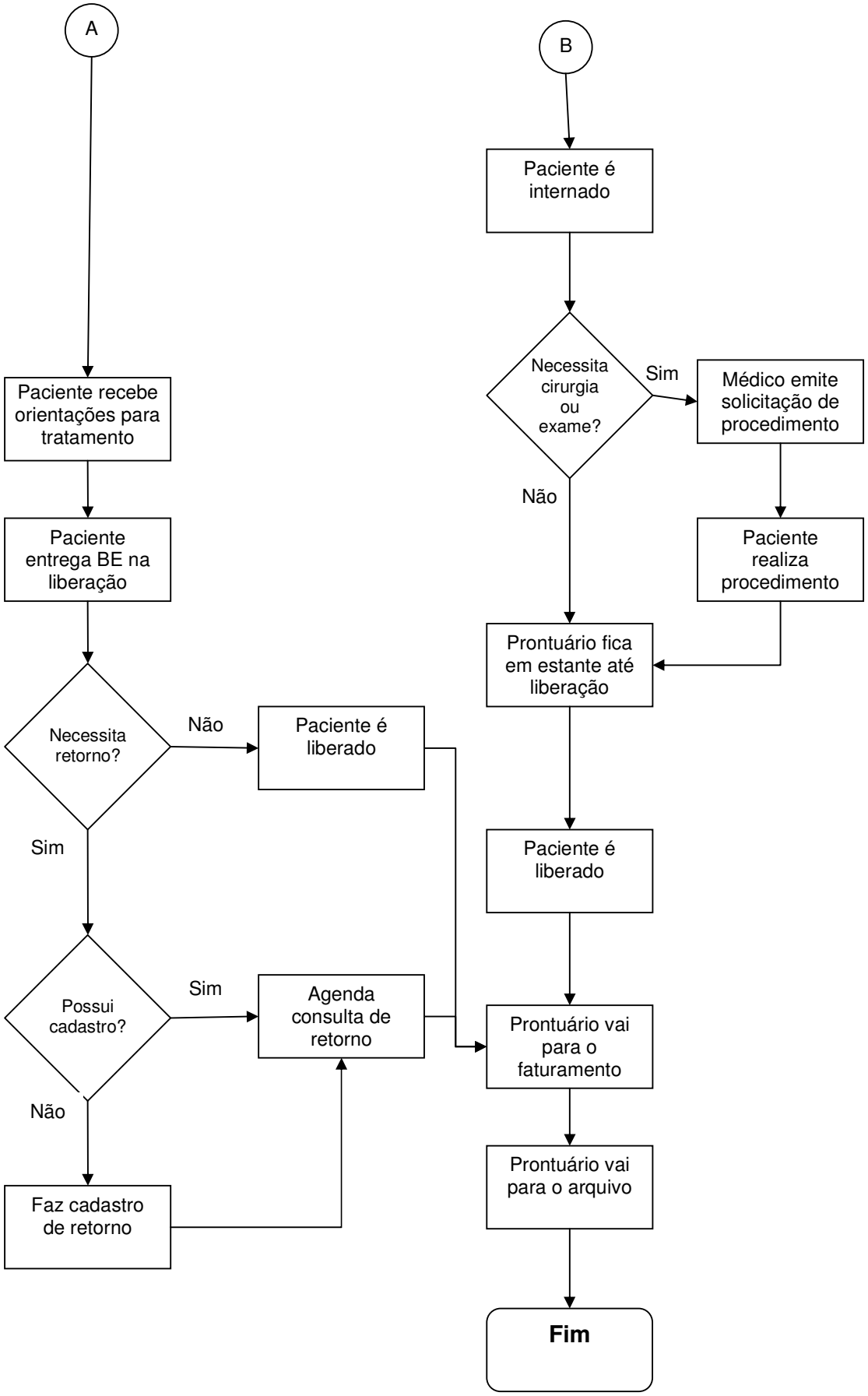
PROCEDIMENTOS BÁSICOS DE UTILIZAÇÃO DO PRONTUÁRIO MÉDICO NO ATENDIMENTO DIÁRIO DOS POSTOS DE INTERNAÇÃO



