UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE UM AMBIENTE SEGURO PARA DISTRIBUIÇÃO DE ÁUDIO E VÍDEO, VIA REDE SEM FIO, NO SENADO FEDERAL

AUDRIM MARQUES DE SOUZA
LEIFE GONÇALVES MONTALVÃO
KELSEN MARMO RAMOS

ORIENTADOR: GEORGES AMVAME-NZE

MONOGRAFIA DE ESPECIALIZAÇÃO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: UNB.LABREDES.MFE.014/2006

BRASÍLIA / DF: SETEMBRO/2006

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

ESTUDO DE UM AMBIENTE SEGURO PARA DISTRIBUIÇÃO DE ÁUDIO E VÍDEO, VIA REDE SEM FIO, NO SENADO FEDERAL

AUDRIM MARQUES DE SOUZA
LEIFE GONÇALVES MONTALVÃO
KELSEN MARMO RAMOS

MONOGRAFIA 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:

GEORGES AMVAME-NZE, Mestre, UnB
(ORIENTADOR)

ROBSON DE OLIVEIRA ALBUQUERQUE, Mestre, UnB
(EXAMINADOR INTERNO)

ODACYR LUIZ TIMM JÚNIOR, Mestre, UnB
(EXAMINADOR EXTERNO)

BRASÍLIA/DF, 26 DE SETEMBRO DE 2006.

FICHA CATALOGRÁFICA

SOUZA, AUDRIM MARQUES DE
MONTALVÃO, LEIFE GONÇALVES
RAMOS, KELSEN MARMO
ESTUDO DE UM AMBIENTE SEGURO PARA DISTRIBUIÇÃO DE ÁUDIO E VÍDEO, VIA REDE SEM FIO, NO SENADO FEDERAL [Distrito Federal] 2006.
xii,69p., 297 mm (ENE/FT/UnB, Especialização, Engenharia Elétrica, 2006).

Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. WI-FI 2. SEM FIO 3. ÁUDIO 4.VÍDEO

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

SOUZA, AUDRIM M., MONTALVÃO, LEIFE G., RAMOS, KELSEN M., (2006). ESTUDO DE UM AMBIENTE SEGURO PARA DISTRIBUIÇÃO DE ÁUDIO E VÍDEO, VIA REDE SEM FIO, NO SENADO FEDERAL. Monografia de Especialização, Publicação UNB.LABREDES.MFE.014/2006, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília , DF, 69p.

CESSÃO DE DIREITOS

AUDRIM M. DE SOUZA, LEIFE GONÇALVES MONTALVÃO, KELSEN MARMO RAMOS
ESTUDO DE UM AMBIENTE SEGURO PARA DISTRIBUIÇÃO DE ÁUDIO E VÍDEO, VIA REDE SEM FIO, NO SENADO FEDERAL.
GRAU/ANO: Especialista/2006.

_____
AUDRIM MARQUES DE SOUZA

_____
LEIFE GONÇALVES MONTALVÃO

_____
KELSEN MARMO RAMOS

Endereço: Senado Federal , Praça dos Três Poderes
Anexo II bloco B
CEP 70.165-900 – Brasília – DF - Brasil

A Deus, pai supremo.
À minha esposa Waldirene e às minhas filhas Luiza e Geovana,
as quais me ensinam a cada dia como é bom viver.
Audrim

À minha esposa Flávia e aos meus filhos César Adriano e Júlia,
pela compreensão e apoio.
Kelsen

A Deus pelos objetivos alcançados.
Aos meus Pais, Francelino e Auta, pelo exemplo de vida que me deram.
À minha esposa Nívian e aos meus filhos Norton, Ana Luisa e Natália,
pela compreensão e apoio no dia a dia.
Leife

AGRADECIMENTOS

Gostaríamos de agradecer, à Mesa Diretora do Senado Federal, na pessoa do presidente, do primeiro secretário e dos demais membros, que contribuiu sobremaneira para a realização deste curso.

Agradecemos, também, ao doutor Agaciel da Silva Maia, diretor geral do Senado Federal, pelo reconhecimento e apoio às iniciativas de aprimoramento profissional que, entre outras ações, culminou na aprovação e realização deste curso de pós-graduação para os funcionários desta casa.

Ao Diretor da Secretaria de Eletrônica - STEL, Sr. Agnaldo Scárdua, por nos proporcionar a participação neste curso.

Ao Unilegis e Prodasen, pela elaboração, estruturação e coordenação deste curso de especialização.

À STEL por disponibilizar recursos que propiciaram a construção de um grande laboratório audiovisual, na forma de um dos maiores centros de documentação – CEDOC, digital do país. O qual foi imprescindível para elaboração desta monografia.

Aos colegas da STEL, pelo suporte, ajuda e troca de experiências na área de digitalização de áudio, que certamente enriqueceram a elaboração desta monografia.

Aos colegas do nosso curso de Gestão em Tecnologia da Informação, que durante todo o período do curso muito nos apoiaram, demonstrando o sentimento de equipe e companheirismo.

Ao professor Georges Amvame-Nze, que mesmo à distância, sabiamente conduziu a orientação deste trabalho. Enfim, a todos profissionais envolvidos neste grande desafio, nossa profunda admiração e alegria por compartilharem suas idéias e expectativas em torno de um projeto que está se tornando, sem dúvida, um novo paradigma para os meios de comunicação.

RESUMO

O objetivo deste trabalho é apresentar as possibilidades de distribuição de áudio e vídeo utilizando uma rede sem fio no ambiente do Senado Federal. O Sistema Wi-Fi foi escolhido para estudo e avaliação. São apresentadas as características da rede sem fio escolhida. São descritas as técnicas de segurança adotadas pelo padrão 802.11 em suas diversas versões. São apresentadas também as ferramentas para detecção de possíveis vulnerabilidades permitindo ao gestor de tecnologia da informação encontrar falhas e soluções para os problemas encontrados. Descreve-se a evolução histórica referente à captação, distribuição e armazenamento de áudio no Senado Federal e como fruto da evolução digital, descreve-se também a mais recente aquisição de um sistema moderno de arquivamento baseado em discos rígidos e fitas magnéticas inteligentes (SAIT), possibilitando assim o armazenamento digital de áudio e vídeo obtido das Sessões Plenárias, Comissões e Sessões do Congresso Nacional realizadas no Senado Federal.

EVALUATION OF A SAFE ENVIRONMENT FOR AUDIO AND VIDEO DISTRIBUTION, USING WIRELESS LOCAL AREA NETWORK, IN THE FEDERAL SENATE.

ABSTRACT

The goal of this work is to introduce the audio and video distribution possibilities using wireless local area network in the environment of the Federal Senate. The system Wireless Fidelity (Wi-Fi) was chosen for study and evaluation. The features of the Wi-Fi are showed. Are described the safety techniques adopted by the standard 802.11 in their several versions and introduced the tools for possible vulnerabilities detection allowing to I.T. manager find out fails and solutions for the detected problems. It describes the historical evolution regarding the capitation, distribution and storage of audio in the Federal Senate. As a consequence of the digital evolution, also it describes the most recent acquisition of a modern system of archives based on hard disks and intelligent magnetic tapes (SAIT), enabling thus the digital storage of audio and video produced from the Plenary Sessions, Committees and Sessions of the National Congress accomplished in the Federal Senate.

