



Universidade Católica de Brasília

MBA – Gestão de Sistemas de Informação

Segurança da Informação
Prof. Ly Freitas Filho

**Segurança da Informação no Governo Federal:
O Caso do Cartão Nacional de Saúde do SUS**

1º Semestre de 2003

Segurança da Informação no Governo Federal: O Caso do Cartão Nacional de Saúde do SUS¹

Equipe do MBA Gestão de Sistemas de Informação
Universidade Católica de Brasília – 01/2003
Disciplina: Segurança da Informação

Fernando Alves Dias²
Humberto Oliveira de Araujo³
Rafael Amaral Miranda⁴
Roberto Saud Limeira Filho⁵

Resumo

Atualmente, a Segurança da Informação é um requisito gerencial de fundamental importância frente à evidência que o valor agregado da informação tem adquirido. Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças a segurança da informação de uma variedade de fontes, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo ou inundação. Por este motivo, o Governo Federal, como grande organização que é, se preocupa em prover um Plano de Segurança para toda a informação que administra. Este artigo apresenta as políticas, diretrizes e modelos seguidos pelo Governo Federal para garantir os princípios de serviços de segurança em seus sistemas de informações; em particular apresentamos o caso do Sistema do Cartão Nacional de Saúde, dispondo suas peculiaridades, exemplificando como age uma parte do Plano de Segurança do Governo Federal.

Palavras-chave

Política de Segurança da Informação; Governo Federal, Cartão Nacional da Saúde, confiabilidade; integridade; disponibilidade.

Brazilian Government Information's Security Summary

The Information's Security, nowadays, is a mainly important management requisite because of the evidence that the value-added information has acquired. In such case, more and more the organizations, their information systems and computer networks are tested by several kinds of threats to the information's security from a diversity of sources, including electronic frauds, espionage, sabotage, vandalism, fire or inundation. For that reasons, the Brazilian Federal Government, as a big organization, concerns to provide a Security Plan for all the information administrated. This article presents the policies, diretrizes and models used by the Brazilian Federal Government to guaranty the principals of security services in its information systems; in particular we present the case of the Nacional Health Card System, exemplifying the function of a part of Brazilian Federal Government's Security Plan.

Keywords

Information Security Policy; Brazilian Government, confidence; integrity; availability.

¹ Trabalho desenvolvido no MBA – Gestão de Sistemas de Informação

² fernando.dias@saude.gov.br

³ haraujo@mymail.com.br

⁴ leafarmiranda@bol.com.br

⁵ robertof@mpdft.gov.br

1. Introdução

O Brasil vive a plena vigência de um estado democrático, onde os cidadãos podem exercer seus direitos sem restrições. No entanto, esse aspecto levanta uma questão essencial: como garantir o direito ao sigilo que, para materializar-se, implica impor restrições ao direito de divulgar informações.

Tal situação caracteriza um aparente paradoxo, pois representa uma limitação ao ideal de transparência dos negócios públicos. De outro lado, percebe-se que cada direito individual ou coletivo, é por natureza, subjetivo. As demandas nesse caso apontam para uma nova realidade tecnológica consoante com a gestão dos processos públicos nacionais, cuja amplitude perpassa toda a sociedade brasileira. Soma-se a isso, a importância da **informação** como a principal riqueza de organizações e **nações**, impondo em consequência, maiores cuidados na sua prospecção, geração, processamento, transmissão, armazenamento, recuperação e no seu uso de forma consciente, garantindo o acesso somente a quem for autorizado.

É nesse contexto que os gestores de Tecnologia da Informação (TI) do Governo Federal encontram os maiores desafios: como garantir o direito à informação e ao mesmo tempo a segurança? Como garantir a transparência e ao mesmo tempo o sigilo?

O que se apresenta nesse artigo reflete uma pequena parte desse enorme *iceberg* da segurança da informação no âmbito do Governo Federal. O caso do Cartão Nacional da Saúde do SUS (Sistema Único de Saúde), demonstra bem aqueles desafios.

2. Políticas e diretrizes

O Governo Federal, em diversas oportunidades tem manifestado sua preocupação no sentido de assegurar a proteção da informação sob sua guarda bem como aquelas de interesse do cidadão. Inclusive na própria Constituição Federal figura a principal fonte para o estabelecimento de uma política de segurança informacional.

O Título II Dos Direitos e Garantias Fundamentais, Capítulo I Dos Direitos e Deveres Individuais e Coletivos, da Constituição da República Federativa do Brasil, em seu Art. 5º preceitua, nos incisos:

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo no último caso por ordem judicial.

A Constituição assegura a cada indivíduo o direito de proteger sua vida particular contra intromissões de estranhos. Tal direito abrange também a inviolabilidade da casa e o sigilo da correspondência e das comunicações.

XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.

A Constituição também assegura o direito de acesso à informação em termos muito amplos. Quando necessário ao exercício profissional, os informantes têm o direito de não revelar suas fontes.

XXXIII – todos tem direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestados no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Esse inciso assegura, em termos amplos, o direito à petição, sendo que o fornecimento de certidões independe do pagamento de taxas. Esse direito complementa-se com o direito de *habeas-data* definido no inciso LXXII deste mesmo artigo, o qual segue abaixo:

LXXII – conceder-se-á “habeas-data”:

- a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
- b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Habeas-data, expressão latina que significa *tenhas os dados*, é a garantia de acesso às informações pessoais que estão em poder do Estado ou de entidades de caráter público.

Outra preocupação governamental se refere aos *websites* públicos, que devem

comprometer-se a garantir a confiabilidade das informações de caráter pessoal que são armazenadas em suas bases de dados, sejam elas relativas aos usuários ou pessoas que compõem a administração pública.

Ou seja, a distribuição da massa informacional e a sua integridade garantida por meio de mecanismos de segurança para as diversas linhas de aplicação é uma diretriz que se materializa gradativamente no âmbito do Governo Federal, dando origem à chamada “**Política de Segurança da Informação nos Órgãos do Poder Executivo Federal – PSIPE**”.