APÊNDICE F – Fluxograma do Pronto Socorro

PROCEDIMENTO DE INICIALIZAÇÃO DO PRONTUÁRIO MÉDICO ATRAVÉS DE ENTRADA PELO PRONTO SOCORRO




A
B
Paciente é internado
Necessita cirurgia ou exame?
Sim
Médico emite solicitação de procedimento
Não
Paciente realiza procedimento
Paciente recebe orientações para tratamento
Paciente entrega BE na liberação
Prontuário fica em estante até liberação
Necessita retorno?
Não
Paciente é liberado
Sim
Paciente é liberado
Possui cadastro?
Sim
Agenda consulta de retorno
Prontuário vai para o faturamento
Não
Prontuário vai para o arquivo
Faz cadastro de retorno
Fim

APÊNDICE G – Política de Segurança da Informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA UTILIZAÇÃO DE PRONTUÁRIO MÉDICO

1 INTRODUÇÃO

O Hospital do Trabalhador, visando a proteção das informações e dos procedimentos com relação aos prontuários médicos, implanta a presente política.

É aplicável a todos os setores e usuários da organização que diretamente ou indiretamente se utilizam do prontuário médico para inserção, obtenção ou outra funcionalidade quanto às informações do prontuário médico.

Trata-se de um documento formal por meio do qual visa garantir a qualidade das informações constantes no prontuário médico, e com isso também a integridade, confiabilidade e disponibilidade.

Destaca-se que o Hospital do Trabalhador tem total direito sobre o conteúdo das informações que circulam em seu interior, portanto se reserva o direito de obter a qualquer momento toda e qualquer informação produzida ou recebida, não garantindo o direito de privacidade aos geradores/produtores da informação.

2 COMITÊ DE SEGURANÇA

Para garantir o efetivo funcionamento da política de segurança da informação, institui-se o Comitê Gestor de Segurança da Informação, a ser composto por pessoas designadas pela direção do hospital.

Esse comitê será composto por 05 (cinco) integrantes ou conforme necessidade, sendo que para atuar no cargo é preciso estar a mais de um ano na instituição e conhecer todos os procedimentos adotados com relação aos prontuários médicos.

Ficará a cargo desse comitê providenciar a manutenção das políticas, a criação das normas e procedimentos legais, o treinamento do pessoal, a inspeção de usabilidade e em caso de incidentes quanto a segurança aplicar as sanções legais e juntamente com a diretoria julgar casos que não constem nesse documento.

3 UTILIZAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

A seguir serão descritas todas as restrições quanto à utilização dos recursos de tecnologia da informação quando aplicados a utilização dos prontuários médicos.

3.1 A utilização de computadores fica restrita as atividades do ambiente de trabalho não sendo permitido a sua utilização para outros fins;

3.2 É vedada a utilização dos recursos de Tecnologia da Informação para copiar, obter, distribuir material contido nos prontuários médicos;

3.3 Cada colaborador é responsável por usar os recursos tecnológicos disponíveis para aumentar a produtividade e contribuir com os resultados de segurança esperados pela organização;

3.4 Cada colaborador é responsável pela guarda, zelo e bom uso dos recursos de TI a ele disponibilizados em virtude da realização de sua atividade;

3.5 O usuário é totalmente responsável pela segurança das informações que estão sob sua responsabilidade;

3.6 Fica reservado a instituição conceder acesso por meio de senhas aos seus sistemas, de forma a prevenir acessos não autorizados;

3.7 A senha concedida ao colaborador é de sua responsabilidade e deve ser mantida confidencialmente, de forma que não seja compartilhada com nenhum outro colaborador;

3.8 É terminantemente proibida a utilização do correio eletrônico para divulgação das informações constantes no prontuário médico ou no âmbito hospitalar por meio diferente do estabelecido;

3.9 As informações do prontuário não podem ser transmitidas a outros via fax, mensagens de celular, telefone, fotos ou outros meios similares sob nenhuma circunstância que não sejam as legais;

3.10 O acesso a Internet é restrito para atividades que não estejam relacionadas às atividades designas pelo hospital;

3.11 Qualquer informação criada dentre da organização é de sua autoria, sendo sujeita às leis de direitos autorais e não podendo ser publicada sem autorização;

3.12 Todas as pastas de computador utilizadas para a guarda de arquivos também devem ter acesso permitido de acordo com os critérios de segurança

estabelecidos pelo gestor da segurança da informação através de mecanismos de autenticação de usuários;

3.13 De forma a prevenir incidentes quanto à segurança, recomenda-se que sejam feitos backups de todos os arquivos e programa utilizados para manipulação, confecção, alteração ou similar quanto aos prontuários médicos, semanalmente, pelos responsáveis de cada setor.