ÍNDICE

Item Página

1 INTRODUÇÃO 1

1.1 JUSTIFICATIVA DO TRABALHO 1
1.2 ESTRUTURA DA MONOGRAFIA 3

2 REDES SEM FIO 6

2.1 INTRODUÇÃO 6
2.2 ELEMENTOS DE REDE SEM FIO 6
2.2.1 – FREQUÊNCIA: *6*
2.2.2 – PROPAGAÇÃO: *8*
2.2.3 – MODULAÇÃO: *11*
2.3 CONEXÃO EM REDE SEM FIO 16
2.3.1 – ESTRUTURA E AUTENTICAÇÃO EM UMA REDE SEM FIO: *16*
2.3.2 – CSMA/CA – CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE: *17*
2.3.3 – ESSID - EXTENDED SERVICE SET IDENTIFIER: *18*
2.3.4 – BEACON: *18*
2.3.5 – CONFIGURAÇÕES DE REDES: *19*
2.3.6 – PADRÕES ATUAIS PARA AS REDES WI-FI [8] *20*
2.3.6.1 - 802.11 b 21
2.3.6.2 - 802.11a 22
2.3.6.3 - 802.11g 22
2.3.6.4 - 802.11i 23
2.3.6.5 - 802.11n 23
2.3.6.6 - 802.1x 23

3 SEGURANÇA EM REDES SEM FIO 25

3.1 TÉCNICAS DE SEGURANÇA 25
3.1.1 – WEP - Wired Equivalent Privacy *26*
3.1.2 – Endereço MAC (Media Access Control) *28*
3.1.3 – WPA – Wi-Fi Protected Access Equivalent Privacy *28*
3.1.4 – VPN - Virtual Private Network *30*
3.2 VULNERABILIDADES EM REDES SEM FIO 31
3.2.1 – Vulnerabilidade nos Protocolos *31*
3.2.1.1 – Vulnerabilidade no WEP 31
3.2.1.2 – Vulnerabilidade no WPA 32
3.2.2 – Vulnerabilidades Físicas *33*
3.2.3 – Vulnerabilidades Espaciais *35*
3.3 FERRAMENTAS PARA TESTE DE VULNERABILIDADES EM REDES SEM FIO 36
3.3.1 – AIRCRACK *36*
3.4 TÉCNICAS DE ATAQUES A REDES SEM FIO 37
3.4.1 – MAC SPOFFING: *38*
3.4.2 – NEGAÇÃO DE SERVIÇO (DoS) *39*
3.4.3 – ASSOCIAÇÃO MALICIOSA: *39*
3.4.4 – ACESSO NÃO AUTORIZADO: *40*

3.4.5 – WARDRIVING: *40*

4 SEGURANÇA DENTRO DO AMBIENTE SENADO FEDERAL..... 42

4.1 INTRODUÇÃO 42

4.2 SISTEMAS DE ARMAZENAMENTO..... 44

4.2.1 – Armazenamento Analógico: *45*

4.2.2 – Armazenamento Digital - Minidisc: *46*

4.2.3 – Armazenamento Digital - PetaSite:..... *47*

4.3 STREAMING DE ÁUDIO 49

4.3.1 – Ferramentas para Streaming: *49*

4.3.2 – Servidores de Streaming: *50*

4.4 SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DO SENADO FEDERAL....51

5 CONCLUSÃO 56

6. REFERÊNCIAS BIBLIOGRÁFICAS..... 58

ANEXO I – DECRETO Nº 4.553, DE 27 DE DEZEMBRO DE 2002 61

ÍNDICE DE FIGURAS

Figura Página

Figura 2.1– Espectro Eletromagnético. 7
Figura 2.2 – Divisão do espectro eletromagnético no Brasil. 7
Figura 2.3 – Modelo Terra Plana. 9
Figura 2.4 – Processo de modulação para transmissão. 11
Figura 2.5 – Processo de modulação FHSS. 13
Figura 2.6 – Processo de modulação DSSS. 14
Figura 2.7 – Processo de modulação OFDM. 15
Figura 2.8 – Processo de autenticação no padrão IEEE 802.11. 17
Figura 2.9 – Topologia Ad-Hoc. 19
Figura 2.10 – Topologia do tipo Infra-Estrutura. 20
Figura 3.1 – Tela do Airmon. 37
Figura 3.2 – Símbolos empregados no Warchalking. 41
Figura 4.1 – Tablets com sistema Wi-Fi instalado no plenário no Senado Federal. 43
Figura 4.2 – Esquema simplificado do sistema de armazenamento do sinal de áudio no Senado Federal. 44
Figura 4.3 – Sistema de armazenamento analógico 45
Figura 4.4 – Mídia de armazenamento do tipo minidisc. 46
Figura 4.5 – Estação de captura de áudio e vídeo 48
Figura 4.6 - Petasite 48

LISTA DE ABREVIATURAS E SIGLAS

ACK – Acknowledgment (Reconhecimento)
ADSL – Asymmetric Digital Subscriber Line (Linha digital assimétrica de assinante)
AES – Advanced Encryption Standard (Padrão de Criptografia Avançada)
AP – Access Point (Ponto de Acesso)
ARP – Address Resolution Protocol (Protocolo de Resolução de Endereços)
CDMA – Code Division Multiple Access (Acesso Múltiplo por Divisão em Código)
CRC-32 – Cyclic Redundance Check 32 (Checagem de Redundância Cíclica 32)
CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance (Acesso múltiplo de sentido de Portador/Vacância de Colisão)
DES – Data Encrypt Standard (Dado Padrão de Encriptação)
DHCP – Dynamic Host Configuration Protocol (Protocolo de Configuração de Servidor Dinâmico)
DoS – Denial of Service (Negação de Serviço)
DSSS – Direct Sequence Spread Spectrum (Espalhamento Espectral em Seqüência Direta)
EAP – Extensible Authentication Protocol (Protocolo de Autenticação para o acesso a rede)
ESSID – Extended Service Set Identifier (Identificador da rede)
FHSS – Frequency Hopping Spread Spectrum (Espalhamento Espectral em Seqüência Saltante)
GO – Geometrical Optics (ótico geométrico)
GPS – Global Positioning System (Sistema de Posicionamento Global)
HTTP – HyperText Transfers Protocol (Protocolo de Transferência de Hipertexto)
IEEE – Institute of Electrical and Electronics Engineers (Instituto de Engenheiros Elétricos e Eletrônicos)
IP – Internet Protocol (Protocolo Internet)
ISM – Industrial, Scientific e Medical (industrial, científico e médico)
IV – Initialization Vector (Vetor de inicialização)
LAN – Local Area Network (Rede de Computadores Local)
MAC – Media Access Control (Controle de Acesso ao Meio)
MAN – Metropolitan Area Network (Rede Metropolitana)
MIC – Message Integrity Check (Código de Integridade da Mensagem)
MOREQ - Modelo de Requisitos para a Gestão de Arquivos Eletrônicos
OFDM – Orthogonal Frequency Division Multiplexing (Divisão de Freqüência Orthogonal de Multiplexação)
PCI – Peripheral Component Interconnect (Interconexão de Componente Periféricos)
PCMCIA – Personal Computer Memory Card International Association (Associação Internacional de Cartões de Memória de Computadores Pessoais)
PDA – Personal Digital Assistance (Assitente Digital Pessoal)
PSK – Pre-Shared Key (Chave Compartilhada)
QoS – Quality of Service (Qualidade de Serviço)
RADIUS – Remote Authentication Dial-In User Service
RSN – Robust Security Network
S-AIT – Super Advanced Inteligent Tape
SGAD - Sistema de Gerenciamento de Arquivos Digitais
SSID – Service Set IDentifier
UTD – Uniform Theory of Diffraction
TCP – Transmission Control Protocol (Protocolo de Controlo de Transmissão)
TI – Tecnologia da informação
TKIP – Temporal Key Integrity Protocol (Protocolo Temporal de Integridade de Chave)
USB – Universal Serial BUS
VPN – Virtual Private Network (Rede Privada Virtual)

WEP – Wired Equivalency Privacy (Privacidade Equivalente ao sistema com cabo)
Wi-Fi – Wireless Fidelity (Fidelidade Sem Fio)
WIRELESS – Sem Fio
WAN – Wide Area Network (Rede Remota de Computadores)
WPA – Wi-Fi Protected Access Equivalent Privacy
WLAN – Wireless Local Area Network (Redes Locais Sem Fio)
WWW – World Wide Web (Rede de Alcance Mundial)
WWAN – Wireless Wide Area Network (Rede de longa Distância sem fio)

1 INTRODUÇÃO

1.1 JUSTIFICATIVA DO TRABALHO

Este trabalho tem como objetivo avaliar as possibilidades para a transmissão de streaming de áudio e vídeo em um ambiente seguro dentro do Senado Federal.

