Arquitetura do Sistema Cartão Nacional de Saúde

Roberto A Hexsel[1], Antonio E Urban[2], Roberto S M Barros[3]

[1,2]Departamento de Informática, Universidade Federal do Paraná
[3]Centro de Informática, Universidade Federal de Pernambuco
[1,2,3]Secretaria de Investimento em Saúde, Ministério da Saúde

Resumo – O Sistema do Cartão Nacional de Saúde, os componentes dos cinco níveis e suas funções são apresentados e descritos. Aspectos de segurança e privacidade dos dados coletados e armazenados no sistema, bem como os desafios associados à capacitação de pessoal e à expansão do sistema são discutidos.

Palavras-chave: Cartão Nacional de Saúde, arquitetura do sistema, privacidade e segurança de dados.

Abstract – The Brazilian National Health Card System, its component subsystems and their funcions are described. The mechanisms devised for keeping the data collected and stored in the system safe and secure are presented. The challenges presented by the system's expansion, especially regarding training are dicussed.

Key-words: National Health Card System, system architecture, data privacy and security.

O Sistema Cartão Nacional de Saúde (SCNS)[1] é um sistema de grande porte e abrangência nacional e foi concebido segundo uma estrutura que reflete a organização do SUS, isto é, como uma hierarquia de cinco níveis e de tal forma que a operação dos cinco níveis possa ocorrer de forma autônoma ao mesmo tempo em que são respeitadas as características federativas do SUS.

O SCNS está em seu primeiro ciclo de implantação. Este ciclo têm as características de um protótipo e algumas das opções tecnológicas efetuadas na concepção do SCNS estão sendo avaliadas quanto a sua adequabilidade e praticidade. No primeiro ciclo o SCNS está sendo implantado em 44 municípios de 9 estados. A arquitetura do SCNS compreende os Níveis de Atendimento, Municipal, Concentrador, Estadual e Federal. Estes cinco níveis compõem um sistema distribuído que atende aos Estabelecimentos Assistenciais de Saúde (EAS), às Secretarias Municipais e Estaduais de Saúde e ao Ministério da Saúde.

Este artigo se atém aos aspectos de tecnologia da informação e descreve a estrutura do SCNS, os vários tipos de equipamentos, software e protocolos de comunicação, bem como os aspectos de segurança e integridade dos dados coletados e armazenados em todo o sistema. O texto está organizado da seguinte maneira. A Seção 1 descreve a arquitetura do SCNS e os componentes dos cinco níveis. A Seção 2 discute aspectos de segurança e integridade dos dados. A Seção 3 discute os problemas que estão sendo enfrentados na implantação do SCNS, e alguns dos desafios que deverão ser enfrentados durante a expansão do sistema.

[1]Artigo apresentado no VIII Congresso Brasileiro de Informática em Saúde, Natal RN, setembro de 2002.

1 Arquitetura do SCNS

O SCNS é composto por cinco níveis, cujas características técnicas e funcionais são discutidas em mais detalhe no que segue. Os três níveis superiores do SCNS são interligados por uma rede permanente enquanto que os dois níveis inferiores são interligados por enlaces discados. A Figura 1 mostra a arquitetura do SCNS. Nesta figura, círculos representam instalações (sítios) do SCNS e as ligações entre os sítios representam os possíveis fluxos de informação.

Excetuando-se o Nível de Atendimento, os equipamentos instalados nos sítios do SCNS consistem de equipamentos de comunicação (rede local e roteadores), computadores de porte proporcional à população adstrita, e equipamentos de suporte como impressora, *nobreak* e instalação elétrica e de rede. Os computadores são chamados de servidores para distingüí-los de computadores com outras funções que não o armazenamento e processamento de dados de saúde do âmbito do SCNS. O banco de dados empregado em todo o sistema é o Oracle 8i.