4 UTILIZAÇÃO DOS RECURSOS DE INFORMAÇÃO

A utilização dos recursos de informação prevê a correta utilização do prontuário médico, bem como de todos os documentos que o compõe, nos diversos setores em que estiver presente.

4.1 CRIAÇÃO

Prevê as políticas quanto à criação dos prontuários médicos

4.1.1 Ao dar entrada no hospital o paciente ou acompanhante sempre deve fornecer documento de identificação do paciente para ser gerado o atendimento, a não ser em casos em que haja impossibilidade. Nos casos de impossibilidade todas as características pessoais devem ser descritas no Boletim de Emergência (BE), para facilitar a identificação futura do paciente;

4.1.2 Após ser feita a correta identificação do paciente, o boletim de emergência deverá ser alterado com as novas informações e agrupado ao boletim anterior;

4.1.3 Nos casos de pacientes que tem entrada pela maternidade, os procedimentos adotados são os mesmos do pronto socorro, com a diferença que as informações são anotadas nos Boletins de Atendimento (BA);

4.1.4 O paciente só poderá adentrar o pronto socorro após o preenchimento de seus dados, a não ser em casos de impossibilidade.

4.2 MANUSEIO

Prevê as políticas quanto ao manuseio dos prontuários médicos durante seu período de utilização.

4.2.1 É proibido ao médico deixar de elaborar prontuário médico para cada paciente;

4.2.2 O médico é obrigado a assinar e carimbar ou assinar, colocar nome legível e inscrição do CRM no prontuário;

4.2.3 Todas as folhas que compõe o documento prontuário devem estar corretamente identificadas com as informações do paciente, sendo essas em etiquetas ou letras legíveis;

4.2.4 Somente é permitido escrever nos prontuários a caneta de tinta azul, preta ou vermelha;

4.2.5 É expressamente proibido usar corretivo líquido ou em outra forma qualquer nos prontuários médicos;

4.2.6 É proibido deixar folhas em branco no prontuário;

4.2.7 É proibido fazer qualquer outro tipo de anotação no prontuário médico que não se refira ao paciente e a seu processo de atendimento;

4.2.8 Todas as folhas que compõe o prontuário médico devem ser mantidas agrupadas durante o período de permanência do paciente no hospital;

4.2.9 Em caso de extravio de alguma folha, seu desaparecimento deve ser comunicado ao comitê de segurança, no entanto, caso sejam reencontradas devem ser imediatamente recolocadas no prontuário;

4.2.10 No momento de utilização do prontuário para consultas médicas, é proibido ao médico entregar ao paciente qualquer documento constante no prontuário, bem como deixar de anexar novos documentos que tenham sido gerados em função da consulta;

4.2.11 A entrada nas salas de atendimento é restrita a médicos, pacientes no período de consultas e funcionários do ambulatório;

4.2.12 É proibida a divulgação de informações do prontuário por parte do médico ou por qualquer outro funcionário da instituição;

4.2.13 No dia da consulta os prontuários devem ser colocados nas salas de atendimento após conferência com a lista de consultas agendadas;

4.2.14 Sempre antes do início do atendimento as informações do paciente devem ser confirmadas pelo mesmo, impedindo que ocorram atendimentos a pacientes trocados;

4.2.15 Se após confirmação dos dados for percebido que o prontuário está trocado, solicitar junto a pessoa responsável a troca e informar ao comitê de segurança o ocorrido;

4.2.16 Após consulta, o paciente somente poderá se ausentar do consultório portando receituário, atestado, exames (se o tiver levado) e, caso necessite, ficha de atendimento ambulatorial para marcação de retorno;

4.2.17 Após o período de consultas todos os prontuários devem ser recolhidos evitando que fiquem expostos a fatores de risco;

4.2.18 Para realização de internação do paciente é indispensável e solicitação de internação feita pelo médico;

4.2.19 Nos postos de internação, os prontuários devem ser mantidos em locais afastados do alcance de pessoas que não sejam autorizadas a utilizá-los ou não pertençam ao setor;

4.2.20 Ao receber o paciente, conferir seus dados com o prontuário recebido;

4.2.21 Todos os documentos gerados devido à internação devem ser mantidos agrupados com o prontuário médico;

4.2.22 Preencher no quadro de internação o nome do paciente, número do prontuário e especialidade de atendimento de acordo com o leito em que o paciente se encontra, fazendo as atualizações necessárias diariamente;

