Faculdade SENAC de Ciências Exatas e Tecnologia

Carlos Alberto Rodrigues Barboza

CONTROLES DE SEGURANÇA EM UM SISTEMA DE *WORKFLOW* PARA O PROCESSO DE PERÍCIA MÉDICA PARA A CONCESSÃO DE BENEFÍCIO.

São Paulo
2005

CARLOS ALBERTO RODRIGUES BARBOZA

CONTROLES DE SEGURANÇA EM UM SISTEMA DE *WORKFLOW* PARA O PROCESSO DE PERÍCA MÉDICA PARA A CONCESSÃO DE BENEFÍCIO.

Trabalho de Conclusão de Curso de Pós Graduação de Segurança de Redes e Sistemas apresentado à Faculdade SENAC de Ciências Exatas e Tecnologia.

Orientador Prof. Dr. Volnys Borges Bernal

São Paulo
2005

Aluno: Carlos Alberto Rodrigues Barboza
Título: Controles de segurança em um sistema de *Workflow* para o processo de perícia médica para a concessão de benefício
A banca examinadora dos Trabalhos de Conclusão em sessão pública realizada em 02/03/2005, considerou o candidato:

(X) aprovado ( ) reprovado

1) Examinador: Luis Gustavo Gaparini Kiatake.
2) Examinadora: Carmen Lucia dos Santos Namur.
3) Presidente: Adilson Eduardo Guelfi.

Aos meus pais e minha família.

AGRADECIMENTOS

Agradeço aos meus pais e familiares, que me iniciaram e apoiaram em meus estudos.

Ao meu orientador, professor Dr. Volnys Borges Bernal, que me forneceu todo o apoio e orientação necessária para a formulação e desenvolvimento deste trabalho.

Aos meus professores do curso de Pós-Graduação de Segurança de Redes e Sistemas e a Faculdade Senac de Ciências Exatas e Tecnologia, pelo acompanhamento acadêmico, que me proporcionou o feliz encontro com o conhecimento.

À empresa, Dataprev – Empresa de Tecnologia e Informações da Previdência Social - e ao Programa de Incentivo à Pós-Graduação, implementado na empresa e o qual fiz parte, que contribuiu e apoiou esta minha formação.

“Se conhecemos o inimigo e a nós mesmos, não precisamos temer o resultado de uma centena de batalhas. Se nos conhecemos, mas não ao inimigo, para cada vitória sofreremos uma derrota. Se não nos conhecemos nem ao inimigo, sucumbiremos em todas as batalhas”.

(Sun Tzu – A arte da guerra.)

RESUMO

A atividade de perícia médica deve ser executada conforme as determinações definidas pelo Conselho Federal de Medicina e pelo Conselho Regional de Medicina do Estado de São Paulo. Essa atividade permite informar suas conclusões em laudos médicos, que são armazenados em forma de prontuários médicos, que por sua vez, devem ser manipulados obedecendo a regras de segurança fundamentais para que as informações que constam nesse documento possam trazer todas as vantagens esperadas e projetadas.

Seguindo a tendência corporativa, a implementação de sistemas informatizados em atividades de perícia médica torna-se um caminho natural atualmente. Na escolha da Tecnologia da Informação mais adequada para esse fim, o Sistema de *Workflow*, apresenta-se como uma estratégia considerável.

Para tratar uma questão tão sensível, na qual as informações trazem repercussões importantes para a sociedade, devemos planejar e aplicar os requisitos de segurança, com cuidado compatível.

Os controles de segurança, propostos nesse trabalho, associados a uma proposta de fluxo de atividades de perícia médica para um sistema de *Workflow*, visam apresentar uma abordagem tecnologicamente atual, tornando as informações provenientes dos processos de perícia médica, plenamente confiáveis e disponibilizados a quem de direito.

Palavras-chave: Sistema de Segurança, Tecnologia da Informação, *Workflow*.

ABSTRACT

The job of medical expertness must to be made abide by rules of the Federal Counsel of Medicine and of the Regional Counsel of Medicine of the estate of São Paulo. It is job allow to put the conclusion in medical document, that are stored like medical prontuary, that must to be handled abide by security rules basics for the information inside it document, may to take all advantages hoped and projected.

Following the corporative trend, the implementation of automatic systems of medical expertness, becomes a natural way nowadays. To choice the Information Technology correct to it, the Systems of Workflow, show like an enough strategy.

For deal with a so sensible question, where the information comes important stuffs to the society, we must to plan and to do the security requests with much care.

The security controls to put in this work, together with the activity flow of medical expertness to systems of Workflow, want to show an approach in TI of today, becoming the information from of process of medical expertness, altogether trusty and availability to right people.

Keywords: Information of Technology, Security System, Workflow.

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O prontuário médico é um instrumento valioso para o paciente, para o médico e demais profissionais de saúde, além da instituição que o atende, bem como para o ensino, a pesquisa, a elaboração de censos, propostas de assistência à saúde pública e para a avaliação da qualidade da assistência médica prestada. O correto e completo preenchimento do prontuário tornam-se grandes aliados do médico para sua eventual defesa judicial junto a autoridade competente, bem como do tratamento mais eficaz ao paciente. A importância desse documento, somente terá toda sua relevância implementada e realmente utilizada, com a manutenção do adequado sigilo das informações confidenciais que ali constam. Para que esse sigilo seja real, torna-se fundamental toda uma infra-estrutura no tratamento da segurança dessas informações.

O processo de perícia médica, dentro da sociedade, é um processo de vital importância, pois possibilita ao médico analisar, avaliar e diagnosticar tanto a saúde do profissional, quanto o seu ambiente de trabalho. Desse modo, o profissional de perícia médica, tem condições de contribuir e auxiliar os profissionais de diversos segmentos da sociedade, a preservar, promover e restabelecer suas condições de boa saúde, promovendo assim a qualidade de vida, além de subsidiar tecnicamente a decisão para a concessão de benefícios. As conclusões inerentes a essa atividade, são disponibilizadas no laudo médico, que por sua vez merece a mesma infra-estrutura de segurança utilizada no prontuário médico.

Atualmente a Tecnologia da Informação tem apresentado um crescimento muito grande, no mundo hoje globalizado, proporcionando as corporações novos métodos de interação entre clientes, fornecedores, governo e sociedade. Dentre esses métodos de interação, temos os desenvolvimentos de processos utilizando a

Tecnologia da Informação, de maneira bastante consolidada, através de sistemas informatizados. Esses sistemas informatizados proporcionam maior rapidez e confiabilidade nos processos realizados dentro das organizações, além de torna-los altamente dinâmicos. Desse modo, esse cenário vem se tornado a cada dia mais fundamental e extremamente necessária.

A segurança corporativa, sempre ocupou posição de destaque nas organizações. Quando as entidades se organizam para tratar a segurança, grandes esforços são direcionados para tratar a segurança dos processos realizados por ela. Com o aumento do uso da tecnologia para a realização de diversificados processos, e a eminente necessidade de oferecer a adequada segurança a esses processos, surge no cenário corporativo, a real necessidade de planejamento, implementação, gerenciamento e manutenção da segurança da Tecnologia da Informação. Aliado a esse cenário atual, temos a crescente atuação de agentes maliciosos, que fazem uso dos recursos proporcionados pela tecnologia, com objetivos escusos. Essa atuação, por sua vez, tem a cada dia aumentado em quantidade e em sofisticação. Por essa razão, as corporações, o governo e a sociedade, devem apresentar constantemente soluções para garantir a segurança de seus processos informatizados.

Os sistemas de *Workflow* têm o objetivo de organizar e gerenciar o fluxo dos processos, utilizando sistemas computacionais de tal forma a aumentar a produtividade, flexibilidade e o gerenciamento dos dados.

As organizações têm como premissa básica, a devida consciência, de que a Tecnologia da Informação, aliado a sistemas de *Workflow*, tendo o devido e correto tratamento do ponto de vista de segurança, tanto das informações quanto dos processos e do ambiente, oferecem ao negócio a realidade de agregar valor.

Baseado nesse cenário e na análise de risco do ambiente, este trabalho visa apresentar controles de segurança para um sistema de *Workflow* que trata da atividade de perícia médica. O sistema de *Workflow* permite o gerenciamento do fluxo deste processo desde a solicitação da perícia médica, até o deferimento ou não da solicitação. Estes fluxos tratam o tramite de emissão, armazenamento e devida disponibilização de laudo médico e resultado de solicitação de benefício, considerando os adequados controles de segurança da informação.

1.1 Escopo

O escopo deste trabalho trata do ambiente, do fluxo do sistema e dos processos inerentes a atividade de perícia médica destinada à concessão de benefícios. A proposta da solução é tratar todo o processo de modo eletrônico, utilizando assinatura digital. Estão excluídos do escopo deste trabalho, a proteção de perímetro, segurança ambiental e física, controle de acesso físico, disponibilidade e escalabilidade.

2 PRONTUÁRIO MÉDICO

Segundo o Conselho Federal de Medicina (RESOLUÇÃO CFM número 1.638, 2002) o prontuário médico é o documento único constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo. Portanto, trata-se do conjunto de documentos padronizados, ordenados e concisos, destinados ao registro de todas as informações referentes aos cuidados médicos e paramédicos, prestados ao paciente.

O Código de Ética Médica (CEM) do Conselho Federal de Medicina (RESOLUÇÃO CFM número 1.246, 1988), estabelece diretrizes a respeito de prontuário médico. A seguir estão apresentadas as principais para este trabalho.

2.1 Preceitos básicos do prontuário médico

As anotações no prontuário ou ficha clínica devem ser feitas de forma legível, permitindo, inclusive, identificar os profissionais de saúde envolvidos no cuidado ao paciente. Além disso, o médico está obrigado a assinar e carimbar ou, então, assinar, escrever seu nome legível e sua respectiva inscrição no CRM. É importante enfatizar que não há lei que obrigue o uso do carimbo. Nesse caso, o nome do médico e seu respectivo CRM devem estar legíveis.

Itens obrigatórios que devem constar do prontuário médico:

- identificação da paciente;
- anamnese;

- exame físico;
- hipóteses diagnósticas;
- diagnóstico(s) definitivo(s);
- tratamento(s) efetuado(s).