1) O *Nível de Atendimento* é composto pelos terminais de atendimento SUS instalados em Unidades de Saúde;

2) O *Nível Municipal* é composto por servidores que efetuam o processamento e armazenamento dos dados de todos os atendimentos realizados no município;

3) O *Nível Concentrador* consiste de servidores que efetuam o armazenamento dos dados de atendimentos de todos os municípios a eles conectados;

4) O *Nível Estadual* é composto por servidores que processam e armazenam informações totalizadas dos atendimentos realizados no Estado; e

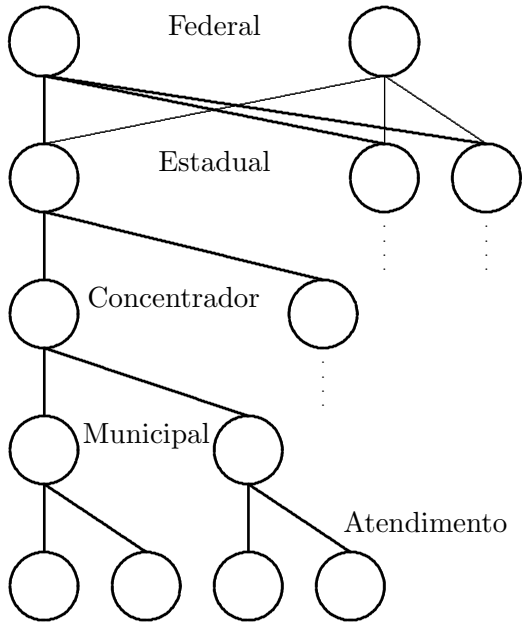

Figura 1: Arquitetura do Sistema Cartão Nacional de Saúde

5) O *Nível Federal* é composto por dois servidores que armazenam e processam informações totalizadas dos atendimentos realizados no País.

1.1 Nível de Atendimento

Do ponto de vista estritamente tecnológico, o Nível de Atendimento consiste dos cartões magnéticos e dos terminais de atendimento instalados nas Unidades de Saúde. O cartão têm a finalidade de identificar o usuário do SUS quando dos eventos de atendimento. Existem dois tipos[2] de cartão: o cartão de usuário, que é usado apenas para identificar o usuário; e o cartão de profissional de saúde[3], que é usado para identificar o profissional de saúde e validar os registros de atendimento coletados pelo SCNS. Um *número de identificação* de 15 dígitos identifica o portador do cartão, seja este usuário ou profissional de saúde.

Para fins deste primeiro ciclo, a tecnologia adotada é o cartão de tarja magnética, somente para a leitura de dados. Essa escolha reflete um compromisso entre diversas variáveis que incluem durabilidade, custo, e o controle de uso. Note que *cartão* é um conceito abstrato e que em grande medida independe do meio físico empregado em determinado período. É possível que, alterando-se as condições de preço e disponibilidade, possam ser adotadas soluções como *smart cards* para armazenar alguns dados de atendimento além dos dados de identificação.

A forma de interação entre o usuário e o SCNS se dá através dos profissionais de saúde, desde a recepção até o atendimento propriamente dito. Os profissionais de saúde envolvidos utilizam o terminal de atendimento para a leitura do cartão do usuário e para o registro dos dados de atendimento. O Terminal de Atendimento SUS (TAS) é o dispositivo no qual é efetuada a captura dos dados do cartão e o registro do atendimento. O TAS é capaz de armazenar centenas de registros de atendimento, e periodicamente estes registros devem ser transmitidos para o Nível Municipal, onde serão processados e armazenados de forma permanente.

Durante a fase de concepção do SCNS foi efetuado estudo quanto aos requisitos funcionais de um terminal de atendimento à saúde. Dentre estes requisitos destacam-se a facilidade de uso nos variados ambientes de atendimento (robustez elétrica e mecânica), facilidade de operação por pessoal de todos os níveis de instrução (ergonomia, simplicidade de operação), baixa atratividade para roubo, segurança, confiabilidade e privacidade das informações capturadas e armazenadas no terminal. Após análise de mercado, optou-se pela especificação de um terminal dedicado, cujas características o colocam em uma posição intermediária entre um equipamento tipo Ponto de Venda e um microcomputador pessoal. O TAS e o software aplicativo de gestão no Nível Municipal, com o qual ele interage, são as duas peças-chave do Sistema do Cartão Nacional de Saúde.

O modelo de terminal de atendimento em uso no primeiro ciclo possui duas versões com as mesmas características básicas, e que são fornecidas pelos dois consórcios vencedores da Licitação Internacional 01/99. Estes consórcios são liderados pela Hypercom (Lotes 1 e 2) e pela Procomp (Lote 3). As duas versões do TAS são equipamentos compactos, com tela de cristal líquido de 5,7", impressora térmica e teclado numérico integrados, além de teclado ABNT e fonte de alimentação externos. Os dois TAS contém leitora de cartão magnético (trilhas 1, 2 e 3), leitor de *smart card*, modem, interface Ethernet, e interface serial RS-232. Parte da memória é em tecnologia *flash*, o que garante a manutenção dos dados coletados mesmo na falta de alimentação elétrica por longos períodos de tempo. A faixa aceitável de tensões de alimentação varia de 90 a 240 VAC.

