UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO E PROPOSTA DE IMPLANTAÇÃO DE UM NOVO SISTEMA DE VOTAÇÃO ELETRÔNICA PARA O SENADO FEDERAL

FRANCISCO JOSÉ FIUZA LIMA

JOÃO JORGE SQUEFF

ORIENTADOR: ROBSON DE OLIVEIRA ALBUQUERQUE

MONOGRAFIA DE ESPECIALIZAÇÃO

PUBLICAÇÃO: UNB.LABREDES.MFE.001/2006

BRASÍLIA / DF: MAIO/2006

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO E PROPOSTA DE IMPLANTAÇÃO DE UM NOVO SISTEMA DE VOTAÇÃO ELETRÔNICA PARA O SENADO FEDERAL

FRANCISCO JOSÉ FIUZA LIMA
JOÃO JORGE SQUEFF

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA.

APROVADA POR:

ROBSON DE OLIVEIRA ALBUQUERQUE, Mestre, UnB
(ORIENTADOR)

RAFAEL TIMÓTEO DE SOUSA JÚNIOR, Doutor, UnB
(EXAMINADOR)

ANDERSON CLAYTON ALVES NASCIMENTO, Doutor,
(EXAMINADOR)

TAMER AMÉRICO DA SILVA, Mestre, UnB
(EXAMINADORA)

ODACYR LUIZ TIMM JR, Ms OM,
(EXAMINADOR)

DATA: BRASÍLIA/DF, 16 DE MAIO DE 2006.

FICHA CATALOGRÁFICA

LIMA, FRANCISCO JOSÉ FIUZA e **SQUEFF, JOÃO JORGE**
Estudo e Proposta de Implantação de um Novo Sistema de Votação Eletrônica para o Senado Federal [Distrito Federal] 2006
xviii, p.101, 297 mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2006)
Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica.
1. Governo 2. Poder Legislativo
3. Votação Eletrônica 4. Processo Legislativo
I. ENE/FT/UnB. II**. Título (Série)**

REFERÊNCIA BIBLIOGRÁFICA

LIMA, F. J. F. (2006), SQUEFF, J. J. (2006) Estudo e Proposta de Implantação de um Novo Sistema de Votação Eletrônica para o Senado Federal [Distrito Federal] 2006, Publicação: UNB.LABREDES.MFE.001/2006, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 101 p.

CESSÃO DE DIREITOS

NOME DOS AUTORES: **Francisco Jose Fiuza Lima e João Jorge Squeff**
TÍTULO DA MONOGRAFIA: Estudo e Proposta de Implantação de um Novo Sistema de Votação Eletrônica para o Senado Federal.
GRAU / ANO: **Especialista**/**2006**

Francisco Jose Fiuza Lima
SQN 402 BL J APTO 105
CEP 70834-100 – Brasília – DF – Brasil

João Jorge Squeff
SHIN QI 08 Conjunto 07 Casa 10 - Lago Norte
CEP 71520-270 – Brasília – DF – Brasil

AGRADECIMENTOS

Agradecemos ao Prof. Robson de Oliveira Albuquerque pelo constante apoio, incentivo e dedicação como nosso orientador, que muito contribuiu para a elaboração deste trabalho.

Agradecemos ao Prof. Odacyr Luiz Timm Jr. pela eficiente coordenação do curso e pela criação de um ambiente apropriado ao aprendizado, o que abriu nossos horizontes e nos deu o suporte necessário à preparação desta monografia.

Agradecemos aos colegas do Prodasen Bernardo Brenicci, Hélio Ferreira Lima, Luiz Flávio Brant Moraes Silva e Rubens Vasconcellos Terra Neto pela colaboração prestada na discussão de temas específicos ao nosso ambiente de trabalho, permitindo-nos aplicar os conhecimentos adquiridos em sala de aula na solução de questões técnicas da realidade do Senado Federal que estavam relacionadas a esta monografia.

Agradecemos a Sérgio Marcos de Souza pela elaboração das figuras do trabalho.

O presente trabalho foi realizado com o apoio institucional e financeiro do Prodasen, órgão responsável pela gestão da Tecnologia da Informação no Senado Federal.

ESTUDO E PROPOSTA DE IMPLANTAÇÃO DE UM NOVO SISTEMA DE VOTAÇÃO ELETRÔNICA PARA O SENADO FEDERAL

RESUMO

O objetivo desta monografia é apresentar estudo e proposta para a implantação de um novo Sistema de Votação de Eletrônica para o Senado Federal (SVE-SF). O SVE-SF é utilizado no plenário do Senado Federal para anunciar as sessões legislativas, registrar a presença dos senadores, cronometrar, orientar e registrar votações nominais e secretas de matérias legislativas, exibir seu resultado nos painéis de exibição, emitir relatórios sobre as votações, divulgar mensagens e executar funções gerenciais.

A necessidade da modernização do sistema atual deve-se ao seu acelerado processo de obsolescência, pois, desde sua implantação, há 04 (quatro) anos, não sofreu modificações, seja de *hardware* ou de *software*, deixando de atender a novas demandas da Casa surgidas durante esse período.

Em conseqüência, o foco da monografia é apresentar requisitos para um novo Sistema Eletrônico de Votação, recomendar a atualização da política de segurança do SVE-SF e propor uma nova configuração do *hardware* e *software* básicos, contemplando a substituição dos terminais de votação dos senadores, do console do presidente, dos terminais de cadastramento biométrico, da rede de comunicação de dados, dos servidores do sistema e do painel de exibição.

STUDY AND PROPOSAL FOR A NEW ELECTRONIC VOTING SYSTEM FOR BRAZILIAN FEDERAL SENATE

ABSTRACT

This work intends to show a proposal for deploying a new Electronic Voting System for Brazilian Federal Senate. The Electronic Voting System is aimed to be used at the Plenary of the House for the announcement of Legislative Sessions, for registering the presence of the representatives, for controlling the voting process of all legislative matters, including secret ones, for registering the votes and for advertising its results in the plenary panels. The system also prints reports, advertise messages in the panels and run administrative issues.

The deployment of a new Electronic Voting System is fundamental because the old one is obsolete. It was deployed four years ago and it never received software or hardware upgrades. Additionally, no demands from the Senate, that occurred during this period, has been incorporated.

The goal of this work is to present specifications for a new Electronic Voting System, for a new hardware and software configuration, including the deployment of new workstations for all activities related to the system, including the senators' workstations, the president workstation and the biometric enrollment workstations. Additionally, it will be presented new specifications for the data network, for the system servers, for the panels and for a new security policy for the Electronic Voting System of Brazilian Senate.

ÍNDICE

Item **Página**

ÍNDICE DE TABELAS

Tabela **Página**

ÍNDICE DE FIGURAS

Figura **Página**

ÍNDICE DE ABREVIAÇÕES

3DES	*Triple Data Encryption Standard*
AD	*Active Directory*
ANSI	*American National Standards Institute*
CBC	*Cipher Block Chaining*
CCD	*Charged Coupled Device*
CD	*Candela*
CHIP	*Integrated Circuit*
CIFS	*Common Internet File System*
CRT	*Cathode Ray Tube*
CSS2	*Cascading Style Sheets, level 2*
DES	*Data Encryption Standard*
DHCP	*Dynamic Host Configuration Protocol*
DLP	*Digital Light Processing*
DMD	*Digital Micromirror Device*
DTV	*Digital Television*
DVI	*Digital Video Interface*
E-BUSINESS	*Electronic Business*
EDTV	*Enhanced Definition Television*
ESP	*Encapsulating Security Payload*
LCD	*Liquid Crystal Display*
LcoS	*Liquid Crystal on Silicon*
LED	*Light Emitting Diode*
LUMEN	*Unit of Luminous Flux*
HDTV	*High Definition Television*
HTML	*Hiper Text Markup Language*
HTTP	*Hiper Text Transfer Protocol*

IP	*Internet Protocol*
IPsec	*Internet Protocol Security*
iSCSI	*Internet Small Computer System Interface*
MD5	*Message-Digest algorithm 5 – cryptographic hash function*
RAID	*Redundant Arrays of Independent Disks*
RFC	*Request for Comments*
RGB	*Red, green and blue*
RSA	*Ron **R**ivest, Adi **S**hamir e Len **A**dleman – (criptographic algorithm)*
SDTV	*Standard Definition Television*
SSELEG	*Subsecretaria de Segurança Legislativa*
SSL	*Security Socket Layer*
SVE-SF	*Sistema de Votação Eletrônica do Senado Federal*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TEMPLATE	*Gabarito*
TFT	*Thin Film Transistor*
UTP	*Unshielded Twisted Pair*
VLAN	*Virtual Local Area Network*
VS	*Virtual Server*
W3C	*The World Wide Web Consortium*
WPA	Wi-Fi *Protected Access*
XHTML	*The Extensible HyperText Markup Language*

1 INTRODUÇÃO

O Sistema de Votação Eletrônica (SVE-SF) é utilizado no plenário do Senado Federal para anunciar as sessões legislativas nos painéis, registrar a presença dos senadores, registrar e exibir a votação nominal e secreta de matérias legislativas, cronometrar e orientar as votações, cadastrar as senhas dos senadores, divulgar mensagens, emitir relatórios e executar funções gerenciais.

O SVE-SF auxilia os senadores no cumprimento da missão constitucional do Senado Federal, definida na Constituição da República Federativa do Brasil [1]. Para tanto, os senadores reunem-se, normalmente, de segunda a sexta-feira em sessões plenárias deliberativas, ordinárias ou extraordinárias ou sessões não deliberativas e especiais.

As sessões deliberativas ordinárias estão programadas para ocorrer de terça a quinta-feira e se destinam ao exame e votação de matérias legislativas [2]. As sessões deliberativas extraordinárias podem ocorrer a qualquer dia e hora, por convocação do Presidente do Senado.

As sessões não deliberativas se destinam aos discursos dos senadores, comunicações, leituras de proposição e outros assuntos de interesse político. Essas sessões ocorrem normalmente às segundas e sextas-feiras. As sessões especiais são exclusivas para comemorações ou homenagens.

Nas sessões não deliberativas e especiais são exibidos nos painéis localizados nas laterais do plenário, o anúncio da sessão, sua finalidade e demais mensagens definidas pela Mesa Diretora.

Nas sessões deliberativas, é necessário registrar a presença dos senadores e conduzir a votação de matérias. O registro de presença pode, por determinação do regimento interno, ser realizado durante todo o dia, a partir das sete horas da manhã até o encerramento da sessão. O registro da presença pode ser efetuado em qualquer terminal do plenário.

As votações nominais ou secretas são realizadas dentro da ordem do dia, sendo seus inícios e términos comandados pelo presidente da sessão, em terminal próprio. Os resultados da votação são exibidos imediatamente nos painéis após o encerramento das votações. O presidente é quem comanda estas operações em um terminal específico. Os senadores podem votar de qualquer terminal do plenário.

Considerando a importância do SVE-SF para os trabalhos do Senado Federal, decidiu-se apresentar uma proposta para a implantação de um novo sistema de votação, assim como em virtude da necessidade da modernização do sistema atual, em acelerado processo de obsolescência, pois, desde sua implantação, há 04 (quatro) anos, não sofreu modificações, seja de *hardware*, seja de *software*, deixando de atender às demandas surgidas na Casa durante esse período.

Essa substituição é uma necessidade já apontada tanto pelo Prodasen quanto pela Secretaria Geral da Mesa - SGM, que tem como principal atribuição cuidar dos trabalhos do plenário do Senado Federal. Outro ponto importante a ser ressaltado é que esta monografia contempla um tema real da infra-estrutura de tecnologia da informação do Senado Federal.

O escopo da monografia se restringe à apresentação de novos requisitos para o SVE-SF, de uma nova configuração de *hardware* e *software* básicos, contemplando a substituição dos terminais de votação dos senadores, do console do presidente, dos terminais de cadastramento biométrico, da rede de comunicação de dados, dos servidores do sistema, do painel apregoador e da atualização da política de segurança do SVE-SF.

O Capítulo 2 apresenta o histórico do SVE-SF, o Capítulo 3 mostra a descrição do atual SVE-SF, após as alterações realizadas em 2002, o Capítulo 4 descreve o sistema da Ordem do Dia Eletrônica, o Capítulo 5 contém os levantamentos dos problemas atuais e as melhorias solicitadas pelos usuários, o Capítulo 6 trata da análise do SVE-SF atual, que será insumo fundamental à elaboração da proposta para o novo sistema, pois reflete os dispositivos constitucionais e regimentais da Casa, que não mudarão.

Com base nas entrevistas realizadas, nas pesquisas documentais, na prospecção tecnológica efetuada e nas pesquisas realizadas junto ao mercado, será apresentada no Capítulo 7 uma proposta de solução para o novo SVE-SF. A proposta de solução a ser apresentada não abordará todo o detalhamento técnico necessário à sua implementação, pois a monografia tem um enfoque de gestão.

A prospecção tecnológica foi mais aprofundada quando os assuntos estudados não estavam diretamente ligados à área de atuação dos alunos, como tecnologia de *cluster*, biometria e painéis de exibição e são apresentadas nos Anexo I a III.

Para elaborar a proposta de solução, foi dado especial destaque aos requisitos de segurança do SVE-SF, que deverão adotar as mais modernas tecnologias em relação ao assunto. A política de segurança do SVE-SF também será revista para incorporar as novas

tecnologias a serem implantadas no sistema. Da mesma forma, os problemas técnicos existentes serão considerados na solução a ser proposta para o novo SVE-SF, bem como o mercado será prospectado em busca de novas tecnologias que venham a permitir a implementação das novas funcionalidades em foco.

O projeto apresentado não tem o objetivo de propor a substituição do SVE-SF, podendo, entretanto, contribuir para a discussão do assunto.

2 HISTÓRICO DO SVE-SF

Com o objetivo de automatizar os trabalhos realizados no plenário, o Prodasen implantou em 1972, o primeiro Sistema de Votação Eletrônica do Senado Federal (SVE-SF), que utilizava um computador Telefunken.

Em 1986 este equipamento foi substituído por um novo sistema, tendo funcionado até fevereiro de 2002, quando sua utilização foi suspensa em virtude da sua violação, em episódio amplamente divulgado e que ocasionou uma séria crise no Senado Federal.

A Unicamp foi contratada pelo Senado Federal para realizar auditoria no sistema, com o objetivo de verificar se o SVE-SF permitia violação do sigilo das votações secretas e se havia evidência da violação do sigilo. A conclusão da auditoria foi que o sistema permitia violações e que havia ocorrido uma violação. O relatório da auditoria apontou também a existência de inúmeras vulnerabilidades de segurança no Sistema de Votação Eletrônica do Senado Federal (SVE-SF) [3], conforme será descrito a seguir.

2.1 VULNERABILIDADES IDENTIFICADAS PELA UNICAMP NO SVE-SF

As vulnerabilidades identificadas pela Unicamp no SVE-SF, conforme auditoria concluída em abril de 2001, estão detalhadas nos capítulos apresentados adiante.

2.1.1 Vulnerabilidades físicas do SVE-SF

Existência de pontos de comunicação de dados entre computadores do SVE-SF em local de acesso pouco restrito.

Existência de portas de comunicação abertas em equipamentos do SVE-SF.

Existência de vários cabos de rede não utilizados na sala de controle do SVE-SF.

Existência de unidades de disquete e de disco ZIP nos computadores do SVE-SF.

Existência, na sala de controle SVE-SF, de 02 (dois) computadores estranhos ao sistema de votação e conectados a uma rede externa.

2.1.2 Vulnerabilidades dos programas de controle do SVE-SF

Comunicação de dados no SVE-SF feita de forma aberta, sem o uso de criptografia.

Armazenamento de dados no SVE-SF feito de forma aberta, sem o uso de criptografia.

Geração de arquivo temporário de votação secreta ou nominal no disco do computador principal do SVE-SF.

Nomes óbvios para os arquivos usados pelo SVE-SF.

Possibilidade do operador do SVE-SF registrar o comparecimento de senadores sem necessidade de senha.

2.1.3 Vulnerabilidades na utilização do SVE-SF

As vulnerabilidades na utilização do sistema foram dividas em ambiente operacional, arquitetura e operação do SVE-SF, apresentadas a seguir.

2.1.3.1 Ambiente operacional

Inexistência de procedimento formal para o controle da instalação de novas versões dos programas.

Armazenamento nos mesmos discos rígidos dos códigos-fonte e dos códigos-objeto dos programas do SVE-SF.

Ambiente de desenvolvimento de programas instalado nos computadores do SVE-SF.

Fragilidade da senha do Administrador do sistema operacional *Windows NT*.

2.1.3.2 Arquitetura do SVE-SF

Ausência de contas separadas para cada operador ingressar no sistema operacional *Windows NT* e operar o SVE-SF.

Compartilhamento irrestrito dos arquivos relacionados ao SVE-SF para todos os computadores conectados à rede.

Falta de política adequada de cópias de *backup* dos arquivos do SVE-SF.

2.1.3.3 Operação do SVE-SF

Procedimento inadequado para a definição e atribuição das senhas de senadores.

Possibilidade de recuperação fácil de uma senha esquecida por um senador.

Possibilidade de mudança do voto do senador enquanto a sessão estiver aberta.

Uso de senhas óbvias por alguns operadores registrados.

2.1.4 Recomendação da auditoria da UNICAMP

O relatório de auditoria não recomendou o desenvolvimento de um novo sistema, mas sim a correção das vulnerabilidades encontradas no sistema violado, pois o sistema antigo era bem conhecido e, se suas vulnerabilidades fossem sanadas, poderia ser considerado seguro e apto para voltar a ser utilizado. Ao contrário, se um novo sistema fosse desenvolvido, este apresentaria novas vulnerabilidades que precisariam ser identificadas. O custo final acabaria sendo maior e o tempo para a entrada em produção do novo sistema também.

O relatório de auditoria da Unicamp foi aprovado pela Comissão Diretora do Senado Federal.

A Polícia Federal também realizou auditoria no SVE-SF.

Com base no resultado das auditorias da Unicamp e da Polícia Federal, a Comissão Diretora determinou ao Prodasen que implementasse, ainda em 2002, a correção das vulnerabilidades apontadas no relatório.

2.2 ALTERAÇÕES EFETUADAS EM 2002 NO SVE-SF

Antes de iniciar os trabalhos para corrigir as vulnerabilidades acima relacionadas, o Prodasen efetuou estudos junto à Secretaria Geral da Mesa e aos operadores do SVE-SF, para identificar outras possíveis demandas que pudessem ser implementadas naquele

momento em que se alteraria o sistema. Foi apresentado relatório à Primeira Secretaria, designada responsável pelo acompanhamento dos trabalhos, que aprovou os estudos do Prodasen.

Devido à abrangência das alterações a serem realizadas e como o Prodasen não dispunha de meios para fazê-lo em curto espaço de tempo, decidiu-se contratar empresa, por meio de licitação, para a realização do trabalho. A empresa vencedora do certame foi a Visual, ficando a supervisão da execução dos trabalhos sob a responsabilidade do Prodasen. Todo o trabalho foi acompanhado pela Unicamp.

As principais mudanças implementadas foram:

- Alteração dos programas aplicativos do SVE-SF para sanar as vulnerabilidades apontadas pela Unicamp e implementar as melhorias aprovadas pela Primeira Secretaria;
- Atualização do *hardware* e *software* dos terminais de votação dos senadores;
- Instalação de novo console do presidente para controle das sessões plenárias;
- Instalação de novo concentrador multiserial dos terminais de votação e do console do presidente da mesa;
- Instalação de novo concentrador/controlador dos painéis de exibição;
- Instalação de rack para armazenamento dos servidores de rede e concentradores;
- Instalação de 03 (três) novos servidores de rede para executar o Sistema de Votação Eletrônica - SVE-SF;
- Instalação de 03 (três) terminais leitores biométricos de digitais nas cabines telefônicas do plenário, para cadastramento e manutenção das senhas dos senadores;
- Recuperação dos painéis de exibição e instalação de novas fontes de alimentação;
- Proteção física dos painéis de exibição;

- Lançamento de novos cabos UTP, categoria 6 [11], para a comunicação dos terminais de votação e do console da mesa do presidente com a sala de controle e operação do sistema;
- Instalação de câmera de monitoramento na sala de operação e controle, conectada ao sistema de vigilância da SSELEG (Subsecretaria de Segurança Legislativa);
- Colocação de piso elevado no interior da sala de controle;
- Aquisição e instalação de aparelho de ar condicionado do tipo SPLIT no interior da sala do SVE-SF para atuar em conjunto com o sistema central de refrigeração do plenário, assim como para servir de backup a este;
- Instalação de um televisor na sala de controle para acompanhamento, pelos operadores do sistema, dos trabalhos em plenário;
- Instalação de bancada de testes e homologação do SVE-SF nas dependências do PRODASEN para a realização de testes reais de futuras modificações que possam ser realizadas no sistema;
- Aquisição de cofre para armazenamento das cópias dos programas fontes que foram certificados pela UNICAMP e da documentação completa do sistema.

A conclusão dos trabalhos de reformulação do sistema deu-se em agosto de 2002, voltando o mesmo a ser utilizado pelo plenário do Senado a partir de outubro daquele ano. A segurança do SVE-SF foi certificada pela Unicamp e é garantida pela aplicação da Política de Segurança, desenvolvida pelo Prodasen e também aprovada pela Unicamp.

3 DESCRIÇÃO DO ATUAL SVE-SF – IMPLEMENTADO EM AGOSTO 2002

Como as funcionalidades do novo sistema serão fundamentalmente as mesmas do sistema atualmente em produção, pois sua abrangência é fortemente determinada pela Constituição e pelo Regimento Interno do Senado Federal, é necessário que se conheça em detalhes o funcionamento do SVE-SF atual.

Conseqüentemente, o objetivo deste capítulo é relacionar os aspectos do sistema atual que são necessários para servir de base, em conjunto com os levantamentos realizados e com o estudo da tecnologia disponível no mercado, apresentados nos capítulos seguintes, permitindo, assim, a elaboração de uma proposta para a implantação de um novo sistema.

3.1 FUNÇÕES BÁSICAS DO SVE-SF

As funcionalidades hoje existentes no SVE-SF são as mesmas implantadas em agosto de 2002, em virtude do sistema não ter sofrido alterações após aquela data. Nos parágrafos seguintes, serão apresentadas as principais funcionalidades do sistema.

Tabela 3.1 - Funções Básicas do SVE–SF

Função	**Descrição**
Registro de Comparecimento	Assinala a presença de senador, que ocorre de uma das seguintes formas: • após sua identificação e autenticação no sistema, por meio de senha, durante o expediente normal da casa; • pelo exercício do voto, pelo menos uma vez, durante as votações do dia, ou • quando houver uma verificação de quorum.
Votações	Os senadores podem votar em qualquer terminal disponível, sendo identificados por sua senha pessoal.

Função	**Descrição**
Votação nominal	Apresenta no painel a opção de voto exercida pelos senadores, além do total de votos *sim*, *não* e *abstenção*. No caso de empate, antes de mostrar o painel, é exigido o Voto de Minerva do presidente da mesa. O sistema armazena os votos dos senadores na base de dados.
Votação secreta	Mostra no painel apenas o total de votos sim, não e abstenção. Não é feito registro dos votos dos senadores, seja no painel, seja na base de dados do sistema.
Cronometragem	Marcação do tempo em ordem ascendente e descendente, com opção de parar e zerar o cronômetro. Durante o tempo regimental, a cor do cronômetro é verde. Nos outros períodos, a cor é vermelha.
Emissão de relatórios gerenciais	Resultado das votações nominais e secretas; Registro de Comparecimento; Relação dos senadores em ordem alfabética, por estado e partido político.
Supervisão dos terminais de votação	É realizada pelo operador do sistema e pelo presidente da mesa. O operador do sistema utiliza o servidor de operação para executar as funções a ele habilitadas, que são definidas de acordo com os privilégios estabelecidos no grupo de Operadores do Sistema do *Windows 2000*. O presidente da mesa utiliza o console do presidente para efetuar os comandos relativos aos Registros de Comparecimento e Votações.
Cadastramento seguro da identificação do senador	É efetuado no terminal biométrico do senador e comandado pelo operador do sistema. Tem por objetivo colher a identificação biométrica das digitais dos senadores, para que esses possam cadastrar ou alterar suas senhas de registro de presença e votação.

Função	Descrição
As demais funções executadas pelo SVE-SF são as seguintes:	• Abertura, acompanhamento e encerramento de sessão; • Identificação e registro do presidente da sessão; • Habilitação e registro de votações nominais; • Habilitação e registro de votações secretas.