2.1. Agentes do processo

Para o estabelecimento de tal política de segurança, foram definidos os seguintes agentes do processo:

DIRETRIZES PARA A IMPLEMENTAÇÃO DA POLÍTICA

- **Secretaria-Executiva do Conselho de Defesa Nacional – SECDN**: órgão vinculado ao Gabinete de Segurança Institucional da Presidência da República;
- **Comitê Gestor da Segurança da Informação - CGSI**

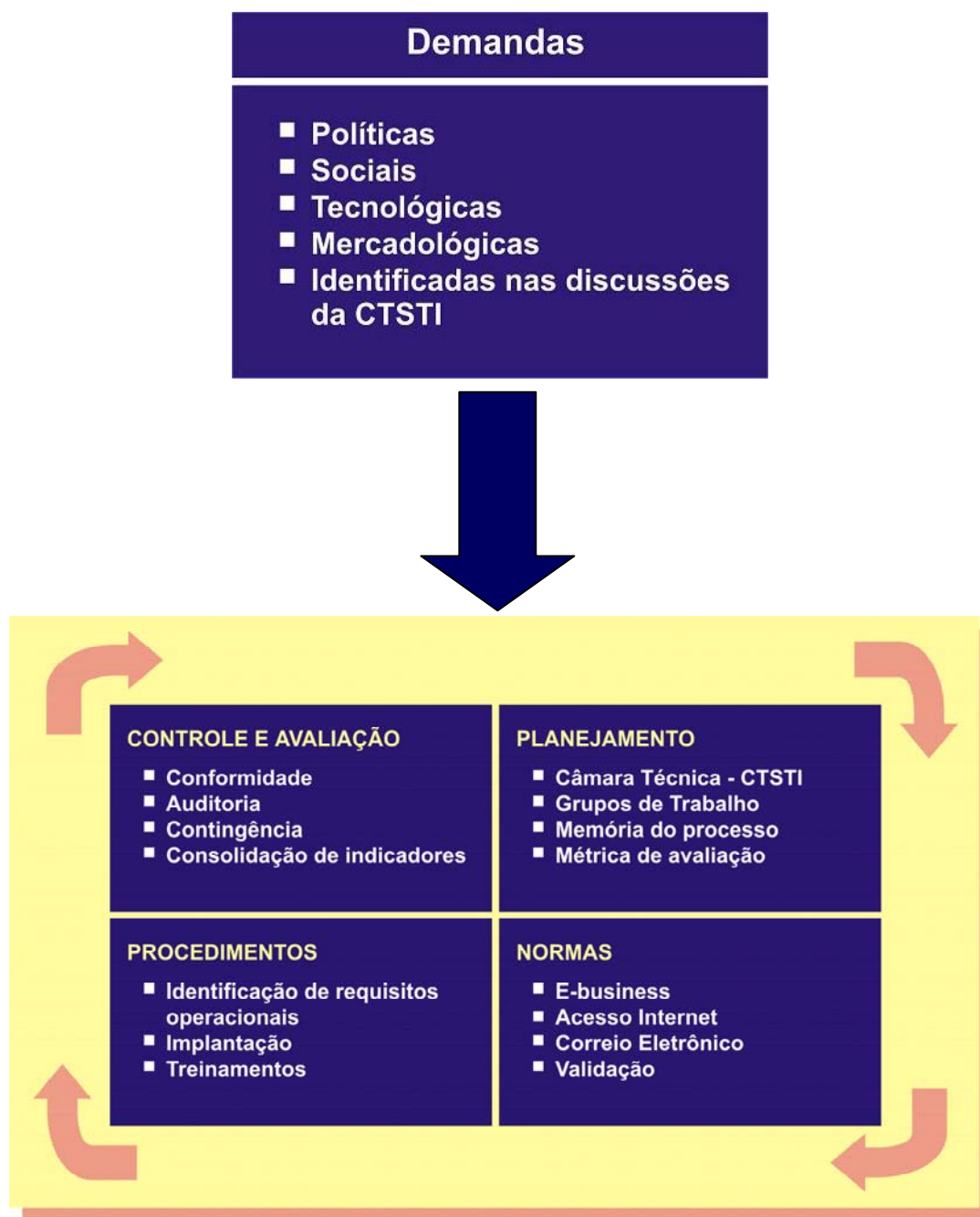
APOIO TÉCNICO OPERACIONAL

- **Câmara Técnica de Segurança da Tecnologia da Informação – CT-STI**: órgão vinculado ao Ministério do Planejamento.

Além dos órgãos acima, a **Secretaria de Logística e Tecnologia da Informação – SLTI** - do Ministério do Planejamento, Orçamento e Gestão, exercerá um papel preponderante na implementação da PSIPE, considerando que a mesma tem entre as suas atribuições a competência de coordenar as atividades do Sistema de Administração de Recursos de Informação e Informática, propondo políticas, diretrizes e normas de Informação e Informática, no âmbito da Administração Pública Federal.

A seguir, tem-se o esquema representativo da dinâmica operacional da Câmara Técnica.

Figura 1 – Dinâmica operacional da Câmara Técnica



Fonte: Adaptado da Cartilha “Fundamentos do Modelo de Segurança da Informação”, Ministério do Planejamento – Governo Federal, agosto de 2000.

3. Os princípios dos serviços de segurança

Os serviços de segurança no âmbito do modelo de segurança da informação do Governo Federal são caracterizados segundo os princípios:

3.1. Disponibilidade

Garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário.

3.2. Integridade

Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

3.3. Confidencialidade

Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

3.4. Autenticidade

Atestar, com exatidão, o originador e o receptor da informação, não permitindo o repúdio quanto à transmissão ou recepção da mesma.

