

Segurança da Informação no Cartão Nacional de Saúde

Airton Cardoso¹

Arlindo Lages

Samantha Coimbra

Resumo

O Sistema Único de Saúde (SUS), estabelecido pela Constituição Federal de 1988, agrega todos os serviços estatais – das esferas federal, estadual e municipal – e os serviços privados, contratados ou conveniados, sendo responsável pela concretização dos princípios constitucionais no que trata da atenção universal à saúde dos cidadãos brasileiros.

O Projeto Cartão Nacional de Saúde foi desenvolvido em atenção à Norma Operacional Básica (NOB) de 1996, como forma de identificar a clientela do SUS, explicitando ao mesmo tempo sua vinculação a um gestor e a um conjunto de serviços bem definido, cujas atividades devem cobrir, integralmente, todo o escopo de atenção à saúde do cidadão, tal como estipulado pela Constituição Federal.

Os aspectos de segurança, que abrangem confidencialidade, privacidade, disponibilidade, integridade, confiabilidade e auditoria foram observados durante a concepção do Projeto e serão tratados neste artigo.

Palavras-chave

Segurança de Sistema de Informação; Auditoria de Sistema; Sistema Único de Saúde; Cartão Nacional de Saúde.

Summary

Information's Security in National Health Card

The Unique System of Health (SUS), established for the Federal Constitution of 1988, joins all of the state services - of the spheres federal, state and municipal - and the services private, contracted or covenant, being responsible for the materialization of the constitutional beginnings in what treats from the universal attention to the Brazilian citizens' health.

The Project National Card of Health was developed in attention to Basic Operational Norma (NOB) of 1996, as form of identifying the clientele of SUS, showing at the same time his entailment to a manager and the a very defined group of services, whose activities should cover, integrally, the whole mark of attention to the citizen's health, just as having stipulated for the Federal Constitution.

Safety's aspects, that include privacy, readiness, integrity, reliability and auditing were observed during the conception of the Project and they will be treated in this article.

Keywords

Security of Information System; System's Audit; Unique System of Health; National Health Card.

¹ Os autores são alunos do MBA em Gestão de Sistemas de Informação da UCB.

1. Introdução

O Cartão Nacional de Saúde foi instituído com o objetivo de identificar o usuário do SUS, possibilitando a construção de uma base de dados cadastrais e a sua vinculação a um conjunto de serviços de saúde bem definido, cujas atividades devem cobrir integralmente todo o escopo de atenção à saúde do cidadão.

O cartão tem numeração nacional, baseada no número do PIS/PASEP, identificando o usuário com o sistema local, mas também agregando informações no âmbito federal, que facilita o acompanhamento do fluxo desse usuário no sistema de saúde.

O processo de implantação do Cartão foi iniciado por um projeto piloto que abrange 44 municípios de 11 estados brasileiros, com cobertura de aproximadamente 13 milhões de usuários do SUS. Essa etapa teve financiamento do Banco Interamericano de Desenvolvimento (BID) e foi contratada por meio de licitação internacional.

O escopo do fornecimento das empresas contratadas abrange a implantação da estrutura de hardware no âmbito federal, estadual e municipal. Inclui ainda o desenvolvimento de software e a construção de uma rede de comunicação de informações em saúde de abrangência nacional.

2. Visão Geral do Projeto

O Cartão Nacional de Saúde foi concebido como estratégia e instrumento de apoio à plena implementação do Sistema Único de Saúde. Suas características e benefícios podem ser assim resumidos:

- Identidade do usuário no SUS;
- Construção de uma base de dados cadastrais baseada na numeração do PIS/PASEP;
- Integração dos sistemas nacionais de informação em saúde;
- Interligação das unidades de saúde em uma grande rede nacional formada pelos municípios, estados e Governo Federal.

Os principais objetivos do Projeto dividem-se em atendimento às necessidades dos usuários ou à gestão do SUS, conforme demonstram os quadros a seguir.