Dependendo do tamanho e complexidade do EAS, os terminais podem se conectar ao Nível Municipal de duas maneiras. Em unidades pequenas com até 5 terminais estes podem compartilhar uma única linha telefônica e o estabelecimento de conexões discadas a partir de cada terminal depende de comando

[2]Há também o "cartão de acesso especial", ou "cartão coringa" que dá acesso temporário ao sistema a profissionais que ainda não receberam seus próprios cartões.

[3]Um profissional de saúde possui dois cartões com o mesmo número, um cartão de usuário e um cartão de profissional.

do operador. Em unidades com mais de cinco terminais, estes são interligados por uma rede local e um *gateway* na rede local efetua as conexões discadas sempre que um terminal necessitar comunicar-se com o Nível Municipal ou Concentrador.

1.2 Nível Municipal

Do ponto de vista de equipamentos, este nível é constituído pelo servidor municipal, periféricos e equipamentos de rede local (comutadores Ethernet), um servidor de acesso discado para aceitar conexões dos TAS, e um roteador para controlar o tráfego de dados entre o servidor municipal e o servidor do Nível Concentrador a que este se conecta.

O servidor municipal é um computador de médio porte que executa o aplicativo de gestão municipal do SCNS e outras funções relacionadas com gestão de informações municipais de saúde. A capacidade de processamento e de armazenamento deste servidor depende da população do município. Os servidores dos Lotes 1 e 2, fornecidos pela Hypercom, são estações[4] Sun E250 ou E450. Os servidores do Lote 3, são servidores Procomp TW-9620 ou 9630[5].

O aplicativo de gestão municipal, executado no equipamento servidor municipal, interage com os terminais de atendimento através de comunicação discada. O aplicativo de gestão municipal, além de consolidar e armazenar as transações recebidas dos terminais de atendimento, transmitir dados para o nível concentrador e obter dados deste mesmo nível, tem ainda as seguintes funções:

a) controlar as versões e manter atualizado o software aplicativo do TAS;

b) recepção e processamento de solicitações de informações geradas pelo operador de um TAS, possivelmente acessando cadastros de usuários ou informações armazenadas nos Níveis Estadual ou Federal[6];

c) mediante solicitação emitida através de um terminal de atendimento, gerar a autorização para certos procedimentos médicos, após consulta às regras pactuadas no Nível Municipal;

d) efetuar a interface com Sistemas de Informações de Base Nacional do Ministério da Saúde, ou outros sistemas de informação pré-existentes.

1.3 Nível Concentrador

O Nível Concentrador é constituído pelo servidor concentrador e por equipamentos de comunicação e periféricos. O servidor concentrador tém três funções principais. A primeira é manter cópia de segurança dos dados de todos os servidores municipais que se conectam a ele. A segunda função é comportar-se como um servidor municipal e substituir temporariamente um servidor municipal indisponível, permitindo aos TAS do município afetado descarregar seus dados. A terceira função é processar os dados recebidos dos municípios de sua área de abrangência e transmiti-los ao Nível Estadual.

A comunicação com os servidores municipais e terminais se dá através de linhas discadas (ou linhas privativas), enquanto que com o servidor do Nível Estadual a comunicação é via enlace de rede permanente (*Frame Relay*). Os servidores concentradores dos Lotes 1 e 2, são estações Sun E3500. No Lote 3, os servidores são Procomp TW-9630.

1.4 Níveis Estadual e Federal

O Nível Estadual é constituído pelo servidor estadual e por equipamentos de comunicação e periféricos. O servidor estadual recebe os dados provenientes dos servidores concentradores, processa-os e os transmite ao Nível Federal. Os servidores são estações Sun E3500 ou E450, conforme a população do estado. No Lote 3, os computadores são servidores Procomp TW-9630, TW-9640 ou TW-9650, conforme a população do estado.

O Nível Federal é constituído por 2 sítios, um instalado em Brasília e o outro no Rio de Janeiro. Estes dois sítios são interligados por enlaces dedicados de tecnologia *Frame Relay*. Neste nível são recebidos e processados os dados provenientes do Nível Estadual, também através de conexão permanente à rede Frame Relay. Cada sítio federal é constituído por um *cluster* de 2 servidores de grande porte Sun E6500, além de roteadores e estações de trabalho para a gerência da rede e do servidor federal.