4. O modelo de segurança da informação do Governo Federal

4.1. Aspectos do modelo

Na metodologia utilizada pelo Governo Federal no processo de modelagem, a segurança é considerada sob os seguintes aspectos:

- **ATAQUES À SEGURANÇA:** qualquer ação que comprometa a segurança da informação governamental;
- **MECANISMOS DE SEGURANÇA:** qualquer mecanismo utilizado para a detecção, prevenção ou recuperação de danos causados pelos ataques à segurança;
- **SERVIÇOS DE SEGURANÇA:** qualquer serviço que garanta a segurança dos sistemas de processamento de dados e as informações que trafegam nas redes. O objetivo desses serviços é a contenção dos ataques à segurança.

A modelagem da segurança, nas suas diversas formas, é um dos componentes que influencia a credibilidade de um sistema de computadores. Esta, sob um contexto mais amplo, propõe um maior controle sobre os ativos de informação, assim como sobre os serviços disponibilizados pelas diversas áreas do Governo.

Nesse sentido, o modelo de segurança que está sendo proposto para adoção em todas as áreas do Governo Federal ultrapassa os limites da segurança das redes de computadores. Ele inclui um amplo conjunto de procedimentos, mecanismos, normas, diretrizes e políticas necessárias à salvaguarda da informação governamental, incluindo assim, todas as informações em processamento, em tráfego nas redes de computadores, armazenadas em meios magnéticos, e aquelas sob a guarda do Governo.

Assim, cada área considerada pelo modelo será tratada sob os seguintes aspectos conceituais: FÍSICO (acesso, localização, instalação, ambiente), LÓGICO (software, desenvolvimento, sistemas computadorizados) e HUMANO (atitudes e comportamento).

4.2. Fases do modelo

O modelo inclui as fases de avaliação, projeto, implementação, gerenciamento, suporte, treinamento e conscientização em segurança da informação, nos seus processos e produtos.

Figura 2 – Fases do Modelo de Segurança da Informação do Governo Federal



Fonte: Cartilha “Fundamentos do Modelo de Segurança da Informação”, Ministério do Planejamento – Governo Federal, agosto de 2000.

As fases deste modelo cíclico serão avaliadas e revistas periodicamente, considerando as normas e procedimentos envolvidos, conforme as exigências tecnológicas impostas pela estruturação do *e-business* e do *e-commerce*, por exemplo, bem como quaisquer aspectos que estejam em evolução.

Dentro do dimensionamento de cada caso específico, o modelo considera o balanceamento de três fatores críticos:

- A probabilidade de sucesso dos ataques às vulnerabilidades do ambiente;
- O custo envolvido em um ataque, incluindo a recuperação dos processos organizacionais e dos serviços envolvidos;
- O custo de prevenção contra possíveis ataques.

A seguir, os componentes específicos de cada fase do modelo:

I - Avaliação

- Análise das necessidades e procedimentos utilizados;
- Identificação dos processos críticos;
- Análise dos riscos e das ameaças.

II - Projeto

- Definição dos conceitos - classificação da informação;
- Definição da equipe responsável pela implantação e manutenção da segurança;
- Elaboração de normas e procedimentos para técnicos e usuários;
- Objetivos da segurança da informação;
- Orçamento (custos);
- Elaboração do plano de contingência;
- Elaboração do termo de compromisso;
- Divulgação do projeto.

III - Implementação

- Aplicação formal das regras e normas definidas na fase de projeto;
- Elaboração e aplicação das modelagens de:

SEGURANÇA FÍSICA	SEGURANÇA LÓGICA
SEGURANÇA HUMANA	FLUXO DE INFORMAÇÃO

IV - Gerenciamento

- Diagnóstico e levantamento da situação atual do sistema;
- Implementação dos controles de segurança;
- Revisão da política de segurança para atender quaisquer mudanças nos níveis de risco;
- Controle do processo;
- Avaliação e ação corretiva.

V - Suporte

- Manutenção do Sistema de Segurança de Informação;
- Avaliação periódica dos riscos e ameaças;
- Monitoração e manutenção da eficácia dos controles de segurança.

5. O caso do Cartão Nacional da Saúde do SUS

5.1. O que é o Cartão Nacional da Saúde - CNS

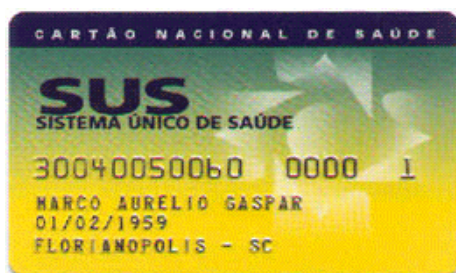
O Cartão Nacional de Saúde é um instrumento que possibilita a vinculação dos procedimentos executados no âmbito do Sistema Único de Saúde (SUS) ao usuário, ao profissional que os realizou e também à unidade de saúde onde foram realizados. Para tanto, é necessária a construção de cadastros de usuários, de profissionais de saúde e de unidades de saúde. A partir desses cadastros, os usuários do SUS e os profissionais de saúde recebem um número nacional de identificação. Hoje o Cartão Nacional de Saúde é um projeto piloto implementado em 44 municípios divididos em 10 estados.

O número de identificação é único, nacionalmente, sendo obtido a partir de um processo de cadastramento de usuários e profissionais de saúde. A base de numeração é o PIS-Pasep. Por meio do processo de cadastramento são gerados números para aqueles profissionais e usuários que ainda não os têm e, para aqueles que já são inscritos no PIS-Pasep, os números anteriormente existentes são identificados e comunicados pela Caixa Econômica Federal ao Departamento de Informática do SUS (Datapus).

O número PIS/Pasep tem 11 dígitos, e a numeração utilizada no Cartão Nacional de Saúde tem 15 dígitos. Os quatro dígitos extras foram introduzidos como reserva, para eventual utilização do cartão como instrumento de outros programas de governo. Eles também podem ser usados provisoriamente para identificação de atendimentos prestados a usuários ainda não cadastrados ou que não estejam de posse do cartão. Nos casos de usuários cadastrados, os quatro dígitos são 000V, onde V representa o dígito verificador.