3.2 AMBIENTE DE SOFTWARE DO SVE-SF

São os seguintes, de forma resumida, os componentes de *software* do SVE-SF:

Tabela 3.2 - Componentes de *Software* do SVE-SF

Componentes de *Software*	Descrição
Sistema Operacional *Windows 2000*	Fornece o serviço de sistema operacional e as funcionalidades de rede e suporte a aplicativos clientes e servidores.
Active Directory (AD)	Fornece ao sistema operacional o serviço de diretório e comanda o domínio SVE-SF, que define o contexto de funcionamento do ambiente do sistema de votação. Garante que apenas computadores e usuários autorizados acessem o sistema, de acordo com a política de segurança.
Biologon	Sistema de suporte a dados biométricos, integrado ao *Windows 2000* e ao *Active Directory* (AD), que permite o acesso ao console do sistema por meio de identificação biométrica e senha.
Banco de Dados SQL Server 2000	Armazena todas as informações do sistema de votação.
Criptografia	Todas as informações que trafegam na rede são transportadas e armazenadas de forma segura, utilizando algoritmos de infra-estrutura de chave pública e chave simétrica.
Linguagem de programação	Delphi V.

3.3 AMBIENTE DE HARDWARE DO SVE-SF

O SVE-SF é composto, de forma resumida, de uma unidade central de controle, composta de (03) três servidores de rede, conectados entre si por meio de uma rede *ethernet* e ao concentrador multiserial por meio da saída paralela.. A comunicação de dados na rede *ethernet* utiliza o protocolo IPsec. Não há *hardware* proprietário instalado nos equipamentos.

Tabela 3.3 - Componentes de *Hardware* do SVE- SF

Componentes de *Hardware*	**Descrição**
Servidor 1 – Operação do SVE-SF	É o console operacional do SVE-SF e é utilizado pelos operadores do sistema. Todos os acionamentos, configurações de comandos, programações de eventos e relatórios são realizados e monitorados em tempo real por esta unidade. Para garantir a segurança, nenhum dado ou informação relevante permanece ou é gravado temporariamente nesta unidade. Esta estação de trabalho é responsável pela execução do sistema de votação, pela coleta das informações sobre os registros de comparecimentos e votos dos senadores e pela coleta de seus dados biométricos.
Servidor 2 - Base de Dados do SVE-SF	Este servidor hospeda a única base de dados do SVE-SF. Apenas o administrador do SVE-SF tem acesso a este servidor.As informações do sistema estão armazenadas em um repositório central, sendo geradas cópias de segurança dos dados, armazenadas nos outros equipamentos do SVE-SF, para permitirem a recuperação da base de dados, em caso de falhas. Este servidor também autentica os usuários, audita os eventos ocorridos e garante que a criptografia do tráfego de rede seja estabelecida. Para a adequada gestão e segurança do sistema, foram criados no *Active Directory o* domínio SVE-SF e as políticas requeridas.

Componentes de *Hardware*	**Descrição**
Servidor 3 - Controle dos Painéis de Exibição	Este servidor executa um programa aplicativo que tem a função de controlar os 02 (dois) Painéis Eletrônicos instalados nas laterais do plenário do Senado Federal. O servidor não armazena dados do sistema. Todas as transações com o servidor de operação são criptografadas. Neste servidor está conectada a única impressora do SVE-SF, por meio de uma porta *USB*.
São unidades periféricas do sistema:	
Concentrador Multiserial	Esta unidade é o elemento de controle e convergência de todos os Terminais do SVE-SF, incluindo o console do presidente, os terminais dos senadores e os terminais biométricos. Neste ambiente, todos os dados do sistema trafegam criptografados. Possui doze canais independentes para o controle físico dos terminais. Cada canal controla, de forma independente, um conjunto de terminais. A utilização de um concentrador multiserial fornece elevada performance ao sistema, garantindo tratamento simultâneo, em tempo real, aos 89 terminais dos senadores e ao terminal do presidente. O concentrador é ligado ao servidor utilizando a porta paralela.
Console do Presidente	O console do presidente é o terminal a partir do qual o presidente da sessão opera o SVE-SF. É por meio desse console que são executados os seguintes comandos básicos relativos à gestão da sessão: Registro de Comparecimento, Cronometragem, Votação Nominal e Votação Secreta.

Componentes de *Hardware*	**Descrição**
Terminal do Senador	O terminal do senador é o instrumento disponibilizado para os registros de comparecimento e voto do senador. O SVE-SF possui 88 (oitenta e oito) terminais, estando instaladas 84 (oitenta e quatro) unidades nas mesas dos senadores e 04 (quatro) unidades na mesa do presidente. Os terminais dos senadores são interligados por meio de uma rede RS-485 [7]. A distribuição é setorizada e alternada por segmento de terminal e canal do concentrador multiserial. Cada unidade possui os comandos necessários para Registro de Comparecimento e Voto do Senador.
Botoeiras de Votação	Embutidas nas bancadas e ligadas por meio de interface serial RS-232C ao terminal de votação do senador. As botoeiras possuem 03 (três) botões que permitem ao senador votar *sim*, *não* ou *abstenção*.
Terminal Biométrico do Senador	O terminal biométrico é utilizado para colher os dados referentes às impressões digitais dos senadores e armazená-las no sistema. Após o cadastramento da digital, o senador é habilitado a gerar sua senha numérica de 07 (sete dígitos), que lhe permitirá operar os terminais do plenário.
Painel Eletrônico Matricial	O funcionamento dos painéis é independente, podendo ser gerado conteúdo distinto para cada painel. O painel localizado à esquerda da mesa do presidente é chamado de Painel A e o localizado à direita, de Painel B. Cada unidade possui matriz tricolor (vermelho, verde e laranja) com resolução de 640 x 112 pontos, totalizando 71.680 pontos. Os painéis são ligados na porta paralela do servidor 3 por meio de um conversor RS 422 [8].

Componentes de *Hardware*	**Descrição**
Interligação dos periféricos	Nenhum cabo de comunicação possui emenda em seu percurso e todas as conexões estão isoladas e lacradas com espaguete termo-retrátil e etiqueta de identificação. Dentro das mesas dos senadores. Todo o cabeamento está protegido por espirais plásticas. Todas as unidades periféricas estão eletricamente equalizadas e aterradas em um único ponto.

3.4 ROTINAS DE AUTENTICAÇÃO DO SVE-SF

Garantem que apenas computadores e usuários credenciados possuam acesso ao ambiente do sistema de votação. Definem os recursos disponíveis para os usuários e como os computadores executam as operações solicitadas.

Tabela 3.3 – Rotinas de Autenticação do SVE-SF

Rotinas de Autenticação	**Descrição**
Cadastro de computadores e usuários	Permite o gerenciamento do cadastro das estações de trabalho, operação e controle de painéis e do gestor, administrador, operador de cópias de segurança e operador de sistema.
Autenticação	Permite que usuários e computadores possam acessar os recursos do sistema.
Auditoria	Permite registrar os eventos ocorridos nos computadores
Aplicação das políticas de segurança	Garante que os computadores e usuários só poderão executar as operações previamente configuradas no *Active Directory*.

3.5 PROCEDIMENTOS E ROTINAS DE OPERAÇÃO DO SVE-SF

Os procedimento e rotinas de operação do SVE-SF estão relacionados a seguir e são considerados essenciais para garantir o perfeito funcionamento do sistema.

3.5.1 Rotinas de operação

Os servidores do SVE-SF permanecem ligados 24 horas por dia, 07 dias por semana, para garantir a integridade e disponibilidade dos equipamentos e a realização das cópias de segurança diárias, que são realizadas automaticamente. Os equipamentos somente podem ser desligados quando forem necessários procedimentos de manutenção. Nesses casos, a solicitação de manutenção deverá informar o motivo do desligamento e deverá ser encaminhada à Diretoria do Prodasen e à SGM.

O horário normal de início de operação do SVE-SF, para abertura do Registro de Comparecimento, é a partir das sete horas, se a sessão for deliberativa.

Qualquer modificação nesse horário deverá ser aprovada pela SGM e registrada no Diário de Ocorrência, com a concordância do Secretário Geral da Mesa.

O horário de fechamento do Registro de Comparecimento será após o término das sessões deliberativas ou conforme solicitação da SGM.

Quando a sessão for não deliberativa, o SVE-SF deverá estar operacional uma hora antes da hora marcada para o início da sessão e será fechado logo após o seu término.

3.5.2 Diário de ocorrência

As ocorrências relativas à operação do SVE-SF são registradas no Diário de Ocorrências, que tem as páginas numeradas. Deverão constar do diário as seguintes anotações:

- Data.
- Dia da semana.
- Horário marcado da sessão ordinária do dia.
- Horário em que o sistema foi ligado, se for o caso.
- Horário de abertura ou reabertura e fechamento do Registro de Comparecimento.
- Horário de abertura e fechamento de sessões extraordinárias realizadas.
- Horário de início e fim das sessões do Congresso realizadas no plenário do Senado.
- Número de votações realizadas pelo SVE-SF nas diversas sessões, separadas

por tipo, se nominal ou secreta.

No caso de pane que impeça o uso parcial ou total do SVE-SF, deverão ser anotados todos os procedimentos tomados, com os respectivos horários e nomes dos técnicos envolvidos.

Alterações no cadastro de senadores deverão ser precedidas de documento formal da SGM e ser anexada ao Diário de Ocorrência, juntamente com a anotação do operador, constando o horário e as alterações efetuadas.

3.6 PROCEDIMENTOS DE MANUTENÇÃO PREVENTIVA E CORRETIVA

Os procedimentos de manutenção preventiva e corretiva estão relacionados a seguir e foram divididos em procedimento gerais, verificação das baterias dos discos e verificação dos registros de auditoria dos servidores.

3.6.1 Procedimentos gerais

As manutenções preventivas são realizadas de acordo com o cronograma estabelecido em conjunto pelo Prodasen e a empresa mantenedora, seguindo os procedimentos definidos no contrato.

As manutenções corretivas são realizadas quando são detectados problemas no funcionamento do SVE-SF, seguindo sempre os procedimentos definidos no contrato.

Para a realização da manutenção preventiva, é aberto o registro de comparecimento, com o título “Registro de Comparecimento para Manutenção Preventiva do dia XX/XX”. A manutenção preventiva é realizada para verificar o funcionamento dos componentes do sistema, incluindo a comunicação com os terminais de votação.

As manutenções preventivas apenas são efetuadas quando não há atividade no plenário do Senado Federal e são acompanhadas pelos operadores do SVE-SF.

Se for necessária a utilização de unidades de leitura e gravação de disquetes ou de CDs, que estão guardados no cofre que fica na sala cofre do Prodasen, deverá ser feita solicitação formal ao Diretor da DSO e à SGM. Após a utilização das citadas unidades, as

mesmas deverão ser retiradas dos servidores e guardadas novamente no cofre.

Todas as intervenções realizadas deverão ser registradas no Diário de Ocorrências.

3.6.2 Verificação das baterias dos discos dos servidores

Os servidores dos SVE-SF fazem a verificação automática do nível de carga das baterias das controladoras de disco. Uma vez detectado nível baixo de carga, o sistema alertará o operador no momento em que for ligado.

Entretanto, como existe a possibilidade desse aviso não ser percebido pelo operador, assim como os servidores podem passar meses sem serem desligados, o procedimento de verificação de bateria deverá ser executado quando da manutenção preventiva dos servidores.

Para tanto, deve-se acessar o programa FAST e selecionar a opção de propriedade da controladora de disco. Será então possível verificar o estado das baterias e, se for o caso, carregá-las.

3.6.3 Verificação dos registros de auditoria dos servidores

Os registros de auditoria de cada servidor foram configurados para armazenar informações até o limite de 100 MB. Se esse valor for atingido, as informações não serão sobrepostas e o sistema ficará inoperante.

Mensalmente, deverá ser verificado o tamanho dos registros de auditoria de cada servidor. Se estiver acima de 80 MB, o fato deverá ser registrado no Diário de Ocorrências.

Formalizar o fato ao Diretor da DSO e da SGM, informando que o arquivo de registros de auditoria será gravado em pastas devidamente identificadas nos discos rígidos dos demais servidores.

- Criar a cópia do arquivo de registros de auditoria na pasta “Registros de Auditoria” e duplicar o arquivo para os outros servidores.
- Limpar o arquivo de registros de auditoria.
- Registrar todo o procedimento no Diário de Ocorrências.

4 DESCRIÇÃO DO SISTEMA DA ORDEM DO DIA ELETRÔNICA

Este capítulo apresenta uma breve descrição de um outro sistema que está em operação no plenário do Senado Federal, a Ordem do Dia Eletrônica. Esta descrição se faz necessária, pois se trata de um sistema que os senadores fazem uso no plenário e, portanto, deve ser levado em consideração na solução a ser proposta para o novo SVE-SF.

Para usar o sistema, cada senador tem à sua disposição um TabletPC [19] que permite o acesso on-line às informações da Ordem Dia [4], à Internet, a seus *e-mails* e aos aplicativos do *Office*. Os TabletPC estão conectados à rede local do Senado Federal por meio de uma rede *wireless* [9]. Para tanto, foram instalados no plenário 03 (três) pontos de acesso, padrão 802.11b [10] com taxa de transmissão máxima de 11 Mbps, operando nas freqüências de 2,4 a 2,5 Ghz. Os pontos de acesso são conectados à rede local *fast ethernet* 100TX por meio de *switches*. As antenas estão configuradas para operar em canais distintos e implementam o protocolo de segurança WPA (Wi-Fi *Protected Access*) [10].

Para 2006 há previsão de migração do padrão 802.11b para o 802.11g [10], com taxa de transmissão máxima de 54 Mbps, operando nas freqüências de 2,4 a 2,5 Ghz.

A menção ao Sistema da Ordem do Dia Eletrônica é importante porque o mesmo utiliza rede *wireless*, uma tecnologia que apresenta vulnerabilidades de segurança, sendo sua utilização contra-indicada em ambientes que requerem alta segurança, como o plenário do Senado Federal.

Por outro lado, o equipamento utilizado como estação para o sistema é o TabletPC, que tem se mostrado adequado ao ambiente do plenário, já estando os senadores acostumados ao seu uso. Na proposta a ser apresentada mais adiante para o novo SVE-SF, o TabletPC será indicado para ser sua estação, porém por meio de rede cabeada.

Essa proposta trará a vantagem de utilizar uma única estação de trabalho para todos os aplicativos hoje existentes no plenário do Senado Federal.

5 LEVANTAMENTO DE PROBLEMAS E SOLUÇÕES PARA O SVE-SF

Serão apresentados a seguir os levantamentos realizados junto a servidores da Secretaria Geral da Mesa, a operadores do SVE-SF e à área técnica do Prodasen, efetuados com o objetivo de verificar quais são os problemas existentes e as melhorias necessárias para um novo SVE-SF.

5.1 PROBLEMAS IDENTIFICADOS

Desde que o SVE-SF voltou a funcionar, em outubro de 2002, foram identificados os principais problemas descritos abaixo:

- Travamento esporádico de alguns terminais de votação, causado pela ocorrência de eletricidade estática, devido às condições do ambiente do plenário, potencializada pela baixa umidade do ar e pela utilização de carpete não orgânico, ou seja, sem tratamento antiestático, que poderia evitar este tipo de problema.
- Eventuais travamentos do concentrador multiserial, ocasionados pela conseqüente falha dos terminais que estão conectados a ele.

5.2 MELHORIAS E ALTERAÇÕES SOLICITADAS

As solicitações de melhorias e alterações são as seguintes:

1. Painel de Exibição:
   a. Aumentar a área do painel para possibilitar a inclusão de novos estados e permitir a exibição das seguintes informações:
      - Apresentação multimídia (vídeos, slides, TV);
      - Indicação da orientação das Lideranças nas votações;
      - Indicação do tipo de votação: “nominal-aberta” ou “nominal-secreta”.

2. SVE-SF:
    a. Implementar o reconhecimento biométrico nos terminais de votação dos senadores, visando dar maior segurança e confiabilidade ao sistema;
    b. Remover os terminais de votação de cima da bancada dos senadores, instalando-os junto ao sistema de leitura biométrica, em local a ser definido;
    c. Mudar a disposição das teclas do terminal de votação do tipo seqüencial para o tipo telefônico.
    d. Ativar os sinais luminosos (LEDs) para identificar qual tecla do console da mesa do presidente foi acionada (votação nominal, votação secreta, etc.);
    e. Efetivar as solicitações feitas pelos operadores e usuários do sistema, procedendo as alterações de algumas telas e funções no sentido de melhorar e facilitar o seu uso;
    f. Programar o sistema de forma que, em qualquer terminal, se um comando ou ação não for totalmente completado num período aproximado de 20 segundos, o sistema envie mensagem de tempo expirado e retorne a mensagem original para reiniciar a operação, a exemplo do que ocorre nos terminais de biometria.
    g. Permitir a rápida substituição do terminal do presidente, em caso de pane.
    h. Eliminar as funções de monitoramento da comunicação em versões futuras do programa svesf.exe;
    i. Limpar o campo “sem base biométrica” quando da inclusão de nomes de novos senadores sem registros de digitais;
    j. Incluir a opção “ocultar relógio dos painéis”, função existente no antigo SVE-SF. Incluir opção para mostrar a hora no formato “HH:MM:SS”, que também já existia no SVE-SF anterior;
    k. Incluir numeração para as “Matérias Votadas” e aumentar o tamanho do campo “Nome do Partido”;

l. Alterar o posicionamento da tela “Ambientes”, para que, quando esta estiver em exibição, o que pode demorar um certo tempo, o operador não fique impedido de executar comandos, tendo a falsa impressão de que o sistema está travado;

m. Incluir a opção “descer pauta”, a ser acionada por um clique do mouse. Na edição de Mensagens (Telas), o sistema deverá permitir que, sendo alterado o nome da tela criada, seja preservada a tela anterior, a exemplo do que acontece com o aplicativo Word;

n. Alterar o posicionamento na tela de mensagens do sistema. A mensagem “Foi detectado periférico sem comunicação no sistema. Verifique!” inviabiliza a operação do SVE-SF. É necessário encontrar solução para resolver definitivamente o problema de falha de comunicação em terminais. Alterar a posição das janelas de aviso do sistema para que não se sobreponham;

o. Liberar o console do presidente ao término das sessões, para evitar a mistura de informações de diferentes sessões, como pode ocorrer hoje no caso das sessões deliberativas.

p. Permitir que a pauta seja digitada antes da abertura da nova sessão de votações nominais e secretas. Os operadores precisam desta opção para evitar que sejam exibidas mensagens erradas nos painéis e a interrupção da digitação da pauta. É necessário que apareça no console do presidente a mensagem de “Aguarde digitação da pauta”, ou algo semelhante;

q. Alterar o sistema para que se no dia anterior o sistema foi fechado com Sessão Extraordinária (fechado Registro de Comparecimento e Sessão), ao abrir a Sessão Ordinária pela manhã, o sistema peça para confirmar a função de limpar o Comparecimento anterior.

r. Adequar os relatórios de votações. Dependendo do número de senadores votantes, os totais saem em colunas diferentes.

s. Aumentar os campos “apelido, Tit.Painel e Tit.Relatório”. Imprimir o resultado das votações em mais de uma página.

t. Verificar como deverá ser impressa a numeração das sessões ordinárias e extraordinárias. Reiniciar a numeração quando for iniciada nova votação em sessão ordinária ou extraordinária. Indicar se o tipo de votação é nominal-aberta ou nominal-secreta.

u. Criar opção de impressão do registro de comparecimento por horário. A opção poderia ficar inoperante para os operadores, sendo autorizado somente o gestor ou os administradores, quando necessário.

v. Criar um relatório com nome dos senadores que presidiram a sessão.

w. No relatório de votação e presença, no lugar do número da sessão, que na verdade, é o número de votações realizadas na sessão, incluir, efetivamente, essa informação – o número da sessão (32ª, 33ª), e também o tipo de sessão (deliberativa ordinária, não deliberativa ou deliberativa extraordinária);

6 ANÁLISE DO ATUAL SVE-SF

Neste capítulo apresentamos uma análise do atual SVE-SF com o objetivo de identificar se os componentes atuais do sistema atendem aos novos requisitos, e se as tecnologias empregadas estão obsoletas, para extrair subsídios para elaborar a proposta da nova configuração do Sistema de Votação Eletrônica.

6.1 REDES DE COMUNICAÇÃO DO PLENÁRIO

Neste item será analisada a situação atual da rede de comunicação de dados dos terminais do SVE-SF e da rede sem fio que usada no Sistema de Ordem do Dia Eletrônica.

6.1.1 Rede de comunicação do SVE-SF

A arquitetura da atual rede de comunicação do SVE-SF é baseada no protocolo RS-485, que conecta as bancadas dos parlamentares entre si e com o concentrador multiserial, conectado a porta paralela do servidor do SVE-SF. Por ser obsoleta, a rede deverá ser substituída por uma rede local *ethernet* padrão de mercado.

Os concentradores responsáveis pela comunicação entre as estações da rede local e os servidores do SVE-SF deverão ser desativados, por serem obsoletos.

A topologia da rede é constituída de sub-redes, cada uma conectando, no máximo, 11(onze) estações, que são instaladas nas bancadas dos senadores.

As estações são conectadas de forma alternada, para evitar que duas estações contíguas sejam simultaneamente desligadas por falha do sistema.

6.1.2 Rede sem fio do plenário

A rede sem fio hoje em funcionamento no plenário, em função das vulnerabilidades de segurança inerentes à tecnologia empregada, deverá ser desativada, especialmente por estar instalada em um ambiente que requer alta segurança.

As questões de vulnerabilidade da tecnologia de redes *wireless* envolvem, resumidamente, tanto aspectos relativos à possibilidade de invasões, onde dados podem ser introduzidos no ambiente da rede, com a conseqüente modificação do conteúdo exibido pelo Sistema de Ordem do Dia Eletrônica, quanto à possibilidade de escuta dos dados que trafegam no ambiente [10].

O TabletPC utilizado pelo Sistema da Ordem do Dia Eletrônica passará a se conectar à rede local do Senado Federal por meio de uma rede *ethernet* com cabos, assim como passará a ser utilizado como estação do novo SVE-SF.

6.2 SERVIDORES DO SVE-SF

Os servidores do SVE-SF necessitam ser substituídos, tanto em razão de sua utilização ininterrupta por (04) quatro anos, quanto por já se encontrarem obsoletos, o que fragiliza a segurança do sistema.

A arquitetura utilizada para os servidores do SVE-SF também precisa ser revista, para incorporar tecnologias modernas.

Cada servidor está equipado com três discos rígidos, todos ligados a uma controladora SCSI proprietária da Dell, chamada PERC3. Essa controladora foi configurada de modo a espelhar dois de seus três discos, de forma que qualquer dado gravado em um dos discos é imediatamente duplicado no outro. Essa característica permite que, em caso de falha de um dos discos, o outro assuma imediatamente o seu lugar. O terceiro disco funciona como disco reserva, ou *hot spare*, cuja função é a de substituir automaticamente qualquer um dos outros dois, em caso de falha. A figura a seguir ilustra essa configuração:

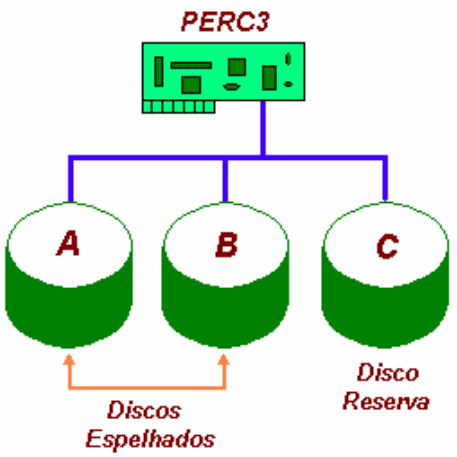


Figura 6.2 - Configuração dos Discos dos Atuais Servidores

Se, por exemplo, o disco “B” vier a falhar, automaticamente o disco “C” assume o seu lugar. Nesse caso, será necessário instalar no sistema um novo disco “C”, para restaurar a configuração original do sistema.

6.3 BANCADA DOS SENADORES

As bancadas dos senadores precisam ser reprojetadas, levando em consideração os equipamentos a serem nelas instalados, como a estação da rede.