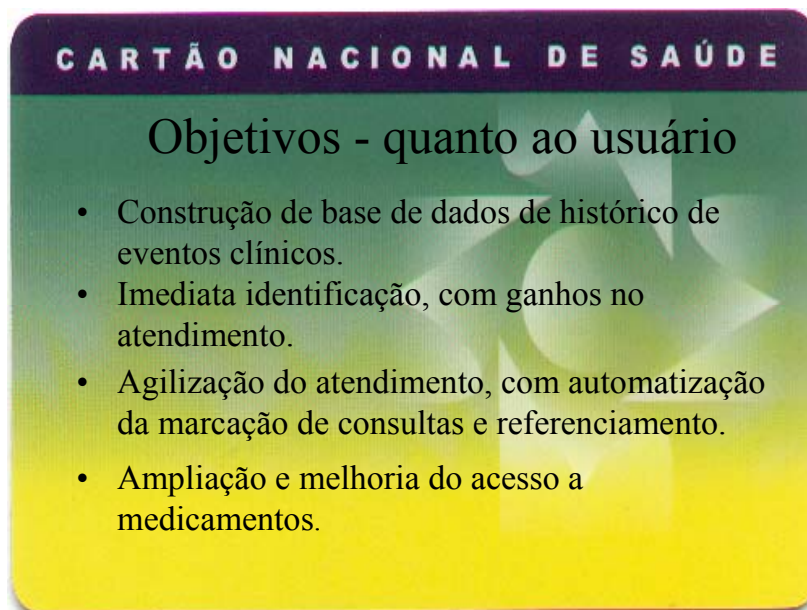


Fig. 1 – Objetivos do Projeto para os usuários do SUS

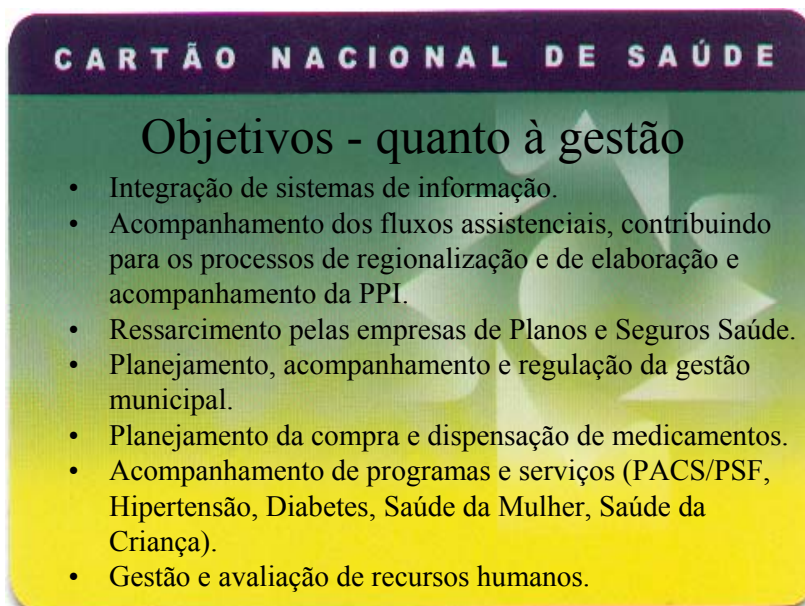


Fig. 2 – Objetivos do Projeto para a gestão do SUS

2.1 O Projeto Piloto

Considerado a primeira etapa de implantação do Cartão, contempla 44 municípios de 11 estados brasileiros. A licitação internacional, dividida em 3 lotes e realizada em 1999, possibilitou a contratação de 2 empresas, em julho de 2000. A divisão em lotes ocorreu para propiciar a experimentação com maior variedade de abordagens e soluções. Os municípios foram agrupados com base em critérios de proximidade/afinidade geográfica. A cobertura de cada um dos lotes foi dividida da seguinte forma:

<p>Lote 1 - Hypercom - Nível Federal, RS, SC, PR, RJ, ES e MG Lote 2 - Hypercom - SP, MS, MT, GO, TO, RO, RR, AP, AC, AM, PA e DF Lote 3 - Procomp - MA, PI, CE, RN, PE, PB, SE, AL e BA</p>

Os estados de Santa Catarina, Paraná, Rio de Janeiro, Espírito Santo, São Paulo, Mato Grosso do Sul, Pará, Pernambuco, Sergipe, Bahia e o Distrito Federal possuem municípios que compõem o projeto piloto.

A solução de informática contratada envolve hardware, software e treinamento dos recursos humanos envolvidos no projeto, que somam mais de 30 mil pessoas.