Além dos cadastros, o Cartão Nacional de saúde é constituído por :

- Cartão do usuário: um cartão magnético, que será lido pelos equipamentos terminais desenvolvidos especificamente para o projeto. Este cartão tem impresso o número nacional de identificação do usuário;
- Cartão do profissional: também é um cartão magnético e permitirá a identificação dos profissionais de saúde perante o sistema;
- Infra-estrutura de informação e telecomunicações, com funções de captar, armazenar e transmitir as informações sobre os atendimentos realizados. Essa infra-estrutura é composta pelos equipamentos terminais, instalados nas unidades de saúde que compõem o SUS, pelos equipamentos servidores instalados nas secretarias estaduais e municipais de saúde e no Ministério da Saúde e por uma rede de comunicações que abrange os níveis municipal, estadual e federal; e
- Aplicativos desenvolvidos especificamente para o sistema Cartão Nacional de Saúde.



Cartão de Usuários do SUS



Cartão de Profissionais de Saúde do SUS

5.2. Objetivos do projeto

O sistema permite a coleta de uma série de informações vinculadas ao atendimento realizado, contribuindo para a organização de serviços de saúde e para ampliar e qualificar o acesso dos usuários aos mesmos. Dentre os objetivos do projeto, destacam-se:

- Construção de uma base de dados de histórico clínico;
- Imediata identificação do usuário, com agilização no atendimento;
- Ampliação e melhoria de acesso da população a medicamentos;
- Possibilidade de revisão do processo de compra de medicamentos;
- Integração de sistemas de informação;
- Acompanhamento dos fluxos assistenciais, ou seja, acompanhamento do processo de referência e contra-referência dos pacientes;
- Revisão dos critérios de financiamento e racionalização dos custos;
- Acompanhamento, controle, avaliação e auditoria do sistema e serviços de saúde;
- Gestão e avaliação de recursos humanos.

Com tudo isso, será possível conhecer quem está sendo atendido, por quem, aonde, como e com quais resultados.

A arquitetura proposta teve como linha mestra a adoção de soluções que representassem:

- **Confiabilidade:** Para garantir que o sistema como um todo seja capaz de trazer bases sólidas para a sua utilização pelo Ministério da Saúde, não somente no que se refere ao escopo do Cartão Nacional de Saúde, mas também em sua evolução nas próximas etapas de desenvolvimento;
- **Disponibilidade:** Para garantir que o sistema esteja disponível praticamente todo o tempo possível, evitando assim que sua operação seja prejudicada ou interrompida, degradando a qualidade e eficiência da solução;
- **Flexibilidade:** Para garantir que o sistema possa ser adaptado, expandido, atualizado e corrigido, sem deterioração da sua qualidade e do investimento realizado pelo Ministério da Saúde;
- **Compatibilidade:** Baseado totalmente na utilização de padrões abertos, o sistema é totalmente compatível com diversas tecnologias com diversos graus de obsolescência, garantindo a incorporação futura de outros sistemas legados, e é também capaz de suportar novas tecnologias, garantindo sua evolução;
- **Capacidade de atualização e evolução:** Entendendo que esta é apenas a primeira de uma série de etapas de desenvolvimento, a solução foi desenhada para não apresentar qualquer tipo de restrição à sua atualização e/ou evolução nas próximas etapas.

5.3. Princípios do sistema

- Qualquer informação identificadora ou diretamente relacionada com os usuários, decorrente da utilização do Cartão, é considerada confidencial e sujeita às normas éticas e legais que regulam o acesso aos prontuários médicos e o seu uso, bem como às sanções legais, civis, administrativas e penais, se comprovada a quebra de sigilo.
- O cidadão não poderá ser coagido ou ter seu acesso aos serviços de saúde negado ou não estar de posse do Cartão.
- Os sistemas de informática e bases de dados, direta e indiretamente relacionados ao Cartão Nacional de Saúde, devem ser administrados pelos gestores públicos de saúde nas três esferas de governo ou estar sob sua coordenação e responsabilidade.
- O Cartão Nacional de Saúde, assim como os sistemas de informática e equipamentos a ele relacionados, deve ser considerados como estratégias e instrumentos de apoio à plena implementação do SUS, sendo resultado dos investimentos públicos já realizados para o fornecimento de informações necessárias à gestão.
- O Cartão Nacional de Saúde deve contribuir para a manutenção, aperfeiçoamento e integração dos sistemas de informações de base nacional.
- Os padrões de representação e troca de informações do Cartão Nacional de Saúde deverão ser abertos, permitindo a integração com sistemas de informação e de gestão existentes e com aqueles a serem constituídos.

5.3.1 Visão Geral e Divisão por Níveis

O primeiro conceito a ser considerado para a compreensão do projeto como um todo é o conceito de divisão em níveis de todo o sistema. Numa visão mais macroscópica, a solução leva em consideração dois grandes blocos:

- **Rede Permanente:** É o bloco superior do sistema, que compreende uma grande rede de comunicações, contemplando a capital federal, todas as unidades da federação e um conjunto de sites concentradores. Essa rede, de abrangência nacional, se constitui como um “back-bone” de informações para o Ministério da Saúde. Além disso, em cada um dos nós desse “back-bone” está presente uma infra-estrutura computacional de processamento e armazenamento onde estarão os sistemas do Cartão Nacional de Saúde.
- **Rede Dial-Up:** É o bloco inferior do sistema, que compreende um grande sistema de captura de informações e processamento de dados, contemplando, nessa fase, 44 municipalidades escolhidas para o projeto do Cartão Nacional de Saúde. Esse sistema é composto por pontos de captura de dados nas unidades de saúde, através do Terminal de Atendimento do SUS – TAS –, e que se comunicam através de conexões discadas com os servidores presentes em cada municipalidade. Esses servidores são responsáveis pelo tratamento e armazenamento das informações capturadas. Esses dois grandes blocos são divididos em 3 e 2 níveis, respectivamente.