Com o advento das tecnologias atuais e sobretudo com o "*boom*" provocado pela internet e pelos aparelhos celulares, surgiu, nos últimos anos a necessidade de aliar-se a mobilidade adquirida com os celulares com a facilidade ao acesso da informação adquirida com a internet. Este trabalho está voltado para a pesquisa dos modelos de transmissão de sinais de áudio e vídeo através de redes sem fio em um ambiente seguro. A estrutura de rede sem fio e o protocolo escolhido para a realização do trabalho foi o Wi-Fi, por tratar-se de uma tecnologia atual com grande aceitação pelo mercado e por, inclusive já possuir redes montadas dentro do Senado Federal. Além disso verificamos que os objetivos estão dentro daqueles descritos no curso de gestão de tecnologia da informação, ou seja, possibilitar a verificação das influências e do impacto na escolha de uma nova tecnologia dentro do ambiente gestacional.

Sabe-se que no ambiente em questão (Senado Federal), diversas informações como discursos proferidos em Comissões Parlamentares de Inquérito - CPI's - ou em reuniões que envolvam a segurança nacional, devem estar a disposição, muitas vezes, apenas de pessoas autorizadas (geralmente Senadores, Deputados e outras autoridades). Estas informações devem ser disponibilizadas em tempo hábil de forma a garantir a celeridade em processos que são de interesse para todo o país. Além do fator tempo e da disponibilidade, devemos levar em consideração o fator segurança, que em se tratando do poder legislativo do país, é primordial que se mantenha dentro de parâmetros extremamente elevados, haja vista fatos recentes ocorridos e que levaram a escândalos enormes (como os grampos telefônicos).

O termo Wi-Fi (Wireless Fidelity) é na realidade uma marca da Wi-Fi Alliance [20], uma associação da industria que tinha a finalidade de certificar os diversos equipamentos que seguiam o protocolo IEEE 802.11, o termo Wi-Fi se associa à transmissão de dados com alta qualidade.

Como a rede Wi-Fi é capaz de prover mobilidade através de aparelhos cada vez menores, como os PDA's (Personal Digital Assistance) e os pilares da segurança da informação estão calcados na confidencialidade, integridade e disponibilidade, criou-se um ambiente propício para o estudo acadêmico desta estrutura dentro do ambiente em questão.

A primeira rede sem fio foi desenvolvida na Universidade do Havaí em 1971, para conectar computadores entre as ilhas sem utilizar a estrutura de fios. Nos anos 80 surgiram as primeiras redes sem fio de computadores pessoais, nesta época os principais meios de transmissão eram por raios infravermelhos, fato que limitava a transmissão pois está sujeita a forte interferência devido aos obstáculos. Em meados dos anos 90, o IEEE (*Institute of Electrical and Electronics Engineers)* estabeleceu um comitê para definir protocolos de trasmissão para redes sem fio, as WLANs (*Wirerless Local Networks),* este comitê foi o 802.11. Em 1999 foram aprovados os padrões IEEE 802.11b e 802.11a.

O IEEE continua trabalhando nos padrões para a industria de WLANs e os principais padrões adotados atualmente para as mesmas são os seguintes:

802.11a - Opera na freqüência de 5 GHz com taxa de 54 Mbps.

802.11b - Opera na freqüência de 2,4 Ghz com taxa de 11 Mbps

802.11g - Opera na freqüência de 2,4 GHz com taxa de 54 Mbps.

802.11i - Este protocolo substitui o sistema de criptografia WEP (**W**ired **E**quivalent **P**rivacy) empregado nos padrões anteriores a ele e opera com o AES (Advanced Encryption System) assim, trata-se de um padrão que preza pela segurança nas redes Wi-Fi.

A tabela 2.1 apresentada a seguir resume os padrões apresentados:

Grupo de tarefa	O que faz
802.11d	As modificações das especificações 802.11 iniciais para compatibilidade com regulamentos em outros países
802.11e	Adiciona qualidade de serviço (QoS) ao 802.11 a,b e g para aplicações de voz e vídeo
802.11f	Melhora a autenticação na comunicação entre pontos de acesso
802.11h	Modificações de outras especificações 802.11 para compatibilidade com

	regulamentos europeus na banda de 5 GHz
802.11i	Melhora a segurança das redes sem fio
802.11j	Modificações de outras especificações 802.11 para compatibilidade com regulamentos japoneses na banda de 5 GHz
802.11k	Fornece melhor informação da intensidade de sinal e outros atributos físicos de rádio
802.11l	Não existe porque um "L" minúsculo é muito parecido com o número 1
802.11m	Modificações e correções menores para as especificações previamente publicadas
802.11n	Concebido para aumentar o throughput bruto de redes sem fio paea 100 Mbps ou mais alto e assegurar que um número maior do throughput bruto seja realmente utilizável

Tabela 2.1– Visão geral dos grupos de trabalho do 802.11

Para se conectar dispositivos inteligentes à rede, como um palm ou um notebook, alguns fatores importantes como a segurança, a capacidade de transmissão de dados e a potência da antena, deverão ser observados. Todos estes fatores serão analisados nos capítulos seguintes.

A medida em que os palms ganharam capacidade multimídia e velocidade de transferência, tornou-se viável a transmissão de sinais de áudio e vídeo via rede sem fio. A tecnologia Wi-Fi permitiu adaptar estes dispositivos de forma bastante econômica para os padrões atuais e com isso assegurando a mobilidade almejada. Para os testes deste trabalho optou-se pelo Palm fabricado pela palm OS.

1.2 ESTRUTURA DA MONOGRAFIA

O texto apresentado neste trabalho está organizado como descrito a seguir. No capítulo 2 são apresentadas as características de uma rede sem fio. São apresentados aspectos como a freqüência utilizada, como ocorre a propagação do sinal de radiofreqüência, inclusive com a descrição do modelo de propagação. As diferentes técnicas de modulação, empregadas nos diversos padrões adotados pelo IEEE, com a intenção de se aumentar a taxa de transmissão,

são apresentadas de forma sucinta. O capítulo também apresenta os elementos componentes de uma rede de transmissão sem fio e as diferentes arquiteturas que podem ser obtidas para as mesmas. É apresentada a definição do padrão IEEE 802.11, com maior ênfase em cada um dos membros da família seja o 802.11a, 802.11b. Foi realizado um estudo a respeito das diferentes taxas de transmissão (*bit rate*) apresentadas por cada um deles. O capítulo encerra-se com uma abordagem a respeito do modo de conexão em uma rede sem fio entre a estação cliente e o servido (ponto de acesso).