1.5 Arquitetura da Rede

A Figura 2 mostra a topologia da rede que interliga os componentes do SCNS. Os sítios dos Níveis Federal, Estadual e Concentrador são interligados permanentemente através de enlaces *Frame Relay*. Os sítios do Nível Municipal se conectam aos seus Concentradores através de conexões discadas. Os terminais de atendimento se conectam ao servidor municipal através de conexões discadas[7].Todos os protocolos de comunicação empregados no sistema utilizam a tecnologia de internet (TCP/IP), e são protocolos abertos publicados pelo IETF ou W3C.

A rede do SCNS é configurada como uma rede IP Classe A com endereçamento 10.X.X.X em todos os

[4]Todos os servidores dos Lotes 1 e 2 são estações Sun e executam Solaris 8.

[5]Todos os servidores do Lote 3 tem processadores Intel/Pentium III e executam MS Windows 2000 Server.

[6]Este tipo de acesso se dá através do Nível Concentrador.

[7]Em alguns municípios, a ligação entre sítio municipal e concentrador, e entre terminais e sítio municipal se dá através de enlaces dedicados.

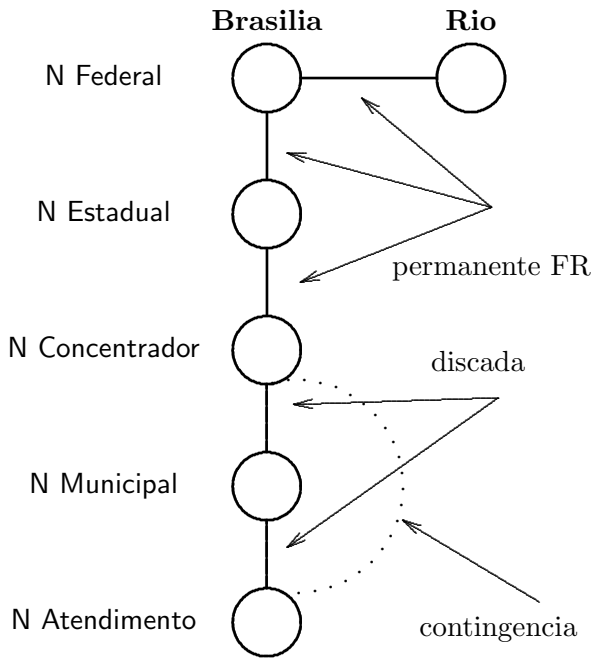

Figura 2: Rede do Sistema Cartão Nacional de Saúde

níveis, exceto o Nível de Atendimento (TAS) que pode usar um esquema de endereçamento independente da rede 10 dos demais níveis. Isso é necessário por causa das conexões discadas, que são sempre iniciadas pelo TAS, e neste caso o endereço IP de cada TAS é atribuído pelo serviço DHCP dos Níveis Municipal ou Concentrador.

Todas as conexões entre os roteadores participantes da rede ocorrem em uma rede privada virtual, utilizando-se o protocolo IPSec com 3-DES/168bits. Além disso, o tráfego de dados entre os servidores, assim como todo o tráfego de serviço (consultas) é realizado com o protocolo HTTPS (HTTP + SSL). As chaves criptográficas utilizadas são de 1024 bits, para chaves assimétricas, e de 128 bits, para chaves simétricas.

Do ponto de vista de aplicação, os TAS e os servidores municipais comunicam-se através de um conjunto de documentos XML, cujas definições são públicas, e portanto independentes de Lote, de versão do TAS, e de sistema operacional do servidor municipal. Do Nível Municipal para os níveis superiores, parte do tráfego é codificado segundo documentos XML, e o restante depende do mecanismo de replicação do sistema gerenciador de banco de dados Oracle. A comunicação que depende dos mecanismos do Oracle foi padronizada pelo MS.

2 Privacidade e Segurança

Os dados e informações registrados nos documentos e arquivos dos serviços de saúde, em qualquer meio, formato ou tecnologia, são propriedade da pessoa (paciente ou usuário) a quem se referem ou de quem descrevem o estado de saúde e condição de vida. Portanto, devem ser garantidos a essa pessoa a privacidade, o sigilo profissional e o segredo pessoal, em relação aos seus dados e informações, por parte de todos os profissionais de saúde direta e indiretamente envolvidos na atenção integral à sua saúde. Adicionalmente, devem ser garantidas a confidencialidade, a integralidade e a segurança no registro, na transmissão, no armazenamento e na utilização das informações individuais existentes no serviço de saúde.