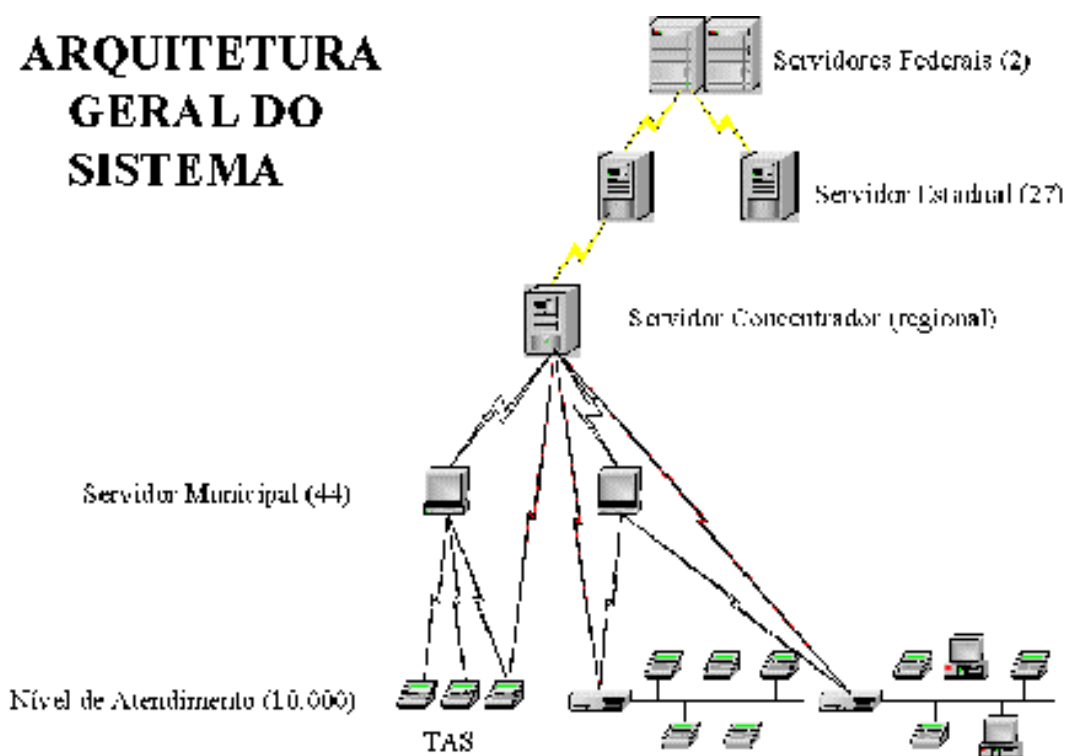
Assim, temos o sistema dividido em 5 níveis:

- (i) **Nível Federal:** Compreende o nível mais superior, englobando os dois sites federais a serem instalados. Um dos sites se localiza na capital federal e o outro na cidade do Rio de Janeiro;
- (ii) **Nível Estadual:** Engloba todas as capitais estaduais;
- (iii) **Nível Concentrador:** É o nível de interface entre a Rede Permanente e a Rede Dial-Up. Compreende localidades especialmente escolhidas a fim de organizar e distribuir os dados de acordo com áreas de afinidade. Nessa primeira etapa, apenas os estados que possuem localidades participantes do projeto terão seus sites concentradores implementados;
- (iv) **Nível Municipal:** É o primeiro nível da Rede Dial-Up. Os sites municipais presentes em todas as 44 localidades participantes do projeto são responsáveis pelo recebimento, tratamento e armazenamento das informações coletadas nas unidades de saúde;
- (v) **Nível de Atendimento:** É o nível mais inferior do sistema e que realiza o contato direto com os usuários do SUS nas unidades de saúde. Compreende todo o conjunto de TAS presente nas unidades de saúde.



TAS – Terminal de Atendimento do Sus

5.4. Arquitetura geral do sistema

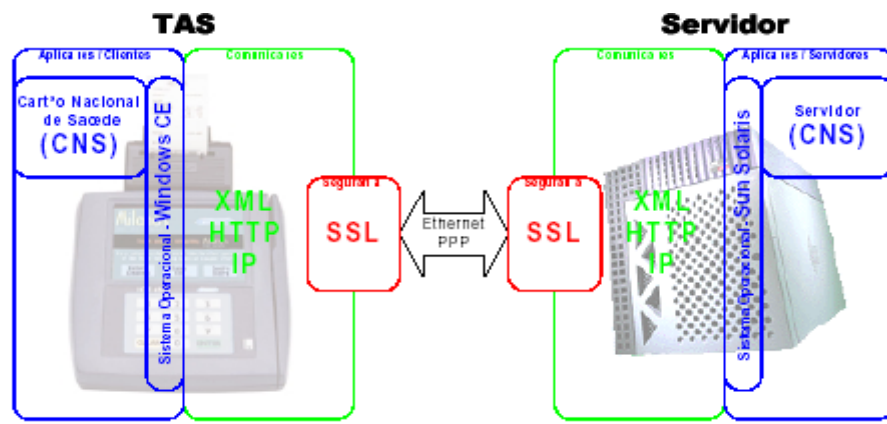


5.4.1 Rede Física de Comunicação

A rede do Cartão Nacional de Saúde está configurada como uma rede TCP/IP do nível federal até o nível municipal. O nível de atendimento pode ter, contudo, um esquema de endereçamento local independente, recebendo um endereço atribuído pelo nível municipal quando realizar uma conexão discada, via um esquema de DHCP.

Toda conexão entre roteadores da rede é realizada criando-se uma VPN, utilizando-se o protocolo IPSec com 3-DES/168bits. Além disso, todo o tráfego de *upload* entre servidores, assim como todo o tráfego de serviço (consultas) é realizado sobre o protocolo HTTPS (HTTP + SSL). As chaves criptográficas utilizadas são de no mínimo 1024 bits, quando assimétricas, e 128 bits, quando simétricas.