6.4 ESTAÇÃO DE TRABALHO DOS SENADORES

A estação de trabalho do senador não é um equipamento padrão de mercado, sendo constituída por diferentes elementos interconectados, como o visor, o teclado numérico e a botoeira. Não existe possibilidade técnica de incorporar leitor biométrico à atual estação. É uma solução obsoleta e que precisa ser substituída.

A estação de trabalho do senador é altamente suscetível aos efeitos da eletricidade estática.

Há uma estação de trabalho para cada sistema existente no plenário. É preciso unificá-las.

6.5 CONSOLE DO PRESIDENTE

O console do presidente não é um equipamento padrão de mercado, sendo constituído por diferentes elementos interconectados. Não existe possibilidade técnica de incorporar leitor biométrico à atual estação. É uma solução obsoleta e que precisa ser substituída.

6.6 TERMINAIS DE COLETA DE DIGITAIS

Os leitores biométricos atualmente instalados nas cabines telefônicas deverão ser integrados a estações de trabalho padrão de mercado.

6.7 AMBIENTE DO PLENÁRIO

O fornecimento de energia elétrica do SVE-SF não é originário de fonte independente da fornecida para o plenário, o que é uma grande vulnerabilidade para o sistema.

Há problemas de descarga de energia estática, o que torna inoperantes alguns terminais ou mesmo o concentrador multiserial, em especial em época de seca, o que torna necessário a adoção de medidas que combatam a geração de eletricidade estática.

O aterramento da energia elétrica do plenário precisa ser revisto, para facilitar o escoamento da energia estática que venha a ser gerada no ambiente.

O SVE-SF sofre interferências de outros sistemas que operam no plenário, em especial dos equipamentos da TV Senado que, por compartilharem a mesma fonte de energia elétrica, causam impactos negativos ao sistema, em especial em função dos refletores de iluminação usados.

Os carpetes utilizados no plenário não possuem propriedades antiestáticas, sendo um dos principais fatores para a geração de eletricidade estática no ambiente, em virtude da movimentação de pessoas no plenário.

6.8 PAINÉIS DE EXIBIÇÃO

Os painéis atuais são obsoletos e só permitem a exibição de textos, não sendo possível a apresentação de conteúdo multimídia, como a exibição de vídeos, sinais de TV e apresentações de slides, como as elaboradas em *softwares* como o *Power Point*.

O ambiente do plenário do Senado é muito iluminado, em especial quando são ligados os refletores da TV Senado ou disparados os flashes dos fotógrafos, dificultando a visualização do painel, que possui baixo brilho e contraste.

6.9 SOFTWARE BÁSICO DO SVE-SF

O sistema operacional hoje utilizado, o *Windows 2000 Server*, assim como o *Active Directory*, deverão ser substituídos por versões mais atualizadas.

O sistema de gerenciamento de banco de dados utilizado pelo SVE-SF não é o padrão do Prodasen, devendo ser analisada a possibilidade da substituição do SQL-Server pelo *Oracle*.

Os algoritmos de codificação de dados e de criptografia utilizados hoje no SVE-SF, seja para armazenamento ou transmissão de dados, precisam ser substituídos por produtos mais atualizados, devido à rápida evolução da capacidade de processamento dos processadores atuais, que torna insegura uma rotina de criptografia considerada segura há quatro anos atrás.

Pelo mesmo motivo, é necessário substituir os *softwares* de segurança por suas versões mais modernas.

6.10 POLÍTICA DE SEGURANÇA

Reformular a política de segurança hoje existente, corrigindo deficiências surgidas no decorrer dos últimos quatro anos e subordinando-a à norma ABNT NBR ISO/IEC 17799:2005 [16], para adequá-la às novas práticas adotadas pelo mercado.

Definir rotinas de contingência para todas as exceções que possam surgir no funcionamento do sistema.

7 PROPOSTA DE SOLUÇÃO

O plenário do Senado Federal é o ponto focal da Casa. Nele, é exercido um dos fundamentos do regime democrático, que é a elaboração de legislação, por meio do voto dos senadores, que representam os seus estados e, indiretamente, o povo que os elegeu.

Conseqüentemente, é necessária a existência de um sistema de gestão das atividades do plenário, em especial aquelas relativas à votação de matérias legislativas, que garanta que a vontade do povo, consubstanciada pelo voto de seus representantes legitimamente eleitos, seja respeitada, para que a democracia seja exercida em sua plenitude.

O novo Sistema de Votação Eletrônica (SVE-SF), a ser proposto neste capítulo, deverá permitir que as atividades executadas no plenário sejam ainda mais seguras, confiáveis e transparentes que no sistema atual.

Como as funcionalidades do novo Sistema de Votação Eletrônica (SVE-SF) continuarão sendo definidas por dispositivos da Constituição Federal e do Regimento Interno do Senado Federal, isso significa que permanecerão basicamente as mesmas do sistema atual.

É importante ressaltar que, para projetar o Sistema de Votação do Senado Federal, algumas áreas de conhecimento exigiram um estudo mais aprofundado, a saber: c*lusters*, dispositivos biométricos e painéis de exibição. O resultado desses estudos está apresentado nos Anexos I, II e III.

Com base nas funcionalidades do atual SVE, na análise de seus componentes, nas necessidades de mudanças apontadas pela SGM e Prodasen, na prospecção tecnológica realizada e, finalmente, nas opções tecnológicas atuais em uso no Senado Federal ou pesquisadas no mercado junto aos fornecedores de equipamentos e serviços, será apresentado a seguir a proposta de solução para o novo SVE, que engloba: requisitos para o novo SVE, nova configuração de rede, *hardware*, *software* operacional, painel de exibição e política de segurança.

7.1 REQUISITOS PARA O NOVO SISTEMA APLICATIVO DO SVE-SF

O aplicativo do novo SVE-SF deverá ser desenvolvido para atender aos novos

requisitos aqui apresentados, sem deixar de observar as determinações da Constituição Federal e do Regimento Interno do Senado Federal.

As funções de divulgação de mensagens, de anúncio das sessões legislativas nos painéis, do registro da presença dos senadores, do registro e exibição da votação nominal e secreta de matérias legislativas, da cronometragem e da orientação das votações, realizadas no plenário do Senado Federal, continuarão a ser objeto do novo SVE-SF.

Da mesma forma, funções acessórias ao trabalho do plenário, como o cadastro das senhas dos senadores, a emissão de relatórios e a execução de funções gerenciais, realizadas pelo SVE-SF atual, continuarão a ser executadas pelo novo sistema.

Os requisitos necessários para executar essas funcionalidades serão descritos nos próximos tópicos.

7.1.1 Controle de presença e votação de matérias legislativas

Como o SVE-SF irá operar em uma das sub-redes da rede local do Senado Federal, diferentemente da condição anterior, em que a rede era exclusiva para o SVE-SF e independente da rede local, quando for comandado o início do processo de qualquer tipo de votação, o *firewall* [10] da sub-rede do SVE-SF deverá fechar todas as portas de comunicação entre a sub-rede e a rede local, até que o processo de votação seja encerrado e o resultado divulgado nos painéis de exibição, quando então o acesso à rede poderá ser liberado, de acordo com as regras definidas no *firewall*.

O controle das votações nominais ou secretas deverá ser processado, exclusivamente, em memória RAM. Somente após o encerramento da votação, as informações que se tornarão públicas serão armazenadas no base de dados. No caso de votações secretas, em sessão pública, serão armazenados os totais da votação e a lista de votantes, sem a qualificação individual do voto. No caso de votações secretas, em sessão secreta, só será armazenada a informação: “votação realizada”. Para isso faz-se necessário que o sistema possua os recursos necessários para distinguir tais tipos de votação, descritos a seguir:

- Designação prévia, pelo operador, do tipo de votação e de sessão para cada matéria em pauta.

- No momento da votação secreta, o presidente aciona a opção de abertura da votação secreta.
- O sistema exibirá automaticamente nos painéis a indicação de “Votação secreta em sessão _____” (pública ou secreta).
- Concluída a votação, deverá ser impresso o resultado e gravado na base de dados a mensagem “Votação realizada” (no caso de sessão secreta) ou a lista de votantes com o resultado da votação (no caso de sessão aberta).
- Antes de ser iniciada nova votação, deverá ser solicitada ao operador a confirmação da finalização correta da votação anterior.
- Deverá haver um mecanismo que garanta a emissão de apenas uma via do relatório.

Na estação de trabalho do presidente, deverá ser identificada qual opção de votação foi acionada, se votação nominal ou secreta.

O presidente poderá solicitar aos lideres dos partidos, antes do início da votação nominal aberta ou nominal secreta, a indicação da orientação da Liderança. O painel deverá exibir a indicação da orientação das Lideranças.

A alteração ou retificação de um voto será permitida se feita a partir do mesmo posto que a registrou.

Deverá existir dispositivo que permita a recuperação das presenças já registradas, em caso de queda do sistema.

O sistema deverá permitir que o horário padrão de registro de comparecimento seja das 07:00 às 20:30 horas. Se houver sessão do Congresso ou do Senado após esse horário, ou se a sessão do Senado se estender, o registro deverá ficar aberto até a hora do encerramento da sessão. O sistema deverá permitir que o operador informe os horários.

O sistema deverá permitir a digitação da pauta do dia com o painel em modo de espera e permitir também a digitação da pauta antes da abertura de novas sessões de votações nominais ou secretas.

Os seguintes eventos deverão ter tempo de resposta inferior a 02 segundos:

- O tempo decorrido entre o registro de voto de senador e sua exibição nos painéis.
- O tempo decorrido entre o comando de encerramento de votação e a

exibição do resultado no terminal do presidente.

- O tempo decorrido entre o comando de proclamação do resultado e sua completa exibição nos painéis.
- O tempo decorrido entre a aposição do dedo do senador no dispositivo de reconhecimento biométrico das estações do plenário e o resultado de sua autenticação, tanto para aceitação ou rejeição.

7.1.2 Rotinas de identificação e autenticação

Para identificar e autenticar com segurança um indivíduo perante um sistema, os estudos constantes do Anexo III indicam a necessidade da utilização conjunta de duas das três características seguintes:

- Algo que o indivíduo conheça;
- Algo que o indivíduo seja;
- Algo que o indivíduo possua.

E cada uma das duas características escolhidas deverá ser usada em fases diferentes do processo de acesso ao sistema: uma delas para a identificação do indivíduo e a outra para a sua autenticação.

No caso do SVE, optou-se por utilizar as duas primeiras características acima relacionadas, pois a terceira opção implica na posse de um cartão, que pode ser perdido facilmente.

Dentre os diversos métodos de identificação biométrica, o mais adequado para ser utilizado no SVE-SF é o de reconhecimento biométrico de digitais, por ter uma excelente relação custo-benefício, em especial no que se refere à acuidade, custo, facilidade de implantação e por não ser invasivo.

A utilização da biometria é importante porque é uma característica do ser humano que não pode ser perdida, esquecida ou emprestada a terceiros, tornando os sistemas que a utilizam mais seguros, por medirem características humanas, oferecendo um meio intransferível de identificar pessoas.

Portanto, as rotinas de identificação dos usuários do SVE-SF, sejam senadores, operadores ou administradores do sistema, será feita por meio de uma senha numérica (algo

que o indivíduo conhece) e sua autenticação será feita por meio de biometria (algo que o indivíduo é).

Os dados biométricos precisam ser cadastrados pelo SVE-SF. Depois de capturadas pelos *scanners*, as informações relativas às minúcias das impressões digitais (curvas, distâncias e ângulos) são submetidas a um algoritmo de compressão, sendo então gerado um gabarito, que é armazenado na base de dados de informações biométricas. Esta fase é crítica para o funcionamento do sistema e necessita ser executada com a maior precisão possível.

Após o armazenamento das informações biométricas, a imagem da impressão digital é descartada. Dessa forma, é impossível reconstruir-se a impressão digital original com base nas informações armazenadas.

O cadastramento dos usuários no sistema será feito nas estações localizadas nas cabines telefônicas do plenário. A senha numérica para que o usuário se identifique perante o sistema também será gerada no momento do cadastramento das informações biométricas.

Durante a operação do SVE-SF, seus usuários (senadores, operadores e administradores do sistema) digitarão em sua estação o código numérico gerado no cadastramento.

Com base no código numérico fornecido, o SVE-SF apresentará ao usuário o seu nome, solicitando a aposição de seu dedo no leitor de digitais, para colher seus dados biométricos.

O SVE-SF submeterá os dados biométricos colhidos aos mesmos algoritmos utilizados no momento do cadastramento, para verificar se a impressão digital colhida corresponde à armazenada na base de dados para aquele código numérico, rejeitando ou aceitando o usuário.

A medida de contingência para os usuários que não conseguirem ter suas digitais capturadas ou que possuem um elevado índice de falsos negativos, é o fornecimento de um código numérico para que ele se autentique perante o SVE-SF.

A base de dados de informações biométricas deverá armazenar também todas as tentativas de acesso ao SVE-SF, tanto as aceitas quanto as rejeitadas.

Para atender as características relacionadas acima, os estudos constantes do Anexo III indicam que as rotinas de identificação e autenticação deverão possuir os seguintes

requisitos:

- A base de dados de informações biométricas deverá conter a identificação do usuário e os dados biométricos gerados no ato do cadastramento, assim como quaisquer modificações e exclusões efetuadas.
- A base de dados de informações biométricas também deverá armazenar os registros relativos a todas as transações de identificação e autenticação efetuadas durante a utilização do SVE-SF.
- O módulo de cadastramento de senha e digitais do SVE-SF deverá coletar dados biométricos de pelo menos três digitais para cada usuário, fazendo a associação dos vários registros biométricos com sua senha numérica de identificação.
- O módulo de cadastramento de senha e digitais do SVE-SF deverá possuir as funções de inclusão, modificação, exclusão e exibição da senha.
- As buscas na base de dados de informações biométricas deverão ser de um para um, ou seja, a chave de acesso às informações biométricas será o código de identificação do usuário, informado no teclado numérico. Este código é usado para identificar o usuário. A digital é utilizada para autenticar o usuário e deverá ser comparada com a que está armazenada na base de dados de informações biométricas.
- O código de identificação do usuário deverá ser gerado aleatoriamente pelo SVE-SF, sendo constituído de 06 (seis) dígitos. Esse código deverá ser único na base de dados de informações biométricas.
    - O sistema não deverá reutilizar códigos de identificação usados anteriormente e já cancelados.
    - O sistema não deverá gerar códigos de identificação em seqüência.
    - O código de identificação deverá ser apresentado ao usuário, junto com o seu nome, durante 10 (dez) segundos.
    - O tempo de cadastramento ou alteração não deverá ser superior a 30 segundos.
    - O tempo de processamento não deverá ser superior a 02 (dois)

segundos, tanto para aceitação, quanto para rejeição.

7.1.3 Hierarquização das informações do SVE-SF

Para aumentar a segurança do SVE-SF, as tarefas de gestão, administração e operação do sistema não deverão ser executadas pelos mesmos servidores.

Da mesma forma, as informações do sistema deverão ser divididas em hierarquias de sigilo, para que os usuários só tenham acesso às informações necessárias à execução das tarefas a eles delegadas.

Os usuários do sistema deverão ser classificados nas seguintes categorias: gestor do SVE-SF, administrador do SVE-SF, operador de cópias de segurança e operador do sistema. Entretanto, outras categorias poderão ser criadas.

O gestor do SVE-SF será o único com acesso a todas as informações do sistema e só poderá utilizar a sua senha em condições de segurança máxima, a serem definidas na Política de Segurança da Informação do SVE-SF. Apenas esse usuário poderá ter acesso a arquivos que armazenem informações mais sensíveis, como a qualidade do voto, o cadastro, senha e dados biométricos dos senadores, a senha dos operadores e suas informações biométricas.

O administrador do SVE-SF terá acesso ao sistema operacional, arquivos e seus demais componentes.

O operador de cópias de segurança estará autorizado apenas a realizar as tarefas de cópia e restauração de arquivos.

Os demais operadores do SVE-SF somente poderão executar as rotinas de operação normal do sistema.

7.1.4 Interface do SVE-SF

O aplicativo do SVE-SF deverá ter interface *web*, com as seguintes características principais:

- Funcionar nos seguintes navegadores: *Microsoft Internet Explorer* 5.5 ou superior, *Netscape* 6.0 ou superior, *Mozilla* 1.7 ou superior e *Mozilla Firefox* 1.0

ou superior.

- Possuir telas específicas para cada função, com as informações e comandos característicos de cada agente.
- Ter padrão visual do sistema de acordo com às normas e padrões de apresentação visual definidas pelo Senado Federal.
- A interface do sistema deverá apresentar as seguintes características:
    - Os textos das interfaces e os dados a serem registrados pelo usuário final deverão estar de acordo com a ortografia da língua portuguesa, conforme legislação brasileira vigente e de acordo com o Vocabulário Ortográfico da Língua Portuguesa, da Academia Brasileira de Letras.
    - A nomenclatura aplicada aos elementos da interface deverá ser homogênea em todas as telas.
    - A nomenclatura dos elementos deverá identificar, sem ambigüidade, as ações que serão executadas.
    - Elementos similares deverão ter identificação similar.
- Deverá permitir fácil navegação entre funcionalidades. A navegação deverá garantir que todas as funcionalidades estejam à distância de, no máximo, três cliques de mouse umas das outras, de forma padronizada quanto à localização de botões, barras e menus.
- Deverá ser implementada ajuda on-line para o usuário final, em HTML, composta de telas de auxílio, índice geral e busca por assunto.
- Deverá habilitar, desabilitar ou ocultar campos, botões e textos de acordo com o contexto, opções escolhidas ou perfil de usuário.
- Deverá criticar todos os campos para evitar erros de lançamento
- Deverá sempre que possível, os erros deverão ser apontados logo após a sua ocorrência, de forma que os usuários possam corrigi-los imediatamente.
- Deverá implementar rotinas para tratamento de exceções, que permitam a exibição de telas informativas quando da ocorrência de problemas, informando

o tipo e a causa do problema, bem como quais os procedimentos a serem adotados pelo usuário.

- Deverá ter o endereço de URL (*Universal Resource Locator*) restrito: nenhuma informação sobre as páginas, servidor ou conteúdo deverá ser visível junto ao endereço *web* na caixa de endereço do navegador do usuário.
- Não deverá ser permitida a exibição do código-fonte das páginas.
- As páginas geradas deverão estar de acordo com a Recomendação W3C XHTML™ 1.0 – Segunda Edição.
- Deverá ser utilizada a tecnologia de folhas de estilo, de forma que a apresentação das páginas possa ser facilmente alterada sem a necessidade de modificação do código HTML.
- As folhas de estilo geradas deverão estar de acordo com a Recomendação W3C CSS2.
- As páginas geradas deverão estar de acordo com as recomendações de acessibilidade do Senado.

7.2 NOVA CONFIGURAÇÃO DO SVE-SF

É necessária a atualização tecnológica dos equipamentos e *softwares* do SVE-SF para que seja possível a implementação dos novos requisitos estabelecidos para o sistema. É importante também que as novas tecnologias incorporadas ao SVE-SF sejam aderentes à plataforma de tecnologia da informação do Senado Federal, por questões de padronização.

Nas Figuras 7.2.2.1 e 7.2.2.2 são apresentados diagramas esquemáticos da nova configuração e da nova topologia da rede para o SVE-SF e, nos tópicos a seguir, os seus principais elementos constituintes, com a subseqüente descrição de cada um deles.

7.2.1 Rede de comunicação

A rede de comunicação do novo SVE-SF será implementada usando tecnologia de

rede local, mesmo padrão de mercado adotado pelo Senado Federal e será a esta interligada, conforme diagramas esquemáticos apresentados nas Figuras 7.2.2.1 e 7.2.2.2.

A rede local do Senado Federal, no nível físico, utiliza no *backbone* [10] a tecnologia *gigabit ethernet* [10] e, nas redes de acesso, faz uso da tecnologia *fast ethernet* 100TX.

Nos níveis de rede e transporte, é utilizada a suíte TCP/IP.

A rede do SVE-SF utilizará o protocolo TCP/IP e as tecnologias *fast ethernet* 100TX e *gigabit ethernet*.

7.2.2 Topologia da rede

A topologia da nova rede do SVE-SF será composta de 05 (cinco) sub-redes independentes, conforme diagramas esquemáticos das Figuras 7.2.2.1 e 7.2.2.2. Cada sub-rede conterá, no máximo, 20(vinte) estações. Cada estação se conectará a uma porta do *switch* controlador de sua sub-rede, usando tecnologia *fast ethernet* 100TX.

Os *switches* controladores, por sua vez, se conectarão ao *switch* principal do plenário por meio de tecnologia *gigabit ethernet*, que fará a comutação das estações entre a rede do SVE-SF e a rede local do Senado Federal.

A topologia da rede do SVE-SF também deverá seguir os padrões de segurança da rede atual do plenário, onde duas estações adjacentes deverão pertencer a sub-redes diferentes, para evitar que ambas sejam simultaneamente desligadas por falha da rede.

Todos os equipamentos que forem conectados à rede do SVE-SF deverão ter placa de rede com protocolo nativo de gerência de rede, para permitir a supervisão e o monitoramento centralizado.

As atividades de gerenciamento da rede deverão ser coordenadas de forma a otimizar sua organização e assegurar que os controles estejam aplicados de forma consistente sobre toda a infra-estrutura da rede.

As características de segurança, níveis de serviço e requisitos de gerenciamento dos serviços de rede deverão ser identificados e incluídos nos acordos de nível de serviço relacionados à rede.

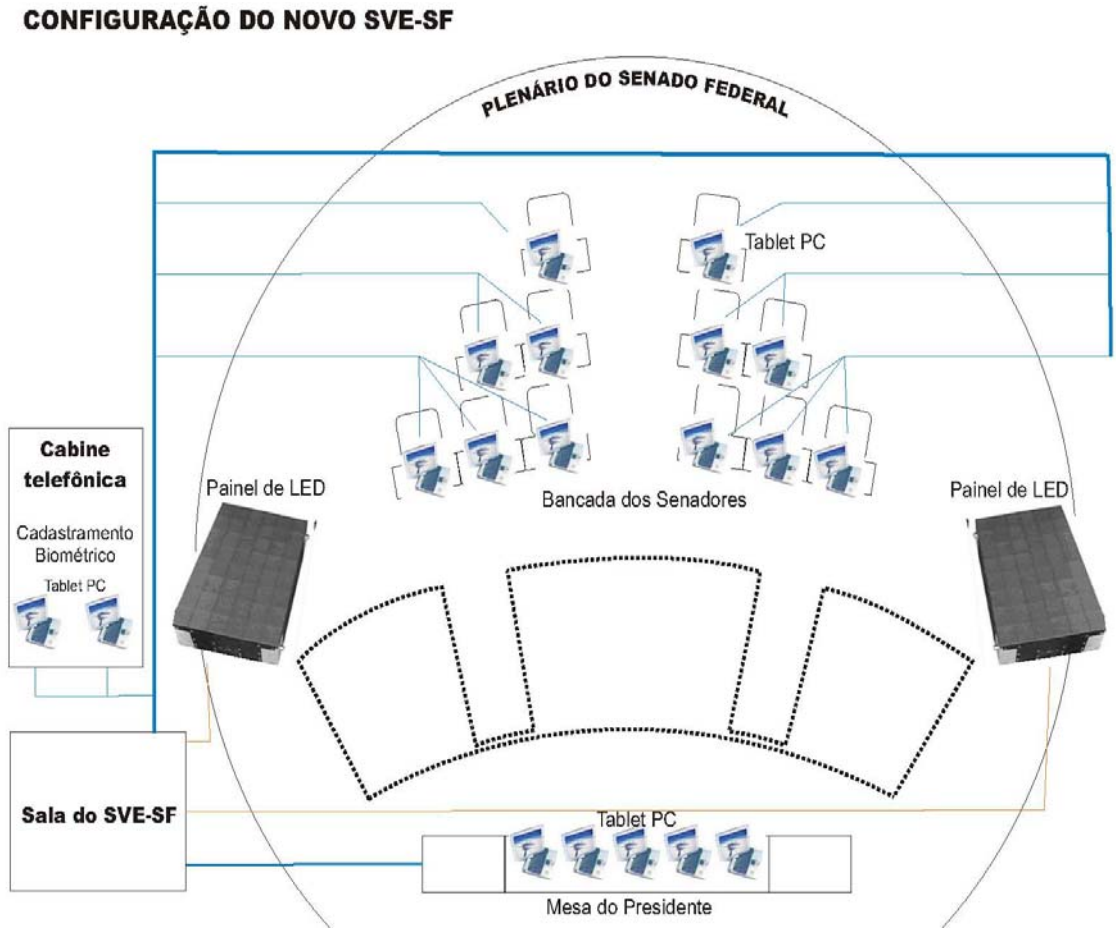


Figura 7.2.2.1 - Nova Configuração do SVE-SF

Farão parte dos serviços de rede o fornecimento de conexões e as soluções de segurança, como *firewalls,* sistemas de detecção de intrusos, autenticação, criptografia e controles de conexões de rede.