Tendo estas observações em conta, o SCNS deve funcionar segundo seis diretrizes definidas pelo MS para regulamentar o acesso aos dados, informações, cadastros, arquivos e bases de dados do Sistema Cartão Nacional de Saúde. As diretrizes são:
1) Serão implementados mecanismos que permitirão o acesso a uma determinada informação somente às pessoas autorizadas a acessarem aquela informação;
2) Somente serão autorizadas a ter acesso a uma informação as pessoas que necessitarem daquela informação para exercer sua função ou executarem seu trabalho;
3) O acesso somente será permitido em razão de necessidade da população ou do paciente (usuário do SUS), de necessidade do profissional ou de necessidade do administrador, nessa ordem, e ainda por determinação judicial e no limite da lei;
4) O paciente ou usuário deve ter acesso aos registros individuais relacionados a sua própria pessoa e àquelas sob sua responsabilidade, respeitados os Códigos de Ética da medicina e das demais profissões da saúde e a legislação que rege a matéria;
5) Em todos os sistemas informatizados de registro, transmissão e armazenamento de dados e informações de saúde serão implementados mecanismos de segurança, controle e auditoria de forma a permitir o registro e o conhecimento sobre quem teve acesso, quando, e qual informação foi acessada; e
6) Serão permitidos o intercâmbio de dados, informações, cadastros e arquivos com instituições governamentais que garantam o sigilo, a confidencialidade, a integridade e a segurança em seu tratamento e utilização. Estes intercâmbios serão limitados aos ítens cadastrais dos sistemas da área da saúde.

2.1 Controle de Acesso

A questão mais complexa a ser resolvida pelas políticas de segurança da informação em saúde é o controle de acesso aos dados de saúde identificados. A política de segurança deve definir quem detém o direito de acesso a quais informações, e a execução desta política depende da participação de todos os

envolvidos no processo.

A política de acesso vigente no SCNS determina que todo e qualquer acesso às bases de dados residentes nos servidores de qualquer dos níveis, para fins de consulta e pesquisa, somente poderá ser efetuado por usuários devidamente autorizados pelo gestor da esfera correspondente. O direito de acesso aos dados é conferido de forma exclusiva para os fins alegados, justificados e autorizados. Isso é possível porque os bancos de dados utilizados em todos os servidores permitem o estabelecimento de regras de controle de acesso que restringem o acesso aos registros, ou aos tipos de pesquisa que podem ser efetuadas, apenas aos usuários autorizados, e que já detenham o direito de acesso ao sistema.

A concepção e o projeto do TAS, que é um equipamento especialmente desenvolvido para o SCNS, incorporou diversos mecanismos de segurança, tais como: (a) diversos níveis de autoridade, permitindo a restrição de acesso a funções de configuração, abertura de sessão e operação do equipamento; (b) solicitação de senha de acesso para operações críticas; e (c) toda a operação do equipamento é realizada sob o controle do programa aplicativo do SCNS, não havendo acesso direto aos recursos do sistema operacional.

Todos os profissionais de saúde que sejam responsáveis pela operação dos TAS e/ou inserção de dados no sistema, possuem o Cartão do Profissional de Saúde, que os identifica e qualifica, e contém uma senha criptografada. Desta forma, todos os registros de eventos do atendimento coletados nas unidades de saúde estarão vinculados a um profissional que foi identificado e autenticado pelo sistema, e que está autorizado a efetuar o atendimento. Os registros de atendimento também estarão simultaneamente vinculados ao EAS onde o atendimento foi realizado.