A rede física provê o meio de comunicação entre diferentes níveis que compõe o sistema. Para manter segurança dos dados no tráfego são utilizados esquemas de criptografia.



5.5. Princípios de segurança adotados

A utilização da base de dados do Cartão Nacional de Saúde 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 venham ferir os direitos constitucionais do cidadão. Um usuário desta base só deve ter direito de acesso aos dados na forma única e exclusiva necessária para os fins alegados, justificados e autorizados ao exercício de sua função.

O Projeto Cartão foi concebido tendo em mente a importância da **segurança das informações**. Para tanto, como parte da arquitetura do sistema, está sendo proposta uma política de segurança abrangendo cinco requisitos básicos: privacidade, autenticidade, integridade, controle de acesso e auditoria dos dados de saúde vinculados ao sistema Cartão Nacional de Saúde. Os mecanismos de segurança adotados pelo projeto incluem os seguintes aspectos:

- **Privacidade/confidencialidade** - os dados são protegidos do monitoramento, tanto na forma ativa, onde poderá ser feita uma alteração, quanto na forma passiva, cujo objetivo é simplesmente o da obtenção da informação.
- **Autenticidade** - toda e qualquer inclusão ou alteração de informações no sistema deve estar vinculada a um operador devidamente cadastrado tanto para operação dos servidores como dos terminais. Todos os profissionais de saúde responsáveis pela operação e fornecimento de dados para o sistema, por meio dos terminais, disporão do cartão de profissional de saúde, que os identifica e qualifica. Esse cartão contém uma senha protegida criptograficamente.
- **Integridade** - existem proteções contra a adulteração dos dados enquanto esses são transferidos ou armazenados nos diversos níveis do sistema. Além disso, o sistema armazena os dados coletados por tempo indeterminado e registra todas as alterações neles ocorridas, sem apagar os registros anteriores.
- **Controle de acesso** - o sistema permite a implementação de uma política de definição de privilégios de acessos para classes de operadores e normas de divulgação da informação. Todas as tentativas de acesso às funcionalidades e informações do sistema são armazenadas para fins de auditoria.
- **Auditoria** - o que se prevê é a capacidade de se avaliar a veracidade dos dados armazenados. Esta avaliação poderá ser realizada nos vários níveis do sistema, de acordo com regras definidas.

Toda conexão entre roteadores da rede é realizada criando-se uma VPN, utilizando-se o protocolo IPSec (*Internet Protocol Security*) com o algoritmo 3DES/168bits, que garante o sigilo de todas as comunicações que ali trafegam. Além disso, todo o tráfego entre um terminal e um servidor, de upload entre servidores ou de serviço (consultas) é realizado sobre o protocolo HTTPS, ou seja, protocolo HTTP (*Hypertext Transfer Protocol*) sobre o protocolo SSL (*Secure Sockets Layer*).

Todos os Servidores serão certificados por uma certificadora digital criada no nível federal, de forma que se autenticam tanto para conexão com os níveis inferiores como com os níveis superiores (ou entre si no caso dos servidores federais).

Adicionalmente, cabe destacar os seguintes aspectos:

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

5.7. Vantagens e Técnicas de Soluções Adotadas

5.7.1. Frame-relay

A solução adotada com a utilização de serviços de **frame-relay** oferece uma série de vantagens para atendimento a um conjunto de novas aplicações de comunicação de dados, quando comparado às soluções oferecidas pelos serviços dedicados e de redes de pacotes (X.25). Entre elas destacam-se:

- **Escalabilidade:** se houver a necessidade de aumentar a largura de banda para transmissão de dados, basta aumentar o CIR (Committed Information Rate) contratado junto à concessionária da malha de frame-relay;
- **Disponibilidade:** O período up-time da rede WAN, irá depender da concessionária do serviço. Este período na grande maioria das concessionárias está acima de 99%, através da utilização de equipamentos robustos;
- **Performance:** A rede proposta foi projetada a atender as necessidades do projeto. As larguras de banda propostas foram calculadas com base nas estimativas de atendimento fornecidas de modo a fornecer alta performance para a aplicação. Além disto as malhas frame-relay permitem o tráfego de dados além da capacidade contratada (CIR), melhorando a performance da aplicação;
- **Segurança:** Todos os dados trafegados na malha frame-relay serão criptografados através de VPN entre os roteadores. Além disto serão utilizadas listas de acessos para bloquear acessos indevidos;
- **Gerenciamento:** A concessionária possui monitoração on-line das malhas de frame-relay, detectando rapidamente qualquer tipo de problema que venha a ocorrer. Além disto os equipamentos propostos possuem facilidades de gerenciamento remoto, através do nível federal. Através destas facilidades é possível obter o status dos equipamentos on-line.

5.7.2. Virtual Private Network (VPN)

Entre os roteadores dos níveis Municipal, Concentrador e Estadual será implementada uma VPN. Para tanto, os roteadores utilizados nessa rede utilizam o protocolo IpSec, com criptografia de 128 bits.

Esse esquema promove a **Privacidade** dos dados de comunicação nessa parte da rede, de forma simples. Também será implementado VPN entre o roteador do nível estadual e o roteador do nível Federal.

5.7.3. Controle de Acesso

Através de política de definição de privilégios de acesso para classes de operadores do sistema.

Os operadores devem ser identificados pelo sistema e possuir uma senha que permita ter acesso às funcionalidades e informações definidas para a classe de operadores a qual pertencem.

5.7.4. Auditoria

Todas as tentativas de acesso às funcionalidades e informações do sistema devem ser armazenadas para fins de auditoria.

Capacidade de se avaliar a veracidade dos dados armazenados.

5.7.5. Operações OnLine e OffLine

Em termos de Segurança, os sistemas OffLine devem ser tratados da mesma forma que os sistemas OnLine.