Convém que sejam consideradas as identificações automáticas de equipamentos como forma de autenticar conexões vindas de localizações e equipamentos específicos.

7.2.3 Switches

Para implementar as sub-redes do plenário e a interconexão com a rede do Senado, deverão ser utilizados 06 (seis) *switches, 01(um)* principal e 5(cinco) de sub-rede.

7.2.3.1 Switch principal

Este equipamento será responsável pela interconexão dos 5 (cinco) *switches* que implementam as sub-redes do plenário com os servidores do SVE-SF, com o servidor de supervisão e pela interligação com a rede do Senado, via *firewall*. Pelas atuais características da rede do Senado e de acordo com a nossa proposta, esse *switch* deverá ter no mínimo 12 (doze) portas *gigabit ethernet*, para receber e conectar-se aos outros 5 (cinco) *switches* das sub-redes do plenário, aos 2 servidores do SVE-SF e ao servidor de supervisão. Deverá ter 02 (dois) *uplinks* redundantes para a interconexão com o *backbone* da rede do Senado Federal, via *firewall*.

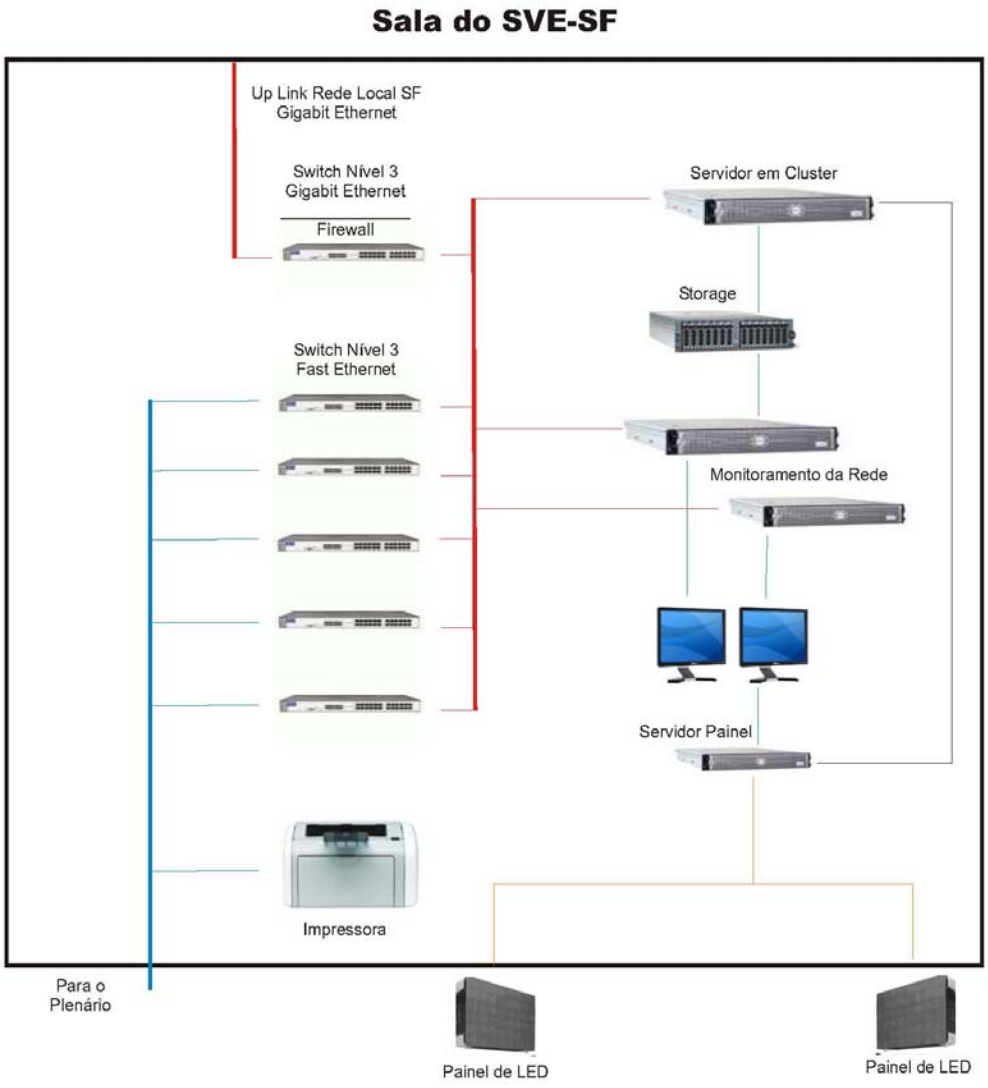


Figura 7.2.2.2 - Configuração da Sala do SVE-SF

Como a tecnologia *gigabit ethernet* é adotada no *backbone* da rede local do Senado Federal, será mantido o mesmo padrão na rede do SVE-SF por questões de compatibilidade.

Este *switch* deverá possuir funcionalidades de roteamento para que o SVE-SF possa ser isolado do resto da rede local nos momentos de votação, conforme previsto no item 7.1. As característica de roteamento e a possibilidade de implementar VLANs *(Virtual Local Area Network)* [10] determinam que esses equipamentos sejam de nível 3.

7.2.3.2 Switches da sub-rede

Estes equipamentos serão responsáveis pela interconexão ao *switch* principal dos 89 (oitenta e nove) terminais dos senadores instalados no plenário, do terminal do presidente e de 02 (dois) terminais de cadastramento de digitais a serem instalados nas cabines telefônicas dentro do ambiente do plenário, conforme já observado na Figura 7.2.2.2.

Também deverão ter as mesmas características dos *switches* instalados na rede local do Senado Federal, cada um com o mínimo de 24 (vinte e quatro) portas *fast ethernet* 100 TX, com conectores RJ 45 [11], para conectarem-se aos terminais do SVE-SF. Deverão possuir também 02 (duas) portas *gigabit ethernet* redundantes, para conexão com o *switch* principal da rede local.

Todos os *switches* deverão suportar pacotes *multicast* [13], [14] e [15], pois está em andamento projeto para disponibilizar, via rede local, utilizando *multicast*, programação da TV Senado e de TV a cabo, que será veiculada a todos os terminais da rede, inclusive aos do plenário.

Os *switches* deverão incorporar nativamente protocolos de gerência de rede [10], para permitir que a supervisão e monitoramento da rede local do futuro SVE-SF seja feita por estação de trabalho dedicada para este fim, a ser instalada na sala de operação do SVE. Dessa forma, será substituída a atual função de supervisão e monitoração incluída no aplicativo do SVE.

Os 06 (seis) *switches* que implementarão as sub-redes do plenário e a conexão com a rede local do Senado Federal deverão ser instalados na Sala do SVE, em *racks* especificamente projetados para tal função.

Deverão ser implementadas 02 (duas) VLANs (*Virtual Local Area Network*) na

rede, a primeira entre as estações e a rede local do Senado Federal e a segunda entre as estações e os servidores do SVE-SF. A VLAN nas sub-redes do SVE, segundo Dantas [10], tem como objetivo criar uma única entidade interligada, assegurando a conectividade e a privacidade nessas múltiplas sub-redes, quando do uso do SVE. A outra VLAN tem o mesmo objetivo de conectividade quando os senadores estiverem usando as demais aplicações disponíveis no plenário.

O único protocolo de rede a transitar na sub-rede do plenário será o *TCP/IP*, padrão da rede do Senado. Os endereços IP serão fornecidos automaticamente pelo servidor DHCP (*Dynamic Host Configuration Protocol)* do SVE-SF, exceto os equipamentos servidores do SVE-SF e de supervisão, que terão endereços IP fixos.

Para acesso à rede local do Senado Federal, à Internet e a todos os demais serviços, será utilizada a infra-estrutura existente na rede do Senado Federal.

7.2.4 Cabeamento

Como a maior distância entre uma estação e o *switch* ao qual estará conectada é inferior a 100 metros, que está dentro da especificação do comprimento máximo para redes *fast ethernet 100TX*, deverão ser utilizados cabos UTP Categoria 6, que também são padronizados no Senado.

O projeto de cabeamento e sua implementação física deverá ser feita, no que for possível, seguindo os requisitos das normas de Sistemas de Cabeamento Estruturado EIA/TIA 568 e 569, ISOC/IEC 11801 [11] e de segurança ABNT NBR ISO/IEC 17799 [17].

O cabeamento da sub-rede do plenário deverá atender a fortes requisitos de contínua disponibilidade, desempenho adequado e estável, integridade, sigilo, controle e gerência.

O cabeamento deverá ser protegido contra interceptação não autorizada ou danos, por meio da utilização de conduítes apropriados, instalados abaixo do piso.

Os cabos de energia deverão ser instalados em dutos separados dos destinados aos cabos de comunicação, para evitar interferências eletromagnéticas.

Deverão ser utilizadas marcações claramente identificáveis nos cabos e nos equipamentos, a fim de minimizar erros de manuseio, como, por exemplo, fazer conexões erradas em cabos da rede.

As conexões entre os cabos deverão ser documentadas para reduzir a possibilidade de erros.

7.3 SERVIDORES DO SVE-SF

As bases de dados e os programas do novo SVE-SF serão instalados em 02 (dois) servidores, configurados em *cluster*, conforme diagrama esquemático da figura 7.2.2.2. A arquitetura de *cluster* a ser utilizada é a de Alta Disponibilidade (*High Availability* ou *Failover*) [5], a mesma empregada em outros servidores do Senado Federal. O Anexo II apresenta um estudo aprofundado da tecnologia de clusters.

Os 02 (dois) servidores do SVE-SF, por estarem configurados em *cluster*, trabalham em conjunto para executar aplicações ou realizar outras tarefas, de forma transparente para os usuários que os utilizam. Essa escolha oferece um incremento substancial na confiabilidade, disponibilidade, distribuição de carga e performance do sistema. Os equipamentos deverão ser montados em *racks*.

Os servidores deverão ser tolerantes a falhas, com fontes redundantes, discos configurados em RAID e discos *hot spare, ou* discos de reserva, que entram em ação em caso de falha dos discos do RAID. Se um ou mais discos do servidor apresentarem defeito, deverão ser automaticamente substituídos pelo disco reserva e o RAID deverá ser reconstruído automaticamente.

Os servidores deverão vir configurados com duas placas de rede *gigabit ethernet,* uma para conexão com o *switch* principal e a outra com o *storage* externo.

Também deverão ser configurados com 02 (duas) placas de vídeo. A primeira controlará o monitor do equipamento, que é o console do SVE. A segunda fará o tratamento e enviará as imagens para os painéis. Essas últimas deverão possuir alta resolução, memória suficiente para executar suas funções, capacidade multimídia e saída de vídeo digital (DVI).

Os relógios dentro do perímetro de segurança deverão estar sincronizados de acordo com a hora oficial de Brasília.

7.4 SUBSISTEMA DE ARMAZENAMENTO DE DADOS DO SVE-SF

O subsistema de armazenamento de dados deverá apresentar, obrigatoriamente, as seguintes características:

- Ser montado no mesmo *rack* dos servidores;
- Utilizar tecnologia *gigabit ethernet* para conexão com os servidores;
- Capacidade de armazenamento mínima de 300 (trezentos) GB, já descontados proteção de RAID e discos *hot spare*;
- Capacidade de armazenamento de cada disco de, no máximo, 75 GB (setenta e cinco *gigabytes*), com velocidade de rotação mínima de 10.000 RPM;
- Possuir 02 (duas) placas *gigabit ethernet* para conexão com os servidores do SVE;
- Os discos *hot spare* deverão entrar em ação automaticamente, sem intervenção humana, para qualquer disco que venha a falhar;
- Possuir, no mínimo, 02 (duas) controladoras redundantes. Essas controladoras deverão estar configuradas no modo de operação de *Cluster* Ativo/Ativo. As controladoras deverão ter suporte a *failover* automático, com mecanismo de proteção de *cache* [5] em caso de falha de energia;
- Possuir tecnologia de RAID 1 [5] ou RAID 5 [5];
- Possuir monitoramento pró-ativo que permita a detecção e isolamento de falhas. Tal função abrangerá auto-monitoração e geração de registros de auditoria referente à detecção e isolamento de erros de memória, à detecção e isolamento de erros no disco, inclusive acionamento automático de disco de reposição;
- Suportar os protocolos TCP-IP, iSCSI, CIFS *e* HTTP;
- Possuir interface de gerenciamento gráfica e *Web*.

7.5 ESTAÇÕES DE TRABALHO E TERMINAIS DE COLETA DE DIGITAIS

O senador deverá utilizar uma única estação de trabalho para acessar os serviços da rede local colocados à sua disposição, assim como para utilizar o SVE-SF.

Como atualmente já está instalado em cada bancada do plenário um equipamento TabletPC, tecnologicamente atualizado e dentro do seu período de vida útil, e considerando que o uso desses equipamentos foi aprovado pelos parlamentares, que os tem utilizado satisfatoriamente, recomendamos a adoção deste equipamento para ser a estação a ser utilizada pelo novo SVE, tanto nas bancadas dos senadores, quanto nas estações de coleta de digitais.

Será necessária a incorporação ao TabletPC de dispositivo de reconhecimento biométrico de digitais e de placa de rede *fast ethernet* 100TX, com protocolo nativo de gerência de rede, para permitir a supervisão e monitoramento centralizado.

A adoção do TabletPC para o novo SVE-SF ajudará a enfrentar o problema da eletricidade estática do ambiente do plenário. A experiência obtida com sua utilização no Sistema de Ordem do Dia Eletrônica tem demonstrado sua robustez em relação aos efeitos da eletricidade estática.

Também deverá ser incorporado ao TabletPC uma película de proteção do tipo da comercializada pela 3M, que impede a visão lateral da tela por parte de terceiros.

7.6 CONSOLE DO PRESIDENTE

Deverá ser um equipamento idêntico às estações a serem instaladas nas bancadas dos senadores.

Deverá implementar as mesmas funcionalidades existentes na console atual, como opções para abrir as votações, para identificar o tipo de votação em andamento, para iniciar a sessão, para encerrar a votação e exibir o resultado nos painéis.

Será necessário incorporar ao console do presidente dispositivo de reconhecimento biométrico de digitais e placa de rede *fast ethernet* 100TX, com protocolo nativo de gerência

de rede, para permitir supervisão e monitoramento centralizado.

7.7 PAINÉIS DE EXIBIÇÃO

O ambiente do plenário do Senado Federal apresenta uma série de características que precisam ser levadas em consideração para a especificação adequada dos painéis de exibição, conforme descrito a seguir:

- O ambiente do plenário do Senado é muito iluminado, em especial quando são ligados os refletores da TV Senado ou disparados os flashes dos fotógrafos, exigindo que o painel possua alto brilho e contraste, para que as imagens sejam exibidas com qualidade, independentemente da luminosidade presente no plenário.
- O painel precisa ser visualizado da mesa do presidente, das bancadas dos senadores e das galerias, o que exige que tenha grandes ângulos de visão vertical e horizontal.
- Os principais itens exibidos nos painéis são textos, como a relação dos senadores presentes ou o resultado de votações, o que implica que estes equipamentos sejam imunes ao efeito *burn-in*, que marca permanentemente a superfície de exibição devido à apresentação de imagens persistentes por longos períodos.

Para atender as características relacionadas acima, os estudos constantes do Anexo II indicam que os painéis deverão possuir os seguintes requisitos:

- Deverão ser modulares e escaláveis, compostos de múltiplos equipamentos de exibição, montados em forma de matriz, formando uma tela única, sem emendas aparentes.
- Deverão ter tempo mínimo de vida útil superior a 50.000 horas, em condições normais de operação.
- A tecnologia de geração de imagem deverá utilizar LED's (*Light Emitting Diode*), com espaçamento entre pontos de, no máximo, 6,22 mm.
- Deverão ser legíveis mesmo em condições adversas de iluminação, como quando estão ligados os refletores da TV Senado. Para tanto, o brilho

mínimo deverá ser superior a 1500 candelas/m² e o contraste mínimo deverá ser de 1000:1. Os painéis deverão possuir controles individuais de contraste e brilho.

- As informações apresentadas deverão ser visíveis de todos os pontos do plenário, inclusive em ângulos horizontais de no mínimo 145º e verticais de no mínimo 50º.
- Suas dimensões deverão ser de, no máximo, 02 (dois) metros de largura e 04 (quatro) metros de comprimento.
- Os textos, como os nomes dos senadores e partidos, deverão ser perfeitamente legíveis a partir da ultima poltrona do plenário e das galerias.
- Deverão permitir a exibição de conteúdo multimídia, como a exibição de vídeos, sinais de TV e apresentações de slides, como as elaboradas em *softwares* como o *Power Point*.
- Deverão ser controlados por um gerenciador de imagens, com capacidade de processar, controlar e exibir as fontes de sinais digitais (HDTV, EDTV, SDTV), S-Vídeo, Vídeo Componente, Vídeo Composto, RGB, devendo suportar, no mínimo, 02 entradas simultâneas de Vídeo Digital (DVI).
- O gerenciador de imagens deverá permitir o cadastramento de usuários e operadores, possibilitando a implementação de restrições de acesso e direitos de operação.
- Deverão permitir a exibição de imagens simultâneas de várias fontes, comandadas por uma central independente.
- Deverão apresentar, no mínimo, 16 milhões de cores.
- Deverão permitir o redimensionamento da imagem na tela.
- Deverão operar em condições de temperatura entre 18º e 30º e de umidade relativa entre 40 e 60%.
- A fonte de alimentação elétrica deverá ser de 110v ou 220v.
- O painel deverá permitir manutenção frontal e traseira.

Apesar da solução proposta ser a mais dispendiosa, é preciso encará-la como um investimento de longo prazo, pois sua vida útil é de 20 (vinte) anos.

7.8 SOFTWARE BÁSICO DO SVE-SF

O sistema operacional hoje utilizado, o *Windows 2000 Server*, deverá ser substituído por sua versão mais atualizada, o *Windows 2003 Server*, por ser mais moderno, robusto e com melhor suporte à utilização de cluster.

Deverá ser adotado o sistema de gerenciamento de banco de dados *Oracle*, em sua versão para Windows, pois esse é o sistema gerenciador de banco de dados padrão da rede do Prodasen.

7.9 SEGURANÇA DE DADOS

Para garantir a segurança dos dados do SVE-SF, serão adotados protocolos e *softwares* padrões de mercado, largamente auditados e reconhecidamente seguros.

Esses protocolos e *software*s trazem embutidos algoritmos de criptografia e de infra-estrutura de chaves simétricas e assimétricas, públicas e privadas, baseados em padrões e normas de segurança amplamente reconhecidos pelo mercado e meios acadêmicos.

Para o armazenamento de dados, será utilizada a infra-estrutura de criptografia do sistema gerenciador de banco de dados.

Para a comunicação de dados, será utilizado o protocolo IPsec [17] do Microsoft *Windows 2003 Server*, sistema operacional a ser adotado no SVE-SF, que é baseado na infra-estrutura de padrões abertos do Internet Engineering Task Force IPsec Working Group.

Para o aplicativo de votação do SVE-SF, como medida de segurança adicional, será utilizado o protocolo SSL (*Security Socket Layer*).

Para gerenciar a comunicação de dados entre os domínios do SVE-SF e o da rede local do Senado Federal, será utilizado uma solução de *appliance* [20], onde o *hardware* que executa o *firewall*, assim como o próprio *software*, são instalados de forma integrada em um único equipamento.

A autenticação dos usuários e equipamentos será feita no *Active Directory* do domínio do SVE-SF.

7.9.1 Base de dados

Para o armazenamento de dados, serão utilizadas as ferramentas de segurança de dados do *Oracle*.

7.9.2 Comunicação de dados

Como citado anteriormente, a segurança dos dados no seu transporte será garantida com a utilização de IPsec, *SSL* e de *firewall*.

7.9.2.1 Internet protocol security (IPSec)

O IPsec, de acordo com as especificações técnicas da Microsoft [17] é uma infra-estrutura de segurança baseada em padrões abertos que busca assegurar que a comunicação de dados seja segura, íntegra, confiável e confidencial, por meio do uso de técnicas de criptografia.

O IPsec suporta autenticação *peer to peer* e autenticação da origem do dado, rodando sobre o protocolo *TCP-IP*.

As políticas do IPsec são estabelecidas de forma a garantir que suas definições possam ser configuradas por domínio, site ou nível organizacional. São configuradas no servidor *Windows 2003 Server*, definindo o comportamento das estações, ou seja, se deverão utilizar ou não o IPsec.

Há três tipos de configuração de políticas:

- *Respond Only* - A estação só utiliza o IPsec quando o servidor requer.
- *Request Security* – Esta política permite que a comunicação seja insegura se as estações não tiverem o IPsec habilitado.
- *Require Security* – Exige que a estação transmita usando IPsec.

No caso das sub-redes do SVE-SF, o IPsec somente será utilizado para esta aplicação. Assim, deverá ser implementada a política *Respond Only*.

O IPsec integra-se à camada de rede (nível 3), fornecendo segurança para todos os protocolos que utilizam o protocolo TCP/IP, dispensando a utilização de outras ferramentas de segurança para cada aplicação que use o TCP/IP. O IPsec elimina a necessidade de modificar-se aplicações para introduzir rotinas de segurança.

O IPsec usa o serviço de *Active Directory* do *Windows 2003 Server* e seu protocolo padrão de autenticação, o *Kerberos* [17].

A seguir, são apresentadas algumas RFCs utilizadas na implementação do IPsec da Microsoft:

- RFC 1828:- Autenticação IP usando chave MD5;
- RFC 1829:- Transformação ESP DES-CBC;
- RFC 2401:- Arquitetura de Segurança para IP;
- RFC 2406:- Encapsulamento do conteúdo seguro de um pacote IP;
- RFC 2451: Algoritmos de cifragem ESP CBC;
- Suporte para infra-estrutura de chave pública.

7.9.2.2 Secure Socket Layer - SSL

O aplicativo do SVE-SF deverá implementar o protocolo SSL *(Secure Socket Layer)* entre as estações de trabalho e os servidores do SVE-SF.

A implementação do protocolo SSL pela Microsoft [17] usa uma combinação de chave pública e criptografia de chave simétrica. A criptografia de chave simétrica é muito mais rápida que a criptografia de chave pública, mas esta última fornece melhores técnicas de autenticação.

Uma sessão SSL sempre começa por uma troca de mensagens chamada de SSL *handshake*, que permite ao servidor autenticar-se junto ao cliente, usando sua chave pública, permitindo então a cooperação entre o cliente e o servidor para criarem chaves simétricas para criptografia e decriptografia rápidas, assim como detectar tentativas de ataque à sessão estabelecida. Opcionalmente, essa técnica permite que o cliente se autentique junto ao servidor.

O SSL *handshake* deverá usar técnicas de criptografia que utilizem troca de chaves RSA, 3DES e DES.

7.9.2.3 Firewall

O *firewall* deverá proteger o perímetro de segurança da sub-rede do SVE-SF,

controlando o acesso e o fluxo de informação entre este domínio e o da rede local, de forma a filtrar o tráfego entre estes domínios e bloquear acessos não autorizados.

O *firewall* deverá ser do tipo *appliance*, ou seja, uma solução integrada de *hardware* e *software*. Deverá ser programável, permitindo implementar todas as funcionalidades inerentes a esses dispositivos.

Os serviços da rede local, como o Sistema da Ordem do Dia Eletrônica, o acesso à Internet e ao correio eletrônico, deverão ser filtrados por esse equipamento.

7.9.2.4 Autenticação

A autenticação dos equipamentos e dos usuários do SVE-SF será feita por biometria e verificação de dados no *Active Directory* do SVE-SF.

7.10 MONITORAMENTO DA REDE

O monitoramento da rede tem o objetivo de detectar atividades não autorizadas de processamento da informação.

O SVE-SF deverá ser monitorado e os eventos de operação e de falhas deverão ser registrados para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.