Os componentes que formam o sistema são:

- **Cartão magnético do usuário** – possui os dados do usuário do SUS e permite sua identificação imediata; apesar de ser de uso e abrangência nacional está referido ao município de residência do usuário;
- **Cartão magnético do profissional** – possui os dados pessoais do profissional e permite o acesso ao sistema por meio de senha; é de uso nacional mas o cadastro do profissional e suas permissões estão vinculadas aos estabelecimentos em que trabalha;
- **Terminal de Atendimento do SUS (TAS)** – responsável pela leitura dos cartões magnéticos e captação dos dados dos atendimentos;
- **Rede Nacional de Saúde** – interliga TAS e servidores formando uma base de dados nacional de atendimentos em saúde.



Fig. 3 – Imagem do cartão do usuário



Fig. 4 – Imagem do cartão do profissional



Fig. 5 – Imagem dos terminais de atendimento

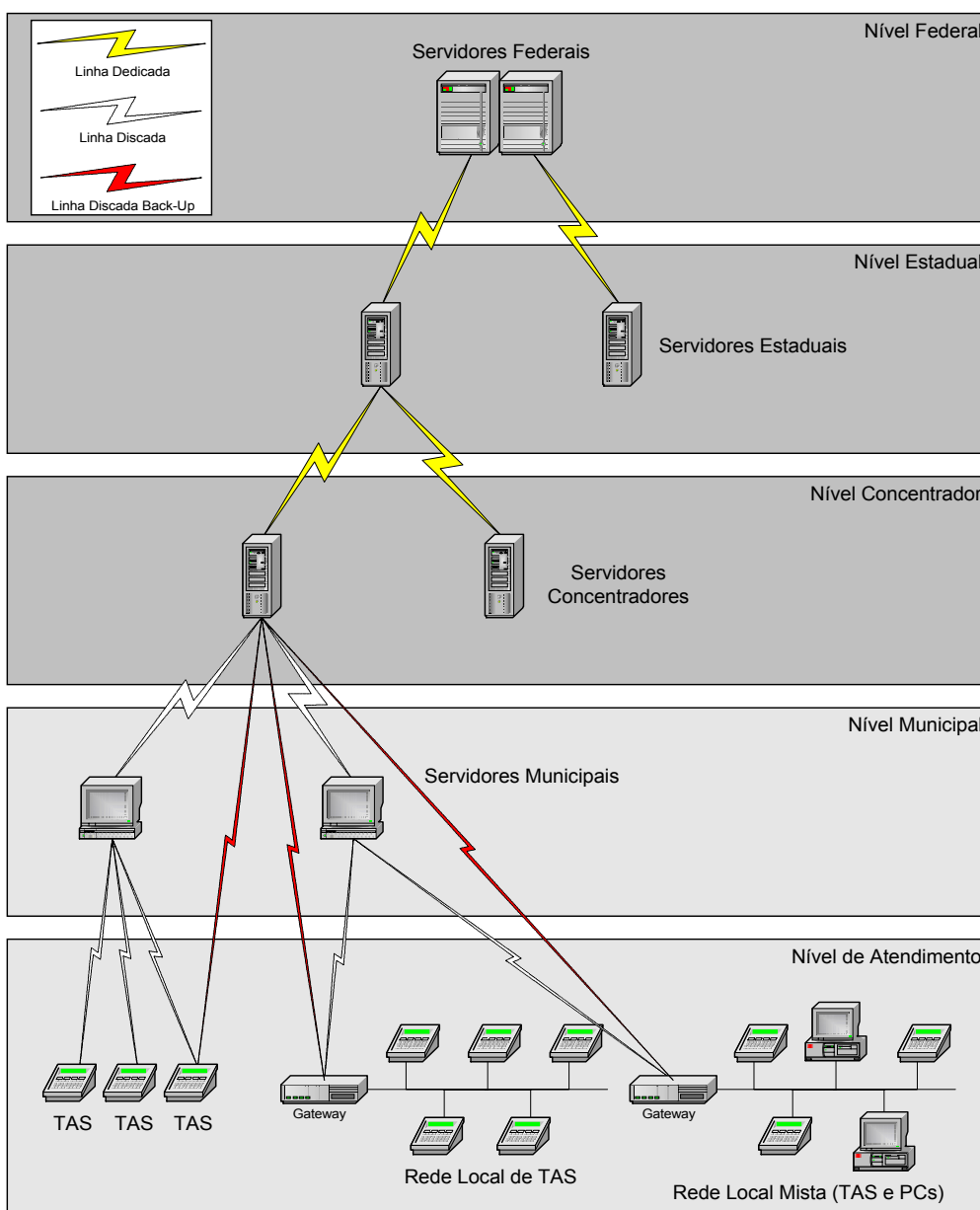


Fig. 6 – Representação da Rede Nacional de Saúde

2.1. A Rede Nacional de Saúde

Representa a arquitetura geral do sistema Cartão Nacional de Saúde. O TAS e o aplicativo municipal compõem os níveis inferiores de um sistema distribuído por uma rede que se estende até o nível federal, interligando municípios via servidores concentradores, estes em agregados estaduais, e finalmente os estados como parte da União.

Os cinco níveis em que o sistema está dividido são:

- **Atendimento** – composto pelos terminais de atendimento instalados nos estabelecimentos de saúde;
- **Municipal** – composto pelos servidores municipais responsáveis pelo processamento e armazenamento dos dados sobre todos os atendimentos realizados no município;
- **Concentrador** – composto por serviços conectados à rede on-line em tempo real e responsáveis pelo armazenamento dos dados de atendimentos de todos os municípios a ele conectados para fins de maior segurança dos dados e possibilidade de acesso pelos níveis estadual e federal;
- **Estadual** – composto por servidores conectados à rede permanente e responsáveis pelo armazenamento das informações totalizadas dos atendimentos realizados no estado;
- **Federal** – composto por servidores conectados à rede permanente e responsáveis pelo armazenamento das informações totalizadas dos atendimentos realizados no país.

3. Aspectos de Segurança

3.1. Política de Segurança

Como parte da arquitetura do sistema Cartão existe uma política de segurança que abrange cinco requisitos básicos:

- **Privacidade** – ocorre tanto na transmissão da informação quanto nos privilégios de acesso aos dados pelos operadores do sistema;
- **Autenticidade** – vinculação de toda e qualquer inclusão e/ou alteração de informações no sistema a um operador devidamente cadastrado; todo profissional responsável pela operação e/ou fornecimento de dados para o sistema por meio dos terminais de atendimento utiliza o cartão do profissional, que o identifica, qualifica e contém uma senha protegida criptograficamente;
- **Integridade** – garantia de que não há alteração dos dados durante a transferência entre os diversos níveis do sistema e de que todas as alterações ocorridas nos dados armazenados serão registradas; os dados coletados são armazenados por tempo indeterminado;
- **Controle de acesso** – implementação de política de definição de privilégios de acessos para classes de operadores do sistema por meio de senhas e armazenamento de todas as tentativas de acesso às funcionalidades e informações do sistema;
- **Auditoria** – os vários níveis do sistema podem avaliar a veracidade dos dados armazenados por meio de regras definidas.

Toda conexão entre roteadores da rede é realizada por meio de uma VPN (*Virtual Private Network*), utilizando o protocolo IPsec (*Internet Protocol Security*) com o algoritmo 3DES/168bits, que garante o sigilo de todas as comunicações que trafegam na rede. Além disso, o tráfego entre um TAs e um servidor, de *upload* entre servidores ou de serviço (consultas), é realizado sobre o protocolo HTTPS – protocolo HTTP (*Hypertext Transfer Protocol*) sobre o protocolo SSL (*Secure Sockets Layer*).

Os computadores servidores são certificados por uma certificadora digital criada no nível federal, de forma que há autenticação tanto para conexão com os níveis inferiores como com os níveis superiores, ou entre si no caso dos servidores federais.

Adicionalmente, ainda são observados os seguintes aspectos:

- os sistemas *off-line* são tratados da mesma forma que os sistemas *on-line*;
- na transferência de dados são garantidos os três requisitos citados: privacidade, autenticidade e integridade, utilizando técnicas criptográficas;
- os algoritmos criptográficos utilizados, quando de chave simétrica, tem tamanho não inferior a 128 bits, e quando de chave assimétrica, não inferior a 1024 bits;
- os certificados digitais utilizados no mecanismo de autenticação entre servidores são gerenciados pelo nível federal, tanto para geração quanto para distribuição.