O prontuário médico é um documento de manutenção permanente pelos médicos e estabelecimentos de saúde. Ele pode ser, posteriormente, utilizado pelos interessados como meio de prova até que transcorra o prazo prescricional de 20 anos para efeitos de ações que possam ser impetradas na Justiça.

Todos os documentos originais que compõem o prontuário devem ser guardados pelo prazo mínimo de 10 anos, a fluir da data do último registro de atendimento da paciente. Ao final desse tempo, o prontuário pode ser substituído por métodos de registro capazes de assegurar a restauração plena das informações nele contidas (microfilmagem, por exemplo) e os originais poderão ser destruídos.

Compete ao médico, em seu consultório, e aos diretores clínicos e/ou diretores técnicos, nos estabelecimentos de saúde, a responsabilidade pela guarda dos documentos.

2.2 Acesso ao prontuário médico

O acesso ao prontuário médico deve ser permitido mediante as seguintes situações:

2.2.1 Solicitação do próprio paciente

É importante salientar que o prontuário pertence ao paciente e que, por delegação deste, pode ter acesso ao mesmo o médico. Portanto, é um direito do

paciente ter acesso, a qualquer momento, ao seu prontuário, recebendo por escrito o diagnóstico e o tratamento indicado, com a identificação do nome do profissional e o número de registro no órgão de regulamentação e controle da profissão (CRM, Coren etc.), podendo, inclusive, solicitar cópias do mesmo.

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

2.2.2 Solicitação dos familiares e/ou do responsável legal do paciente

Quando da solicitação do responsável legal pelo paciente – sendo este menor ou incapaz – o acesso ao prontuário deve ser-lhe permitido e, se solicitado, fornecer as cópias solicitadas ou elaborar um laudo que contenha o resumo das informações lá contidas. Caso o pedido seja feito pelos familiares do paciente, será necessária a autorização expressa dele. Na hipótese de que ele não tenha condições para isso ou tenha ido a óbito, as informações devem ser dadas sob a forma de laudo ou até mesmo cópias. No caso de óbito, o laudo deverá revelar o diagnóstico, o procedimento do médico e a "*causa mortis*". Entenda-se que, em qualquer caso, o prontuário original, na sua totalidade ou em partes, não deve ser fornecido aos solicitantes, pois é documento que, obrigatoriamente, precisa ser arquivado pela entidade que o elaborou. Entenda-se, também, que os laudos médicos não devem ser cobrados facultando-se, porém, a critérios da entidade, a cobrança das xerocópias quando fornecidas por ela.

2.2.3 Solicitação em ações judiciais

Em ações judiciais, o prontuário médico, exames complementares ou outros documentos, só podem ser liberados por autorização expressa do próprio assistido.

Deve o perito-médico judicial, fornecer cópia de todos os documentos disponíveis para que os assistentes-técnicos elaborem seus pareceres. Em caso da necessidade do perito-médico judicial vistoriar a empresa (tanto os locais de trabalho como os documentos sob sua guarda), ele deverá informar, oficialmente, o fato, com a devida antecedência, aos assistentes-técnicos das partes (ano, mês, dia e hora dessa perícia).

2.2.4 Solicitação por outras entidades

Salvo com autorização expressa do paciente, é vedado ao médico fornecer tais informações. Sem o consentimento do paciente, o médico não poderá revelar o conteúdo de prontuário ou ficha médica (Artigo 102 do CEM), salvo por justa causa, isto é, quando diante de um estado extremo de necessidade. Haverá justa causa quando a revelação for o único meio de conjurar perigo atual ou iminente e injusto para si e para outro. Os diretores técnicos ou clínicos que autorizarem a saída de prontuário das suas instituições violam o artigo 108 do CEM. O acesso ao prontuário pela figura do médico auditor enquadra-se no princípio do dever legal, já que tem ele atribuições de peritagem sobre a cobrança dos serviços prestados pela entidade, cabendo ao mesmo opinar pela regularidade dos procedimentos efetuados e cobrados, tendo, inclusive, o direito de examinar o paciente, para confrontar o descrito no prontuário. Todavia, esse acesso sempre deverá ocorrer dentro das dependências da instituição de assistência à saúde responsável por sua posse e

guarda, não podendo a instituição ser obrigada, a qualquer título, a enviar os prontuários aos seus contratantes públicos ou privados (Resolução CFM número 1614, 2001).

2.2.5 Segredo médico

O segredo médico é uma espécie de segredo profissional, ou seja, resulta das confidências que são feitas ao médico pelos seus clientes, em virtude da prestação de serviço que lhes é destinada. O segredo médico compreende, então, confidências relatadas ao profissional, bem como as percebidas no decorrer do tratamento e, ainda, aquelas descobertas e que o paciente não tem intenção de informar. Desta forma, o segredo médico é, penal (artigo 154 do Código Penal) e eticamente, protegido (artigo 102 e seguintes do Código de Ética Médica), na medida em que a intimidade do paciente deve ser preservada. Entretanto, ocorrendo as hipóteses de "justa causa" (circunstâncias que afastam a ilicitude do ato), "dever legal" (dever previsto em lei, decreto, etc.) ou autorização expressa do paciente, o profissional estará liberado do segredo médico. Assim, com as exceções feitas acima, aquele que revelar as confidências recebidas em razão de seu exercício profissional deverá ser punido. É de se ressaltar, que o segredo médico também não deve ser revelado para a autoridade judiciária ou policial. Não há disposição legal que respalde ordens desta natureza. É oportuno salientar que este entendimento foi sufragado pelo Colendo Supremo Tribunal Federal ao julgar o "*Habeas Corpus*" nº 39308 de São Paulo, cuja ementa é a seguinte:

Constitui constrangimento ilegal a exigência da revelação do sigilo e participação de anotações constantes das clínicas e hospitais. Conseqüentemente, a requisição judicial, por si só, não é "justa causa". Entretanto, a solução para que as

autoridades obtenham informações necessárias é que o juiz nomeie um perito médico, a fim de que o mesmo manuseie os documentos e elabore laudo conclusivo sobre o assunto. Ou então, solicitar ao paciente a autorização para fornecer o laudo médico referente a seu estado.

Outrossim, deverão ser sempre resguardadas todas as informações contidas no prontuário médico por força do sigilo médico que alcança, além do médico, todos os seus auxiliares e pessoas afins que, por dever de ofício, tenham acesso às informações confidenciais constantes do prontuário.

A observância do sigilo médico constitui-se numa das mais tradicionais características da profissão médica. O segredo médico é um tipo de segredo profissional e pertence ao paciente. Sendo o médico o seu depositário e guardador, somente podendo revelá-lo em situações muito especiais como: dever legal, justa causa ou autorização expressa do paciente. Revelar o segredo sem a justa causa ou dever legal, causando dano ao paciente, além de antiético é crime, capitulado no artigo 154 do Código Penal Brasileiro (http://www.cremesp.org.br, 2004).

2.3 Prontuário eletrônico

O Prontuário eletrônico do paciente, conforme definições internacionais é um registro eletrônico de dados do paciente armazenado em um sistema capaz de capturar, transmitir, receber, armazenar, disponibilizar e manipular dados, oferecer aos usuários disponibilização de dados confiáveis e recursos como sistemas de apoio à decisão, *links* para bases de conhecimento médico e outros. O prontuário eletrônico deve obedecer aos preceitos básicos inerentes ao prontuário médico, conforme o CEM do Conselho Federal de Medicina (RESOLUÇÃO CFM número 1.246, 1988).

Para possibilitar a elaboração e o arquivamento do prontuário eletrônico, foi elaborado pelo Conselho Federal de Medicina, as Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico (RESOLUÇÃO CFM Número 1.639, 2002), que determina um conjunto de requisitos que são descritos a seguir.

2.3.1 Integridade da informação e qualidade do serviço

O sistema de informações deverá manter a integridade da informação através do controle de vulnerabilidades, de métodos fortes de autenticação, do controle de acesso e métodos de processamento dos sistemas operacionais conforme a norma ISO/IEC (ISO/IEC 15408, 1999), para segurança dos processos de sistema. Possuir mecanismos de certificação de origem que garantam que somente informações oriundas de servidores internos a rede sejam aceitas por estações clientes e vice-versa. Considerar a premissa do caminho não autorizado a fim de evitar o acesso ao banco de dados por conexões de rede diferente que não a do servidor de aplicação ou estações que contenham aplicação real do sistema, evita-se, desta forma, o acesso direto ao arquivo fonte do banco de dados bem como a visualização ou manipulação do seu conteúdo. Garantir a verificação da integridade dos dados armazenados no prontuário eletrônico, sempre que houver recuperação da informação.

2.3.2 Cópia de segurança

Deverá ser feita cópia de segurança dos dados do prontuário pelo menos a cada 24 horas. Recomenda-se que o sistema de informação utilizado possua a funcionalidade de forçar a realização do processo de cópia de segurança

diariamente. O procedimento de *backup* deve seguir as recomendações da norma da Associação Brasileira de Normas Técnicas (ABNT) (NBR ISO/IEC 17799), através da adoção dos seguintes controles:

a) Documentação do processo de *backup* e *restore*;

b) As cópias devem ser mantidas em local distante o suficiente para livrá-las de danos que possam ocorrer nas instalações principais;

c) Mínimo de três cópias para aplicações críticas;

d) Proteções físicas adequadas de modo a impedir acesso não autorizado;

e) Possibilitar a realização de testes periódicos de restauração.

Implementar mecanismo que assegure que os dados só possam ser retirados do sistema prontuário eletrônico para o caso de comunicação, conforme descrito abaixo ou para salva guarda (*backup*) da base de dados, contemplando as seguintes características de exportação e importação:

I) Exportar os atributos de segurança em conjunto com os dados;

II) Garantir na restauração de uma cópia de segurança que os atributos de segurança e suas associações sejam automaticamente recuperados, sem a intervenção do administrador;

III) Assegurar que somente o administrador do sistema prontuário eletrônico ou usuário com perfil específico possa restaurar uma cópia de segurança.

2.3.3 Bancos de dados

Os dados do prontuário deverão ser armazenados em sistema que assegure, pelo menos, as seguintes características:

a) Compartilhamento dos dados;

b) Independência entre dados e programas;

c) Mecanismos para garantir a integridade, controle de conformidade e validação dos dados;

d) Controle da estrutura física e lógica;

e) Linguagem para a definição e manipulação de dados (SQL - *Standard Query Language*);

f) Funções de auditoria e recuperação dos dados.