2.2 Política de Segurança

Informações armazenadas em meio eletrônico podem ser copiadas ou pesquisadas de formas muito mais rápidas e eficientes do que informações mantidas em prontuários de papel. Portanto, uma parte fundamental da arquitetura de um sistema como o SCNS é uma política de segurança que atenda às diretrizes enunciadas acima, satisfazendo aos seguintes requisitos básicos de segurança de dados:

a) Privacidade: deve-se proteger os dados do monitoramento, tanto na forma ativa, onde podem ser feitas alterações, quanto na forma passiva, cujo objetivo é a obtenção de informações.

b) Autenticidade: toda e qualquer inclusão e/ou alteração de informações no sistema deve estar vinculada a um operador devidamente cadastrado.

c) Integridade: deve ser garantido que não haverá alteração dos dados quando estes são transferidos entre os diversos níveis do sistema. Além disto, o sistema deve manter registros de todas as alterações ocorridas nos dados armazenados.

d) Controle de Acesso: o sistema deve funcionar segundo uma política de definição de privilégios de acessos para classes de operadores do sistema. Todas as tentativas de acesso às funcionalidades e informações do sistema devem ser armazenadas para fins de auditoria.

e) Auditoria: deve existir a capacidade de se avaliar a veracidade dos dados armazenados. Esta avaliação poderá ser realizada pelos vários níveis do sistema, de acordo com regras bem definidas.

Do ponto de vista tecnológico, as condições e requisitos enunciados acima são atendidas pelo SCNS, porque este sistema foi concebido para prover amplas garantias quanto a segurança e privacidade dos dados. Por exemplo, optou-se pelo uso de terminais dedicados como o TAS, ao invés de computadores pessoais (PCs), porque aqueles não são projetados, e nem construídos, para garantir a segurança dos dados que processam e armazenam. O sistema operacional mais popular para PCs é reconhecidamente instável e inseguro. Os riscos decorrentes do uso de PCs tornariam o SUS e seus gestores vulneráveis à publicação de registros clínicos e às sanções legais decorrentes deste tipo de evento.

3 Problemas e Desafios

A implantação de um projeto com escopo, amplitude geográfica, e complexidade como os do SCNS invariavelmente enfrenta problemas de diversas ordens. Nesta sessão alguns deles são brevemente discutidos, enfocando-se principalmente os aspectos relacionados à informática e capacitação de pessoal para uso e operação do sistema. Quando da expansão do SCNS, estes problemas tenderão a se repetir mas em escala muito maior.

Há uma grande diversidade de municípios entre aqueles envolvidos no primeiro ciclo do SCNS, seja em tamanho e população, seja em estágio de desenvolvimento econômico e tecnológico. A implantação do SCNS está se dando em municípios como São José dos Campos (SP), onde se localizam organizações como Embraer, ITA e INPE, e Tunas do Paraná, distando 90 Km de Curitiba, com população de aproximadamente 6.000 pessoas e economia baseada em agricultura de subsistência. Evidentemente, estas diferenças determinam variados ritmos de implantação do projeto, o que pode compor-se com os distintos níveis de engajamento dos gestores municipais e/ou estaduais.

As diferenças entre populações e desenvolvimento econômico se refletem na capacitação do pessoal em

tecnologia da informação. Os profissionais de saúde das cidades pequenas tendem a oferecer maior rejeição à utilização do sistema e têm menos familiaridade com equipamentos de informática. Além disso, é notável a virtual ausência de uma cultura de uso de informação em saúde pelos gestores e profissionais, e não só em cidades pequenas. Outro problema é a necessidade de constante e eficiente trabalho de convencimento dos profissionais de saúde quanto aos aspectos de segurança e integridade dos registros de atendimento armazenados no sistema.

Uma parcela significativa do custo do projeto está alocada à atividades de treinamento e capacitação de pessoal no uso dos terminais e na operação dos equipamentos e sistemas instalados nos sítios do SCNS. Um problema, mas que é também um desafio, é a necessidade de repetição dos programas de treinamento e reciclagem do pessoal envolvido na operação do sistema. A re-edição dos programas de treinamento deverá ocorrer porque assim que o profissional se capacita, seu "valor de mercado" aumenta e este tem maior probabilidade de mudar de emprego. Do ponto de vista dos gestores do sistema, a capacitação tém um custo elevado, enquanto que para a sociedade verifica-se uma maior oferta de pessoal capacitado em informática.

Agradecimentos

O trabalho dos autores foi financiado pela UNESCO, contrato 914BRZ01. A concepção da arquitetura do SCNS deve-se à cooperação do Ministério da Ciência e Tecnologia com o MS, e especialmente à participação de Tadao Takahashi, Daniel Cavalcante, Dulcídio Pedrosa, Gorgonio Araújo, Manoel Lemos e um dos autores (RSMB). Joel G Silva Filho e Emílio B Lucena, da Coordenação de Desenvolvimento e Tecnologia do SCNS, têm participado ativamente da elaboração da política de segurança do SCNS.