O capítulo 3 trata dos aspectos de segurança em redes sem fio, inicia-se com a descrição das técnicas de segurança adotadas pelo padrão IEEE 802.11, como as chaves WEP e WPA e os procedimentos para tornar ativas estas técnicas. Em seguida, são abordadas as principais vulnerabilidades encontradas na adoção destas técnicas, uma vez que estas já foram há bastante tempo encontradas, provando que o sistema não é de todo confiável se baseado apenas na adoção das técnicas descritas no padrão. Neste capítulo também são apresentadas as principais ferramentas para detecção das referidas vulnerabilidades, permitindo, desta forma, ao gestor de tecnologia de informação encontrar falhas no sistema e procurar por soluções. Deve ser ressaltado que a maioria destas ferramentas está disponível para o sistema operacional Linux, ou seja, trata-se de soluções de código aberto e gratuito, o que facilita enormemente o trabalho do gestor e, em se tratando do serviço público, como é o caso do Senado Federal, possibilita a aquisição sem os trâmites burocráticos tradicionais. O capítulo trata ainda das técnicas de ataque mais comuns utilizadas pelos invasores de uma rede sem fio, o conhecimento destes tipos de ataque é fundamental para que se possam utilizar as ferramentas de teste de maneira mais eficiente. Embora saibamos que os atacantes estão sempre criando novas modalidades de ataque e gerando novos desafios para o gestor, que precisa estar sempre atento às novas atitudes maliciosas que podem ser provocadas. Algumas destas modalidades são completamente inusitadas, como o wardriving, onde uma comunidade de atacantes cria um conjunto de símbolos para identificar redes sem fio e através de pichações comunica a outros membros da comunidade a descrição da rede.

A apresentação de todo o sistema de arquivamento utilizado dentro do Senado Federal bem como da tendência em se implementar um software para envio de streaming de áudio e vídeo estão no capítulo 4. Foi apresentada toda a tecnologia envolvida, incluindo a gravação em fitas de rolo, minidisc e armazenamento em HD. A estrutura administrativa envolvida e o processo de captação de sinais, armazenamento e distribuição também são apresentados. Especial atenção foi dada ao sistema de armazenamento denominado PetaSite, pois trata-se de

uma solução de TI recente, que ainda está em processo de implantação e que está exigindo bastante esforço por parte dos engenheiros da empresa desenvolvedora da solução e dos engenheiros do Senado Federal. Várias empresas de broadcast (rádio e televisão) estão adotando esta solução como forma de prover um sistema de armazenamento de grandes dimensões.

A forma como um streaming pode ser distribuído é apresentada de forma detalhada, por se tratar do foco principal deste trabalho. Assim, são explanados os principais protocolos definidos pelo IETF – RFC 1633.

No capítulo 5 tem-se a conclusão do trabalho e são apresentadas propostas de continuidade.

2 REDES SEM FIO

2.1 INTRODUÇÃO

O termo wireless provém do inglês: *wire*: fio, e *less:* sem; ou seja: sem fios. Wireless então caracteriza um tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar. Pela extrema facilidade de instalação e uso, as redes sem fio estão crescendo cada vez mais. Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como Wi-Fi, InfraRed (infravermelho), Bluetooth e Wi-Max.

As redes sem fio são muito mais susceptíveis a interferências do que as redes cabeadas. Tal situação acontece por não existirem, nas primeiras, proteção em relação ao meio por onde as informações trafegam, uma vez que as ondas eletromagnéticas estão sendo propagadas através do ar e não confinadas em um cabo. Nas redes convencionais, os cabos podem se valer de diversos tipos de materiais para proteção isolando, tanto quanto for a qualidade do material, o que ali trafega do resto do ambiente. Para as Redes sem fio, as ondas eletromagnéticas não dispõem de nenhuma proteção física, a vantagem é que elas podem atingir locais de difícil acesso para redes cabeadas.

As principais características de uma rede sem fio são apresentadas a seguir:

2.2 ELEMENTOS DE REDE SEM FIO

2.2.1 – FREQUÊNCIA:

As ondas eletromagnéticas, também conhecidas como ondas de rádio, são colocadas dentro de uma escala de valores conhecidos como espectro eletromagnético. Tal espectro é apresentado na figura a seguir [3]:

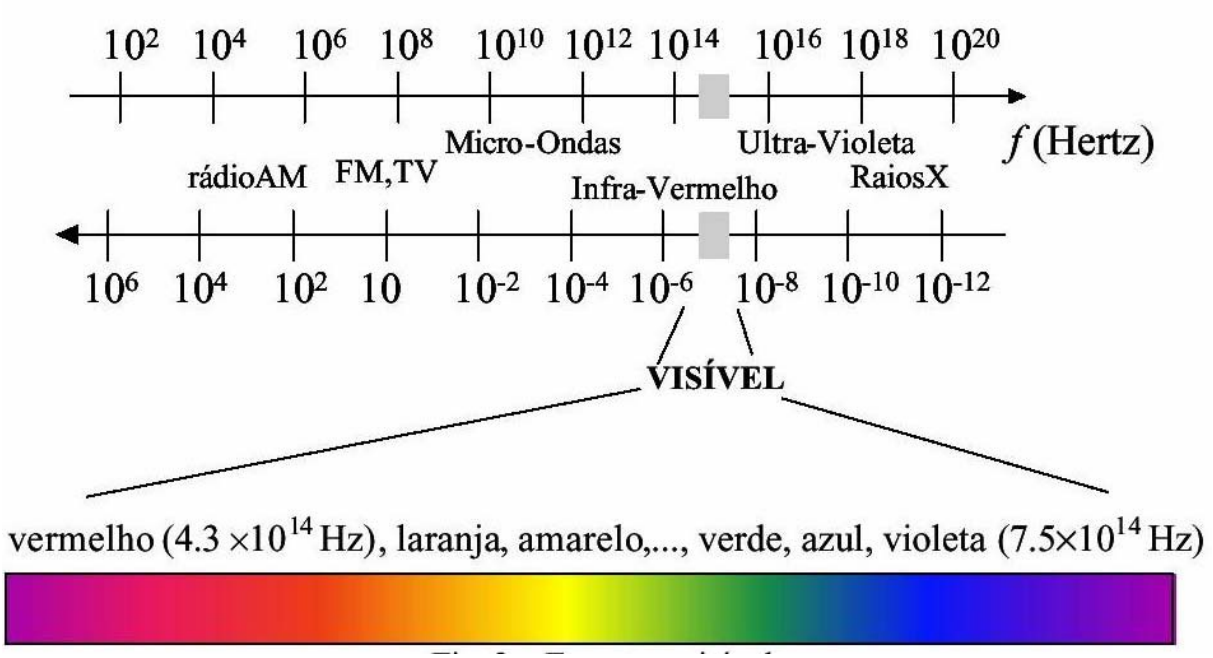

Figura 2.1– Espectro Eletromagnético.

O espectro eletromagnético é dividido em intervalos de freqüência os quais serão utilizados em infra-estruturas comerciais (estações de rádio e TV, operadoras de telefonia móvel, etc) e as de uso militar, aquelas utilizadas em por serviços comunitários e de rádio amador. Porém, a maioria das faixas destinadas a cada um desses serviços não é padronizada internacionalmente. Uma faixa livre em determinado país poderá ser utilizada, por exemplo, em uma aplicação militar em outro, o que torna a comercialização e o uso de algumas dessas soluções por vezes complicadas. No Brasil o órgão do governo responsável pela normatização das freqüências é a Anatel – Agência Nacional de Telecomunicações. A figura a seguir ilustra a divisão atual do espectro eletromagnético no Brasil:

Banda	Uso
535 KHz – 1700 KHz	Rádio AM
5,9 MHz – 26,1 MHz	Rádio Onda Curta
26,96 MHz – 27,41 MHz	Rádio amador
54 MHz – 88 MHz	TV (canais VHF 2 a 6)
88 MHz – 108 MHz	Rádio FM
174 MHz – 220 MHz	TV (canais VHF 7 a 13)
470 MHz – 806 MHz	TV (canais UHF)

Figura 2.2 – Divisão do espectro eletromagnético no Brasil.