Os eventos a seguir deverão ser registrados:

- datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*logon*) e saída (*logoff*) no sistema;
- registros das tentativas de acesso aceitas e rejeitadas ao sistema;
- registros das tentativas de acesso aceitas e rejeitadas a outros recursos e dados;
- alterações na configuração do sistema;
- uso de privilégios;
- uso de aplicações e utilitários do sistema;
- arquivos acessados e tipo de acesso;
- endereços e protocolos de rede;

- alarmes provocados pelo sistema de controle de acesso;
- ativação e desativação dos sistemas de proteção, tais como sistemas de antivírus;
- sistemas de detecção de intrusos.

O monitoramento é necessário para assegurar que os usuários executarão apenas as atividades que lhes foram delegadas.

As falhas ocorridas na utilização do SVE-SF deverão ser registradas e analisadas, para que sejam adotadas as ações corretivas apropriadas.

Os registros relativos aos eventos deverão ser protegidos contra falsificação e acesso não autorizado.

A utilização dos recursos do SVE-SF deverá ser monitorada para detectar em tempo hábil a necessidade de expansão dos equipamentos, de forma a garantir o desempenho requerido pelo sistema.

7.11 INSTALAÇÕES FÍSICAS DO SVE-SF

Nos itens a seguir, serão apresentadas as recomendações sobre como deverá ser projetada a nova sala do SVE-SF, a bancada dos senadores e o ambiente do plenário, com base na norma ABNT NBR ISO/IEC 17799:2005, que estabelece técnicas e práticas voltadas à segurança da informação.

7.11.1 Sala do SVE-SF

Elaborar projeto de fornecimento de energia para a sala do SVE-SF, de fonte independente da que fornece energia para o plenário, de acordo com as especificações dos fabricantes dos equipamentos instalados na sala do SVE, de forma a fornecer energia estabilizada e balanceada.

O projeto deverá prever a instalação de *nobreak* e gerador independentes dos que atendem ao plenário, para manter o funcionamento contínuo dos equipamentos do SVE-SF, mesmo em casos de interrupção prolongada do suprimento de energia. Estes equipamentos deverão ser verificados em intervalos regulares, para assegurar sua disponibilidade nos momentos em que forem necessários.

Deverá ser considerado o uso de múltiplas fontes de energia, para evitar que uma falha em um único ponto comprometa o suprimento de energia.

As chaves para o desligamento da energia deverão ficar localizadas em local de fácil acesso, para facilitar o desligamento rápido da energia em caso de emergência. Deverá ser instalada iluminação de emergência para o caso de queda da força.

A sala do SVE-SF deverá ser adequadamente protegida, por meio da definição de um perímetro de segurança, pois nela estão instalados os servidores e estações de operação da rede.

A sala do SVE-SF deverá ser reformada para garantir sua inviolabilidade em relação a brechas que possam proporcionar invasões, incluindo pontos de passagem de dutos de energia elétrica e ar-condicionado.

O perímetro de segurança deverá estender-se às demais áreas do plenário onde estejam instalados equipamentos do SVE-SF e que não tenham proteção adequada, como as canaletas por onde passa o cabeamento e a parede das galerias onde estão instalados os painéis de exibição.

A sala do SVE-SF deverá possuir sistemas de detecção de incêndio, temperatura e de movimento.

A sala do SVE-SF deverá ser monitorada por sistema de CFTV (Circuito Fechado de Televisão).

O acesso à sala do SVE-SF deverá ser controlado por biometria e a porta da sala deverá permanecer trancada quando o sistema não estiver sendo utilizado.

Deverão ser consideradas as seguintes diretrizes para assegurar que apenas pessoas autorizadas tenham acesso à sala do SVE:

- a data e hora da entrada e saída de visitantes deverão ser registradas, e todos os visitantes deverão ser supervisionados. As permissões de acesso deverão ser concedidas apenas para finalidades específicas.
- deverá ser exigido que todos os funcionários, fornecedores, terceiros e visitantes portem alguma forma visível de identificação. A área de segurança deverá ser avisada imediatamente caso pessoas não autorizadas estejam nas dependências da sala do SVE-SF ou não estejam usando uma identificação visível.

- o acesso à sala do SVE-SF aos terceiros que realizam serviços de suporte deverá ser autorizado e monitorado.
- os direitos de acesso à sala do SVE-SF deverão ser revistos e atualizados em intervalos regulares, sendo revogados quando necessário.

7.11.2 Bancada dos senadores

Reprojetar as bancadas dos senadores, por meio de um estudo de ergonomia que considere as funções executadas pelo parlamentar, levando também em consideração os equipamentos a serem nelas instalados, como a estação da rede, que deverá ser utilizada para todos os sistemas disponibilizados no plenário, incluindo o SVE-SF.

Elaborar projeto para conectorização das estações à nova tecnologia de rede a ser adotada e à rede elétrica.

7.11.3 Ambiente do plenário

Revisar as instalações elétricas do plenário, para evitar interferências dos outros sistemas que lá funcionam, como os da TV Senado, Rádio Senado, iluminação e taquigrafia.

A rede elétrica que alimenta os equipamentos do SVE-SF distribuídos pelo plenário deverá ser fornecida pelas mesmas fontes que abastecem a sala do SVE-SF, para evitar interferências de outros sistemas, como, por exemplo, o da TV Senado, que possui elevada necessidade de energia elétrica, em especial devido aos refletores de iluminação usados.

O projeto também deverá considerar as necessidades de aterramento do plenário, para facilitar o escoamento da energia estática gerada no ambiente, de forma a contribuir para a eliminação do problema e evitar que ocorram interrupções no funcionamento do SVE-SF.

Os carpetes utilizados no plenário deverão ser substituídos por carpetes orgânicos com características antiestáticas, para evitar que a movimentação de pessoas no plenário, em especial nos meses de seca em Brasília, gere excessiva eletricidade estática no ambiente. Não sendo possível a substituição, aplicar um tratamento antiestático no carpete atual.

Deverá ser verificada a possibilidade de instalar umidificadores no plenário, para aumentar a umidade relativa do ar do ambiente.

7.12 PROCEDIMENTOS OPERACIONAIS DE SEGURANÇA

Os ativos do SVE-SF deverão ser claramente identificados e deverá ser elaborado um inventário dos mesmos.

Os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros deverão ser claramente definidos e documentados.

Os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações deverão ser bem especificados. Para tanto, é necessário o desenvolvimento de procedimentos operacionais apropriados.

Deverá ser garantida a operação segura e correta dos recursos de processamento da informação.

Deverá haver segregação de funções para a gestão, administração e operação do SVE-SF, recurso que reduzirá o risco de uso indevido, acidental ou mesmo doloso dos sistemas.

Deverão ser adotados procedimentos para impedir que uma única pessoa possa acessar, modificar ou usar o SVE-SF sem a devida autorização ou detecção, para reduzir a possibilidade da existência de conluios.

Deverão ser elaborados procedimentos para a execução das atividades de operação do SVE-SF, como a inicialização e encerramento do sistema, a geração de cópias de segurança e a manutenção de equipamentos.

Deverão ser elaboradas instruções para tratamento de erros ou outras condições excepcionais que possam correr durante a execução do SVE-SF, incluindo restrições de uso dos utilitários do sistema.

Deverão ser elaborados procedimentos para o reinício e recuperação em caso de falhas do sistema.

Todas as ocorrências de alterações e manutenções realizadas em dado período deverão ser registradas utilizando as rotinas do sistema operacional. Nos casos em que a utilização dessas rotinas não seja suficiente para registrar todos os eventos necessários, deverá ser prevista a utilização de rotinas complementares àquelas do Windows.

Os documentos gerados pelos procedimentos de exceção deverão ser tratados como documentação formal.

7.13 SEGURANÇA E RECUPERAÇÃO DE DADOS NO SVE-SF

As cópias de segurança do SVE-SF serão geradas pelo programa de *backup* do Windows e gravadas nos próprios servidores do SVE-SF.

Os dados do SVE-SF armazenados na base de dados deverão ser duplicados diariamente e automaticamente.

As operações de cópia de segurança e de recuperação de dados deverão conservar, dentre outras, as configurações de criptografia, permissões, entradas de auditoria e propriedade dos arquivos copiados.

A sistemática de cópias de segurança e de recuperação deverá proteger o SVE-SF de uma perda acidental de dados, devido a uma falha de *hardware* ou de *software*, conforme as especificações descritas a seguir:

- Permitir a execução de cópias de segurança incremental, diferencial, diária e completa.
- A sistemática de cópias de segurança deverá prever a criação de cópias diárias, semanais, mensais e anuais dos dados do SVE-SF, assim como especificar critérios para a liberação dos arquivos de cópias de segurança.
- A sistemática de cópias de segurança deverá prever procedimentos para a recuperação do sistema em caso de desastre.
- Deverá ser definida rotina para a cópia dos *backups* para mídias externas aos servidores do SVE, segundo critérios de segurança a serem estabelecidos. Para a execução dessa rotina, é imprescindível a presença da autoridade certificadora.
- Permitir o agendamento de cópias de segurança ou da recuperação de dados, de forma que essas operações possam ser executadas, automaticamente, em uma freqüência ou hora específica.
- A rotina deverá fornecer uma visão de árvore das unidades de disco rígido, pastas e dos arquivos que estão nos servidores do SVE-SF, para permitir a seleção dos arquivos e pastas dos quais se deseje fazer cópias de segurança.
- A rotina deverá gravar um registro completo de todas as operações de cópias de segurança ou de recuperação de dados.

- A rotina deverá efetuar a verificação da cópia de segurança após ter sido concluída, para garantir que os dados copiados são idênticos aos originais.
- Permitir definir se o local de destino dos arquivos e pastas, em uma recuperação de dados, será o local original ou um local alternativo.
- Permitir definir se a operação de restauração deverá copiar ou não os arquivos que estão sendo recuperados sobre arquivos que já estejam no disco.

7.14 POLÍTICA DE SEGURANÇA

A nova Política de Segurança do SVE-SF deverá ser escrita com base na norma ABNT NBR ISO/IEC 17799:2005, que estabelece técnicas e práticas voltadas à segurança da informação.

A referida norma foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela Comissão de Estudo de Segurança Física em Instalações de Informática (CE-21:204.01).

A Nova Política de Segurança também deverá incorporar a política atualmente em uso, atualizando os tópicos necessários, em função das mudanças a serem efetuadas no SVE-SF.

A nova Política de Segurança deverá também possuir os controles necessários para garantir a segurança do SVE-SF. Esses controles deverão ser baseados em requisitos legais e nas práticas de segurança da informação normalmente usadas.

Os requisitos de segurança da informação deverão ser estabelecidos com base na identificação dos riscos a que o SVE-SF está submetido. Controles apropriados deverão ser selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável.

Os controles considerados importantes para garantir a segurança do SVE-SF são os seguintes:

a) documento da política de segurança da informação;

b) atribuição de responsabilidades para a segurança da informação;

c) conscientização, educação e treinamento em segurança da informação;

d) processamento correto nas aplicações;

e) gestão de vulnerabilidades técnicas;

f) gestão da continuidade do negócio;

g) gestão de incidentes de segurança da informação e melhorias;

h) proteção de dados;

i) proteção de registros organizacionais.

Convém observar que outros controles previstos na norma ABNT NBR ISO/IEC 17799:2005 deverão ser considerados, dependendo dos riscos específicos relativos ao SVE-SF.

O sucesso da implementação da segurança da informação no SVE-SF dependerá dos seguintes fatores críticos de sucesso:

a) existência de uma política de segurança da informação que reflita os objetivos do SVE-SF;

b) existência de uma abordagem e estrutura para a implementação, manutenção, monitoramento e melhoria da segurança da informação que seja consistente com a cultura organizacional;

c) comprometimento e apoio visível de todos os níveis gerenciais;

d) bom entendimento dos requisitos de segurança da informação e da análise, avaliação e gestão de riscos;

e) divulgação eficiente da segurança da informação para todos os servidores envolvidos na operação e administração do SVE-SF;

f) distribuição de diretrizes e normas sobre a política de segurança da informação para todos os servidores envolvidos na operação e administração do SVE-SF;

g) estabelecimento de um eficiente processo de gestão de incidentes de segurança da informação;

h) implementação de um sistema de medição que seja usado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria do SVE-SF.

8 CONCLUSÃO

A proposta de solução para o novo SVE-SF ora apresentada engloba novos requisitos para o desenvolvimento do aplicativo do sistema, uma nova configuração de rede, *hardware*, *software*, painel de exibição e uma nova política de segurança. Quando implementada, trará grandes melhorias aos trabalhos executados pelos senhores senadores no plenário do Senado Federal.

A solução proposta utilizará a mais atualizada infra-estrutura de tecnologia da informação, seguindo a padronização adotada pelo Senado Federal. Dessa forma, diferentemente do sistema atual, que usa tecnologia obsoleta e proprietária, de pouco conhecimento dos técnicos do Prodasen, o novo SVE, por adotar tecnologia padrão de mercado e largamente utilizada no Senado Federal, poderá, a qualquer tempo, sem a dependência de terceiros, ser mantido, corrigido e atualizado.

Os novos requisitos especificados para o SVE-SF atenderão a todas as necessidades de mudanças e melhorias propostas pelo Prodasen e pela Secretaria Geral da Mesa, responsável pela gestão das atividades do plenário do Senado.

A rede de comunicação de dados do novo SVE-SF, que adotará o padrão *ethernet*, incorporará elementos que proverão maior desempenho, confiabilidade e integridade à rede local do plenário.

A arquitetura dos novos servidores do SVE-SF utilizará tecnologias que fornecem maior tolerância a falhas que o sistema atual, como *clusterização* e RAID, além de possuírem componentes que oferecem maior desempenho e confiabilidade, incluindo processadores, módulos de memória e discos.

A presença de uma única estação em cada bancada facilitará e racionalizará o trabalho dos senadores no plenário.

O uso da biometria para a identificação e autenticação dos usuários do SVE, sejam senadores ou servidores da casa, incrementará substancialmente a atual segurança do sistema. No detalhamento do projeto de implementação da biometria por digitais deverão ser levado em conta todos os aspectos de segurança amplamente conhecidos sobre o assunto.

O novo painel melhorará a qualidade das imagens exibidas no plenário, possibilitando a apresentação de conteúdo multimídia, incluindo sinais de TV e de outras

mídias, além de permitir a exibição de informações adicionais, inclusive o nome de novos senadores quando novas unidades federativas forem criadas.

A supervisão do sistema será facilitada com a colocação de equipamento para esse fim na sala do SVE, que fica localizada no plenário. Consequentemente, as atividades de manutenção serão realizadas com maior rapidez e eficácia.

A nova política de segurança baseada na norma ABNT NBR ISSO/IEC 17799:2005, aumentará ainda mais a segurança do SVE-SF e dos demais sistemas do plenário.

As recomendações da norma ABNT NBR ISSO/IEC 17799:2005 também foram utilizadas para estruturar o estudo e a proposta de solução para um novo SVE-SF. Foi uma decisão estratégica propor um novo sistema, totalmente aderente às recomendações de segurança amplamente divulgadas e reconhecidas internacionalmente.

Pretende-se que a proposta ora apresentada para o desenvolvimento de um novo Sistema de Votação Eletrônica (SVE-SF) para o plenário do Senado Federal seja submetida à Secretaria Geral da Mesa, para aprovação e conseqüente implementação.

O contexto atual é altamente favorável a esse encaminhamento, devido à obsolescência do sistema atual e à intenção do Senado Federal de realizar uma reforma geral no plenário, o que nunca foi feito desde sua inauguração, em abril de 1960.

Naturalmente, serão necessários estudos técnicos complementares sobre biometria, *switches, firewall e cluste,* que permitam aprofundar e detalhar adequadamente a proposta apresentada nesta monografia, para dotar o plenário da tecnologia mais atualizada, contribuindo efetivamente para a racionalização, melhoria e transparência dos trabalhos executados no plenário do Senado Federal.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] - Constituição da Republica Federativa do Brasil - Título IV - Da Organização dos Poderes, Capítulo I do Poder Legislativo Seção IV do Senado Federal –

[2] - Regimento Interno Resolução Nº 93, de 1970 - Título VII, das Sessões, Capítulo I Da Natureza das Sessões Art. 154. As sessões do Senado podem ser:(*) Texto editado em conformidade com a Resolução nº 18, de 1989, consolidado com as alterações decorrentes de emendas à Constituição, leis e resoluções posteriores, até 2002.Volume I Brasília – 2003

[3] - Relatório Final da Análise do Sistema de Votação Eletrônica do Senado Federal – SVE-SF – UNICAMP – Abril de 2001.

[4] - Senado Federal - Ordem do Dia, Acessado em 30/01/2006
http://www.senado.gov.br/sf/atividade/plenario/ordia/ordia.asp

[5] - Computação Distribuída de Alto Desempenho – Mario Dantas - ISBN: 85-7323-240-4

[6] Clube do Hardware - Computação em cluster - Marcos Pitanga, Acessado em 01/02/2006
http://www.clubedohardware.com.br/artigos/153-

[7] – B&B Eletronics -Application Note Table of Contents, Acessado em 14/02/2006
http://www.bbelec.com/tech_articles/rs422_485_app_note/selecting_rs485_devices.asp#top
RS422/485 - Application Note Table of Contents

[8] - Redes de Computadores das Lans, Mans e Wans às Redes ATM – 1995 Editora Campus.

[9] - Arquitetura de Redes de Computadores – Brisa 1994 - Makron Books

[10] - Tecnologia de Redes de Comunicação e Computadores – Mario Dantas ISBN: 85-7323-169-6

[11] - Rede Nacional de Ensino e Pesquisa -- Sistemas de Cabeação Estruturada EIA/TIA 568 e ISOC/IEC 11801, Acessado em 26/02/2006 http://www.rnp.br/newsgen/9806/cab-estr.html

[12] - Categorias e Classes Categorias e Classes Cabeamento - José Maurício Santos Pinheiro, Acessado em 03/03/2006
http://www.projetoderedes.com.br/artigos/artigo_categorias_e_classes.php -

[13] - Rede Nacional de Ensino e Pesquisa – Multicast, Acessado em 06/03/2006
http://www.rnp.br/multicast

[14] – Cisco- Multicast, Acessado em 06/03/2006
http://www.cisco.com/warp/public/779/largeent/learn/technologies/multicast.html

[15] – UFRGS - Multicasting em IP, Acessado em 06/03/2006
http://penta2.ufrgs.br/rc952/trab2/hl_intro.html

[16] – Oracle - Oracle Database, Acessado em 07/03/2006
http://www.oracle.com/database/index.html

[17] - Microsoft - Módulo 4 – Comunicações Seguras, Acessado em 17/04/2006
http://www.microsoft.com/brasil/security/guidance/topics/devsec/secmod04.mspx -

[18] - ABNT NBR ISO/IEC 17799:2005 - Código de Prática para a Gestão da Segurança da Informação Teoria e Prática e ISO/IEC 27001:2005 Sistemas de Gestão da Segurança da Informação – Requisitos

[19] – Acer – Tablet PC, Acessado em 24/04/2006
http://global.acer.com/products/tablet_pc/tmc310.htm

[20] – Cisco – Firewall, Acessado em 26/04/2006
http://www.cisco.com/

[21] – Opto Tech – Full Color Led Display, Acessado em 27/04/2006
http://www.opto.com.tw/Products/Sys-ProductIntro-b.asp?langtype=eng

[22] - Actone – Led Total Solution, Acessado em 27//04/2006
http://www.actone1.com/

[23] - Barco – I Lite 6, Acessado em 27/04/2006
http://www.barco.com/branding/en/products/product_specs.asp?element=697

[24] – Mitsubishi – Diamond Vision – Led Display, Acessado em 28/04/2006
http://www.diamond-vision.com/

[25] - Lighting Desing Glossary, Acessado em 29/04/2006
http://www.schorsch.com/kbase/glossary/luminance.html

[26] - The Led Product Store, Acessado em 30/04/2006
http://www.ledproductstore.com/

[27] - Bright Idea For LCDs
Revista Computer Power User, dezembro de 2004 - Vol. 4, ed. 12 – Pags. 40-41

[28] - Lights, Camera, Action!
Revista Smart Computing, julho de 2003 - Vol. 9, ed.7 – Pags. 38-41

[29] - High-Definition Nuts & Bolts
Revista Smart Computing, abril de 2004 - Vol. 2, ed. 4 – Pags. 64-67

[30] - Portable Digital Projectors
Revista PC Today, maio de 2005 - Vol. 3, ed. 5 – Pags. 88-90

[31] - The Future of Video Takes us Way Beyond HDTV
Revista First Glimpse, abril de 2005 - Vol. 2, ed. 3 – Pags. 46-48

[32] - Biometrics - Advanced Identity Verification - Julian D. M. Ashbourn
Published by Springer Verlag (ISBN 1-85233-243-3)

[33] - Avanti, Acessado em 29/04/2006

http://www.avanti.1to1.org/

[34] –International Biometric Group, Acessado em 23/03/2006

http://www.biometricgroup.com/

[35] - Biometric Tecnology, Inc., Acessado em 25/04/2006

http://www.bio-tech-inc.com/

[36] - Biometric Consortium, Acessado em 25/04/2006

http://www.biometrics.org/

[37] - International Biometric Industry Association, Acessado em 20/04/2006

http://www.ibia.org/

[38] - Biometrics: Fingerprint Authentication, Acessado em 12/04/2006

http://www.giac.org/certified_professionals/practicals/gsec/0368.php

ANEXO I - TECNOLOGIA DE CLUSTERS

O estudo da tecnologia de clusters teve por base consultas realizadas nas referências bibliográficas de números de [5] a [6].

INTRODUÇÃO

Segundo definições constantes nas referências bibliográficas citadas anteriormente, *cluster* é um sistema que compreende dois ou mais computadores ou sistemas, denominados nodos, que trabalham em conjunto para executar aplicações ou realizar outras tarefas, de forma transparente para os usuários que os utilizam, que trabalham como se acessassem um único sistema. Este conceito é denominado transparência do sistema.

Um *cluster* deve oferecer, como características fundamentais, um incremento substancial na confiabilidade, disponibilidade, distribuição de carga e performance do sistema.

Sua utilização é fundamental para o processamento de informações críticas, para o fornecimento de capacidade de processamento ou para a disponibilização ininterrupta de serviços computacionais. Há muitas tecnologias para a construção de *clusters*, mas nesse estudo serão consideradas apenas aquelas que tenham aplicação no ambiente do SVE-SF.

ALTA DISPONIBILIDADE (HIGH AVAILABILITY OU FAILOVER)

Este modelo de *cluster* é construído para prover disponibilidade de serviços e recursos de forma ininterrupta, através do uso da redundância implícita ao sistema. A idéia geral é que se um nó do *cluster* vier a falhar (*failover*), aplicações ou serviços possam estar disponíveis em outro nó. Estes tipos de *cluster* são utilizados para base de dados de missões críticas, *e-mail*, servidores de arquivos e aplicações.

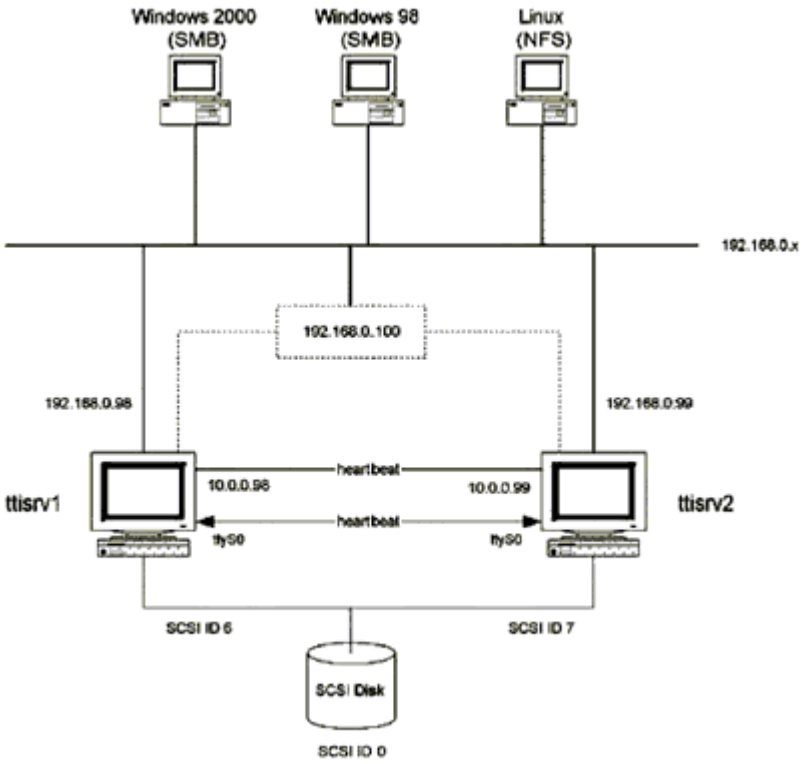


Figura AI.1 - Cluster de Alta Disponibilidade

A Alta Disponibilidade está ligada diretamente a nossa crescente dependência aos computadores, pois agora eles possuem um papel crítico, principalmente em empresas cuja maior funcionalidade é exatamente a oferta de algum serviço computacional, como e-*business*, notícias, *sites web e* base de dados, dentre outros.