4.2.23 Cabe ao médico informar todas as restrições de cuidados e alimentação do paciente a equipe de enfermagem e órgãos necessários, bem como anotar todas as informações de atendimento no prontuário;

4.2.24 Diariamente todos os atendimentos necessários devem ser realizados e anotados ou anexados aos prontuários médicos;

4.2.25 Todos os documentos gerados diariamente em função do atendimento do paciente devem ser anexados ao seu prontuário;

4.2.26 Ao receber alta, o paciente poderá se ausentar dos postos de internação portando apenas receituário, atestado e ficha de alta;

4.2.27 Durante o atendimento no pronto socorro todas as informações recolhidas e fornecidas devem ser anotadas no BE;

4.2.28 Solicitações de exames devem ser feitas em documento específico em 2 vias e anotado no BE;

4.2.29 Caso o paciente necessite ficar em observação, é necessário que seja realizada solicitação de internação, que junto com o BE devem ser entregues ao departamento específico para procedimentos necessários;

4.2.30 Caso o paciente seja liberado, ele deve se dirigir com seus documentos de atendimento até a liberação e assinar seu BE, recebendo ticket que autoriza a saída;

4.2.31 Em casos em que seja necessário o retorno do paciente, o colaborador deverá efetuar o cadastro no sistema de consultas, caso ainda não possua, e agendar a consulta fornecendo ao paciente anotação da data de retorno e médico que o atenderá;

4.2.32 Só é permitido ao paciente se ausentar do pronto socorro do hospital portando receituário, atestado e exames em caso de preenchimento do Termo de responsabilidade;

4.2.33 Todos os termos de responsabilidade assinados deverão permanecer arquivados conforme lei que dispõe sobre documentos administrativos.

4.3 RETIRADA

Prevê as políticas quanto à retirada e circulação dos prontuários médicos dos setores nos quais circula.

4.3.1 É vetado ao paciente, acompanhante ou visitante ausentar-se do local portando o prontuário médico;

4.3.2 É proibida a retirada do prontuário médico do hospital por colaboradores ou terceiros que não estejam autorizados;

4.3.3 O prontuário médico só é entregue para consulta se a pessoa possuir autorização;

4.3.4 Em toda e qualquer circunstância de transferência de prontuários para outras unidades do hospital é de responsabilidade do setor emissor e do setor

receptor, dar saída e entrada, respectivamente, no sistema de localização de prontuários;

4.3.5 Sempre que houver saída ou entrada de um prontuário junto ao Serviço de Prontuário do Paciente (SPP) é imprescindível a conferência dos documentos que compõem esse prontuário;

4.3.6 Todos os relatórios de agenda devem ser assinados e datados pelos setores envolvidos e devem ser guardados conforme lei vigente quando a documentos administrativos.

4.3.7 Para ter acesso a todas as informações constantes em seu prontuário médico o paciente, responsável com procuração ou em caso de falecimento responsável com identificação e dados corretos do paciente, é necessário fazer solicitação de cópia do prontuário inteiro ou parte dele junto a Ouvidoria do hospital;

4.3.8 Todas as solicitações de prontuário médicos devem ser feitas via sistema que se encontra disponível na Intranet;

4.3.9 Podem retirar do SPP ou Faturamento o prontuário apenas médicos, diretores, colaboradores do faturamento e residentes e acadêmicos com autorização do diretor acadêmico;

4.3.10 A retirada de prontuário do SPP não é autorizada a nenhuma outra categoria de colaboradores da organização;

4.3.11 Todas as retiradas de prontuários médicos, independente do setor, devem ser devidamente protocolizadas.

4.4 ARMAZENAMENTO

Prevê as políticas quanto a guarda e armazenamento dos prontuários médicos.

4.4.1 A guarda dos prontuários médicos deve ser feita conforme lei específica vigente;

4.4.2 No SPP ou prontuários devem ser guardados dentro de envelopes, sendo o envelope devidamente identificado com as informações do paciente e o número do prontuário;

4.4.3 É proibido o acesso ao arquivo a pessoas não autorizadas;

4.4.4. É proibido guardar o prontuário no arquivo antes que o mesmo seja faturado;

4.4.5 É proibido guardar os prontuários médicos sem que estejam devidamente identificados;

4.4.6 O descarte de qualquer um dos documentos que compõe o prontuário médico só poderá ser realizado de acordo com as legislações de arquivo e desde que se preencha a ficha de descarte de material;

4.4.7 O descarte de um prontuário médico é considerado infração à ética médica, sendo proibido a qualquer usuário não habilitado para essa atividade;

4.4.8 O descarte só pode ocorrer durante o tempo de guarda previsto por lei se não tiver sido utilizado no prazo de 10 anos da última consulta e desde que seja garantida a sua guarda em meio eletrônico.