2.3.4 Privacidade e confidencialidade

Com o objetivo de garantir a privacidade, confidencialidade dos dados do paciente e o sigilo profissional, faz-se necessário que o sistema de informações possua mecanismos de acesso restrito e limitado a cada perfil de usuário, de acordo com a sua função no processo assistencial:

a) Recomenda-se que o profissional entre pessoalmente com os dados assistenciais do prontuário no sistema de informação;

b) A delegação da tarefa de digitação dos dados assistenciais coletados a um profissional administrativo não exime o médico, fornecedor das informações, da

sua responsabilidade desde que o profissional administrativo esteja inserindo estes dados por intermédio de sua senha de acesso;

c) A senha de acesso será delegada e controlada pela senha do médico a quem o profissional administrativo está subordinado;

d) Deve constar da trilha de auditoria quem entrou com a informação;

e) Todos os funcionários de áreas administrativas e técnicas que, de alguma forma, tiverem acesso aos dados do prontuário deverão assinar um termo de confidencialidade e não-divulgação, em conformidade com a norma ABNT NBR ISO/IEC 17799.

2.3.5 Autenticação

O sistema de informação deverá ser capaz de identificar cada usuário através de algum método de autenticação. Em se tratando de sistemas de uso local, no qual não haverá transmissão da informação para outra instituição, é obrigatória a utilização de senhas. As senhas deverão ser de no mínimo 5 caracteres, compostos por letras e números. Trocas periódicas das senhas deverão ser exigidas pelo sistema no período máximo de 60 (sessenta) dias. Em hipótese alguma o profissional poderá fornecer a sua senha a outro usuário, conforme preconiza a norma da ABNT NBR ISO/IEC 17799. O sistema de informações deve possibilitar a criação de perfis de usuários que permita o controle de processos do sistema.

Incorporar o uso de certificados digitais emitidos por Autoridade Certificadora (AC) de terceira parte confiável, (Medida Provisória 2.200-2, 2001),

para processos de autenticação dos profissionais nos sistemas de prontuário eletrônico.

Incorporar mecanismos de assinatura digital pelo certificado digital pessoal do profissional usuário com acesso ao sistema prontuário eletrônico. Assegurar que os certificados digitais sejam utilizados apenas para a assinatura eletrônica de registros incluídos em um sistema prontuário eletrônico.

2.3.6 Auditoria

O sistema de informações deverá possuir registro (log) de eventos, conforme prevê a norma ABNT (NBR ISO/IEC 17799, 2001). Estes registros devem conter:

a) A identificação dos usuários do sistema;

b) Datas e horários de entrada (*log-on*) e saída (*log-off*) no sistema;

c) Identidade do terminal e, quando possível, a sua localização;

d) Registro das tentativas de acesso ao sistema, aceitas e rejeitadas;

e) Registro das tentativas de acesso a outros recursos e dados, aceitas e rejeitadas;

f) Registro das exceções e de outros eventos de segurança relevantes devem ser mantidos por um período de tempo não inferior a 10 (dez) anos, para auxiliar em investigações futuras e na monitoração do controle de acesso;

g) Informações de controle de acesso à inclusão e manutenção de informações no prontuário eletrônico;

h) Informações sobre as funções administrativas realizadas pelo administrador de sistema;

i) Informações das transações criptográficas;

j) Informações sobre os avisos de realização de *backup*;

k) Informações sobre a exportação e importação de informações;

l) Informações sobre o processo de auditoria;

m) Informações sobre erros do *software* em qualquer um de seus módulos.

2.3.7 Transmissão de dados

Para a transmissão remota de dados identificados do prontuário, os sistemas deverão possuir um par de chaves e o respectivo certificado digital de aplicação única emitido por uma Autoridade Certificadora (AC) credenciada pelo Instituto Nacional de Tecnologia da Informação (ITI) responsável pela AC Raiz da Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil), a fim de garantir a identidade do sistema. Possuir mecanismos de canais seguros para comunicação entre estações cliente e servidores, servidores de aplicação e banco de dados, utilizando técnicas de criptografia. Para sistemas de prontuário eletrônico desenvolvidos em plataforma *WEB*, a comunicação entre clientes navegadores (*browsers*) e servidores, deve fazer uso do protocolo HTTPS para a autenticação de servidor e tráfego criptografado dos dados do prontuário eletrônico.

3 PERÍCIA MÉDICA

Tendo em vista que todo médico, ao atender seu paciente, deve avaliar a possibilidade de que a causa de determinada doença, alteração clínica ou laboratorial possa estar relacionada com suas atividades profissionais, investigando-a da forma adequada e, quando necessário, verificando o ambiente de trabalho, a atividade de perícia médica tem o objetivo de emitir parecer técnico conclusivo na avaliação da incapacidade laborativa, em face de situações previstas em lei, bem como a análise do requerimento dos benefícios.

Conforme a Resolução do Conselho Regional de Medicina do Estado de São Paulo (RESOLUÇÃO CREMESP número 76, 1996), a atividade de perícia médica deve obedecer a alguns preceitos básicos. Os principais, para este trabalho que visa a perícia médica para a concessão de benéfico, são descritos a seguir.

3.1 Responsabilidades do médico em situação de perícia médica

São responsabilidades do médico no atendimento de seu paciente, avaliar a oportunidade de que a causalidade de determinada doença, alteração clínica ou laboratorial, possa estar relacionada ao trabalho, investigando-a clinicamente, laboratorialmente e, caso necessário, verificando o ambiente de trabalho. São atribuições do médico:

a) Tratar o trabalhador, elaborar seu prontuário médico e fazer todos os encaminhamentos devidos;
b) Fornecer atestados de pareceres para os afastamentos do trabalho sempre que necessário, considerando que o afastamento para repouso, para acesso a

terapias ou para afastar-se de determinados agentes agressivos, é parte do tratamento.

3.2 Responsabilidades do médico em relação ao laudo médico

Cabe aos médicos que atendem o paciente fornecer laudos, pareceres e relatórios de exame médico e dar encaminhamentos, sempre que necessário, para benefício do paciente e dentro dos preceitos éticos, quanto aos dados de diagnóstico, prognóstico e tempo previsto de tratamento. Quando requerido pelo paciente, deve o médico pôr à sua disposição tudo o que se refira ao seu atendimento (cópia dos exames e prontuário médico).

São atribuições e deveres do Perito Médico de instituições previdenciárias e seguradoras:

a) avaliar a (in) capacidade de trabalho do segurado, através do exame clínico, analisando documentos, provas e laudos referentes ao caso;
b) subsidiar tecnicamente a decisão para a concessão de benefícios;
c) comunicar, por escrito, o resultado do exame médico-pericial ao periciando, com a devida identificação do perito médico (CRM, nome e matrícula);
d) orientar o periciando para tratamento quando eventualmente não o estiver fazendo e encaminhá-lo para reabilitação quando necessário.

3.3 Acesso ao laudo médico

As anotações efetuadas no laudo médico e provenientes da atividade de perícia médica tornam esse registro efetivamente um prontuário médico. Portanto, as

regras de acesso a essas informações, devem ser as mesmas apresentadas na Resolução CFM número 1.246 (capitulo 2.2. deste trabalho).

4 REQUISITOS DE SEGURANÇA PARA REGISTRO ELETRÔNICO EM SAÚDE - RES

Segundo o Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (SBIS-CFM, 2004), o Registro Eletrônico em Saúde – RES é um repositório de informação a respeito da saúde de um ou mais indivíduos numa forma processável eletronicamente.

O objetivo do Registro Eletrônico em Saúde (RES) é apoiar o processo assistencial. Os primeiros beneficiários do RES são os pacientes e profissionais de saúde.

O RES é classificado em duas grandes subdivisões:

- RES compartilhável (RES-C)
- RES não compartilhável (RES-NC).

O RES-C é um modelo padronizado de informação, passível de acesso por vários usuários autorizados utilizando diferentes aplicações.

A diferença entre o RES-C e o RES-NC é a mesma que existe entre sistemas que são executados de forma isolada em um microcomputador e os sistemas distribuídos, baseados em rede, e que possibilitam maior troca de informação e compartilhamento de recursos.

4.1 Sistema de registro eletrônico de saúde - SRES

O Sistema de Registro Eletrônico de Saúde é o conjunto de componentes que constituem o mecanismo pelo qual os registros eletrônicos de saúde são criados, utilizados, armazenados e recuperados, incluindo pessoas, dados, regras e

procedimentos, dispositivos de armazenamento e processamento, comunicação e manutenção.

Categorias de Sistema RES:

- Sistema Local de RES – SRES-L.
- Sistema de RES Compartilhável – SRES-C

O Sistema Local de RES é um sistema de âmbito local de um prestador de assistência, contendo informação detalhada sobre os diversos encontros de uma pessoa com os serviços de saúde.

O Sistema de RES Compartilhável é um sistema local de RES que é capaz de enviar partes da sua informação a outros Sistemas de RES e receber extratos de informação de outros Sistemas de RES.

A arquitetura de Sistemas RES deve ser aberta e padronizada. A principal característica de um Sistema RES é a sua capacidade de compartilhar informação entre usuários habilitados. Existem dois níveis de compartilhamento de informação:

- Interoperabilidade funcional - A propriedade de um ou mais sistemas trocarem informação;
- Interoperabilidade semântica – A propriedade que garante que a informação compartilhada entre sistemas seja reconhecida a partir da definição formal de conceitos do domínio.

Conforme documento da *International Organization for Standardization Technical Committe* 215 (ISO/TC 215, 2004), para se atingir a interoperabilidade semântica, quatro pré-requisitos devem ser contemplados conforme descrito abaixo. Os dois primeiros também são necessários para a interoperabilidade funcional:

- Modelo padronizado de RES.

- Modelos padronizados de interface de serviços.
- Conjunto de modelos conceituais padronizados específicos do domínio.
- Conjunto padronizado de terminologias.

4.2 Níveis de garantia de segurança de sistemas de RES

Existem dois níveis de garantia de segurança (NGS) dos sistemas RES:

- Sistemas de registro eletrônico com assinatura manual (SRESAM), nível de garantia de segurança 1 (NGS1).
- Sistemas de registro eletrônico com assinatura digital (SRESAD), nível de garantia de segurança 2 (NGS2).