Um *cluster* de Alta Disponibilidade visa manter a oferta dos serviços prestados por um sistema computacional, replicando serviços e servidores, através da redundância de *hardware* e reconfiguração de *software*. Vários computadores juntos agindo como um só, cada um monitorando os outros e assumindo seus serviços caso algum deles venha a falhar. A complexidade do sistema estará no *software*, que cuidará do monitoramento das outras máquinas da rede, identificando os serviços que estão sendo executados, quem os está executando, e como se deverá proceder em caso de falha. Perdas na performance ou na capacidade de processamento são normalmente aceitáveis. O objetivo principal é não parar. Existem algumas exceções, como sistemas de tempo real e de missão crítica.

A tolerância a falhas é conseguida através de *hardware*, como sistemas RAID, fontes, placas redundantes e sistemas de rede totalmente ligados para prover caminhos alternativos na quebra de um *link*.

CLUSTER DE BALANCEAMENTO DE CARGA (LOAD BALANCING)

Os sistemas de cluster baseados em balanceamento de carga integram seus nodos para que todas as requisições provenientes dos clientes sejam distribuídas de maneira equilibrada entre os nodos. Os sistemas não trabalham juntos em um único processo, mas redirecionando as requisições de forma independente, assim que chegam, baseados em um escalonador e em um algoritmo próprio. Todos os nodos são responsáveis por controlar os pedidos. Se um nó falhar, as requisições são redistribuídas entre os nós disponíveis no momento.

O balanceamento de carga entre servidores faz parte de uma solução abrangente em uma explosiva e crescente utilização da rede e da Internet, permitindo o aumento da capacidade da rede e melhorando sua performance. Um consistente balanceamento de carga mostra-se hoje como parte integrante de todo o projeto de *Web Hosting* e comércio eletrônico. Entretanto, essa tecnologia pode ser usada para os clientes internos das empresas.

Quando não fazemos o balanceamento de carga entre servidores que possuem a mesma capacidade de resposta a um cliente, começamos a ter problemas, pois um ou mais servidores podem responder à requisição feita e a comunicação fica prejudicada.

É preciso que o *software* responsável pelo balanceamento da carga fique entre os servidores e os usuários. Pode-se também colocar múltiplos servidores de um lado, fornecendo aos clientes a impressão que estão tratando com uma única máquina.

Um exemplo clássico é o *Linux Virtual Server*. Os clientes tentam acessar o endereço do servidor, que é o do *software* responsável pelo balanceamento da carga, chamado de *Virtual Server* (VS), que redireciona o tráfego para um dos servidores do pool.

Pode-se usar, no lugar de um *software* dedicado a fazer todo o gerenciamento, um equipamento de rede que combine a performance do *hardware* e do *software* para fazer o encaminhamento dos pacotes e o balanceamento de carga em um só equipamento.

Quando o VS recebe uma requisição de processamento, o algoritmo usado para o balanceamento de carga deverá ser capaz de selecionar o servidor que fará o processamento de modo transparente e imperceptível para o usuário, como se não existisse o balanceamento.

A verificação do correto funcionamento dos servidores é ponto de vital

importância para que a comunicação não seja erroneamente redirecionada para um servidor que tenha acabado de falhar.

O balanceamento de carga é mais que um simples redirecionamento do tráfego dos clientes para os servidores. O equipamento responsável pelo balanceamento precisa ter características como verificação permanente da comunicação, checagem dos servidores e redundância.

É necessário monitorar sempre o balanceamento da carga para garantir que não ocorrerão gargalos ou pontos de falha.

Os algoritmos para balanceamento são um dos fatores de maior importância neste contexto. Serão apresentados três métodos básicos:

- *Least Connections*

  Esta técnica redireciona as requisições para o servidor baseado no menor número de requisições/conexões. Por exemplo, se o servidor 01 está controlando atualmente 50 requisições/conexões, e o servidor 02 controla 25 requisições/conexões, a próxima requisição/conexão será automaticamente direcionada para o servidor 02, por possuir naquele momento um número menor de requisições/conexões ativas.

- *Round Robin*

  Este método usa a técnica de sempre direcionar as requisições para o próximo servidor disponível, de forma circular. Por exemplo, as conexões de entrada são dirigidas para o servidor 01, depois para o servidor 02 e, finalmente, para o servidor 03, retornando depois ao servidor 01.

- *Weighted Fair*

  Esta técnica dirige os pedidos para os servidores com base na carga de requisições de cada um e na capacidade de resposta dos mesmos. Por exemplo, se o servidor 01 for quatro vezes mais rápido no atendimento aos pedidos do que o servidor 02, o administrador coloca um peso maior de trabalho para o servidor 01 do que para o servidor 02.

CLUSTER COMBINADO - ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA

Combina as características dos dois tipos de *cluster* vistos anteriormente, aumentando a disponibilidade e escalabilidade de serviços e recursos. Esta solução visa prover alta performance aliada à possibilidade da não existência de paradas críticas. Este tipo de *cluster* é a solução perfeita para servidores de Internet e aplicações de rede nas quais a continuidade de suas operações é muito crítica, como em servidores *web*, *e-mail*, *news* ou *ftp*. As principais características desta plataforma são:

- Redirecionamento dos pedidos feitos a nodos defeituosos para nodos reservas;
- Melhoria na qualidade de nível de serviço para as aplicações típicas de rede;
- Integração transparente para as aplicações *stand-alone* e não *cluster*, juntos em uma única rede virtual;
- A arquitetura do *cluster* deverá ter um *framework* altamente escalável.

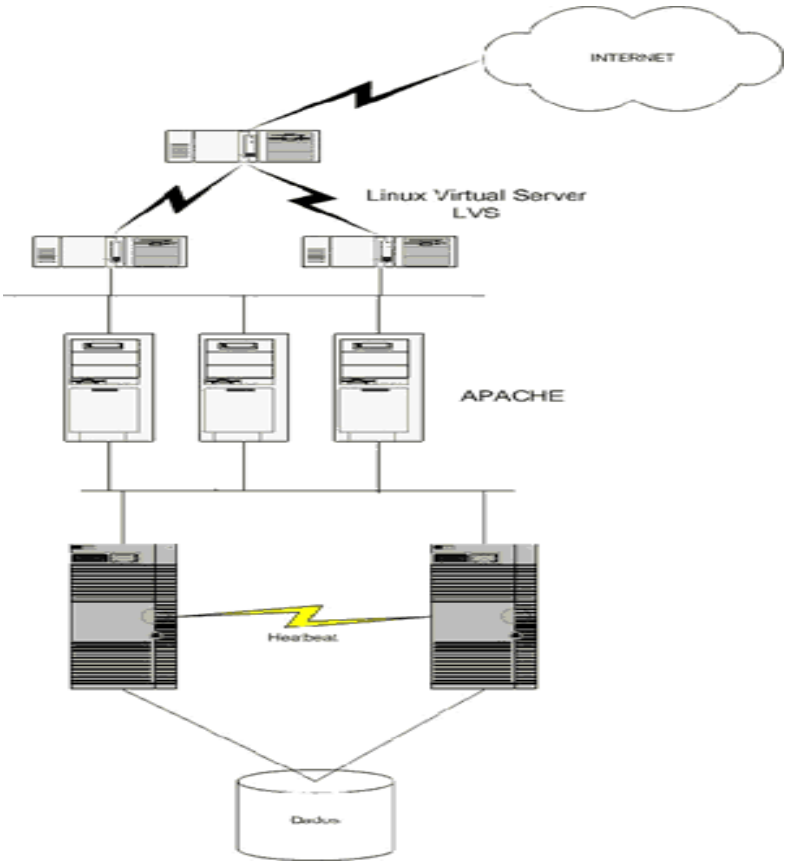


Figura AI.2 - Cluster Combinado - Alta Disponibilidade e Balanceamento de Carga

ANEXO II - TECNOLOGIA DE PAINÉIS

INTRODUÇÃO

O estudo da tecnologia de painéis teve como base consultas realizadas nas referências bibliográficas de números [21] a [31].

A exibição de imagens em painéis pode ser feita por visão frontal direta, por retroprojeção ou por projeção frontal. Para grandes áreas de exibição, podem-se adotar soluções modulares e escaláveis, compostas por múltiplos equipamentos montados em forma de matriz.

Também existem tecnologias que permitem a exibição de várias fontes de informação simultaneamente, com liberdade de disposição das informações em qualquer ponto do painel, seja ele constituído de equipamento único ou de um conjunto de equipamentos interligados.

Para ser exibida, a imagem precisa ser previamente codificada segundo um padrão analógico ou digital. Os padrões analógicos mais utilizados no país para os equipamentos de exibição de imagem são o NTSC e PALM.

Depois de codificada segundo um determinado padrão, a imagem precisa ser gerada. Há várias tecnologias utilizadas pela industria para a geração de imagens. As principais são as seguintes: CRT *(Cathode Ray Tube),* DLP *(Digital Light Processing),* LCD *(Liquid Crystal Display),* LCD de polisilício, LcoS *(Liquid Crystal on Silicon*), plasma e LED *(Light Emitting Diode*).

Para a definição da solução de exibição de imagens a ser adotada para um determinado ambiente, as seguintes questões precisam ser analisadas:

1. De quantas pessoas se compõe a audiência?

   Essa informação determinará o tamanho que terá a imagem para ser bem visualizada por todos os presentes. Imagens maiores necessitam de equipamentos de maior brilho.

2. Qual o tipo e a intensidade da iluminação do ambiente?

   Apesar de ambientes escuros serem mais propícios para a exibição de imagens, as salas de trabalho são iluminadas, pois requerem luz ambiente

para anotações e comunicação entre as pessoas. Além disso, quando se exibem textos e imagens com muitos detalhes, esses precisam estar suficientemente nítidos para serem bem visualizados por todos. Por isso, quanto mais brilhante for o equipamento de exibição, melhor.

Além do brilho, outras características dos equipamentos também precisarão ser consideradas para a escolha da solução, como a resolução, o contraste e o formato de exibição da imagem.

TECNOLOGIAS DE EXIBIÇÃO DA IMAGEM

Como vimos na introdução do documento, imagens podem ser exibidas por visão frontal direta, por retroprojeção ou por projeção frontal. Entretanto, nem todas as tecnologias de geração de imagem se aplicam a todas as formas de exibição.

Para a exibição de imagens em dispositivos de visão frontal direta, são utilizadas as seguintes tecnologias: CRT, plasma, LCD e LED.

Para a exibição de imagens por retroprojeção, são utilizadas as tecnologias de CRT, LCD transmissivo, *LCD* de polisilício, DLP e LCoS.

Para a exibição de imagens por projeção frontal, são utilizadas as tecnologias de LCD e DLP.

TIPOS DE EXIBIÇÃO DA IMAGEM

Frontal Direta

Dispositivos de visão frontal direta são aqueles onde a imagem é gerada diretamente na tela onde é exibida, sem o uso de recursos de projeção.

Retroprojeção

Na retroprojeção, o equipamento de projeção é colocado por trás de uma tela opaca, sendo a imagem transmitida de trás para frente, de forma que a audiência, que se encontra em frente à tela, possa ver a imagem projetada.

Projeção Frontal

Sistemas de projeção frontal são instalados na parte de trás da sala, de forma a projetarem a imagem em uma tela no outro extremo do ambiente, para onde a audiência está olhando.

Utilizam lentes de longo alcance, tipo *long throw*. Esses sistemas de projeção não possuem os problemas de reflexos apresentados pelos retroprojetores.

Projetores frontais oferecem flexibilidade em relação ao formato de exibição da imagem. Essa flexibilidade é proporcionada pela possibilidade de instalação de máscaras acionadas por comando elétrico. Dessa forma, não importa a proporção original da imagem que você está projetando, pois são colocadas molduras ao redor da imagem projetada. Com esse tipo de sistema, nunca haverá barras cinzas nas laterais da imagem ou negras em cima e em baixo.

PADRÕES DE CODIFICAÇÃO DA IMAGEM

Digital versus Analógico

A mudança da codificação de vídeo de analógica para digital trouxe muitas vantagens. Dados digitais permitem acesso aleatório às informações de modo quase instantâneo, tornando fácil editar e gravar imagens. Sinais digitais não são imunes aos efeitos de interferências eletromagnéticas, mas certamente são menos suscetíveis a estas que os sinais analógicos. Na maior parte dos casos, os dados digitais de alta resolução recebidos no aparelho são idênticos aos que foram gerados no transmissor.

Outra característica muito importante do formato digital é a possibilidade de compressão da imagem. Podem-se aplicar algoritmos ao vídeo digital para reduzir acentuadamente o tamanho dos arquivos, sem modificar substancialmente a qualidade da imagem. O padrão MPEG-2, utilizado para a gravação de DVDs, é um exemplo perfeito dessa técnica, pois um DVD tem capacidade para armazenar apenas alguns minutos de vídeo sem compressão. Entretanto, é capaz de armazenar horas de vídeo comprimido.

Padrões Analógicos

Numa transmissão NTSC, a imagem é composta de quadros individuais.

Entretanto, devido à velocidade em que são apresentados, o olho humano os percebe como movimento contínuo.

O padrão NTSC possui uma resolução horizontal de 704 *pixels* por linha e resolução vertical de 480 linhas, com formato 4:3 de exibição da imagem. São exibidos 337.920 *pixels* para cada quadro.

Cada quadro do vídeo possui aproximadamente 480 linhas de informação de imagem e é exibido linha a linha, em duas fases. Na primeira fase, são exibidas as linhas ímpares, de baixo para cima, em um tempo de 1/60 segundo. Na segunda fase, são exibidas as linhas pares, também em 1/60 segundo. Dessa forma, no tempo de 1/30 segundo, a imagem de cada quadro é exibida inteiramente. Essa técnica é chamada de entrelaçamento.

Numa transmissão de vídeo NTSC, é preciso considerar o tempo necessário entre a exibição de um quadro e o próximo. Para isso, existe um intervalo de 45 linhas entre os quadros, onde não é transmitida nenhuma informação. Assim, o número total de linhas para cada quadro é de 525 linhas. Porém, apenas 480 linhas contêm informação de vídeo.

O padrão de transmissão da TV analógica também é chamado de 525i, significando 525 linhas entrelaçadas. Algumas fontes se referem a ele como 480i, que significa 480 linhas ativas de vídeo entrelaçado. Entretanto, com a definição do novo padrão digital SDTV *(Standard Definition Television)* entrelaçado de 480 linhas, o termo 480i deverá ser utilizado para o padrão SDTV e o 525i para o padrão NTSC.

Padrões Digitais

Há três padrões principais de codificação digital, todos referenciados pela sigla DTV, de *Digital Television*. Esses padrões são o SDTV *(Standard Definition Television)*, o EDTV *(Enhanced Definition* TV*)* e o HDTV *(High Definition Television)*.

O padrão EDTV refere-se ao formato 480p e possui resolução de 852 colunas por 480 linhas. Este formato utiliza a técnica *progressive scan*, onde a imagem é formada pela varredura progressiva da tela por um feixe de elétrons, de forma não entrelaçada.

O padrão SDTV refere-se ao formato 480i, que utiliza a técnica de vídeo entrelaçado para apresentar a imagem. A imagem é gerada em duas etapas, onde a primeira exibe as linhas ímpares e a segunda as linhas pares.

O padrão HDTV possui duas variantes, ambas utilizando o formato 16:9 de exibição da imagem.

A primeira variante do padrão HDTV, referenciada por 1080i, tem resolução horizontal de 1920 *pixels* por linha e resolução vertical de 1080 linhas por imagem, totalizando 2.073.600 *pixels* por imagem exibida. A imagem HDTV é produzida por varredura entrelaçada de linhas.

A segunda variante do padrão HDTV, referenciada por 720p, tem resolução horizontal de 1280 *pixels* por linha e resolução vertical de 720 linhas por imagem, totalizando 921.600 *pixels* por imagem exibida. A geração da imagem é feita segundo a técnica de *progressive scan*, onde a imagem é produzida pela varredura progressiva da tela por um feixe de elétrons, de forma não entrelaçada.

O fato dos equipamentos possuírem resoluções pré-definidas não significa necessariamente que exibirão o número exato de *pixels* recebidos. Poucos equipamentos de tecnologia digital aderem totalmente aos formatos 720p ou 1080i. Muitas vezes é necessária a utilização de técnicas de interpolação para converter o sinal recebido para uma resolução maior ou menor, de forma a adequá-lo à resolução nativa do equipamento.

TECNOLOGIAS DE GERAÇÃO DE IMAGEM

Cathode Ray Tube (CRT)

Esta tecnologia é utilizada em aparelhos de TV tradicionais, onde um único tubo de raios catódicos usa três canhões de elétrons para iluminar pontos da tela do aparelho, que é recoberta internamente com fósforo. Cada ponto de fósforo da tela possui, alternadamente, uma das cores do padrão RGB (vermelho, verde e azul).

É também utilizada em retroprojeção, quando a imagem é gerada por três pequenos tubos de raios catódicos localizados na parte de trás do equipamento. Essa imagem é então ampliada por espelhos e projetada na tela.

Digital Light Processing (DLP)

Uma lâmpada de projeção emite luz através de uma roda de cores RGB em movimento. As cores, uma vez iluminadas, atingem seqüencialmente um dispositivo formado por minúsculos espelhos digitais, sendo a imagem então projetada sobre uma superfície. Esses espelhos estão em um *chip* da Texas Instruments, o DMD (*Digital Micromirror Device*), que possui 100.000 horas de vida, o equivalente a 10 anos de uso.

O *chip* DMD pode conter até 1.300.000 espelhos microscópicos, cada um com sua própria dobradiça. Cada um dos espelhos projeta um *pixel* da imagem. Em resposta a sinais digitais gerados por eletrodos, um para cada espelho, o mesmo gira para refletir ou não a luz que o ilumina. Essa operação pode acontecer milhares de vezes por segundo. O percentual do tempo em que ele reflete a luz determina o brilho de cada *pixel*, dentre 1024 possibilidades, gerando uma imagem de alta definição. A cor é adicionada por meio de roda de cores colocada entre a lâmpada e o *chip*. A roda possui três filtros, um para cada cor.

LCD

Visão frontal: Cristais líquidos são injetados entre dois vidros e duas placas com eletrodos. Uma corrente elétrica é então aplicada alternadamente em regiões selecionadas da placa de vidro para bloquear ou deixar a luz passar pelos cristais. Os displays TFT-LCD *(Thin Film Transistor – Liquid Crystal Display)* apresentam características técnicas muito similares aos displays de plasma, diferenciando-se por um tempo de vida um pouco maior e uma menor propensão aos efeitos *burn-in* e *shadowing*.

Projeção/retroprojeção: Uma lâmpada de alta intensidade emite luz através de três micro-painéis RGB transmissivos de cristal líquido, um para cada cor, sendo a imagem projetada sobre uma superfície ou sobre a tela frontal do aparelho.

LCD de polisilício

A imagem é gerada por um conjunto de três painéis TFT-LCD de Polisilício, um para cada cor básica, cujas imagens são mescladas por meio de espelhos e lentes para obtenção da imagem final projetada.

É uma tecnologia utilizada em equipamentos de retroprojeção de qualidade, oferecendo saturação de cores superior, com contraste acima de 200:1.

***Liquid Crystal on Silicon* (LCoS)**

Cristais líquidos são depositados sobre uma placa de metal reflexivo. Uma luz brilha sobre a placa e os cristais. A luz é emitida por uma lâmpada de alta pressão, que atravessa um prisma. Uma corrente elétrica é aplicada alternadamente em regiões selecionadas da placa para bloquear ou deixar a luz refletir no metal, sendo a imagem projetada sobre uma superfície, após passar por dispositivos óticos que a ampliam.

A tecnologia LCoS é usada em equipamentos de retroprojeção. É uma tecnologia híbrida das tecnologias LCD e DLP. Utiliza espelhos para refletir a luz, mas esses não se movem como na tecnologia DLP. Esta tecnologia proporciona a construção de equipamentos de retroprojeção menores com qualidade de imagem superior aos de LCD.

Plasma

Milhões de células separadas são preenchidas por um gás que emite luz ultravioleta quando uma carga elétrica lhes é aplicada. A luz ultravioleta atinge então uma tela recoberta com fósforos RGB, que emitem luz visível.

A tecnologia é similar à dos LCDs. O plasma é um gás inerte que fica entre duas camadas de vidro e é ativado por eletrodos.

***Light Emitting Diode* (LED)**

Os painéis são compostos de diodos emissores de luz, podendo ser montados com *pixels* de 3, 6, 8 ou 10 mm. Quanto menor o *pixel*, melhor a resolução e a qualidade da imagem gerada. Os LEDs apresentam alto contraste e brilho, sendo adequados para ambientes muito iluminados, com luz solar ou iluminação artificial de grande intensidade.

O brilho proporcionado pelos painéis de LED é excepcional, mesmo para ângulos de visão muito amplos. É possível perceber-se metade do brilho total em ângulos de até 145 graus. O efeito *screen-door* é totalmente eliminado, não sendo percebido mesmo a distâncias de apenas três metros.

São modulares, permitindo a montagem de grandes painéis, sendo a imagem apresentada sem emendas. São apropriados para a exibição simultânea de conteúdos originados de diversas fontes, independentemente da forma ou tamanho da imagem.

PROPRIEDADES DOS EQUIPAMENTOS

Resolução

Quando se analisa a resolução de um equipamento, não se pode deixar de considerar sua resolução real ou nativa. Se a resolução nativa é 800 x 600, isto significa que o número de *pixels* físicos existentes no aparelho são 480.000 (800x600). Em alguns equipamentos, as especificações apresentam compatibilidade com resoluções maiores.

Equipamentos de alta resolução exibem imagens com mais detalhes que os de baixa resolução. Como o tamanho dos *pixels* é menor, esses são menos visíveis na tela e há mais *pixels* para a exibição da imagem.

Equipamentos de baixa resolução são mais baratos e podem gerar imagens tão boas e brilhantes quanto os de alta resolução. A menos que seja realmente necessário exibir imagens que mostrem muitos detalhes, os equipamentos de baixa resolução têm uma melhor relação custo/benefício.

As resoluções reais/nativas mais utilizadas pelos equipamentos são as seguintes:

- SVGA, ou "800 x 600" – Essa resolução é muito utilizada em função do baixo preço dos equipamentos que a usam e da boa qualidade de imagem.
- XGA, ou "1.024 x 768" – Equipamentos XGA, em princípio, são um pouco mais caros que os SVGA, mas também são largamente adotados.
- SXGA, ou "1.280 x 1.024" – Produtos SXGA apresentam alta resolução e são muito mais caros que os XGA. Esta resolução é adotada para apresentação de imagens CAD/CAM e de engenharia, onde a visualização dos detalhes é muito importante.
- UXGA, ou "1.600 x 1.200" – Os equipamentos que se utilizam desta resolução também são muito caros e voltados para aplicações que exijam a apresentação de muitos detalhes na imagem.

Brilho

O brilho é medido em lumens. Quanto maior o número de lumens que um equipamento fornece, maior será sua luminosidade. Como o brilho no centro de uma imagem é maior do que nas suas bordas, a medida do brilho em lumens ANSI fornece um resultado mais correto do que a simples medida do brilho no centro da imagem.

O cálculo do número de lumens é feito dividindo-se a área da imagem em nove retângulos iguais, fazendo-se então a leitura do brilho no centro de cada retângulo e calculando-se a média desses nove pontos.

Pode-se classificar os equipamentos existentes no mercado em quatro grupos:

- Inferior a 1000 lumens – são os equipamentos mais baratos e de menor luminosidade existentes no mercado. É adequado para utilização em ambientes escuros.