As faixas de freqüência definidas pela Anatel são subdivididas em freqüências menores, uma vez que, de acordo com a aplicação, serão necessário apenas alguns Megaherts para permitir a transmissão dos sinais desejados.Essas freqüências menores (ou sub freqüências) são chamadas de canais, que já fazem parte do nosso dia-a-dia há bastante tempo, como os canais de rádio AM/FM e de televisão.

De acordo com convenções internacionais, há pelo menos três diferentes segmentos de radiofreqüência que podem ser usados sem a necessidade de obter licença da agência reguladora governamental. Esses segmentos foram reservados para uso industrial, científico e médico (Industrial, Scientific e Medical - ISM) e por este motivo são denominados de bandas ISM, portanto podem ser utilizados de maneira irrestrita por qualquer aplicação que se adapte a uma dessas categorias.

As freqüências disponíveis em cada uma das três faixas são [1]:

- 902 - 928 MHz;
- 2,4 - 2,5 GHz;
- 5,150-5,825 GHz.

2.2.2 – PROPAGAÇÃO:

As ondas eletromagnéticas, em um sistema Wi-Fi ou em qualquer sistema de transmissão sem fio, propagam-se pelo ar e estão sujeitas à expressão geral para perdas no espaço livre, assim sendo é importante para o gestor desta tecnologia conhecer este importante parâmetro a fim de definir se o mesmo será suficiente para a cobertura da rede a ser adquirida ou remanejada.

Os modelos para as perdas de potência consistem na determinação de um valor representativo para a queda do nível do sinal emitido por uma antena transmissora, conforme é observada a variação na distância entre esta e uma antena receptora. Geralmente, este valor é apresentado como sendo a perda de propagação *L*.

Tal perda é definida como a relação entre a potência recebida (P_r) pela antena receptora e a potência transmitida (P_t) pela antena transmissora. Em decibéis temos [4]:

$$L = 10\log\frac{P_t}{P_r} \qquad (2.1)$$

Para se levar em consideração o ganho das antenas, pode-se utilizar a fórmula de Friis [6] que resulta na potência recebida em uma antena receptora de ganho G_r a uma distância d da transmissora.

$$P_r = \frac{P_t G_r G_t \lambda^2}{(4\pi)^2 d^2} \qquad (2.2)$$

Onde λ é o comprimento de onda (em metros), G_t, e G_r são os ganhos das antenas transmissora e receptora, respectivamente; d é a distância entre as antenas.

Em termos da perda definida na expressão (2.1), a figura a seguir apresenta o modelo indicado para representação da transmissão de sinais entre duas antenas:

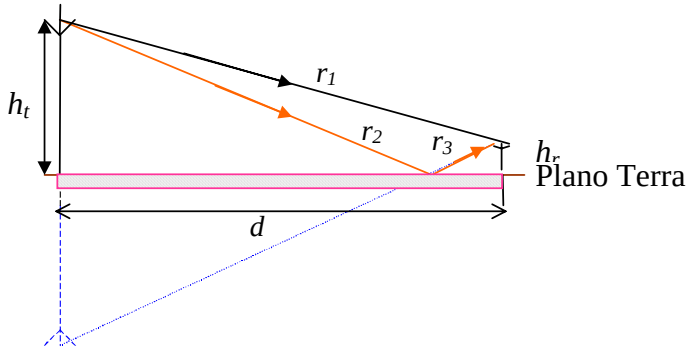

Figura 2.3 – Modelo Terra Plana.

Na figura, h_t e h_r são as alturas das antenas transmissora e receptora em metros, respectivamente.

O modelo plano-terra apresentado na figura acima é o mais importante modelo para as perdas de propagação de um sistema (ele também é denominado modelo dos dois raios). Neste modelo a antena transmissora e a receptora estão sobre a terra (considerada perfeitamente refletora) e a propagação ocorre via um raio direto e um raio refletido na terra, como ilustrado na figura 2.3.

A distância percorrida por cada um dos raios apresentados é dada por [4],

$$r_1 = \sqrt{(h_t - h_r)^2 + d^2} \qquad (2.3)$$

$$r_2' = r_2 + r_3 = \sqrt{(h_t + h_r)^2 + d^2} \qquad (2.4)$$

onde h_t é a altura da antena transmissora, e h_r é a altura da antena receptora.

A diferença entre estas duas distâncias é dada por:

$$r_2^{'} - r_1 = d\left[\sqrt{\left(\frac{h_t + h_r}{d}\right)^2 + 1} - \sqrt{\left(\frac{h_t - h_r}{d}\right)^2 + 1}\right] \qquad (2.5)$$

Se a altura das antenas é pequena quando comparada à distância *d*, pode-se aplicar a expansão binomial

$$(1 + x)^n \cong 1 + nx \quad , |x| < 1; \qquad (2.6)$$

nas raízes em (2.5) para obter

$$r_2^{'} - r_1 = 2\frac{h_t h_r}{d}. \qquad (2.7)$$

De posse destes valores e com mais algumas manipulações matemáticas, chega-se à seguinte relação entre a potência do sinal total P_{total} e do sinal direto enviado pela antena P_{direto}:

$$\frac{P_{total}}{P_{direto}} = 2\left(\frac{\lambda}{4\pi d}\right)^2 \left|1 + \cos\left(k\frac{2h_r h_t}{d}\right)\right|^2, \qquad (2.8)$$

como consideramos $h_r h_t << d$ (o produto da altura das antenas muito menor do que a distância percorrida pelos raios [6]), tem-se um valor pequeno para o argumento do cosseno, desta forma pode-se empregar mais uma aproximação:

$$\cos\theta \cong 1 - \theta^2/2,$$

para obter

$$\frac{P_{total}}{P_{direto}} \cong \left(\frac{\lambda}{4\pi d} \; k \; \frac{2h_r h_t}{d} \right)^2 \cong \frac{h_r{}^2 h_t{}^2}{d} \qquad (2.9)$$

Expressando (2.12) em dB, tem-se

$$L = 40 \log d - 20 \log h_r - 20 \log h_t \qquad (2.10)$$

Que é a expressão para a perda de propagação em um sinal eletromagnético e que pode ser aplicada aos casos de transmissão em redes sem fio. Outros modelos existem e que levam em consideração as reflexões nos diversos objetos, perdas por difrações em paredes e outras considerações, porém, estes modelos fogem ao escopo deste trabalho.

2.2.3 – MODULAÇÃO:

Para que o sinal que se deseja transmitir possa atingir o receptor ele deve ser adicionado às ondas transmissoras em um processo conhecido como modulação. A figura a seguir ilustra o processo de modulação [3]:

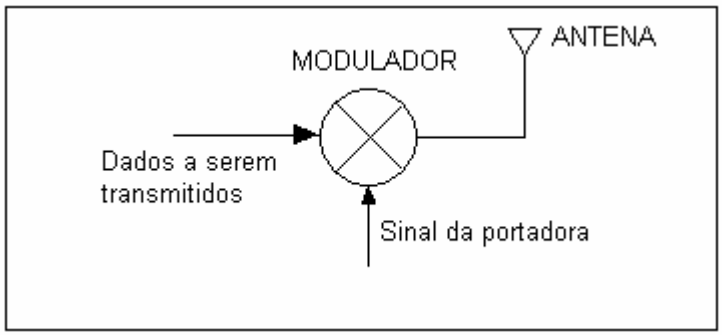

Figura 2.4 – Processo de modulação para transmissão.