4.2.1 Requisitos do nível de garantia de segurança NGS1, sistemas denominados SRESAM

- Requisito RSEGM1: controle da versão do *software*.
- Requisito RSEGM2: autenticação e controle de acesso.
- Requisito RSEGM3: controle de fluxo da informação e integridade de dados para sistemas isolados.
- Requisito RSEGM4: controle de fluxo de informação e integridade de dados. para sistemas baseados em arquitetura cliente-servidor ou arquitetura WEB.
- Requisito RSEGM5: controle de sigilo e integridade.
- Requisito RSEGM6: copia de segurança e restauração de dados.
- Requisito RSEGM7: canais seguros de comunicação para sistemas de RES baseados em arquitetura cliente-servidor ou implementado em arquitetura WEB.

- Requisito RSEGM8: utilização de recursos computacionais.
- Requisito RSEGM9: auditoria.
- Requisito RSEGM10: documentação.

4.2.2 Requisitos do nível de garantia de segurança NGS2, sistemas denominados SRESAD.

Para atingir o NGS2 é necessário que o SRES atenda os requisitos para NGS1 e apresente ainda total conformidade com os requisitos abaixo:

- Requisito RSEGD1: origem dos certificados digitais.
- Requisito RSEGD2: controle de autenticação pelo uso de certificados digitais utilizados para assinatura digital.

5 SISTEMAS DE *WORKFLOW*

Segundo o *Workflow Management Coalition* (WfMC), uma associação de empresas e instituições que tem por objetivo, padronizar e disseminar os serviços de suporte a *Workflow*, é a automação, total ou parcial, de processos do negócio, na qual documentos, informações ou tarefas são passadas de um participante para outro através de ações, de acordo com regras configuradas de procedimentos. Um processo pode ser considerado como um conjunto de atividades que quando realizadas, atingem um determinado objetivo de trabalho.

Sistema de *Workflow* é um sistema que define, cria e gerencia a execução do fluxo de trabalho através de uso de *software*s que objetivam a automação e gestão do fluxo de trabalho. O sistema de *Workflow* interpreta o processo, interage com os participantes do fluxo de trabalho e conforme o projeto do sistema, invoca o uso de ferramentas de Tecnologia da Informação e aplicativos. Possibilita o acompanhamento e distribuição das atividades que compõem o fluxo de trabalho durante sua execução.

Workflow normalmente é composto de um número de níveis lógicos e cada qual é conhecido como uma atividade. Uma atividade pode envolver interação manual com um usuário ou participante do *Workflow*, ou a atividade poderia ser executada usando recursos computacionais.

Todo sistema de *Workflow* é orientado a processo. Um processo é criado, e normalmente sub-dividido em alguns sub-processos. Cada processo e sub-processo são compostos por algumas atividades. Uma atividade é um simples nível lógico no processo. Por isso, algumas vezes não é prático automatizar todas as atividades durante um projeto. Porém, o *Workflow* executa atividades automatizadas, enquanto

a definição dos processos descreverá todas as atividades, se eles são automatizadas ou manuais.

5.1 Conceitos de um Sistema de *Workflow*

A seguir são apresentados alguns conceitos relacionados à sistema de *Workflow* e que são relevantes para este trabalho.

5.1.1 Processo

Processo é um conjunto de atividades que tem o objetivo de transformar, montar, manipular e processar recursos para produzir bens e serviços.

5.1.2 Fluxo de trabalho

O fluxo de trabalho determina o que é executado e como as atividades interagem entre si. Ele é composto dessas atividades e baseado em regras do negócio, e são executados por participantes do processo que podem ser indivíduos, grupos de indivíduos ou sistemas automatizados (USIRONO, 2000).

5.1.3 Regras

Segundo Cruz (2000, p.109), regras são atributos que definem de que forma os dados que trafegam no fluxo de trabalho devem ser processados, roteados e controlados pelo sistema de *Workflow*. Cada dado enviado no *Workflow* contém informações que serão usadas por outro componente do *Workflow*. Associados a esses dados existem regras que determinam objetivamente a operação dos dados,

quais as atividades que devem recebe-lo, quais as rotas a seguir e quais cuidados especiais devem haver para tratar o dado.

São atributos da regra:

- Inicio: Indica a condição que inicia o processo, atividade ou rotina.
- Tempo: Determina o tempo mínimo e máximo para que cada atividade realize sua operação.
- Execução: Define quais tecnologias serão usadas.
- Notificação: Define como os usuários são avisados sobre ocorrências tais como, aprovação, reprovação, devolução ou envio de documentos.
- Segurança: Define quais usuários podem participar do processo, o que podem fazer e a quais informações terão acesso.
- Termino: Indica a condição que finaliza o processo, atividade ou rotina e se essa finalização será normal ou não.

5.1.4 Rotas

Segundo Cruz (2000, p.111), rota é o caminho lógico que, definido sob regras especificas, tem a função de transferir a informação dentro do processo, ligando as atividades associadas ao fluxo de trabalho. Rotas, para *Workflow*, é o controle de movimentação exercido sobre os documentos. Os tipos de rota são:

- Serial: Nesse tipo de rota existe apenas uma atividade anterior e uma atividade posterior. Cada atividade deve ser completada antes que ocorra a atividade seguinte.
- Paralelo: É quando um grupo de atividades podem ocorrer ao mesmo tempo, ou seja, paralelamente, e tem as mesmas atividades anterior e posterior.

- Condicional: Ocorre quando existe a possibilidade de serem usadas múltiplas rotas e a escolha da rota a ser usada é determinada por uma regra.

5.1.5 Papel ou *Role*

Segundo Cruz (2000, p.101), papel é o conjunto de características e habilidades necessárias para executar determinada tarefa ou tarefas pertencentes a uma atividade.

5.1.6 Instância

Segundo Cruz (2000, p.99), instância é uma ocorrência individual dentro de atividade corrente no processo produtivo. Cada vez que o sistema *Workflow* é acionado, cria-se uma nova instância.

5.1.7 Itens, listas de trabalho e atores

As instâncias que são criadas cada vez que o sistema *Workflow* é acionado, são itens de trabalho. O conjunto de itens de trabalho que cada usuário do *Workflow* deverá executar é chamado lista de trabalho. Os usuários por sua vez, são chamados de atores do *Workflow*.

5.1.8 Formulários e documentos

Documentos são coleções de dados, que colocados no *Workflow* são usados por uma instância dentro de um processo. Documentos contêm também

informações sobre o formato, processamento e a apresentação desses dados, recebendo a denominação de formulário.

5.1.9 Visões

Segundo Usirono (2003, p.60), visões são consultas pelas quais os usuários ou grupos de usuários vêem os documentos através de um ou mais atributos para que seja possível a execução de determinada atividade. As visões tornam possível o acompanhamento do fluxo de atividades que é coordenado pelo sistema de *Workflow*, possibilitando um controle do que foi ou do que está sendo executado.

5.2 Classificação dos sistemas de *Workflow*

O tipo de *Workflow* que uma organização deve usar depende da meta que se quer alcançar. Muitas organizações grandes usam mais que um produto de *Workflow* fornecido por diferentes empresas. Muitas vezes é usual para organizações usar o modelo que mistura todos esses tipos. Segundo Cruz (2000, p.84), de uma maneira geral, a seguinte divisão é adotada:

5.2.1 *Workflow* Ad Hoc

O tipo de *Workflow* Ad Hoc é o tipo mais simples de *Workflow* existente. É usado quando os processos são pouco estruturados. É característica desse tipo de *Workflow*, a negociação, e um novo definido por cada usuário, ou seja, os próprios usuários definem seus próprios processos. As tarefas que compõem esse sistema, geralmente são imprevisíveis ou desconhecidas, até o momento da sua execução, necessitando que os usuários sejam gerentes de seus próprios processos.

5.2.2 *Workflow* Administrativo

O tipo de *Workflow* Administrativo é voltado para rotinas administrativas, fazendo o tratamento de formulários e documentos inerentes as rotinas administrativas. Esse tipo de *Workflow* apresenta um grau maior de estruturação para gerenciar os processos, que o tipo Ad Hoc. Nesse tipo, as tarefas têm uma maior previsibilidade, e um processo pode ser repetido várias vezes. Os fluxos dos processos são pré-definidos e as regras são simples.

5.2.3 *Workflow* de Produção

O tipo de *Workflow* de Produção é orientado para grandes volumes de dados, complexas políticas de negócio, e altos recursos financeiros. Ou seja, esse tipo de *Workflow* é usado quando os processos estão bastante estruturados em suas regras. Nesse tipo, as tarefas são previsíveis, e com alto grau de repetição. As intervenções humanas são minimizadas. Devido a complexidade de desenvolvimento e automação empenhada nesse tipo de *Workflow*, geralmente ele suporta os processos da organização, o que o torna um sistema de missão critica. É característica desse tipo de *Workflow*, otimizar produtividade.

5.3 Conclusão

O Sistema de *Workflow* é uma tecnologia que permite a automação dos processos de um fluxo, aumentando o controle desses processos, minimizando as intervenções no gerenciamento e o atraso das atividades. Também obtemos a eliminação da realização de tarefas por pessoal ou setor errado.

Verificamos que com a utilização dessa tecnologia obtemos o aumento da qualidade do serviço executado e a rapidez na realização das atividades.

Portanto, com a implementação de um sistema de *Workflow*, a corporação obtém condições de implementar melhorias aos seus processos, e conseqüentemente, agregar valor ao negócio.

6 PROPOSTA DE FLUXO PARA PERÍCA MÉDICA

A proposta de um sistema para a automação do fluxo de trabalho da atividade de perícia médica envolve os seguintes itens:

- Definição da arquitetura do sistema de suporte ao *Workflow*;
- Modelagem do fluxo no *Workflow*.

As definições desses itens são descritas a seguir.

6.1 Arquitetura

A arquitetura recomendada é uma arquitetura em 3 camadas. Essa arquitetura permite a independência entre os componentes, e atinge os objetivos de eficiência, reutilização e facilidade de manutenção desejada. Essa arquitetura fornece uma maneira de dividir a funcionalidade envolvida na manutenção e apresentação dos dados de uma aplicação (VASKEVITCH, 1995). As três camadas são as seguintes:

- Camada de Apresentação;
- Camada de Aplicação;
- Camada de Banco de dados.