- Entre 1000 e 2000 lumens – Há muitos equipamentos com resolução SVGA e XGA nessa categoria. São adequados para uso em salas de aula e de conferências. Sua utilização é adequada para salas pouco iluminadas.
- Entre 2000 e 3000 lumens – São equipamentos de alta performance. São ideais para grandes salas de conferência. Oferecem maior flexibilidade em relação à iluminação ambiente, pois a imagem possui brilho suficiente para não ficar esmaecida. Também podem projetar uma imagem maior sem muita perda de qualidade.
- Acima de 3000 lumens – São equipamentos ultra brilhantes, podendo atingir até 12.000 lumens. São utilizados em salas de conferência, salas de treinamento, auditórios, igrejas e salas de concerto.

Contraste

O contraste é a razão entre as áreas mais brilhantes e as mais escuras da imagem. Para se obter imagens de qualidade o contraste deverá ser superior a 400:1. A luz ambiente prejudica muito o contraste. Portanto, para utilização em áreas iluminadas, deverão ser considerados equipamentos com alto contraste.

Quanto maior o contraste, maior a capacidade do equipamento em mostrar muitos detalhes de cores e de tolerar iluminação ambiente. Para medir o contraste, a imagem deverá ser dividida em 16 retângulos, que exibirão, alternadamente, brancos e pretos. Calcula-se a média da luz emitida pelos retângulos brancos e divide-se esse resultado pela média da luz emitida pelos retângulos pretos.

FORMATO DE EXIBIÇÃO DA IMAGEM

O formato de exibição da imagem é a razão entre sua largura e sua altura. Por exemplo, um painel com formato de exibição 16:9 apresentará uma imagem com 16 unidades de largura por 9 unidades de altura. Esse formato também é chamado de 1.78:1, o que significa que a largura da tela é 1,78 vezes sua altura.

Formato de exibição nativo refere-se ao formato de exibição físico que o painel possui. Por exemplo, um painel de 1280 x 720 pixels tem um formato de exibição 16:9. Um

painel de 640 x 360 pixels também possui um formato de exibição 16:9, mas tem apenas ¼ da resolução do painel maior.

Atualmente, quase todos os equipamentos suportam múltiplos formatos de exibição da imagem. Entretanto, o fabricante precisa decidir para qual finalidade está construindo seu aparelho e otimizá-lo para a audiência pretendida. Isso quer dizer que cada equipamento tem um formato de exibição que é otimizado para uma específica programação.

Quando o equipamento mostra a imagem em seu formato de exibição nativo, ele utiliza a resolução máxima do painel, atingindo brilho máximo. Quando a imagem é exibida em formatos diferentes do nativo, o resultado será uma resolução inferior e uma imagem com menos brilho.

Formatos de exibição apresentam ainda outro grande problema. Resoluções HDTV de 1280 x 720 (720p) e de 1960 x 1080 (1080i) apresentam um formato de exibição de 16:9, o que faz com que praticamente todos os painéis construídos para exibir programação digital sigam esse formato de tela larga.

O problema é que grande parte da programação existente ainda está codificada nos padrões 480i e 480p, com resolução de 640 x 480 *pixels*, tendo, portanto, um formato de exibição muito mais estreito, de 4:3.

Se você assistir programações no formato de exibição 4:3 em equipamentos que possuem formato de exibição 16:9, faixas negras precisam ser colocadas nas laterais da tela. Além de o equipamento estar sendo subutilizado, está sendo submetido ao problema de *burn-in*, em especial no centro do painel. Esse problema ocorre quando alguns *pixels* do painel são mais utilizados que outros ou quando recebem uma carga de brilho maior, por longos períodos de tempo. Quando isso ocorre, é possível que os *pixels* que foram submetidos a essa sobrecarga percam contraste, apresentando partes da imagem mais apagadas que as demais.

Equipamentos baseados nas tecnologias DLP, LCD, ou LCoS são imunes ao efeito *burn-in*, pois não usam fósforos ou gases para gerar as imagens. Já as telas de plasma ou CRT, especialmente os CRTs de retroprojeção, são suscetíveis ao efeito *burn-in*.

ANÁLISE DAS TECNOLOGIAS DE GERAÇÃO DE IMAGEM

Cathode Ray Tube (CRT)

- Visão Frontal:

Vantagens:

São dispositivos robustos, de custo relativamente baixo, possuindo alta durabilidade e baixa necessidade de manutenção. As imagens por eles geradas possuem níveis de preto profundos e excelente contraste.

Desvantagens:

Peso elevado, tamanho grande e imagem sem muita nitidez. Não são adequados à montagem de matrizes, pois não permitem justaposição. Sua resolução só permite boa visualização de textos em distâncias de até seis metros.

- Retroprojeção:

Vantagens:

Excelente relação preço/performance, sendo a solução de menor custo. A imagem possui níveis de preto profundos e contraste excelente.

Desvantagens:

Além dos problemas ocasionados pela convergência dos raios catódicos, muitas vezes apresenta distorção geométrica e problemas de foco, exigindo calibragem constante para obter-se imagem ótima. A imagem não é muito brilhante e os ângulos de visão são limitados. Requerem muito espaço para sua instalação, além de serem muito pesados.

DLP

- Projeção frontal e Retroprojeção:

Vantagens:

Os equipamentos são pequenos, leves, possuem imagem brilhante e com excelente geometria, não requerendo ajuste de convergência. Alguns equipamentos

atingem resolução de 720 p (720 x 1280). Resoluções de 800 x 600 e de 1280 x 1024 também estão disponíveis.

A profundidade média do equipamento é de 60 cm. O contraste varia entre 300:1 e 1000:1, dependendo do modelo do *chip* DMD utilizado. A lâmpada de projeção tem durabilidade entre 8000 e 9000 horas, equivalente a um ano de uso.

Com a retroprojeção é possível montar matrizes de exibição. As matrizes são modulares e escaláveis, criadas com o uso de múltiplos cubos de alta resolução, mantendo assim a qualidade da imagem independente do tamanho da tela, sem aumento da profundidade do equipamento. Apresentam diversas vantagens sobre as soluções que contemplam um único dispositivo, pois apresentam flexibilidade na visualização, seja de várias imagens em múltiplas telas ou de um número pequeno de imagens ampliadas em grandes dimensões, com elevado grau de detalhamento, adequado a um grande número de usuários simultâneos.

Permitem a montagem de matrizes de tamanho virtualmente ilimitado, sujeitas somente às restrições do sistema gerenciador e do peso suportado pela estrutura de sustentação. É possível a composição de sistemas de projeção sem divisão aparente entre os cubos de projeção, pois utiliza molduras finíssimas (separação entre cubos menores que 01 mm).

Apresentam pequena profundidade. Por serem mais compactos, possibilitam instalação com pequena ocupação de espaço do ambiente.

Desvantagens:

A montagem do projetor pode ser difícil. A roda de cores produz efeitos indesejáveis, como cansaço visual e efeitos arco-íris e de pontilhamento. Há falta de detalhes nas sombras. As lâmpadas de projeção são caras. É possível a existência de micro espelhos com defeito, seja de fabricação, seja ao longo do uso. Seu uso requer que o ambiente possua iluminação controlada, pois a qualidade da imagem exibida é dramaticamente afetada pelo aumento da luminosidade ambiente. Como o tamanho da imagem projetada é proporcional à distância entre o projetor e a superfície de projeção, quanto maior a dimensão da imagem pretendida, menores serão sua definição e luminosidade, uma vez que a resolução e luminosidade máximas do projetor são fixas.

Para uma mesma resolução, quanto maior a imagem, menor a definição. Os projetores frontais não garantem uniformidade de brilho na imagem projetada, podendo haver focos de menor ou maior brilho nos cantos ou no centro da imagem. Esta ausência de uniformidade também torna os projetores frontais pouco adequados à montagem de matrizes de projeção.

LCD

- Visão Frontal

Vantagens:

São equipamentos razoavelmente leves, podendo ser construídos com diagonais de até 60 polegadas e com apenas 10 centímetros de profundidade. Sua durabilidade é, em média, de 30.000 horas, podendo chegar a 60.000 horas. A imagem possui mais brilho que a gerada com plasma. A imagem de alguns aparelhos é de qualidade quase fotográfica se a programação for transmitida em alta definição e estando o observador posicionado na frente da tela. A geometria da imagem é excelente.

Desvantagens:

Preço alto, pois requer uma base de matriz ativa com pelo menos um transistor para cada *subpixel*. Há a possibilidade de existência de pixels permanentemente apagados. Apresenta limitações de ângulos de visualização. Possuem moldura, o que dificulta a montagem em painéis. Não são apropriados para ficarem ligados 24 horas por dia, sete dias por semana.

- Projeção frontal:

Vantagens:

Pequeno e leve, permite a projeção das imagens em diversos tamanhos, sem perda de qualidade. Imagem brilhante e com excelente geometria.

Desvantagens:

A montagem do projetor pode ser difícil. As lâmpadas de projeção são caras e tem vida útil limitada, durando em torno de 5000 a 8000 horas. A imagem tem níveis de preto fracos em função do baixo contraste característico dessa tecnologia.

O principal problema de projetores LCD é o efeito *screen-door*. As pessoas que se sentam muito próximo da tela onde a imagem está sendo projetada tem a impressão de que estão vendo a imagem através de uma tela reticulada. Esse efeito é causado porque os projetores LCD não conseguem preencher todo o espaço destinado a cada *pixel*, ficando, portanto, uma máscara preta ao redor da parte iluminada. Quanto mais longe da tela de projeção, menor o efeito *screen-door*.

Os *pixels* são visíveis se a imagem é observada de perto e há a possibilidade de existência de *pixels* permanentemente apagados. Seu uso requer que o ambiente possua iluminação controlada, pois a qualidade da imagem exibida é dramaticamente afetada pelo aumento da luminosidade ambiente.

Os projetores frontais não garantem uniformidade de brilho na imagem projetada, podendo haver focos de menor ou maior brilho nos cantos ou no centro da imagem. Esta ausência de uniformidade também torna os projetores frontais pouco adequados à montagem de matriz de projeção.

Como o tamanho da imagem projetada é proporcional à distância entre o projetor e a superfície de projeção, quanto maior a dimensão da imagem pretendida, menores serão sua definição e luminosidade, uma vez que a resolução e luminosidade máximas do projetor são fixas. Para uma mesma resolução, quanto maior a imagem, menor a definição.

Essa tecnologia é menos adequada para uso em ambientes com iluminação normal de escritório, se comparada a outras soluções de durabilidade, robustez e custo similar, como Polisilício-LCD ou DLP.

LCD de Polisilício

Vantagens:

Utilizado em equipamentos de retroprojeção, possui alta eficiência no aproveitamento da fonte de luz, permitindo o uso de lâmpadas especiais de projeção de baixa potência (tipicamente lâmpadas UHP de 100 watts), mantendo alto nível de brilho.

Seu funcionamento é estável e o brilho é uniforme, mesmo em regimes de operação de 24 horas por dia durante toda a semana. Maior vida útil das lâmpadas. O ajuste de convergência é feito em fábrica. Não requer reajuste ao longo da vida útil, que pode chegar a 50.000 horas. A lâmpada tem vida útil entre 3000 e 9000 horas.

Desvantagens:

Peso elevado e tamanho grande. A profundidade média do projetor é de 57 cm e sua diagonal varia entre 40 e 84 polegadas.

LCoS

Vantagens:

Utilizado em equipamentos de retroprojeção, os *pixels* são praticamente invisíveis, mesmo se a tela for observada de perto. As imagens são bem reais e tem boa saturação de cores.

Os projetores de LCoS não sofrem dos efeitos *screen-door* e arco-íris, pois o espaço entre os *pixels* é menor e não há roda de cores. O resultado é uma imagem brilhante e com cores adequadamente saturadas.

Desvantagens:

Há a possibilidade de existência de *pixels* permanentemente apagados. A imagem tem baixo contraste e seus níveis de preto não são profundos. As lâmpadas de projeção são bem mais caras que a dos projetores LCD e DLP e tem vida útil limitada, entre 1000 e 1500 horas.

Sua principal desvantagem é o baixo contraste, não exibindo níveis de preto adequados. A duração da lâmpada não é longa e sua substituição é mais cara que as usadas nos projetores LCD ou DLP. Entretanto, considerando os equipamentos de retroprojeção, sua imagem só perde para aqueles baseados na tecnologia CRT.

Plasma

Vantagens:

O painel é fino, relativamente leve e plano. A saturação das cores e a geometria da imagem são excelentes. Os ângulos de visualização também são muito bons, chegando a 160º. Pode ser fabricado em grandes tamanhos (40”, 50”, 61”e 71”) e com pequena espessura, em torno de 10 cm. Seu tempo de vida é da ordem de três anos de uso, equivalentes a 30.000 horas.

O tempo de resposta para a exibição da imagem é melhor que a dos LCD's, além de possuírem contraste superior, gerando imagens mais nítidas com cores mais reais. Seu ângulo de visão também é maior.

Desvantagens:

É caro e há a possibilidade de existência de *pixels* permanentemente apagados. Podem apresentar o efeito *burn-in*, que são áreas da tela permanentemente marcadas pela mesma imagem exibida por longos períodos, como o logotipo de uma emissora de TV exibido sempre na mesma posição do vídeo. Também podem apresentar o efeito *shadowing*, que é a permanência de uma imagem muito brilhante sobre uma outra menos brilhante que seja exibida em seguida.

O vidro da frente do painel pode causar degradação da imagem sob luz direta. O brilho do painel diminui com o tempo. Não são apropriados para montagem de matriz de projeção, por terem moldura larga. Também não são adequados para ficarem ligados 24 horas por dia, sete dias por semana. Geram mais calor que os displays de LCD.

***Light Emitting Diode* (LED)**

Vantagens:

Apresentam alto contraste e brilho, sendo adequados para ambientes muito iluminados, mesmo com luz solar ou iluminação artificial de grande intensidade. Possuem alta resolução, com pixels de até 1,5mm, com durabilidade de até 45.000 horas, equivalentes a quase cinco anos de uso. Não são apropriados para ficarem ligados 24 horas por dia, sete dias por semana.

O brilho proporcionado pelos painéis de LED é excepcional, mesmo para ângulos de visão muito amplos. É possível perceber-se metade do brilho total em ângulos tão

extremos quanto 145 graus. O efeito *screen-door* é totalmente eliminado, não sendo percebido mesmo a distâncias de apenas três metros.

Podem trabalhar em temperaturas elevadas, pois possuem sensores de temperaturas e ventiladores. São modulares, permitindo a montagem de grandes painéis, sendo a imagem apresentada sem emendas. São apropriados para a exibição simultânea de conteúdos originados de diversas fontes, independentemente da forma ou tamanho da imagem.

A manutenção dos painéis de LED é simplificada por sua modularidade, sendo necessário trocar-se apenas os módulos defeituosos.

Desvantagens:

O custo dos painéis de LED é muito elevado, devendo, portanto, ser encarado como um investimento de longo prazo.

CONCLUSÕES

Para atender as necessidades do plenário do Senado Federal as seguintes premissas deverão ser consideradas:

- As informações deverão ser visíveis de todos os pontos do plenário, inclusive em ângulos horizontais de no mínimo 145º e verticais de no mínimo 50º.
- O brilho deverá ser superior a 1500 candelas/m²;
- O contraste deverá ser, no mínimo, de 500:1;
- Deverão existir controles individuais de contrastes e brilho;
- Compatibilidade de sinal para os seguintes padrões: digital (HDTV, EDTV, SDTV), S-Vídeo, vídeo componente, vídeo composto; vídeo Digital (DVI), RGB;
- No mínimo 16 milhões de cores.
- Permitir a exibição de imagens simultâneas de várias fontes, comandadas por uma central independente;
- Permitir o redimensionamento da imagem na tela;
- Baixa emissão de ruídos;

- O painel deverá ser modular e escalável;
- Tempo de vida útil mínimo do painel de 50.000 horas, em condições normais de operação;
- O painel deverá ser controlado por um gerenciador de imagens, com capacidade de processar, controlar e exibir as fontes de sinais digital (HDTV, EDTV, SDTV), S-Vídeo, vídeo componente, vídeo composto; vídeo digital *(*DVI), RGB, devendo suportar no mínimo 2 entradas DVI simultâneas.

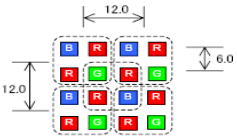
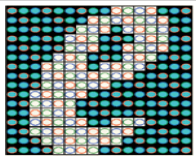
Para atender a estes requisitos mínimos a melhor tecnologia atual, conforme apresentado nos itens anteriores é a de um painel de LED. Equipamento de alto brilho e contraste, com ângulo de visão superior a 145º, modular e escalável, composto de múltiplos equipamentos de exibição, montados em forma de matriz e são os únicos que podem apresentar uma tela sem emendas.

Devido à durabilidade da solução recomendada, que poderá chegar até a 45.000 horas, algo em torno de 20 (vinte) anos de utilização, o investimento feito deverá ser encarado como de longo prazo.

Alternativamente, pode-se optar pela tecnologia de matriz de cubos de retroprojeção com DLP ou LCD polisilício, que possuem características técnicas inferiores aos de LED, mas que podem também atender as necessidades do plenário do Senado Federal a um custo inferior ao de LED. O painel, composto por cubos de retroprojeção de até 60 polegadas, possui molduras finíssimas, com emendas de até 1mm, quase imperceptíveis a grandes distâncias.

Na tabela a seguir, é apresentado quadro comparativo das especificações técnicas dos 03 (três) principais fornecedores mundiais de painéis de LED.

Tabela AII.1 - Comparativo das especificações técnicas de Painéis

ESPECIFICAÇÕES	BARCO (Ilite 6)	MITSUBISHI (AVL¨-ID6)	OPTO (AVI-V6)
Dot pitch	6 mm (Pixel pitch- Cluster Pitch/Physical Resolution 6.22 mm)	6 mm (doth pitch) (Pixel Pitch 12 mm)	6 mm (Pixel center to center spacing)
LED Pixel Arrangement and Layout of Color Pixel			
Virtual Pixel Pitch	-	8,4 mm	
Pixel density	25.920/m² (2.410/ft²) ,5.184/tile (72x72)	27.778 dots/sq. m	27,777 Pixels per square meter
LED configuration	3-in-1 SMD		3-in-1 SMD
Brightness	1.800 NIT	1.500 cd/sq. (NIT)	5.000 nits (adjustable)
Calibrated Brightness	1.500 NIT (calibrated at 6500°K)	-	Adjustable
Image Control		Dynamic Pixel Control	Vitual pixel technology
Image Processing	-	Progressive Scan Converter + Interpolation	24-bit; 100% digital
Grey Level	-	4096 Steps	
Brightness Adjustment Level	-	64 Steps	
Hor. viewing angle	145° + (min. 50% brightness)	160 degree (+/- 80 degree)	180º
Vert. viewing angle	145° + (min. 50% brightness)	160 degree (+/- 80 degree	50º
Minimum Viewing Distance	-	more than 5 m	15,24m typical viewing distance required where image will not apear pixelated
Contrast ratio	"950:1"	-	1,000:1 + with louvers providing extra contrast
Lifetime	100.000h (typical use) 45.000h (full white - half brightness)	50,000 h (Half Brightness)	100.000 h (led lifetime)
Power consumption	maximum: 400 W/Tile average: 100 W/Tile	averege: 0.65 kW/sq. m	80 W (Maximum power per module)
Power Requirement		9 kVA (3-Phase 3-Wire + Earth AC200 to AC240 V 50/60Hz)	
Weight	13 Kg (28,7 lbs)	75 kg/sq.m	6 kg (Display weight per module)
Processing	14 bit/color (Color), 8 bit/color (Greyscale)	18 bit (greysacle)	
Colors	4,4 trillion		16-bit (281 trillion colors with 65,536 shades of Red, Green and Blue)
Refresh rate	400 Hz (PAL/NTSC minimum)		
Temperature range	operating:0 - 40°C (32 - 104°F) storage: -20 -60º (-4 - 140F)		
Humidity	operating:35 - 85% storage: 10 -90%		
Source compatibility	S-Video / Composite / YUV / RGB / SDI / HDSDI / Data DVI up to SXGA	VGA-SVGA(DVI), HDTV(SDI), SDTV(SDI), NTSC/PALM	VGA,NTSC,PAL or SECAM video
Tile dimensions	Width: 448mm (17.6")	384 mm	192 mm
	Height: 448mm (17.6")	384 mm	192 mm
	Depth: 127mm (5")		
Resolução	74,66666667	64 x 64 dots (linhas)	32 x 32 (linhas) Module configuration - pixels (HXW)
No. of Scanning Line		64	32

ANEXO III - BIOMETRIA

O estudo da tecnologia biométrica teve como base consultas realizadas nas referências bibliográficas de números [32] a [38].

OBJETIVO

Identificar e autenticar os senadores para utilização do SVE-SF, de forma a garantir a segurança e inviolabilidade do sistema.

POR QUE BIOMETRIA?

A biometria é a medida das características fisiológicas ou comportamentais dos indivíduos.

As tecnologias biométricas utilizam métodos automáticos para identificar ou autenticar a identidade de pessoas, baseados nas características acima citadas.

Uma característica biométrica não pode ser perdida, esquecida ou emprestada a terceiros, o que torna os sistemas de identificação biométrica superiores aos demais, por oferecerem um meio não transferível de identificar pessoas. Eles medem características humanas como a geometria da mão e da face, a impressão digital, o padrão da íris ou da retina, a verificação dinâmica de assinatura e a voz.

As tecnologias biométricas evitam a duplicação de identidade e dificultam a ocorrência de erros de identificação.

TIPOS DE BIOMETRIA E FORMAS DE ARMAZENAMENTO

O estudo aqui realizado restringiu-se aos dispositivos de reconhecimento de características físicas, como os leitores de digitais, de íris e de geometria da mão, por serem menos intrusivos. Não foram analisados dispositivos que medem características comportamentais, como aqueles que efetuam o reconhecimento de voz e de assinatura, por serem tecnologias ainda em desenvolvimento para adoção em larga escala, não havendo

muitos produtos no mercado.

Foram analisados fatores relativos à acuidade, custo, facilidade de implantação e se a tecnologia é invasiva. Cada leitor tem seus pontos fortes e fracos. Os leitores de íris têm maior acuidade, porém são os mais caros e invasivos. Já os leitores de digitais e de geometria da mão possuem uma boa relação custo benefício, sendo, portanto, considerados mais adequados para serem utilizados no SVE-SF. Entretanto, os leitores biométricos de digitais apresentam a vantagem de poderem ser incorporados a notebooks, ocupando um espaço bem menor que os leitores de geometria da mão, que são muito grandes para serem instalados na bancada dos senadores.

Quanto ao arquivamento da informação biométrica, esta pode ser armazenada em um cartão de circuito integrado, numa base de dados instalada em um servidor ou, nos casos em que os dispositivos de leitura estão integrados a equipamentos, na memória dos mesmos. Também há vantagens e desvantagens nos diversos tipos de armazenamento.

Se for utilizado um *smartcard*, o usuário terá a segurança de que seus dados biométricos estarão guardados com ele e poderá identificar-se com rapidez em qualquer unidade de leitura da rede, bastando inserir o cartão no leitor de cartões e colocar o dedo no leitor biométrico. Entretanto, não haverá um repositório central das informações biométricas e, caso o usuário perca o cartão, os dados terão que ser novamente colhidos.

No caso de leitores integrados a equipamentos, a implantação é mais simples, pois as digitais ficam armazenadas nos próprios equipamentos. Entretanto, as informações biométricas dos usuários possivelmente estarão distribuídas pelos diversos equipamentos, pois esses dispositivos possuem memória limitada. Isso exigirá a montagem de uma rede de comunicação entre os equipamentos.

Finalmente, a solução que oferece maior flexibilidade é a que armazena as informações em servidores, que é a solução sugerida.

PERFORMANCE DE SISTEMAS BIOMÉTRICOS

As métricas tradicionais utilizadas para medir a performance dos equipamentos de biometria não são suficientes para estimar o desempenho real dos sistemas em que serão integrados, pois são obtidas em testes realizados em ambiente controlado e medem, normalmente, a capacidade dos algoritmos de efetuar a extração das características das

digitais e compará-las com uma base de dados de gabaritos (*templates*) de digitais. Dessa forma, os índices de performance fornecidos pelos fornecedores deverão ser utilizados apenas como uma referência para a avaliação da solução de biometria como um todo.

Os principais índices utilizados para medir a performance dos equipamentos de biometria são a taxa de falsos positivos, a taxa de falsos negativos e o tempo de verificação. Esses índices deverão ser analisados em conjunto, pois o valor de um é dependente do valor do outro. Se o limite (*threshold*) definido para se aceitar um dado coletado for muito alto, para diminuir a ocorrência de falsos positivos, teremos uma alta taxa de falsos negativos e vice-versa. E o tempo de verificação também dependerá do ajuste que se fizer para o limite de aceitação.