Nos primórdios das telecomunicações o tipo de modulação mais empregado foi o AM (modulação em amplitude da freqüência), a seguir passou-se para o FM (freqüência modulada, que, inclusive, foi aplicada nos primeiros sistemas de telefonia celular). Hoje em

dia com a necessidade crescente de se adicionar uma maior quantidade de dados em uma banda limitada de freqüências e os aspetos de segurança, a modulação passou a ter um papel primordial no fenômeno da transmissão das ondas eletromagnéticas. Com isso diversos esquemas de modulação foram implementados como o QAM, PSK, FSK, etc. Os principais mecanismos de modulação aplicados à redes sem fio são descritos a seguir:

Spread Spectrum [1]

Spread Spectrum é uma técnica de codificação para a transmissão digital de sinais. Ela foi originalmente desenvolvida pelos militares durante a segunda guerra mundial, com o objetivo de transformar as informações a serem transmitidas num sinal parecido com um ruído radioelétrico evitando assim a monitoração pelas forças inimigas.

Este tipo de modulação emprega a distribuição do sinal a ser transmitido em toda a faixa do espectro disponível. O Spread Spectrum consome mais banda, porém garante maior integridade ao tráfego das informações e está menos sujeito a ruídos e interferências que outras tecnologias que utilizam freqüência fixa predeterminada, já que um ruído em uma determinada freqüência ira afetar apenas a transmissão nessa freqüência, e não na faixa inteira. Desta maneara, o sinal necessitaria ser retransmitido somente quando - e se -fizer uso daquela freqüência. Pelo fato de preencher toda a faixa, pode ser mais facilmente detectada, mas se o receptor não conhecer o padrão de alteração da freqüência, tudo que receber será entendido como ruído. O padrão de comunicação para todos os tipos de redes sem fio atuais usa essa tecnologia. Basicamente, a técnica do Spread Spectrum é implementada através dos seguintes processos: Salto de Freqüência (Frequency Hopping), Seqüência Direta (Direct Sequence) ou então uma combinação dos dois processos chamada de Sistema Híbrido. A seguir veremos estes dois tipos de implementação:

Frequency-Hopping Spread-Spectrum (FHSS)

Este tipo de modulação divide a banda de 2,4 GHz em 75 canais, a informação é enviada utilizando todos esses canais numa seqüência pseudo-aleatória em que a freqüência de transmissão dentro da faixa vai sendo alterada em saltos, por isso é denominada Hopping. Essa seqüência segue um padrão conhecido pelo transmissor e pelo receptor, que, uma vez sincronizados, estabelecem um canal lógico. O sinal é recebido por quem conhece a seqüência

de saltos e aparece como ruído para outros possíveis receptores. Com essa técnica, limita-se a velocidade de transmissão a 2MBps, já que todo o espectro é utilizado e as mudanças de canais constantes causam grande retardo na transmissão do sinal.

A figura 2.5 ilustra o processo empregado para o espalhamento em freqüências por salto:

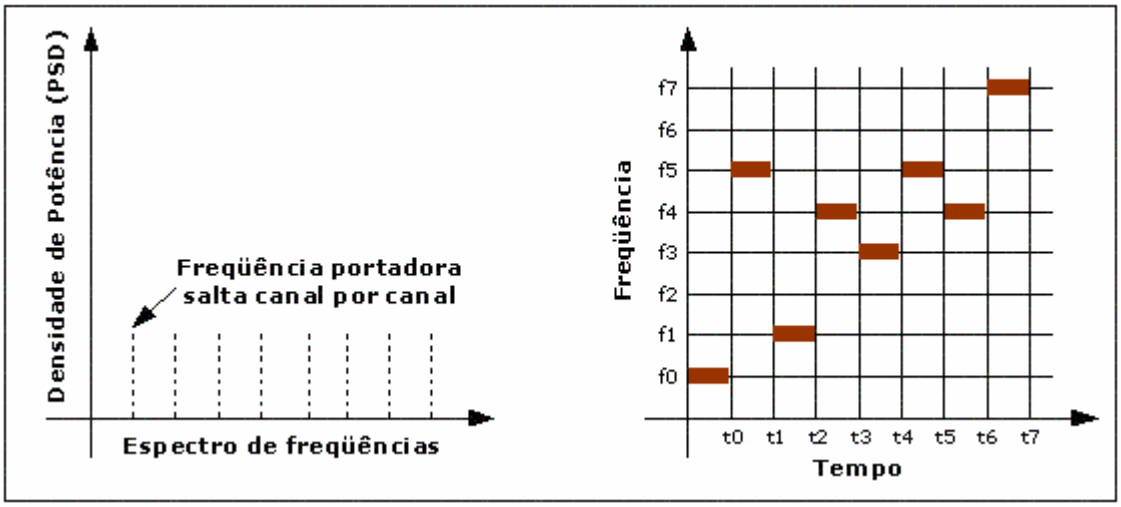

Figura 2.5 – Processo de modulação FHSS.

As vantagens na utilização desta técnica são:

- Os canais que o sistema utiliza para operação não precisam ser seqüenciais.
- A probabilidade de diferentes usuários utilizarem a mesma seqüência de canais é muito pequena.
- A realização de sincronismo entre diferentes estações é facilitada em razão das diferentes seqüências de saltos.
- Maior imunidade às interferências.
- Equipamentos de menor custo.

Direct Sequence Spread Spectrum (DSSS)

Este é o tipo de modulação utilizado no padrão Wi-Fi 802.11b, o DSSS utiliza uma técnica denominada code chips, que consiste em separar cada bit de dados em 11 subbits, que são enviados de forma redundante por um mesmo canal em diferentes freqüências, e a banda

de 2,4 GHz é dividida em três canais. Essa característica torna o DSSS mais susceptível a ataques diretos em uma freqüência fixa e a ruídos que ocupem parte da banda utilizada.

O sinal codificador é um sinal binário gerado numa freqüência muito maior do que a taxa do sinal de informação. Ele é usado para modular a portadora, de modo a expandir a largura da banda do sinal de rádio freqüência transmitido.

A figura 2.6 ilustra o processo de codificação:

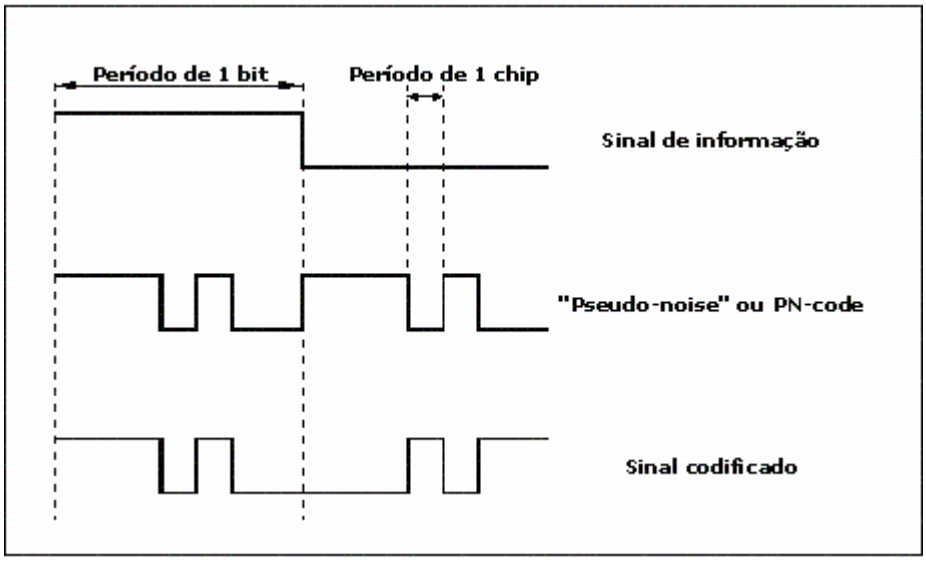

Figura 2.6 – Processo de modulação DSSS.