A arquitetura em três camadas separa a apresentação para o usuário, a base de dados e as ações tomadas. Essa separação é feita de tal modo que a lógica de negócio resida na camada de aplicação. Essa é chamada de camada física intermediária ou camada física de negócios. A maior parte do código escrito reside na camada de apresentação e de aplicação. Os dados da aplicação e as regras do negócio que governam o acesso e a modificação dos dados são representados separadamente, ou seja, toda a lógica do negócio fica no servidor de aplicação. A proposta da arquitetura é representada na figura 6.1.

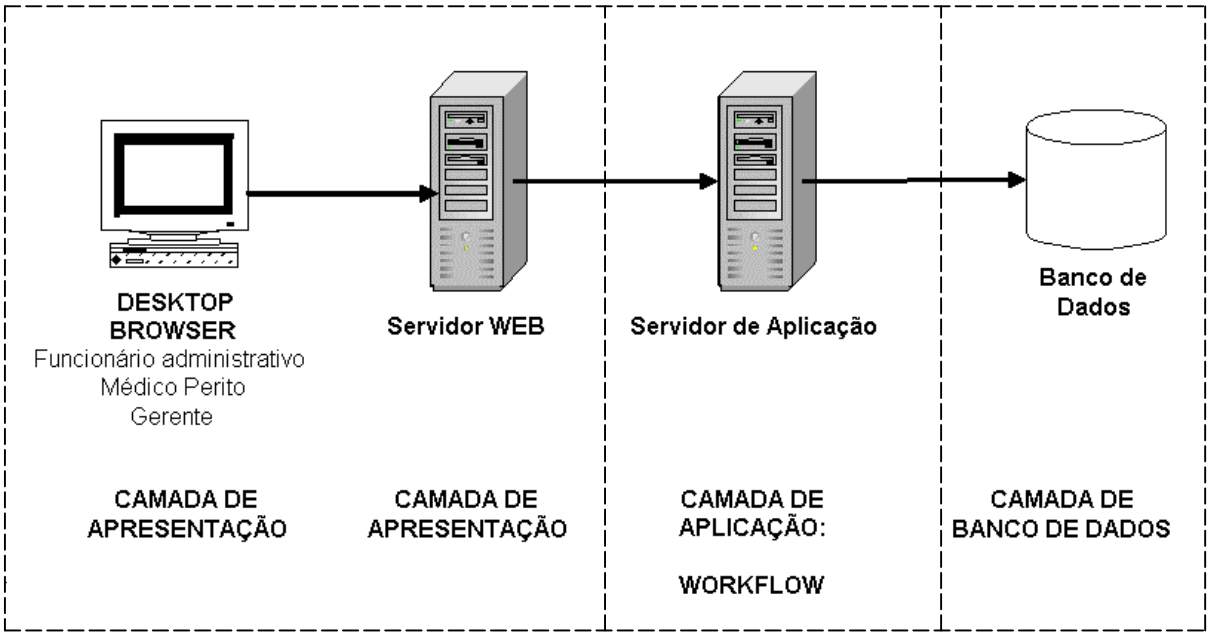


Figura 6.1 Arquitetura em 3 Camadas

6.1.1 Camada de apresentação

Na camada de apresentação temos duas partes. Primeiro o conceito de cliente *WEB* através do uso do *browser*, que é um cliente universal. O *browser* funciona como um componente de visualização para o usuário, é a interface com o usuário, trazendo o conteúdo da camada de aplicação para a interação do usuário através da segunda parte que é servidor *WEB*. Inclui os elementos de exibição no cliente, como HTML, XML, ASP, *Applets*. É usada para receber a entrada de dados e apresentar o resultado. O servidor *WEB* disponibiliza páginas criadas dinamicamente pelo servidor de aplicação, para os usuários autenticados. Na camada de apresentação é definido como os dados devem ser apresentados.

6.1.2 Camada de aplicação

O servidor de aplicação é responsável pela implementação da lógica do sistema, baseada nas regras do negócio, interagindo com o banco de dados e

disponibilizando paginas HTML para o servidor *WEB*. É responsável por tudo que a aplicação vai executar. Modela os dados e o comportamento por trás do processo de negócios.

6.1.3 Camada de banco de dados

Essa camada mantém um repositório de dados. Contém mecanismos de armazenamento persistente.

6.2 Sistema *Workflow* para processo de perícia médica

A seguir são descritos os atores e o fluxo de trabalho identificando regras, rotas e áreas funcionais pelas quais flui o processo de perícia médica. Em seguida temos o respectivo fluxograma, que faz o mapeamento dos processos e a representação dos fluxos de trabalho.

6.2.1 Principais atores

Os usuários do sistema são: paciente, pessoal administrativo, perito, gerente, sistema e auditor. O auditor em um fluxo somente para ele e que não será apresentado neste trabalho. Esses atores são responsáveis pela interação no sistema de *Workflow*.

6.2.2 Descrição do processo, fluxo de trabalho e interfaceamento com entidades, atores e rotas.

O modelo proposto é um sistema de *Workflow* tipo Produção. Nesse *Workflow* temos a existência de rota serial e rota condicional. O paciente solicita

benefício informando dados, que são entrados no sistema de agendamento pelo pessoal administrativo, dando inicio ao processo de concessão. O sistema faz os levantamentos e críticas verificando se o pedido é procedente e para isso é efetuada uma verificação no banco de dados da arrecadação e no banco de dados do Cadastro de Informações Sociais (CIS), no qual constam os vínculos empregatícios do paciente. Se pedido é procedente, é efetuado o agendando utilizando o banco de dados de peritos. O funcionário administrativo informa ao paciente a notificação do agendamento com o nome do médico, local, data e horário. Se pedido não é procedente, o paciente é notificado da reprovação da solicitação do benefício.

Na realização do atendimento médico para a execução da perícia, o funcionário administrativo realiza acesso ao módulo de atendimento médico para verificar a agenda e obter os dados do paciente e esse se apresenta para a perícia, confirmando a sua presença. O médico executa a perícia no paciente informando nesse sistema o laudo da perícia e informações a respeito do diagnóstico. O laudo é arquivado pelo sistema. Se a conclusão do laudo for negativo para a concessão do benefício, o paciente é notificado. Caso o benefício seja concedido, o sistema acessa o banco de dados da arrecadação e do CIS para o cálculo do valor do benefício. A autenticação dos laudos e conclusões de perícia médica são de competência dos setores de benefício, através da aprovação do benefício por parte do gerente. Se o benefício não for aprovado, o paciente é notificado. Se for aprovado, o sistema gera o documento de benefício para o paciente. O sistema arquiva o benefício ou a sua reprovação. A proposta de *Workflow* é representada nas figura 6.2 e 6.3. A figura 6.4 representa a simbologia utilizada no fluxograma.