A medida da performance de um sistema de biometria deverá considerar o contexto em que o mesmo está inserido. Por exemplo, se o sistema fizer parte de uma rede local e se suas informações estiverem armazenadas em bases de dados corporativas, o tráfego de dados na rede e a capacidade de processamento dos servidores deverão ser considerados na análise da performance do sistema. O uso concorrente de dispositivos de biometria também deverá ser considerado na medida de performance.

Uma última variável que tem um forte impacto na performance dos sistemas biométricos é o comportamento do usuário frente ao sistema. Deverá ser realizado um bom trabalho de divulgação, para destacar as vantagens que advirão para os usuários. Também deverá ser preparado um treinamento que cubra todos os aspectos da interação homem-máquina, para minimizar as reações ao sistema que, com certeza, ocorrerão.

O DISPOSITIVO BIOMÉTRICO PERFEITO

Dispositivos biométricos distintos oferecem diferentes vantagens e desvantagens.

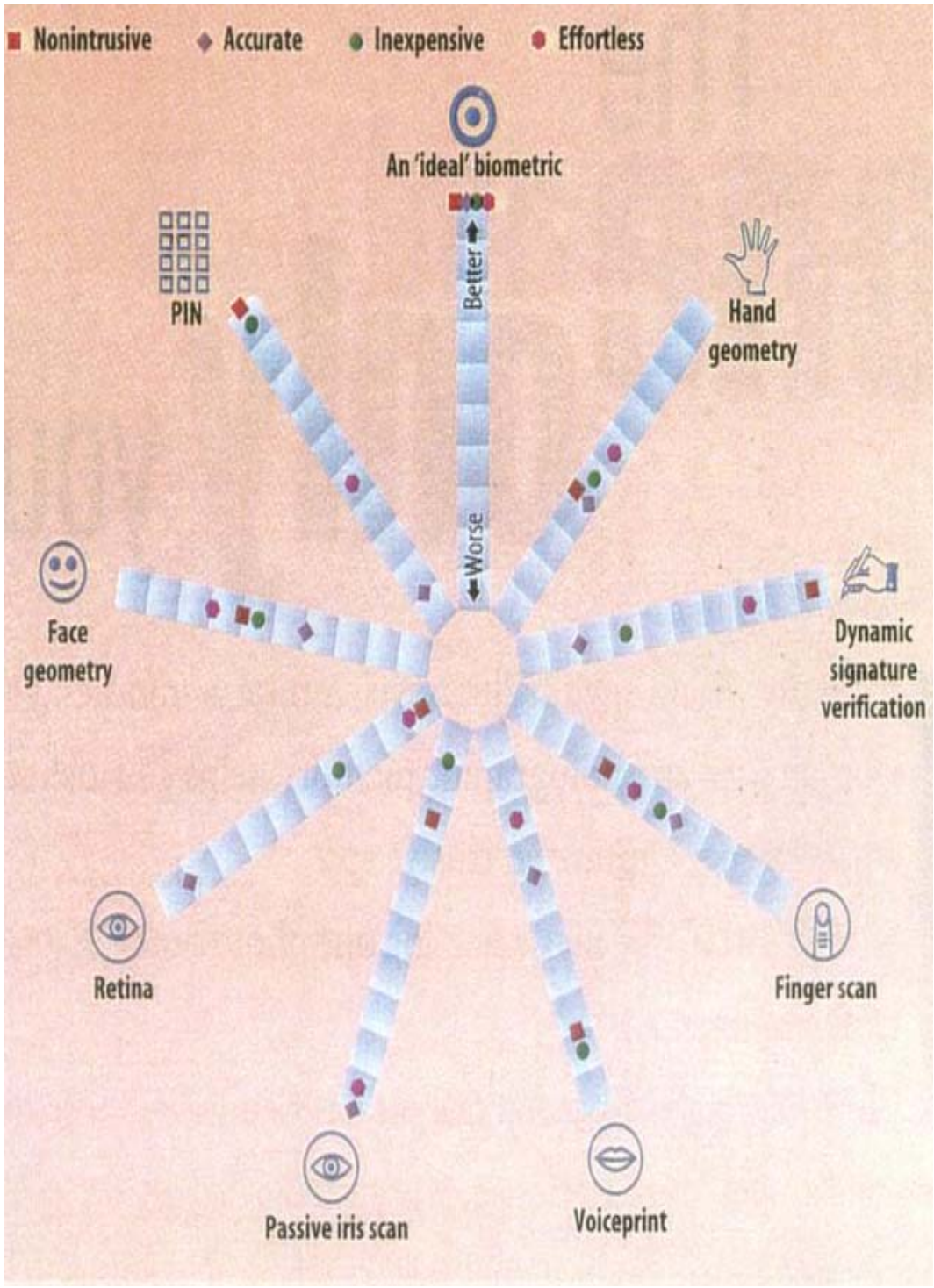


Figura AIII.1 - Vantagens e Desvantagens dos Dispositivos Biométricos

Tabela AIII.1 - Comparação entre Sistemas Biométricos-1998-IBG

Caracte-rística	**Digitais**	**Geome-tria da Mão**	**Retina**	**Íris**	**Face**	**Assinatura**	**Voz**
Facilidade de uso	Alto	Alto	Baixo	Médio	Médio	Alto	Alto
Incidência de erros	Secura, sujeira, idade	Idade, mão machucada	Óculos	Pouca iluminação	Iluminação, Idade, óculos, cabelos	Assinatura modificada	Ruído, gripes, clima
Acuidade	Alto	Alto	Muito alto	Muito alto	Alto	Alto	Alto
Aceitação pelo usuário	Média	Média	Baixa	Baixa	Média	Média	Alta
Segurança requerida	Alta	Média	Alta	Muito Alta	Média	Média	Média
Estabilidade	Alta	Média	Alta	Alta	Média	Média	Média

SISTEMA BIOMÉTRICO DO SVE-SF

Todos os sistemas biométricos possuem as fases de cadastramento e verificação. A primeira fase refere-se ao cadastramento dos dados biométricos. Depois de capturadas pelos *scanners*, as informações coletadas são submetidas a um algoritmo de compressão, sendo então gerado um gabarito (*template*), que é armazenado na base de dados de informações biométricas.

A fase de verificação ocorre durante a operação normal do sistema, quando é feita à leitura da informação biométrica do usuário, para verificar se a mesma é ou não válida. Novamente, é efetuado o processamento da informação pelo algoritmo de codificação, para

que a mesma seja comparada com a informação colhida na fase de cadastramento.

Esta fase pode ser implementada tanto para identificar quanto para autenticar pessoas. Os sistemas que procuram identificar pessoas são usados mais freqüentemente em aplicações policiais e judiciárias. Nesses sistemas, não se conhece a identidade da pessoa que se procura identificar, pois sobre ela se tem apenas uma informação coletada previamente, como suas digitais.

Nos sistemas de identificação biométrica, a pesquisa na base de dados é do tipo 1:m (um para muitos) e o resultado normalmente apresenta uma lista múltipla de possíveis candidatos, que precisará ser refinada em seguida, até identificar-se o dono da digital conhecida.

Os sistemas de autenticação, antes de efetuarem a pesquisa na base de dados, recebem uma informação que identifica previamente o usuário. Para identificar-se um indivíduo, solicita-se a ele que informe algo que ele tenha (um cartão de proximidade ou *smart card*) ou que ele saiba (uma senha) ou que ele seja (uma informação biométrica). Como a informação biométrica já será usada para autenticar o usuário, é mais adequado identificá-lo com algo que ele tenha ou possua. Como queríamos evitar a possibilidade de que o usuário viesse a perder um cartão, optamos pela senha para identificá-lo.

Nos sistemas de autenticação, o que se procura saber é se o usuário é quem ele diz ser. A pesquisa é de 1:1, onde, depois de informada a matrícula do usuário, o sistema acessa a base de dados relativa àquela matrícula e exibe o nome do usuário no leitor do teclado para que esse possa certificar-se que foi corretamente identificado. Em seguida, o sistema solicita ao usuário que coloque seu dedo sobre o leitor.

A informação captada é então codificada e comparada com os gabaritos (*templates*) armazenados nos registros da base de dados para aquele usuário (dois ou três registros). Para efetuar a validação, o sistema faz uma comparação entre os dados colhidos na leitura e o armazenado na base de dados, devolvendo um resultado que tem que ser superior ao limiar de aceitação (*threshold*) definido para o usuário. Em seguida, é enviada uma mensagem para o usuário, informando-o se ele foi aceito ou rejeitado.

A medida de contingência para os senadores que não conseguirem ter suas digitais capturadas ou que possuam um elevado índice de falsos negativos, recebem senhas para acessar o sistema.

As informações das digitais dos senadores serão armazenadas na base de dados de informações biométricas.

A base de dados de transações armazenará todos os acessos ao sistema por meio de biometria, seja no cadastramento, na identificação e na autenticação.

CONSIDERAÇÕES SOBRE O CADASTRAMENTO DE DIGITAIS

Um cadastramento bem feito das digitais dos usuários é um fator crítico para o sucesso do sistema. Se essa fase não tiver a atenção requerida, a implantação do sistema pode fracassar. As digitais precisam ser colhidas com a maior exatidão e qualidade possível. O leitor e o dedo deverão estar limpos e o dedo deverá ser colocado corretamente no leitor, centralizado e sem inclinações.

Cabe aqui uma rápida explicação do que ocorre quando uma digital é colhida. Após a coleta da digital, o sistema procura identificar e classificar as suas minúcias, que são as características únicas de cada digital. Se a digital não oferecer um número mínimo de informações que permita ao sistema catalogá-la, para uma dada qualidade especificada, a leitura é rejeitada.

Grande parte dos sistemas de biometria estabelece esse fator qualidade para validar uma digital coletada. A qualidade é medida em número de pontos. Normalmente, em sistemas de controle de acesso, não se procura obter a qualidade máxima possível na coleta dos dados biométricos, pois isso poderia ocasionar um elevado índice de falsos negativos. Apenas em instalações de alta segurança deve-se trabalhar com índices de qualidade muito elevados. Também se estabelece um índice mínimo de aceitação, abaixo do qual a qualidade é rejeitada, para se evitar a ocorrência de falsos positivos.

O índice ideal deverá ser determinado para cada caso. Na verdade, a definição do limiar de aceitação da informação coletada (*threshold*) deverá ser feita com base em uma análise de quão importante é nunca aceitar usuários não autorizados ou, então, nunca rejeitar usuários autorizados.

A primeira tentativa de coleta da digital sempre é feita com uma exigência de qualidade média. Se não se consegue, vai-se baixando gradativamente a exigência, até se atingir um valor que permita a coleta de um mínimo de pontos que possam ser trabalhados, sem perda de segurança. Para as pessoas que não conseguem ter sua digital colhida nem

com esse nível mínimo de qualidade, como já foi dito anteriormente, é fornecida uma senha para que o usuário possa autenticar-se.

Depois de colhida a digital, identificada e classificada, é gerado um gabarito (*template*) com essas informações, que é então armazenado na base de dados, dando-se por concluído o cadastramento. Observe-se que não se armazena a digital do usuário, mas apenas informações obtidas de cálculos matemáticos efetuados sobre suas minúcias.

Quanto maior a qualidade da digital obtida no cadastramento, mais informações serão colhidas sobre a mesma e mais fácil será o reconhecimento do usuário quando do uso rotineiro do sistema. Isso porque, quando o usuário submete sua digital para reconhecimento, o número de pontos analisados é inferior àqueles coletados no cadastramento, pois não é preciso uma correspondência perfeita entre os gabaritos (*templates*) do cadastramento e da leitura para autenticar um usuário.

Se um número determinado de pontos for idêntico, o que é determinado pelo limiar de aceitação (*threshold*) especificado para aquele usuário, o mesmo é aceito. Isso permite que leituras de dedos sujos, ligeiramente inclinados ou com pequenos machucados não impeçam a autenticação do usuário. Entretanto, digitais mal colhidas no cadastramento terão menos pontos armazenados para serem confrontados com os captados na leitura, o que exige que os gabaritos sejam quase que idênticos para que haja o reconhecimento. Isso aumenta o número de falsos negativos. Ou seja, quanto mais bem feito for o cadastramento, maiores as variações aceitas na fase de leitura de verificação e menor o índice de rejeições.

O limiar de aceitação na fase de leitura é expresso por um número, que representa a qualidade da leitura. Quanto maior esse número, maior a necessidade de coincidência entre os pontos coletados na leitura com os do cadastramento. Mas a experiência também mostra que um valor intermediário é mais do que adequado para as necessidades dos sistemas de controle de acesso, reduzindo-se o número de falsos positivos para um valor próximo de zero e sem gerar um número excessivo de falsos negativos.

Se, ainda assim, o usuário continuar com dificuldades para ser reconhecido, deve-se tentar um novo cadastramento. Se os problemas persistirem, estaremos então diante do segundo caso em que é necessária a atribuição de senha para o usuário, pois, apesar de ter sido possível a coleta de sua digital no cadastramento, sua qualidade não é suficiente para autenticá-lo.

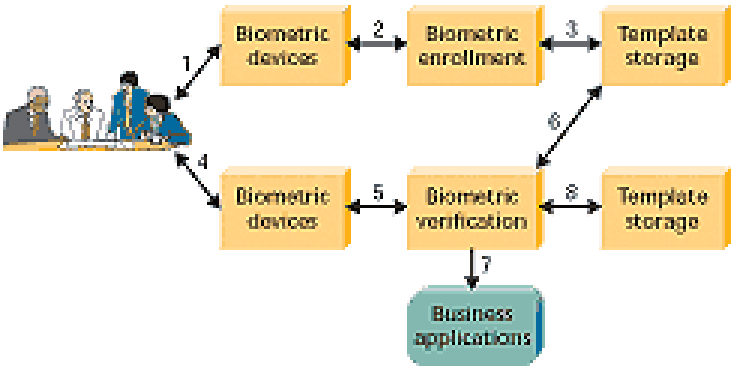


Figura AIII.2 - Coleta de Digitais

TECNOLOGIAS DE COLETA BIOMÉTRICA DE DIGITAIS

A aura de criminalidade que acompanha o termo impressão digital não tem impedido de forma significativa a aceitação da tecnologia de leitura biométrica de digitais, porque os dois métodos de autenticação são muito diferentes. Os sistemas que tratam de identificação por impressão digital colhem e armazenam a imagem real dos dedos dos seres humanos, com todos os seus detalhes. Esses sistemas são usados há décadas na condução de investigações criminais. O espaço em meio eletrônico necessário para armazenar uma impressão digital de qualidade é da ordem de 250 KB.

Já os sistemas de coleta biométrica de digitais também colhem a impressão digital, mas não armazenam sua imagem completa. O espaço necessário para armazenar os dados relativos a uma digital é da ordem de 250 a 1000 bytes. Após os dados serem extraídos, a imagem da impressão digital é descartada. Dessa forma, é impossível se reconstruir a impressão digital original com base nas informações coletadas e armazenadas em um sistema de coleta biométrica de digitais.

CARACTERÍSTICAS DAS IMPRESSÕES DIGITAIS

A impressão digital humana é composta de vários tipos de padrões de sulcos, descritos da seguinte forma: curvas para a esquerda, curvas para a direita, arcos, espirais e arcos fechados. As curvas representam quase dois terços de todas as impressões digitais, as espirais são quase um terço e os arcos representam algo em torno de 5 a 10% do total. Essa classificação é relevante em muitas aplicações policiais de larga escala, mas são raramente

usadas em autenticação biométrica.

Já as minúcias são as descontinuidades que interrompem o fluxo suave dos sulcos e são a base para a maioria dos sistemas de autenticação biométrica de digitais. Codificadas no final dos anos 1800, as minúcias são, de forma geral, os pontos onde os sulcos terminam ou se bifurcam. Muitos outros pontos de minúcias existem, incluindo os pontos (sulcos muito pequenos), as ilhas (sulcos um pouco maiores que os pontos, que se encontram entre dois outros sulcos divergentes), lagos (espaços vazios entre sulcos divergentes), fendas (cortes sobressaindo de um sulco), pontes (pequenos sulcos que conectam dois sulcos adjacentes) e cruzamentos de sulcos.

Outra característica essencial utilizada para a autenticação biométrica digital é o ponto central da impressão digital, ao redor do qual se localizam as espirais, as curvas e os arcos.

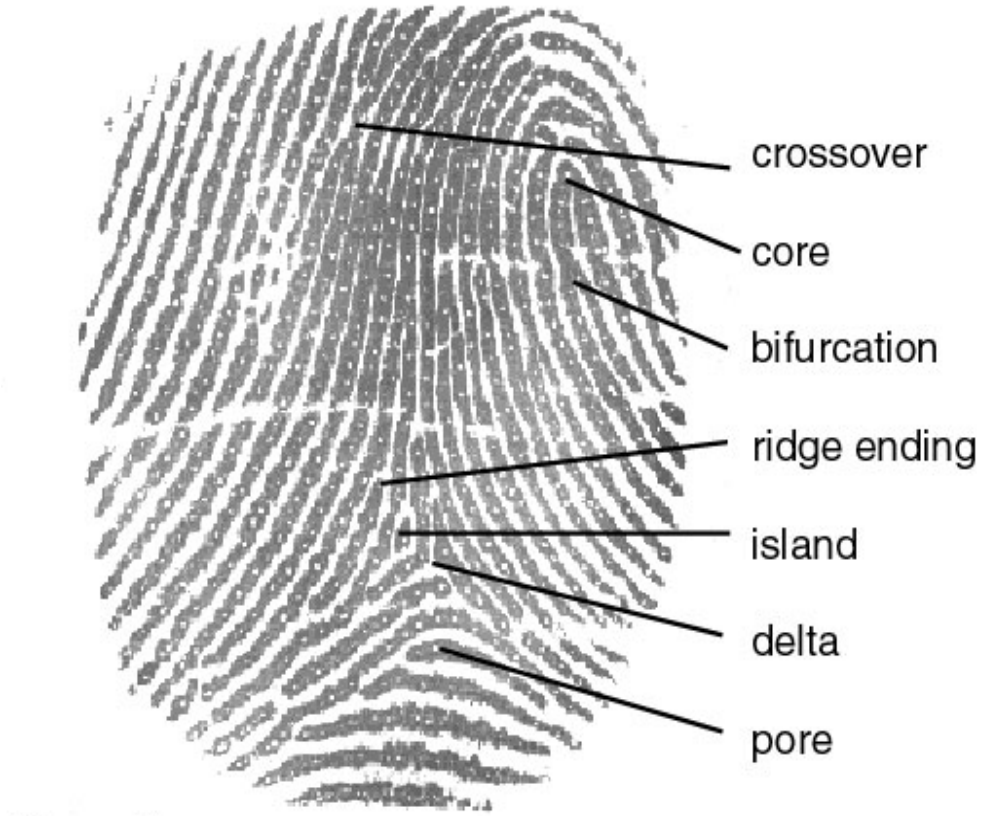


Figura AIII.3 - Propriedade das Impressões Digitais

EXTRAÇÃO DAS PROPRIEDADES DAS IMPRESSÕES DIGITAIS

Uma vez que uma imagem de alta qualidade seja capturada, há vários passos que precisam ser seguidos para converter suas propriedades únicas em um gabarito compacto. Esse processo, conhecido como extração de características, está no âmago da tecnologia de digitalização biométrica. Cada fabricante de leitores biométricos de digitais tem um algoritmo proprietário de extração de características e guardam esses algoritmos como segredo industrial.

Entretanto, o processo seguido é baseado em um conjunto de princípios básicos. Após a captura de uma imagem de qualidade, esta precisa ser convertida para um formato que possa ser facilmente utilizado. Se a imagem é capturada em tons de cinza, áreas que sejam mais claras que um determinado limiar são descartadas e aquelas mais escuras são transformadas em preto.

A localização das minúcias começa após este processamento inicial da imagem. Nesse ponto, mesmo uma imagem que possua muita precisão terá distorções e minúcias falsas que precisam ser descartadas. Anomalias causadas por cicatrizes, suor ou sujeira são minúcias falsas e os algoritmos procuram localizar pontos e padrões que não são comuns em uma digital, como uma marca diferenciada encontrada em uma ilha (que provavelmente é falsa) ou um sulco que cruza perpendicularmente dois outros (provavelmente uma cicatriz ou sujeira). Uma porcentagem alta de falsas minúcias é descartada nesse processo.

O ponto em que um sulco termina ou se bifurca são as minúcias mais comuns e são usadas pela maioria das aplicações. Adicionalmente, a distribuição espacial das minúcias e o ângulo entre as mesmas também são usados.

Complementarmente à localização e ao ângulo da minúcia, alguns fabricantes as classificam por tipo e qualidade. A vantagem dessa classificação é que as pesquisas tendem a ser mais rápidas, pois uma minúcia que tenha uma particularidade especial pode ser diferente o suficiente para conduzir autenticar uma pessoa.

A obtenção de boas imagens dos sulcos e de suas minúcias não é uma tarefa simples. A impressão digital é uma área pequena a partir da qual são feitas as medidas que serão capturadas e armazenadas para uso biométrico. Mecanismos cada vez mais sofisticados são desenvolvidos para capturar a imagem das impressões digitais com suficiente detalhe e resolução. Utilizam-se tecnologias óticas, capacitivas, termais e ultra-sônicas para a construção dos leitores de digitais.

A tecnologia ótica é a mais antiga e a mais largamente utilizada. O dedo é colocado numa superfície plana com um revestimento especial, normalmente feita de vidro ou de plástico transparente, dependendo de cada fabricante. O revestimento é aplicado para minimizar a latência (ou fantasmas) que as digitais deixam no vidro, degradando o reconhecimento das digitais das pessoas que vêm a seguir, pois suas digitais se sobrepõem às marcas que ficaram, gerando uma imagem dupla, o que dificulta o reconhecimento.

O leitor ótico tem vários pontos fortes: são os mais resistentes; podem suportar, até um certo ponto, variações de temperatura; são relativamente baratos e fornecem resoluções de até 500 DPI. Os pontos negativos dessa tecnologia incluem seu tamanho, que precisa ser relativamente grande para obter uma boa imagem e marcas de digitais que ficam nos leitores. Com o tempo, a proteção do vidro do leitor e o CCD vão se desgastando, reduzindo a precisão dos equipamentos.

A tendência atual é em direção aos leitores capacitivos. Esta tecnologia tem obtido cada vez mais aceitação desde que foi introduzida, nos últimos anos da década passada. Esses equipamentos são constituídos de um circuito integrado e seu funcionamento é baseado em capacitores. O sensor de circuito integrado funciona como um dos condutores do capacitor e o dedo como o outro. A capacitância entre as duas superfícies é convertida em uma imagem digital monocromática de oito bits, que é então processada e armazenada.

Os leitores capacitivos geralmente produzem uma qualidade de imagem melhor que os leitores óticos numa superfície de coleta menor. Como o circuito integrado é constituído de mais ou menos 200 a 300 linhas e colunas, em uma pastilha de apenas 1cm x 1,5cm, os mesmos podem capturar imagens muito detalhadas. O pequeno tamanho do circuito integrado indica que seu custo deverá cair significativamente nos próximos anos. Devido ao seu tamanho, eles podem ser instalados em pequenos dispositivos onde não é possível colocar um leitor ótico.

A durabilidade dos leitores capacitivos ainda não é conhecida, apesar dos fabricantes estarem usando películas de proteção para esses dispositivos. Adicionalmente, com a redução do tamanho do sensor, torna-se ainda mais importante que se assegure que o cadastramento e a verificação das digitais seja feito com muito cuidado.

A tecnologia de leitores termais baseia-se no uso de sensores muito pequenos que produzem uma boa imagem da digital e é independente do contraste. Ainda não é muito utilizada.

A tecnologia de ultra-som, embora também não seja muito utilizada, está sendo considerada superior às demais. Ela transmite ondas sonoras e mede a distância baseada na impedância do dedo, da superfície do leitor e do ar. O ultra-som é capaz de penetrar na sujeira de um dedo, eliminando um dos maiores problemas da tecnologia ótica. Até que a tecnologia de ultra-som obtenha um uso mais abrangente, será difícil verificar sua performance.

Entretanto, projetos-piloto que se utilizam dessa tecnologia mostram que seu futuro é promissor. A tecnologia de ultra-som combina os pontos fortes da tecnologia ótica com os da tecnologia dos circuitos integrados.