3.2. Segurança da Informação

A implementação do Projeto permite o uso de equipamentos para leitura dos cartões magnéticos e acesso eletrônico a um cadastro de usuários por parte de gestores do SUS. A utilização dessa base de dados tem como finalidade única a gestão dos serviços de saúde pelas diferentes esferas de governo, não podendo, sob hipótese nenhuma, servir a fins comerciais ou outros que possam ferir os direitos constitucionais do cidadão.

As preocupações do Cartão quanto à gestão e segurança da Informação contemplam a normatização e criação de mecanismos que garantem que:

- quaisquer informações identificadoras ou diretamente correlacionáveis com os usuários decorrentes da utilização do cartão, serão consideradas confidenciais e sujeitas às mesmas éticas que regulam o acesso aos prontuários médicos e o seu uso, bem como a sanções legais, civis, administrativas e penais, se comprovada quebra de sigilo;
- em nenhuma circunstância, o fato do indivíduo possuir ou não o Cartão Nacional de Saúde poderá ser utilizado como forma de coação ou de obstáculo ao seu acesso aos serviços de saúde;
- os aplicativos e bases de dados, direta ou indiretamente relacionados ao Cartão Nacional de Saúde, deverão ser administrados pelos gestores públicos de saúde nas três esferas de governo e/ou sob sua coordenação e responsabilidade diretas.

Os números envolvidos na gestão do SUS legitimam plenamente todas essas preocupações, pois a dimensão do sistema brasileiro de atenção à saúde demonstra que anualmente cerca de 12 milhões de autorizações de internação são emitidas e os procedimentos ambulatoriais realizados ultrapassam a quantidade de 1 bilhão por ano. Ao todo, cerca de 1,3 bilhão de transações são registradas, anualmente, pelos sistemas de informações do Ministério da Saúde. Essas informações são provenientes de cerca de

67 mil estabelecimentos de saúde, entre hospitais e ambulatórios, que registram seus procedimentos e faturamentos contra o Sistema Único de Saúde. Destes estabelecimentos, aproximadamente 2 mil encontram-se nos municípios que fazem parte do projeto piloto onde o Cartão Nacional de Saúde está sendo implantado.

4. Fiscalização e Auditoria

Além do respeito ao requisito auditoria que consta na política de segurança em uso, foi contratada uma empresa para fiscalização e auditoria externa, atendendo ao que trata o edital para a solução de informática do Cartão Nacional de Saúde. O CPqD – Telecom & IT Solutions está cumprindo essa tarefa que abrange o monitoramento e a fiscalização do cumprimento das etapas, objetivos e prazos estabelecidos.

A Secretaria Federal de Controle, ligada ao Ministério da Fazenda, também fiscaliza o Projeto e faz o acompanhamento da implantação e do uso do sistema nos municípios do projeto piloto, que inclui auditoria no sistema e nos processos em funcionamento.

5. Conclusão

Após a análise do escopo do Projeto Cartão Nacional de Saúde, principalmente no que diz respeito à segurança da informação, podemos concluir que muitos são os detalhes que envolvem a implantação de um projeto de tamanha abrangência. Os aspectos de segurança devem ser observados e devidamente tratados de forma a garantir a aplicação dos recursos e atingir os benefícios almejados.

A formação dos recursos humanos envolvidos deve possuir uma atenção especial, uma vez que o bom funcionamento do sistema depende bastante da conscientização de cada ator envolvido. O Cartão Nacional de Saúde foi criado como um instrumento para ajudar a melhorar o sistema de saúde brasileiro, mas sozinho não conseguirá mudar ou melhorar nada.

6. Referências

[ASPECTOS DE SEGURANÇA DA INFORMAÇÃO DO CARTÃO NACIONAL DE SAÚDE, 2000] *Política de Segurança da Informação* – Cartão Nacional de Saúde

[CONCORRÊNCIA INTERNACIONAL Nº 001/99] Edital Solução de Informática para Implementação do Cartão Nacional de Saúde, Ministério da Saúde, 1999

[CLAUDIA DIAS, 2000] DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação*. Rio de Janeiro: Axcel Books do Brasil, 2000.