4.4.9 Diariamente todos os BE's devem ser recolhidos, organizados em ordem decrescente e entregues no faturamento juntamente com os exames que não foram entregues aos pacientes.

5 CONTROLE DE ACESSO FÍSICO

O controle de acesso físico visa proteger as instalações da organização de qualquer entrada não autorizada e que possam prejudicar as políticas de segurança da informação, garantindo que em todos os locais da organização o acesso seja realizado apenas por pessoas autorizadas.

5.1 Qualquer acesso às dependências da organização só poderá ser feita mediante identificação pessoal e do motivo que conduz ao local;

5.2 Para terem acesso às dependências da organização, os colaboradores precisam portar identificação pessoal e apresentá-las ao vigilante de plantão;

5.3 Prestadores de serviço, consultorias, manutenção e afins deverão apresentar motivo de estarem no ambiente devidamente identificado, com uso de identificação especifica colada em sua roupa e acompanhado de uma pessoa da organização durante todo o tempo em que estiver no ambiente;

5.4 Pacientes, acompanhantes e visitantes só poderão adentrar as dependências do hospital apresentando-se na recepção com identidade ou outro

documento oficial com foto e portando crachá de identificação do setor especifico em que necessita ir;

5.5 É expressamente proibida a entrada de pessoas que não desenvolvam suas atividades naquele local ou estejam lá acompanhadas de outras pessoas nas dependências do SPP e faturamento.

5.6 O acesso a área de tecnologia da informação é restrito a funcionários do setor;

5.7 Não é permitido a terceiros o acesso às redes elétricas, de água, gás, oxigênio e similares dentro da organização, somente pessoas devidamente autorizadas e com comunicado antecipado;

6 GERENCIAMENTO DE INCIDENTES DE SEGURANÇA

O gerenciamento de incidentes de segurança da informação é definido como um incidente, um evento adverso, uma atividade realizada incorretamente que afeta os critérios de confidencialidade, integridade ou disponibilidade da informação, prejudicando o andamento normal da política. A seguir serão descritos os cuidados necessários em ocorrência de incidentes e as punições cabíveis.

6.1 Caracteriza-se como incidente de segurança da informação roubo ou extravio das informações, perda de informações ou equipamentos que armazenem informação, ataques de negação de realização do serviço conforme procedimentos, acesso ou uso não autorizado de um sistema, acesso às instalações da organização sem a devida identificação ou qualquer outro fator que desrespeite a política de segurança da informação estabelecida;

6.2 É de responsabilidade do Comitê de Segurança avaliar continuamente as atividades realizadas para verificação da usabilidade das políticas;

6.3 Todo o incidente que for detectado pelo Comitê de Segurança ou por qualquer um dos colaboradores da instituição deve ser imediatamente registrado;

6.4 Após o registro, cabe ao comitê aplicar as sanções legais para resolução do problema, seja em adaptação do procedimento realizado ou da política;

6.5 Os incidentes detectados de maior importância devem constar em um relatório de ocorrências em posse da Comissão de Segurança, para que posteriormente possa ser encaminhada solução cabível a falha;

6.6 A partir do momento em que for detectado um incidente de informação o problema deve ser solucionado pelo Comitê de Segurança o mais rápido possível, de maneira eficiente, evitando que afete outras determinações da política;

6.7 Com a apresentação do relatório de incidentes também é necessária a apresentação de uma investigação do incidente e de suas causas;

6.8 Os incidentes de segurança da informação podem ser classificados em: baixo, médio e alto, sendo de responsabilidade do Comitê de Segurança julgar a classificação dos incidentes;

6.9 A denúncia de irregularidade quanto a política devem ser informados ao Comitê de Segurança e registrado por eles no livro de incidentes de segurança da informação, apresentando o infrator, a data, a hora e o incidente;

6.10 Cabe ao Comitê de Segurança julgar quais serão as sanções aplicáveis aos infratores da segurança da informação em conjunto com a diretoria do hospital, sendo que essas sanções podem ser comunicados e treinamentos ou até mesmo demissões.