A técnica de DSSS é também empregada pelo CDMA (Code Division Multiple Access) na telefonia celular.

As vantagens desta técnica são:

- O circuito gerador de freqüência (sintetizador) é mais simples, pois não tem necessidade de trocar de freqüência constantemente.
- O processo de espalhamento é simples, pois é realizado através da multiplicação do sinal de informação por um código.
- Maior capacidade de transmissão, da ordem de 11 Mbit/s.

No receptor o sinal de informação é recuperado através de um processo complementar usando um gerador de código local similar e sincronizado com o código gerado na transmissão

Orthogonal Frequency Division Modulation (OFDM)

A modulação OFDM se baseia na técnica de transmissão de sinais conhecida como FDM - Frequency-Division Multiplex, onde cada canal, em uma freqüência determinada, transporta um *stream* de dados. No OFDM as freqüências são escolhidas de modo que os *streams* de dados sejam ortogonais uns aos outros.

Na modulação FDM as freqüências estão suficientemente espalhadas de modo que para a recepção do sinal, basta que se proceda à filtragem adequada da freqüência desejada. Já na modulação OFDM existe uma sobreposição entre as freqüências que serão transmitidas, obtendo-se desta forma uma maior eficiência espectral, conforme ilustrado na figura:

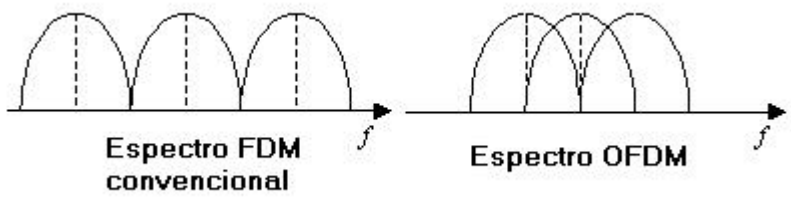

Figura 2.7 – Processo de modulação OFDM.

A característica chave envolvida na OFDM é que a modulação de baixas taxas de sinal sofre menos interferência do que a modulação de altas taxas. O OFDM consegue este benefício dividindo o espectro de freqüências em diversas subbandas e então transmitindo os sinais em uma taxa de bits menor sob cada uma destas subbandas. Assim, uma portadora OFDM é formada pelo somatório de diversas subportadoras.

A modulação OFDM é considerada a mais eficiente, sendo utilizada não somente por equipamentos sem fio como no 802.11a, mas também por redes cabeadas, como ADSL, cujas características de modulação do sinal e isolamento de interferências podem também ser aproveitadas. A maioria dos padrões atuais de redes sem fio adota esse modo de transmissão, principalmente por sua capacidade de identificar interferências e ruídos, permitindo troca ou isolamento de uma faixa de freqüência, ou mudar a velocidade de transmissão.

2.3 CONEXÃO EM REDE SEM FIO

2.3.1 – ESTRUTURA E AUTENTICAÇÃO EM UMA REDE SEM FIO:

A estrutura de uma rede sem fio é composta dos seguintes elementos:

- Sistema de transmissão com antena.
- Pontos de acesso (Access Points – AP).
- Adaptadores para rede sem fio.
- Antena.
- Concentrador.

O padrão IEEE 802.11 define duas formas de autenticação: *open system* e *shared key*. Independentemente da forma escolhida, toda autenticação deve ser realizada entre pares de estações, nunca havendo comunicação *multicast.* Em sistemas BSS (*Basic Service Set*) as estações devem se autenticar e realizar a troca de informações através do *Access Point* [1]. As formas de autenticação previstas definem:

· Autenticação *Open System* - é o sistema de autenticação padrão sendo que, neste sistema, qualquer estação será aceita na rede, bastando requisitar uma autorização. É o sistema de autenticação nulo.

· Autenticação *Shared key* - nesta autenticação, ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo. A troca de informações durante o funcionamento normal da rede é realizada através da utilização do protocolo WEP.

A forma de obter esta autenticação é a seguinte [12]:

1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.

2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudorandômicas.

3.A estação requisitante deve então provar que conhece o segredo compartilhado,

utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.

4.O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

O procedimento de autenticação é ilustrado na figura a seguir:

Figura 2.8 – Processo de autenticação no padrão IEEE 802.11.

2.3.2 – CSMA/CA – CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE:

Para o estabelecimento de uma conexão em redes Ethernet, é necessário que se proceda a uma verificação de se a transmissão/recepção dos dados é possível. O meio de prevenir colisões e realizar esta verificação é fazer com que todos os participantes consigam ouvir o segmento de rede, para saber se podem ou não iniciar um diálogo. Esta técnica é conhecida como Carrier Sense Multiple Access With Collision Detection (CSMA/CD). No caso das redes sem fio, imaginou-se um modelo semelhante de verificação, entretanto, essa equivalência não pode ser completa, tendo em vista a dificuldade de reprodução desse

mecanismo em redes sem fio. Para tanto, seriam necessários dois canais, um para recepção e outro para transmissão. E ainda assim haveria outros problemas, como, por exemplo, se duas estações em lados opostos do concentrador quisessem estabelecer comunicação.

A forma encontrada para resolver essa questão foi adotar uma solução que garantisse que no momento da liberação do meio, para que uma estação trafegasse informações, não houvesse nenhuma outra transmissão. O CSMA/CA é semelhante ao CSMA/CD no que tange à liberação imediata do meio, caso não exista trafego, e à geração de retardo para consulta, caso esteja havendo transmissão no momento do pedido. Essas características geram acessos rápidos em redes com tráfego pequeno, os quais passam a ter resposta mais lenta quanto maior for o volume de tráfego da rede em questão. Só que, diferentemente do CSMA/CD, quando uma estação não consegue acesso ao meio após o período aleatório de espera, não recebe um novo prazo, entrando em uma fila de prioridade. Quando o meio estiver liberado, a fila vai sendo processada, o que permite que estações que estão esperando há mais tempo tenham vantagem de uso do meio para transmissão, em relação aos pedidos mais recentes.

2.3.3 – ESSID - EXTENDED SERVICE SET IDENTIFIER:

O conjunto de identificação de serviços é também denominado de o "nome da rede", trata-se dos valores de chaves que devem ser conhecidos tanto pelo concentrador, ou grupo de concentradores, como pelos clientes que desejam realizar uma conexão. Em geral, o concentrador envia sinais com ESSID, estes sinais são detectados pelos receptores interessados em realizar uma conexão, fazendo com que estes enviem um pedido de conexão. Quando o ESSID não está presente, ou seja, quando os concentradores não enviam seu ESSID de forma gratuita, os clientes têm de conhecer de antemão os ESSIDs dos concentradores disponíveis no ambiente, para, então, requerer conexão.

2.3.4 – BEACON:

Concentradores enviam sinais informando sobre sua existência, para que clientes que estejam procurando por uma rede percebam sua presença e estabeleçam corretamente conexão com um determinado concentrador. Essas informações são conhecidas como Beacon frames, sinais enviados gratuitamente pelos concentradores para orientar os clientes. Entretanto, essas

características podem não existir em alguns ambientes, já que a inibição do envio desses sinais é facilmente configurável nos concentradores atuais, a despeito dessa ação, em alguns casos, comprometer a facilidade de uso e retardar a obtenção da conexão em determinados ambientes.