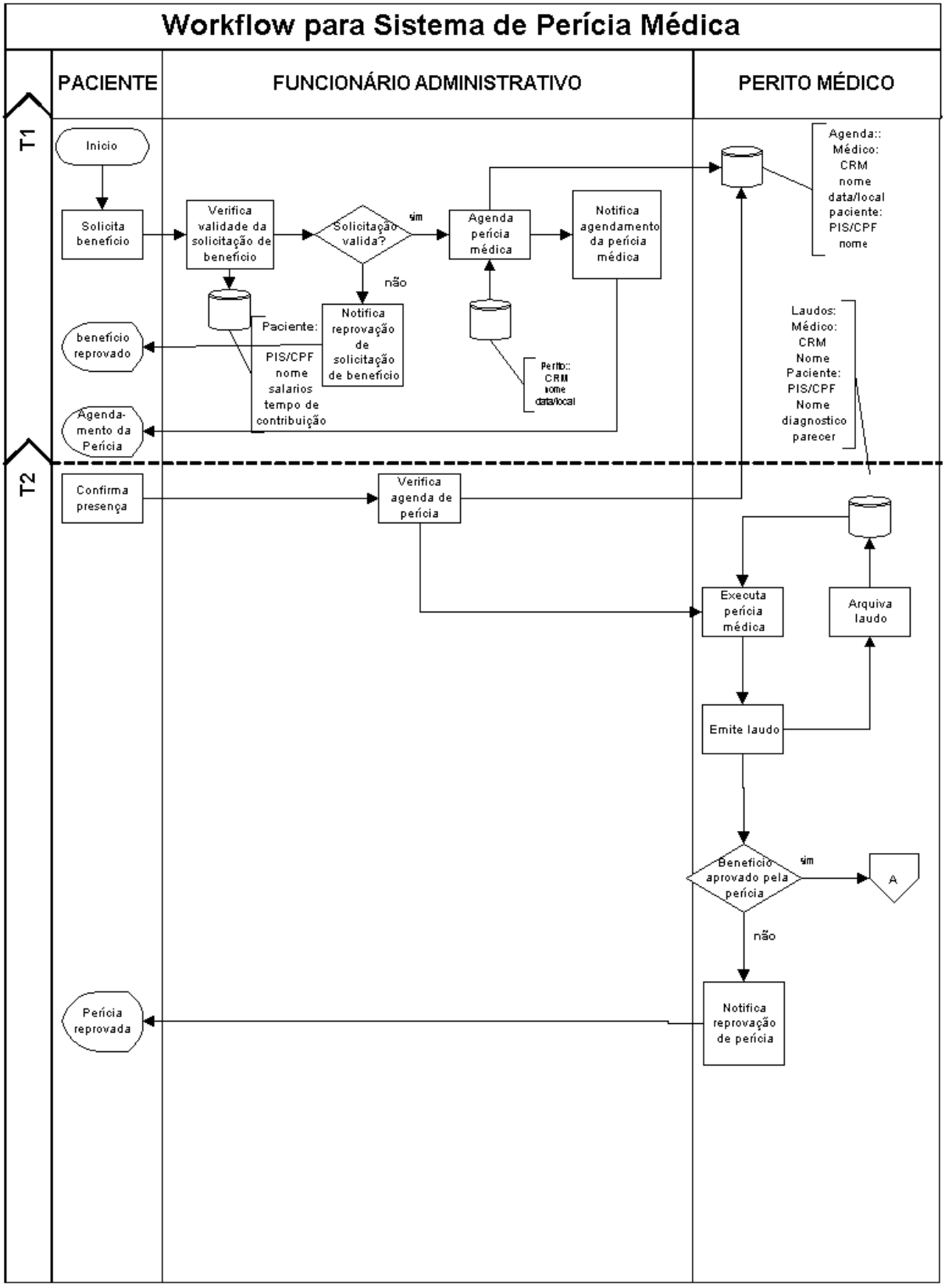


Figura 6.2 Fluxo para Perícia Médica

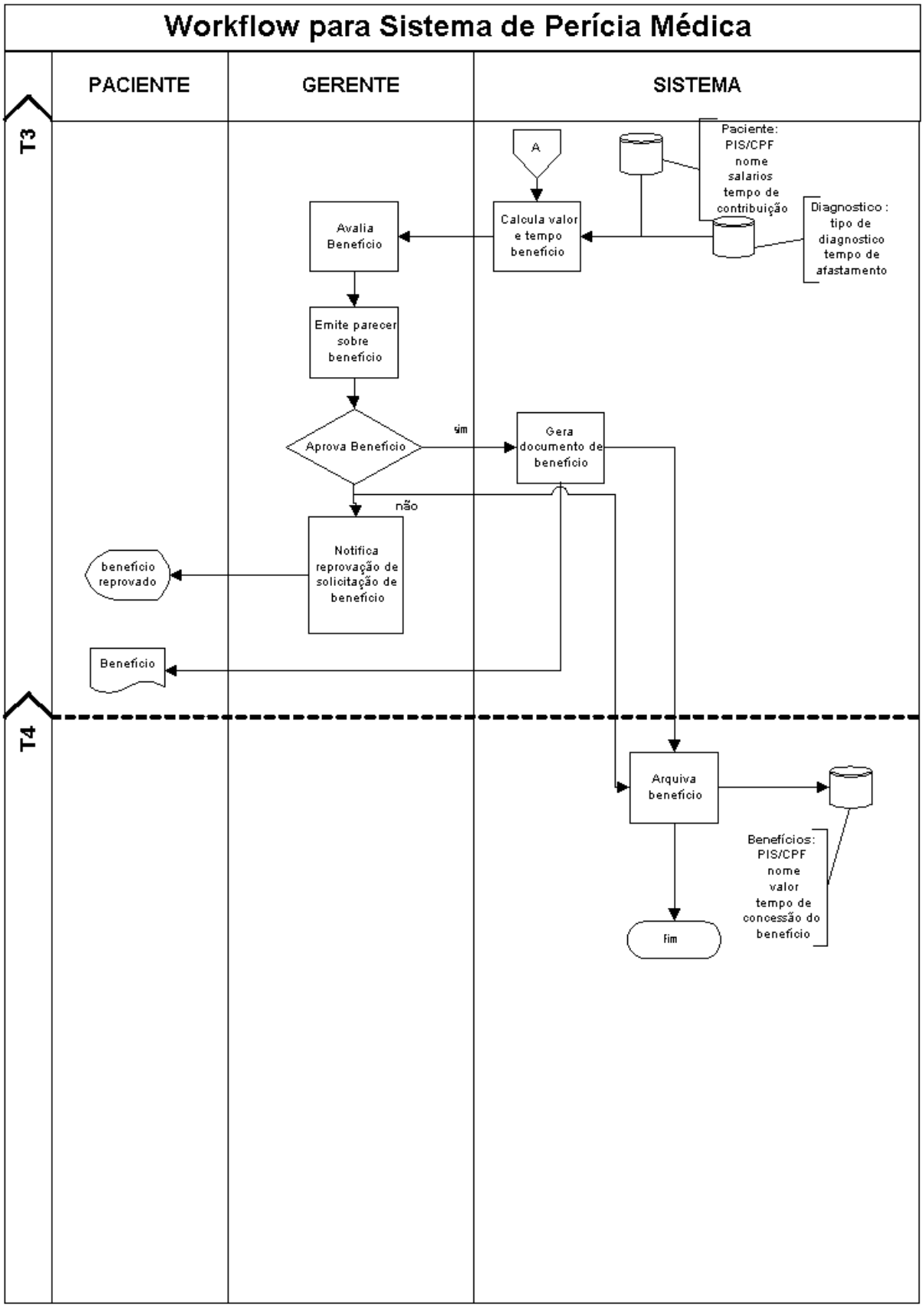


Figura 6.3 Fluxo para Perícia Médica

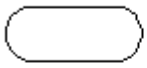
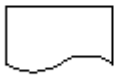
SIMBOLOGIA	DESCRIÇÃO
	Início e Término de um processo
	Operação
	Decisão
	Arquivo definitivo
	Espera ou Demora
	Conector de fluxo
	Conector de pagina ou folha
	Terminal
	Documento
	Banco de Dados
	Direção do Fluxo de informações

Figura 6.4 Simbologia de Fluxograma

7 ANÁLISE DE RISCO E CONTROLES DE SEGURANÇA

As definições sobre os controles de segurança a serem adotados devem estar baseadas em análise de risco. A seguir são apresentados alguns cenários de ameaças relevantes a serem consideradas na proteção do sistema de perícia médica e em seguida, os controles de segurança adequados.

7.1 Análise de risco

A Análise de Risco identifica os ativos da informação que o sistema possui, bem como as vulnerabilidades e as ameaças que podem afetá-lo, determinando a sua probabilidade de ocorrência e verificando o impacto no negócio. Tem por objetivo identificar os riscos de segurança presentes no processo, fornecendo conhecimento para que sejam implementados controles eficazes de segurança.

A análise de risco foi dividida do seguinte modo:

- Riscos de Infra-Estrutura.
- Riscos de Aplicação.

A seguir são apresentados cada um desses itens.

7.1.1 Riscos de infra-estrutura

Os riscos de infra-estrutura são aqueles que podem afetar as instalações e meios básicos para o funcionamento do sistema. Estão sujeitos a essas ameaças os *desktops*, servidores e meios de comunicação envolvidos no processo.

A seguir são listados alguns desses riscos.

a) Acesso não autorizado a registros do banco de dados - O banco de dados no qual estão armazenados os dados do sistema pode ser acessado por entidade

não autorizada. Uma entidade não autorizada pode inserir, consultar, modificar ou remover registros. Uma entidade não autorizada também pode apoderar-se através de roubo ou engenharia social, de um acesso legítimo de usuário do sistema. Existem diversos tipos de acesso, cada qual apresentando riscos específicos, que são apresentados na tabela 7.1.;

TIPO DE ACESSO	RISCO	IMPACTO
Consulta	Entidade não autorizada observar perícia, laudos e benefícios.	Não atendimento a determinações legais que obriga manter o sigilo.
Inserção	Entidade não autorizada inserir registros de perícia, laudo e benefícios indevidos.	Emissão de perícia e laudo falso e conseqüente benefício falso. Ocorrência de fraude. Prejuízo financeiro.
Remoção	Entidade não autorizada remover registros de perícias, laudos médicos e benefícios.	Impossibilidade de emissão de benefício. Imagem corporativa abalada.
Alteração	Entidade não autorizada a alterar registros pode alterar dados de perícia, laudo e benefícios.	Emissão de falso laudo e benefício indevido. Ocorrência de fraude. Prejuízo financeiro

Tabela 7. 1

b) Confidencialidade e integridade de comunicação entre *desktop* e servidor *WEB* - A comunicação entre o *desktop* e o servidor *WEB* pode ser observada, e/ou modificada por entidade não autorizada. Existem diversos tipos de acesso ao servidor WEB via *desktop*, cada qual apresentando riscos específicos, que são apresentados na tabela 7.2.;

USUÁRIO	RISCO OBSERVAÇÃO	RISCO MODIFICAÇÃO	IMPACTO
Funcionário Administrativo	Entidade não autorizada observar agendamentos.		Não atendimento a determinações legais que obriga manter o sigilo.
Funcionário Administrativo		Entidade não autorizada inserir agendamentos falsos e alterar registros de agendamentos de perícia.	Pacientes sem direito a solicitar o benefício executa perícia ou paciente com direito, tem agendamento desmarcado. Imagem corporativa abalada
Médico Perito	Entidade não autorizada observar perícia, laudos.		Não atendimento a determinações legais que obriga manter o sigilo.
Médico Perito		Entidade não autorizada inserir, alterar e remover registros de perícia e laudo indevidos.	Emissão de laudo e/ou benefício indevido. Ocorrência de fraude. Prejuízo financeiro.
Gerente	Entidade não autorizada observar perícia, laudos e benefícios aprovados.		Não atendimento a determinações legais que obriga manter o sigilo.
Gerente		Entidade não autorizada inserir, alterar e remover aprovações de benefícios.	Emissão de benefício falso. Ocorrência de fraude. Prejuízo financeiro.

Tabela 7. 2

c) Confidencialidade e integridade de comunicação entre servidor *WEB* e servidor de aplicação – A comunicação entre o servidor *WEB* e o servidor de aplicação pode ser observada, e/ou modificada por entidade não autorizada. Impacto: Não atendimento a determinações legais que obriga a manter o sigilo. Ocorrência de fraude. Prejuízo financeiro.

d) Confidencialidade e integridade de comunicação entre servidor de aplicação e servidor de banco de dados - A comunicação entre o servidor de aplicação e o servidor de banco de dados pode ser observada, e/ou modificada por entidade não autorizada. Impacto: Não atendimento a determinações legais que obriga a manter o sigilo. Ocorrência de fraude. Prejuízo financeiro.

e) Autenticação de parceiro de comunicação - Existem diversos riscos no qual podem ocorrer problemas relacionados à comunicação entre equipamentos como por exemplo, um servidor de banco de dados recebendo acesso de um servidor de aplicação impostor. Desse modo os dados enviados e recebidos do sistema de atendimento ao cliente podem ser inerentes a uma comunicação fraudulenta. Impacto: geração de agendamentos, laudos médicos e benefícios falsos, prejuízo financeiro.

f) Disponibilidade do sistema - Em caso de pane em *software* ou *hardware* de algum servidor envolvido no processo, o sistema pode ficar indisponível, tornado impossível o atendimento, a execução da perícia ou a aprovação de benefícios. Impacto: Imagem corporativa abalada.

7.1.2 Riscos de aplicação

Os riscos de aplicação são aqueles que podem afetar o funcionamento do sistema, afetando principalmente a qualidade da informação. Estão sujeitas a essas ameaças as interações dos usuários envolvidos no processo.