7 MANUTENÇÃO DA POLÍTICA

Para que a política de segurança da informação possa estar sempre em conformidade com as mudanças de procedimentos e as adaptações da própria organização é necessária uma revisão constante.

7.1 Cabe ao Comitê de Segurança revisar anualmente as políticas de segurança da informação com o objetivo de realizar mudanças ou adaptações;

7.2 Entretanto, a qualquer momento que for percebida a necessidade de uma alteração ela pode ser realizada;

7.3 Todos os fatos novos que venham a ser percebidos e não estejam incorporados à política deverão ser incluídos;

7.4 É necessário que o Comitê de Segurança esteja atento às mudanças na estrutura organizacional da empresa para verificar se esse fato pode acarretar impactos à política;

7.5 O processo de revisão deve abranger, no mínimo, os critérios de: riscos identificados, alterações na legislação do negócio, incidentes de segurança, vulnerabilidades percebidas, alterações na estrutura organizacional e nos clientes da organização;

7.6 Em caso de alteração da política o novo modelo proposto deverá ser avaliado e autorizado pelas diretorias do hospital, constando a assinatura das diretorias e do Comitê de Segurança;

7.7 Sempre que forem feitas alterações nas políticas todos os colaboradores deverão ser informados por meio de palestras, treinamentos, comunicados ou meios similares.

8 APROVAÇÃO DA ALTA GERÊNCIA DO HOSPITAL DO TRABALHADOR

Por estar ciente dos termos constantes nessa política de informação, declaro que a partir de sua publicação ela passa a valer em todo o ambiente da organização bem como dos órgãos a ele subordinados.

Curitiba, 01 de Dezembro de 2008

_____

Direção Geral

APÊNDICE H – Formulário de Validação da Política de Segurança da Informação

FORMULÁRIO DE VALIDAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Caro colega,
Nesse momento de finalização do projeto, é de grande importância que você responda a esse questionário com sinceridade. Minha intenção é avaliar o quanto a política de segurança da informação proposta é capaz de atender o Hospital do Trabalhador.
Marque apenas uma das opções que melhor represente a sua opinião.
Agradeço a sua colaboração.

Suelen

1. As políticas de segurança da informação sugeridas foram compreendidas facilmente por mim.
(1) Discordo totalmente
(2) Discordo parcialmente
(3) Indiferente
(4) Concordo parcialmente
(5) Concordo totalmente

2. Acredito que com a implantação das políticas de segurança da informação meu trabalho será favorecido.
(1) Discordo totalmente
(2) Discordo parcialmente
(3) Indiferente
(4) Concordo parcialmente
(5) Concordo totalmente

3. Utilizaria as políticas de segurança da informação sem restrições, se aprovadas pela alta gerência.
(1) Discordo totalmente
(2) Discordo parcialmente
(3) Indiferente
(4) Concordo parcialmente
(5) Concordo totalmente

4. Sinto-me mais seguro em saber que existem políticas específicas para a realização de minhas atividades.
(1) Discordo totalmente
(2) Discordo parcialmente
(3) Indiferente
(4) Concordo parcialmente
(5) Concordo totalmente

5. Acredito que com as políticas de segurança da informação todas as atividades relacionadas a prontuários médicos serão melhoradas.
(1) Discordo totalmente
(2) Discordo parcialmente
(3) Indiferente
(4) Concordo parcialmente
(5) Concordo totalmente

6. Com as políticas de segurança da informação os riscos de incidentes com os prontuários médicos são minimizados.
(1) Discordo totalmente
(2) Discordo parcialmente
(3) Indiferente
(4) Concordo parcialmente
(5) Concordo totalmente

7. Dê uma breve declaração de seus pensamentos quanto às políticas de segurança da informação.
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Obrigada!

APÊNDICE I – Formulário de Solicitação de alteração das Políticas de Segurança da Informação

FORMULÁRIO DE SOLICITAÇÃO DE ALTERAÇÃO DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

NOME:

SETOR:

PROBLEMA DETECTADO

SOLUÇÃO PROPOSTA

JUSTIFICATIVA

DATA: _____/_____/_____ **_____**

ASSINATURA

ANEXO A – Formulários de Validação da Política de Segurança da Informação Respondidos