5.7.6. Alteração periódica das chaves de comunicação

As chaves utilizadas para comunicação dos dados deverão ser mudadas periodicamente. A geração e distribuição dessas chaves serão efetuadas pelo nível Federal.

5.7.7 Logs de Operação

Cada operação gerada por operador no TAS é registrada em seu log de operações, que é posteriormente enviado e armazenado no Servidor Municipal associado a esse TAS. Da mesma forma, cada operação gerada por operador nos Servidores dos vários níveis será registrada em seu log de operações.

Tanto nos TAS quanto nos Servidores, as operações são precedidas de abertura de sessão pelo operador, com sua identificação. Essa identificação permite que as aplicações nesses equipamentos possam associar as operações ao operador. Cada registro do log de operações contém tanto a operação realizada quanto a identificação do operador que a executou.

O sistema registra também as tentativas de execução de operações que não puderam se realizar por falta de direitos de acesso do operador. Assim, por exemplo, o sistema registra a tentativa de abertura de sessão de um operador com senha inválida. Este item responde ao requisito do Edital que pede que todas as tentativas de acesso às funcionalidades e informações do sistema sejam armazenadas para fins de auditoria. Também responde ao edital com relação à **Autenticidade**: Vinculação de toda e qualquer inclusão e/ou alteração de informações no sistema a um operador devidamente cadastrado.

5.7.7.1. Resumo nos Logs de Operação

O sistema gera um resumo do registro, para cada operação. O resumo é gravado junto com o registro, tanto no log de operações do TAS quanto no log de operações dos Servidores.

Esse resumo é gerado de forma a impedir que uma alteração fraudulenta nos dados do registro possa produzir um novo registro cujo resumo coincida com o previamente gravado. Para tanto é utilizado um algoritmo matemático de HASH, padrão MD5, para a geração do resumo.

Esse HASH é mantido com o registro da operação e o controle de acesso do banco de dados garante que nenhum operador pode alterá-lo. Os Auditores, em seus vários níveis, terão direito de execução de validação dos registros, utilizando o HASH para tanto.

Com isso garante-se que um Auditor sempre consiga **avaliar a veracidade dos dados armazenados**.

5.7.8. Controle de Acesso às funções dos TAS

Os operadores dos TAS são Profissionais de Saúde. Para definição dos direitos de acesso, cada Profissional de Saúde pertencerá a uma Classe de Operadores do TAS, dentre as seguintes:

- Normal;
- Privilegiado;
- Super Usuário.

Os direitos de Acesso de cada uma dessas Classes de Operadores são definidas no Servidor Municipal, dentre as Operações Executadas no TAS como: Identificação de Usuário, Atendimento de Usuário, Atualização de Dados Cadastrais, envio de lote ao Servidor, etc.

Os operadores de TAS são identificados pela passagem de seu cartão SUS no TAS, em momento de abertura de sessão no mesmo. Isso associa um responsável às operações efetuadas, já que toda a operação executada no TAS será gravada juntamente com o operador que a digitou.

5.7.9. Contingências contra falhas de infra-estrutura

Todos os Níveis de Servidores poderão enfrentar falhas de infra-estrutura. Para cada tipo de falha serão descritas as medidas que devem ser tomadas.

5.7.9.1 Falha de Energia Elétrica

Na eventual falta de energia no Nível de Atendimento, os operadores dos TAS deverão preencher manualmente os boletos de atendimento – FAA (Ficha de Atendimento Ambulatorial) e FAU (Ficha de Atendimento com Urgência). Após o retorno da energia, as informações destes boletos manuais deverão ser digitadas nos TAS, pelos operadores.

Na falha do fornecimento de energia elétrica para os equipamentos dos Níveis Municipal, Concentrador e Estadual, o No-Break será acionado automaticamente e fornecerá energia por 60 minutos para todos os equipamentos daquele Nível (Servidor, Roteador, Switch e Modem).

O No-Break também será programado para enviar um comando de desativação (*shutdown*) para os servidores, quando faltar alguns minutos para acabar a sua carga total. Se a energia voltar ao fornecimento normal antes deste comando ser enviado, o envio do comando será cancelado.

Medidas de O&M: Após 45-50 minutos sem retornar a energia (este tempo é programável), desligar todos os equipamentos para evitar que, após o fim da carga do No-Break, os mesmos recebam picos no momento do retorno da energia e sejam danificados.

5.7.9.2 Falha de Comunicação

- **Contingência do link principal no Nível Concentrador**

Quando o Concentrador não está no mesmo site físico do Estadual, em contingência do link principal, a comunicação do Nível Concentrador com o Nível Estadual será através de linha discada, acionada automaticamente, não necessitando de intervenção do operador. Esta funcionalidade é configurada no próprio roteador do Nível Concentrador acoplado a um modem externo, sem necessidade de software adicional.

Quando o link principal retornar a operação, o roteador efetuará o chaveamento da linha dial back-up para a linha principal automaticamente, sem a necessidade de intervenção do operador.

Quando os dois sites (Concentrador e Estadual) estiverem localizados no mesmo endereço, a contingência estará presente somente no roteador estadual.

- **Contingência do link principal no Nível Estadual**

Numa contingência do link principal, a comunicação do Nível Estadual com o Nível Federal será através de linha discada, acionada automaticamente, não necessitando de intervenção do operador. Esta funcionalidade é configurada no próprio roteador do Nível Estadual acoplado a um modem externo, sem necessidade de software adicional.

Quando o link principal retornar a operação, o roteador efetuará o chaveamento da linha dial back-up para a linha principal automaticamente, sem a necessidade de intervenção do operador.

Procedimento de contingência para os casos de problemas de comunicação com o município por períodos prolongados: o TAS permite, mediante comando do operador, fazer uma conexão diretamente com o servidor do Nível Concentrador correspondente ao município, para descarregar o lote acumulado. Se ocorrer algum problema, o TAS fará um certo número de tentativas. Se nenhuma funcionar, nada mais será feito. O operador receberá a seguinte mensagem: “tente outra vez”.