A seguir são listados alguns desses riscos.

a) Riscos na autenticação de usuários - Um usuário não autorizado pode personificar usuários autorizados. Existem diversos tipos de acesso, cada qual apresentando riscos específicos, que são apresentados na tabela 7.3.;

USUÁRIO	RISCO	IMPACTO
Funcionário Administrativo	Uma entidade não autorizada pode personificar-se como funcionário administrativo e acessar o sistema para efetuar uma solicitação falsa em nome de algum paciente.	Geração de solicitação falsa de perícia médica. Imagem corporativa abalada.
Médico Perito	Na autenticação do perito, pode haver a personificação de um perito médico por uma entidade não autorizada, executando falsa perícia médica.	Emissão de falso laudo médico, e de benefício indevido. Ocorrência de fraude. Prejuízo financeiro.
Gerente	Uma entidade não autorizada pode personificar o acesso como gerente.	Aprovação de benefício indevido. Ocorrência de fraude. Prejuízo financeiro.

Tabela 7. 3

b) Riscos na manipulação do laudo médico - Como o resultado da conclusão do laudo médico pode determinar a concessão ou indeferimento do requerimento do benefício, esse documento apresenta riscos específicos conforme os diversos tipos de acesso por uma entidade não autorizada, ocasionando impactos relevantes, tornado esse documento de importância crítica para o processo de perícia médica. São apresentados os principais riscos na tabela 7.4.;

TIPO DE ACESSO AO LAUDO MÉDICO	RISCO	IMPACTO
Consulta	Risco de uma entidade não autorizada ler e conhecer o conteúdo de laudos médicos que estão no banco de dados.	Não atendimento a determinações legais que obriga manter o sigilo.
Inserção	Risco de uma entidade não autorizada emitir laudo em nome de perito médico autorizado. Deve-se garantir que foi o médico que emitiu o laudo e não um impostor.	Laudo falso. Emissão de benefício indevido. Ocorrência de fraude. Prejuízo financeiro.
Remoção	Risco de eliminar do banco de dados um laudo médico.	Impossibilidade de avaliação do requerimento de benefício por parte do gerente. Imagem corporativa abalada.
Alteração	Risco de modificar um laudo médico, transformando um parecer negativo em positivo.	Laudo falso. Emissão de benefício indevido. Ocorrência de fraude. Prejuízo financeiro.

Tabela 7. 4

c) Riscos na manipulação de parecer de benefício - São apresentados os principais riscos na tabela 7.5;

TIPO DE ACESSO IRREGULAR	RISCO	IMPACTO
Modificação do parecer sobre benefício efetuado pelo gerente	Uma entidade não autorizada pode modificar o parecer sobre o benefício.	Emissão de benefício indevido; prejuízo financeiro.
Remoção de parecer sobre benefício emitido pelo gerente por entidade não autorizada.	Uma entidade não autorizada pode remover parecer sobre benefício emitido pelo gerente.	Perda de elementos do processo, impossibilidade de emissão de benefício; imagem corporativa abalada.
Leitura de parecer de benefício emitido pelo gerente por entidade não autorizada.	Uma entidade não autorizada pode ler o parecer sobre benefício emitido pelo gerente.	Não atendimento a determinações legais que obriga manter o sigilo.;

Tabela 7. 5

7.2 Controles de segurança

Os controles de segurança propostos são baseados na avaliação dos riscos que o sistema sofrerá e visa proporcionar os requisitos de confidencialidade, integridade, disponibilidade e irretratabilidade adequados as necessidades do sistema e desse modo, proteger a informação de uma gama extensiva de ameaças.

7.2.1 Autenticação

A autenticação visa comprovar a identidade de uma entidade. A autenticação deve ser realizada através de um método forte. O método escolhido é o de certificação digital com *smart card* pois, além de autenticar, é possível realizar a assinatura digital. A assinatura digital possibilita garantir a origem da geração de um documento, sua irretratabilidade e sua integridade durante todo o processo.

Um *smart card* é um cartão que pode ser comparado com um simples microcomputador, que pode obter, armazenar, processar e proteger dados. Ele é

equipado com um chip, ou seja, o cartão possui um circuito eletrônico de microcomputador com CPU, memórias, interface de entrada/saída e dispositivos antifraude. Este processamento pode proteger o conteúdo do usuário solicitando a entrada de uma senha por exemplo, e caso se entre com a senha errada em um número de vezes pré-determinado ele pode recusar por um período também pré-determinado. Cada usuário dever ter as chaves privadas e públicas geradas no *smart card*. A chave privada é armazenada e protegida por uma senha de acesso, o PIN. Esse cartão será programado para desempenhar a função de certificação digital X.509 (RFC 3280) nas autenticações do *logon* de todos os usuários do sistema de perícia médica.

7.2.2 Controle de acesso

O controle de acesso é a habilidade de limitar ou controlar o acesso a informação visando garantir que somente as entidades autorizadas consigam acesso a um determinado recurso. Visa garantir também que autorizações de acesso a um determinado recurso sejam dadas apenas pelos responsáveis e não sejam alteradas indevidamente. O controle de acesso à informação deve considerar as políticas de autorização e distribuição da informação.

O controle de acesso deve ser realizado através da definição de perfis e grupos baseados nos diferentes papéis da área de perícia médica. Devem existir os perfis de Funcionário administrativo, Perito médico, Gerente, Administrador, Auditor e *backup*. Esses perfis serão gerenciados por um administrador que por sua vez será autenticado no sistema através de assinatura digital via *smart card*.

Seguindo determinação da ABNT (NBR ISO/IEC 17799, 2001) terminais inativos devem ser desligados automaticamente após um período pré-determinado

de inatividade. Restringir os tempos de conexão às horas normais de expediente quando não existir requisitos para jornada extra de trabalho, ou trabalhos fora do horário habitual.

7.2.3 Integridade

A integridade garante que a informação não seja modificada por uma entidade não autorizada.

Garantir a autenticidade e integridade da informação através da assinatura digital de todos os dados inseridos no sistema, os quais deverão ser assinados digitalmente pelo respectivo usuário, através de *smart card.* O *smart card* será usado para a assinatura digital da solicitação de benefício realizada pelo funcionário administrativo, autenticação do laudo médico realizado pelo médico perito, aprovação do benefício realizada pelo gerente. O sistema realizará de maneira obrigatória, na consulta do laudo médico e do benefício, a verificação da assinatura digital.

7.2.4 Canal seguro de comunicação

A garantia de um canal seguro de comunicação é necessária para evitar ataques e análise das informações em trânsito nas redes de comunicação.

Utilizar autenticação de parceiro de comunicação através do protocolo *Secure Socket Layer (*SSL) (NETSCAPE COMMUNICATIONS, 1996) para manter o sigilo de comunicação entre as estações cliente e servidores WEB, servidores de aplicação e servidores de banco de dados. O SSL fornece autenticação de parceiro de comunicação, confidencialidade e integridade dos dados, sendo utilizado para

autenticar equipamentos. O SSL permite que o cliente se conecte ao *Web Site* e, de forma transparente, seja criado um canal de comunicação seguro entre o *site* e o cliente.

Os sistemas deverão possuir um certificado digital de aplicação emitido por Autoridade Certificadora (AC) credenciada pelo ITI responsável pela AC Raiz da estrutura da ICP-Brasil, a fim de garantir a identidade do sistema (COMITÊ GESTOR DA ICP BRASIL, 2001).

7.2.5 Controle de acesso para sigilo das informações no banco de dados

O controle de acesso para a manutenção do sigilo das informações armazenadas no banco de dados é a habilidade de limitar e/ou controlar o acesso à informação armazenada no repositório, visando garantir que somente as entidades autorizadas consigam acesso. Visa garantir também que autorizações de acesso ao banco de dados sejam dadas apenas pelos responsáveis e não sejam alteradas indevidamente

Para efetivar essa manutenção, utilizar Sistema Gerenciador de Banco de Dados (SGBD). Esse SGBD deve ter recurso de criptografia implementado, para manter o sigilo das informações.

7.2.6 Disponibilidade

Apesar de disponibilidade não fazer parte do escopo deste trabalho devido a complexidade, é necessário menciona-la devido a sua relevância.

Para garantir que os servidores estejam sempre disponíveis para as entidades autorizadas do sistema, pode ser utilizada redundância de servidor,

através de implementação de *cluster* de alta disponibilidade. *Cluster* é a interação de múltiplos servidores que trabalham em conjunto para executar aplicações, com múltiplos dispositivos de armazenamento e conexões redundantes de modo a garantir alta disponibilidade, de tal modo que os usuários que os utilizam tenham a impressão que somente um único servidor responde para eles. Se um nó do *cluster* vier a falhar, o sistema estará disponível em outro nó. Utilização de sistema de tolerância a falha de disco com RAID 0, RAID 1 e RAID 5, sendo configurado conforme a necessidade.

7.2.7 Auditoria

Para a realização de auditoria no sistema, deve ser realizada a geração de registro de eventos (LOG). O registro do log do sistema deve conter:

a) identificação dos usuários do sistema;

b) datas e horários de entrada (*log-on*) e saída (*log-off*) no sistema;

c) identidade do terminal e, quando possível, a sua localização;

d) registro das tentativas de acesso ao sistema, aceitas e rejeitadas;

e) registro das tentativas de acesso a outros recursos e dados, aceitas e rejeitadas;

f) registro das exceções e de outros eventos de segurança relevantes devem ser mantidos por um período de tempo não inferior a 10 (dez) anos, para auxiliar em investigações futuras e na monitoração do controle de acesso;

g) informações de controle de acesso à inclusão e manutenção de informações no RES;

h) informações sobre as funções administrativas realizadas pelo administrador de sistema;

i) informações das transações criptográficas;

j) informações sobre os avisos de realização de *backup*;

k) informações sobre a exportação e importação de informações;

l) informações sobre o processo de auditoria;

m) informações sobre erros do *software* em qualquer um de seus módulos.

Os registros do LOG devem ser protegidos com criptografia usando um algoritmo forte. Os registros de LOG devem ser utilizados também para identificar comportamento malicioso.

7.3 Riscos residuais

Os controles de segurança implementados não eliminam totalmente os riscos. Alguns riscos ainda persistem. Os principais são:

- Um usuário autorizado remover um registro - Esse risco deve ser eliminado por consistência do sistema.
- Rede de comunicação indisponível - Essa questão deve ser tratada em conjunto com a provedora de serviços de rede, para a implantação de redundância de rota de rede.
- Acesso ao local físico indisponível por motivo de sinistro ou roubo de equipamentos - Essa questão deve ser trata no plano de contingência e continuidade dos negócios das organizações envolvidas no processo.

7.4 Controles para atender aos requisitos de segurança para sistemas de RES

Conforme o Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (SBIS-CFM, 2004), o Sistema de RES proposto é o Sistema de RES Compartilhável – SRES-C, SRESAD – Sistema RES com Assinatura Digital, Nível de Garantia de Segurança NGS2.

7.4.1 Requisitos de segurança para sistemas denominados SRESAD - NGS2

a) Requisito RSEGM1: controle da versão do *software*.

O sistema deve possuir a versão junto com o nome, fabricante e número de versão única. Essa identificação deve constar no código fonte.

b) Requisito RSEGM2: autenticação e controle de acesso.

O método de autenticação escolhido é o de certificação digital com *smart card*. O controle de acesso será através da definição de perfis e grupos baseados nos diferentes papéis da área de perícia médica.

c) Requisito RSEGM3: controle de fluxo da informação e integridade de dados para sistemas isolados.

Requisito RSEGM4: controle de fluxo de informação e integridade de dados para sistemas baseados em arquitetura cliente-servidor ou arquitetura WEB.

Requisito RSEGM5: controle de sigilo e integridade

Manter a qualidade da informação, com a avaliação do conteúdo, da veracidade, dos meios legítimos, da precisão, do equilíbrio da troca. Para tal deve ser implementado os seguintes mecanismos: O *smart card* será usado para a assinatura digital de dados sensíveis inseridos no sistema.

Manter a integridade da informação através de certificação digital e assinatura digital. Sempre que houver o acesso aos dados utilização de certificação para garantir a origem da informação.

d) Requisito RSEGM6: copia de segurança e restauração de dados.

Deve ser feita cópia de segurança dos dados do prontuário pelo menos a cada 24 horas. No processo de *backup* a ser realizado por usuário especifico e com sua autenticação através de assinatura digital de *smart card*, deverá ser exportado os atributos de segurança em conjunto com os dados e na recuperação os atributos deve ser recuperados automaticamente. A restauração deve ser feita somente pelo administrador. As cópias devem ser mantidas em local distante o suficiente para livrá-las de danos que possam ocorrer nas instalações principais. Segundo o Código de Ética Médica (CEM) do Conselho Federal de Medicina (RESOLUÇÃO CFM número 1.246, 1988), as mídias com os registros de *backup* devem ser devem ser guardados pelo prazo mínimo de 20 anos.

e) Requisito RSEGM7: canais seguros de comunicação para sistemas de RES baseados em arquitetura cliente-servidor ou implementado em arquitetura WEB.

Autenticação de parceiro de comunicação realizada através do protocolo SSL.

f) Requisito RSEGM8: utilização de recursos computacionais.

A questão de disponibilidade de informação em caso de falha de *hardware* ou *software* operacional, de tal modo a garantir a integridade da informação, será garantido através de uso de redundância de servidores.

g) Requisito RSEGM9: auditoria.

O sistema deve manter histórico de acessos e alterações através de auditoria e *logs*, para que sempre seja identificado o autor de consultas e alterações no sistema.

h) Requisito RSEGM10: documentação.

O sistema deve possuir manual de instalação e requisitos de sistemas, manual do usuário, manual do administrador, manual dos mecanismos de segurança e manual de praticas de segurança.

i) Requisito RSEGD1: origem dos certificados digitais.

Requisito RSEGD2: controle de autenticação pelo uso de certificados digitais utilizados para assinatura digital.

Os certificados digitais devem ser emitidos por uma AC (Autoridade Certificadora) credenciada pelo ITI responsável pela AC Raiz da estrutura do ICP-Brasil. Os certificados digitais devem ser usados somente para a assinatura eletrônica de registros incluídos no sistema.

8 CONCLUSÃO

A atividade de perícia médica tem sua regulamentação conforme a legislação apresentada, sendo o resultado armazenado no prontuário médico.

A Tecnologia da Informação encontra-se em estágio avançado e pode proporcionar todas as vantagens de um sistema informatizado e com recursos de segurança eficazes.

Independentemente da obrigatoriedade da lei, atualmente as soluções de Tecnologia da Informação, reúnem condições de atender a realidade. Apresentar uma proposta com essas condições foi justamente o objetivo deste trabalho.

Para a adoção de uma solução tecnologicamente satisfatória é necessário conhecer o negócio, suas regras e os riscos aos quais estão sujeitos. A solução de Tecnologia de Segurança apresentada tem a proposta de desenhar um sistema dotado de mecanismos de segurança adequados. A base dessa proposta é o conhecimento do negócio, as vulnerabilidades ao qual pode ser exposto, e conseqüentemente, na implementação de ferramentas de segurança em TI, atuais, eficientes e que atendam a necessidade de tornar a atividade de perícia médica confiável e ágil.

Na implantação de uma solução para a atividade de perícia médica acompanhando a atual tendência tecnológica e obedecendo a legislação, o encontro de uma solução baseada na tecnologia *Workflow* permite atender essas premissas iniciais.

A solução baseada em *Workflow* proporciona o adequado controle dos processos realizados, o que é muito importante devido ao caráter social que essa

atividade apresenta. As intervenções manuais e o constante perigo de ter alguma atividade em atraso são minimizados.

Os controles de segurança apresentados, associados às características e vantagens próprias do sistema de *Workflow*, proporcionam direcionar o fluxo de atividades às entidades autorizadas. Os atuais recursos de criptografia garantem os importantes serviços de integridade, confidencialidade, irretratabilidade tão necessários para a confiabilidade, o sigilo e a continuidade do negócio.

REFERÊNCIAS

CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO. **Resolução CREMESP número 76**. Diário Oficial do Estado, Poder Executivo, São Paulo, SP, 16 julho de 1996.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM número 1.246 - Código de Ética Médica.** Diário Oficial da União, Poder Executivo, Brasília, DF, 26 janeiro de 1988.

PUBLICAÇÕES CREMESP. **Prontuário e Segredo Médico - Código de Ética Médica - CEM- sobre Prontuário e Segredo Médico**. Disponível em: <http://www.cremesp.org.br/?siteAcao=PublicacoesConteudoSumario&id=57> Acesso em: 25 maio 2004.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM número 1.638 -** Diário Oficial da União, Poder Executivo, Brasília, DF, 10 julho de 2002.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM número 1.614 -** Diário Oficial da União, Poder Executivo, Brasília, DF, 08 fevereiro de 2001.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM número 1.639 - Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico**. Diário Oficial da União, Poder Executivo, Brasília, DF, 12 agosto de 2002.

USIROMO, Carlos Hiroshi. **Tecnologia *Workflow*:** o impacto de sua utilização nos processos de negócio. Um estudo de casos múltiplos. 2003. 178 f. Dissertação (Mestrado em Administração de empresas) – Faculdade de Administração e Contabilidade da Universidade de São Paulo.

CRUZ, Tadeu. ***Workflow*: A Tecnologia que Vai Revolucionar Processos.** São Paulo: Atlas, 2000.

PLESUMS, Charles. **An Introduction to *Workflow*** – Disponível em: <http://www.wfmc.org/information/introduction_to_*Workflow*02.pdf> Acesso em 23 agosto 2004.

ALLEN, Rob. ***Workflow* – an Introduction.** – Disponível em: <http://www.openflow.it/EN/Documentation/Files/*Workflow*Introduction/WfMC_*Workflow*_Introduction.pdf > Acesso em 23 agosto 2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação.** NBR ISO/IEC 17799. Rio de Janeiro: ABNT, 2001.

VASKEVITCH, David. **Estratégias: Cliente/Servidor.** São Paulo: Berkeley, 1995.

SOCIEDADE BRASILEIRA DE INFORMÁTICA EM SAÚDE. **Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES).** São Paulo: SBIS, fevereiro de 2004.

INTERNATIONAL STANDARDS ORGANIZATION TECHNICAL COMMITTEE 215. **Health Informatics – Electronic Health Record – Definition, Scope and Context. – Draft Technical Report.** Toronto – Canadá: ISO/TC 215, 2004.

INTERNATIONAL STANDARDS ORGANIZATION TECHNICAL COMMITTEE 215. **Requirements for an Electronic Health Record Architecture**. Toronto – Canadá: ISO/TC 215, 2004.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **IT Security techniques - Evaluation criteria for IT security.** ISO/IEC 15408, 1999.

NETSCAPE COMMUNICATIONS. **Protocolo Secure Sockets Layer – SSL versão 3.0** – Disponível em: <http://wp.netscape.com/eng/ssl3/draft302.txt> Acesso em: 01 dezembro 2004.

MEDIDA PROVISÓRIA Nº 2.200-2. **Infra-Estrutura de Chaves Publicas Brasileiras – ICP-Brasil**. 24 agosto de 2001.

COMITÊ GESTOR DA ICP BRASIL. **Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil Resolução nº 1 -** Brasília 25 setembro 2001.

REQUEST FOR COMMENTS. **Internet X.509 Public Key Infrastructure Certificate and CRL Profile**. RFC 3280. abril de 2002.

GLOSSÁRIO

Anamnese: Informação acerca do princípio e evolução duma doença até a primeira observação do médico; reminiscência; recordação.

Censo: conjunto de dados estatísticos dos habitantes de uma cidade, província, estado, nação, etc; com todas as suas características; recenseamento.

Conciso: Em que há concisão; sucinto, resumido; breve, preciso, exato.

Escuso: escondido, suspeito, misterioso, ilícito, oculto, recôndito; que foi objeto de escusa.

Iminente: Que ameaça acontecer breve; que está em via de efetivação imediata.

Impetrar: Interpor (um recurso); rogar, suplicar, requerer; obter mediante súplicas; procurar obter mediante súplicas.

Incapacidade Laborativa: Impossibilidade do desempenho das funções específicas de uma atividade ou ocupação, em conseqüência de alterações morfopsicofisiológicas provocadas por doença ou acidente.

Irretratabilidade: Que não pode ser retratar; irrevogável, imutável.