Com a conexão efetivada, os dados do TAS serão transmitidos para o servidor do Nível Concentrador e gravados na base do Servidor Concentrador e, depois disto, o log do TAS será esvaziado e a conexão encerrada.

Na próxima conexão do Servidor Municipal com o Servidor Concentrador, o Servidor Municipal buscará os atendimentos recebidos pelo Servidor Concentrador diretamente dos TAS. Estes atendimentos estarão enfileirados no Servidor Concentrador, onde cada fila se refere a um Servidor Municipal. Em casos de perda de conexão durante a transmissão dos dados, a chamada ao destino será efetuada automaticamente sem a necessidade de uma intervenção do operador.

- **Contingências contra falhas de hardware/software do sistema Falhas de Hardware Redes**

Nos casos de falha de hardware de rede (Roteador, Servidor de Acesso, Switch e Hub) nos Níveis Estadual e Concentrador, o operador deverá acionar a Central de Atendimento para a sua manutenção, detalhando o defeito/problema encontrado.

- **TAS**

Nos casos de falha de hardware de um equipamento TAS, Nível de Atendimento, o operador deverá acionar a Central de Atendimento para a sua manutenção.

As transações de identificação do usuário deverão ser efetuadas novamente pelo operador, em outro equipamento TAS em funcionamento, ficando a cargo do Servidor Municipal tratar as duplicidades. Os dados dos boletos de atendimentos deverão ser digitados novamente, sem necessidade de nenhuma opção extra.

- **Servidores dos Níveis: Municipal, Concentrador e Estadual**

Todos os Servidores dos Níveis Municipal a Estadual possuem fontes e ventilação redundantes e mecanismos de redundância de discos com tecnologia *Hot Swap*, o que se traduz em um aumentando da confiabilidade/disponibilidade das

máquinas e, por consequência, dos Sistemas. Nos casos de falha de hardware de qualquer servidor ou impressora a laser dos Níveis: Municipal, Concentrador e Estadual, o operador daquele nível deverá acionar a Central de Atendimento para a sua manutenção, detalhando o defeito/problema encontrado que ele poderá obter informações nas Logs de Operação.

a) Nível Municipal:

Durante a indisponibilidade do Servidor Municipal, os atendimentos feitos nos TAS serão recebidos pelo Servidor Concentrador. Procedimento de contingência para os casos de problemas de comunicação com o município por períodos prolongados. Serão configurados mecanismos de redundância de discos com implementação de RAID 5 (paridade), nos Servidores Municipais de portes Médio e Grande;

b) Nível Concentrador:

Durante a indisponibilidade do Servidor Concentrador, os atendimentos recebidos, os dados totalizados e os relatórios gerados pelo Servidor Municipal, que numa operação normal são replicados para o Servidor Concentrador, serão mantidos pelo Servidor Municipal e só serão replicados quando o Servidor Concentrador se tornar novamente disponível.

Serão configurados mecanismos de redundância de discos com implementação de RAID 5 (paridade), nos Servidores Concentradores;

c) Nível Estadual:

Durante a indisponibilidade do Servidor Estadual, os dados totalizados e os relatórios gerados do Servidor Concentrador, que numa operação normal são replicados para o Servidor Federal, serão mantidos pelo Servidor Concentrador e só serão replicados quando o Servidor Estadual se tornar novamente disponível.

Serão configurados mecanismos de redundância de discos com implementação de RAID 5 (paridade), nos Servidores Estaduais.

5.7.9.3.Falhas de Software

- **Nível de Atendimento: TAS**

Nos casos em que os dados de um determinado TAS, usado na identificação de pacientes, tenham sido perdidos, a digitação dos boletos com identificadores provenientes deste TAS deverá incluir também a digitação do código do paciente, natureza da procura, grupo de atendimento e encaminhamento e, nos casos de internação, diagnóstico inicial - usando o CID 10 (Código Internacional de Doenças) - e o procedimento indicado, que foram impressos no boleto quando da identificação original do paciente. O software municipal se encarregará de resolver o problema de duplicidade, sempre que possível usando os dados da identificação original.

A perda de dados de um TAS usado para digitar dados de boletos de atendimentos não precisará de nenhuma opção extra, já que bastará digitar novamente os boletos.

- **Servidores dos Níveis: Municipal, Concentrador e Estadual**

Nos manuais de operação dos servidores dos Níveis Municipal, Concentrador e Estadual serão fornecidos os procedimentos a serem executados no momento de falha de software. Caso ocorram maiores complicações, o operador deverá acionar a Central de Atendimento, detalhando os problemas encontrados. Informações sobre os problemas encontrados, o operador poderá obter através das Logs de Operação.

Em caso de perda de dados no Servidor de um determinado nível devido a alguma falha, estes serão restaurados através dos últimos backups (total e incrementais) feitos. Se mesmo após a restauração do último backup for identificado que o Servidor do nível imediatamente superior possui dados mais atuais, o operador do nível superior deve ativar, através da Tela de Administração, as réplicas das tabelas contidas no seu Servidor para o Servidor do nível inferior.

Referências

[NBR ISO/IEC 17799] – ABNT – Associação Brasileira de Normas Técnicas, Agosto 2001.

[DIAS, CLÁUDIA , 2000] – Dias, Cláudia . “Segurança e Auditoria da Tecnologia da Informação” . Axcel Books do Brasil, 2000.

[MINISTÉRIO DO PLANEJAMENTO, GOVERNO FEDERAL] – Ministério do Planejamento, Câmara Técnica de Segurança da Tecnologia da Informação. “Fundamentos do Modelo de Segurança da Informação”, Agosto 2000.

[SECRETARIA EXECUTIVA DO MINISTÉRIO DA SAÚDE, GOVERNO FEDERAL] - <http://www.saude.gov.br/cartao/>