2.3.5 – CONFIGURAÇÕES DE REDES:

Com relação à estrutura física de uma rede Wireless existem duas configurações, a saber:

Rede *Ad-Hoc:*

É o tipo de estrutura em que não existe um ponto central de distribuição, neste caso as estações estão interconectadas entre si. A principal vantagem deste tipo de estrutura reside no fato de que podemos conectar vários equipamentos sem necessitarmos de um cabo, desta forma podemos atingir locais distantes ou em que a infra-estrutura necessária seria muito dispendiosa. Este modo de operação pode ser mais apropriado em situações em que não haja um concentrador disponível ou mesmo em pequenas redes, porém deve-se enfatizar que a ausência do concentrador cria vários problemas de segurança, administração e gerência da rede. Contudo, por outro lado, pode resolver questões pontuais, como acesso momentâneo para troca de arquivos em um aeroporto ou permitir comunicação rápida em um campo de batalha etc. A figura 2.9 ilustra essa topologia:

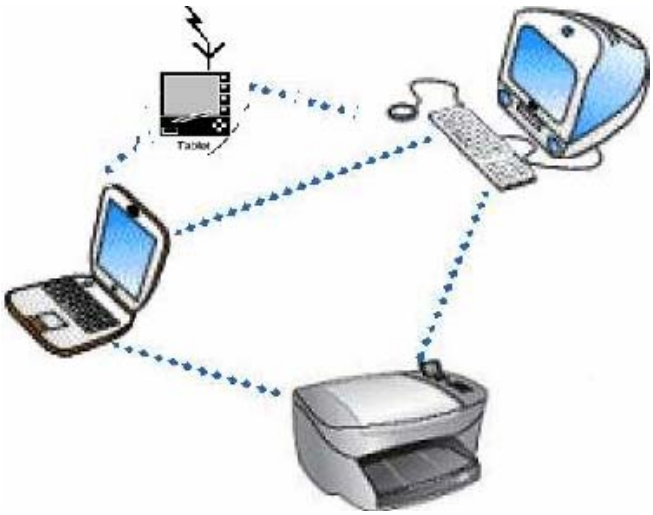

Figura 2.9 – Topologia Ad-Hoc.

Rede do tipo *Infra-Estrutura:*

É o tipo de estrutura em que existe um elemento concentrador, este se torna o equipamento central da rede. Desta forma temos um ponto único de comunicação o qual estabelece a comunicação com várias estações clientes. Assim, as configurações de segurança estarão concentradas em um ponto único da rede. Esta característica permite que se controle todos os itens de acesso à rede em um ponto único (autorização, autenticação, controle de banda, filtros de pacote, criptografia, etc). Outra vantagem deste modelo é facilitar a interligação com redes cabeadas e/ou com a Internet, já que em geral o concentrador também desempenha o papel de gateway ou ponte.

A topologia para a rede no modelo infra-estrutura é apresentada na figura a seguir:

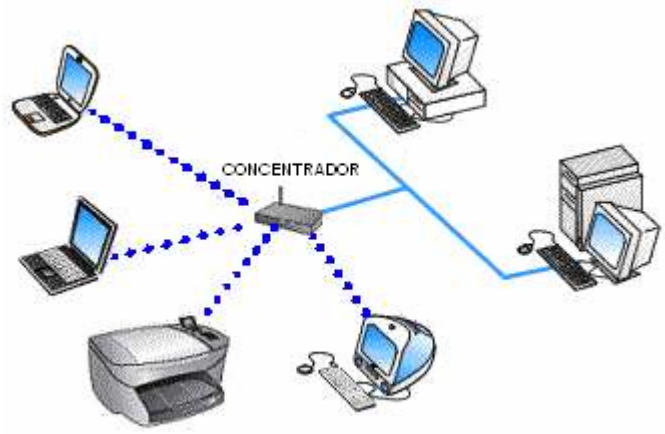

Figura 2.10 – Topologia do tipo Infra-Estrutura.

2.3.6 – PADRÕES ATUAIS PARA AS REDES WI-FI [8]

O Institute of Electrical and Electronics Engineers (IEEE) formou um grupo de trabalho com o objetivo de definir padrões de uso em redes sem fio. Um desses grupos de

trabalho foi denominado 802.11, que reúne uma série de especificações as quais, basicamente, definem como deve ser a comunicação entre um dispositivo cliente e um concentrador ou a comunicação entre dois dispositivos clientes. Ao longo do tempo foram criadas várias extensões destas especificações, onde foram incluídas novas características operacionais e técnicas. O padrão 802.11 original (também conhecido como Wi-Fi), em termos de velocidade de transmissão, provê, no máximo, 2Mbps, operando na freqüência de 2,4 GHz.

Os padrões para a família 802.11 são descritos a seguir:

2.3.6.1 - 802.11 b

O primeiro sub padrão a ser definido permite 11 Mbps de velocidade de transmissão máxima, porém pode comunicar-se a velocidades mais baixas, como 5, 2 ou mesmo 1 Mbps. Opera na freqüência de 2,4 GHz e usa a modulação DSSS. Permite um número máximo de 32 clientes conectados. Foi ratificado em 1999 e definiu padrões de interoperabilidade bastante semelhante aos das redes Ethernet. Há limitação em termos de utilização de canais, sendo ainda hoje o padrão mais popular e com a maior base instalada, com mais produtos e ferramentas de administração e segurança disponíveis. Porém, está claro que esse padrão chegou ao seu limite e já está sendo preterido em novas instalações e em atualizações do parque instalado.

Na tabela 2.2 consta a associação entre cada canal do padrão 802.11.b e sua respectiva freqüência:

Canal	Freqüência (GHz)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452

10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

Tabela 2.2– Freqüência e canais no padrão 802.11b

2.3.6.2 - 802.11a

Definido após os padrões 802.11 e 802.11.b e tentando resolver os problemas existentes nestes, o 802.11a tem como principal característica o significativo aumento da velocidade para um máximo de 54 Mbps (108 Mbps em modo turbo), mas podendo operar em velocidades mais baixas. Outra diferença é a operação na freqüência de 5 GHz, uma frequêcia com poucos concorrentes, porém com menor área de alcance. Oferece também aumento significativo na quantidade de clientes conectados (64) e ainda no tamanho da chave usada com WEP, chegando em alguns casos a 256 bits (mas possui compatibilidade com os tamanhos menores, como 64 e 128 bits). Finalmente, adota o tipo de modulação OFDM, diferentemente do DSSS usado no 802.11b. Outra vantagem deste padrão consiste na quantidade de canais não sobrepostos disponíveis, um total de 12, diferentemente dos 3 canais livres disponíveis nos padrões 802.11b e 802.11g, o que permite cobrir uma área maior e mais densamente povoada, em melhores condições que outros padrões.

O principal problema relacionado à expansão deste padrão tem sido a inexistência de compatibilidade com a base instalada atual (802.11b), já que elas utilizam faixas de freqüência diferentes. A despeito disso, vários fabricantes têm investido em equipamentos neste padrão, e procedimento similar começa a ser usado em redes novas, onde não é necessário fazer atualizações nem há redes sem fio preexistentes.

2.3.6.3 - 802.11g

Este padrão é mais recente que os comentados anteriormente e equaciona a principal desvantagem do 802.11a, que é utilizar a frequência de 5GHz e não permitir interoperação

com 802.11b. O fato de o 802.11g operar na mesma freqüência do 802.11b (2,4 GHz) permite até que equipamentos de ambos os padrões (b e g) coexistam no mesmo ambiente, possibilitando assim evolução menos traumática do parque instalado. Além disso, o 802.11g incorpora várias das características positivas do 802.11a, como utilizar também modulação OFDM e taxa próxima aos 54 Mbps nominais.

2.3.6.4 - 802.11i

Homologado em junho de 2004, este padrão diz respeito a mecanismos de autenticação e privacidade e pode ser implementado, em vários de seus aspectos, nos protocolos já existentes. O principal protocolo de rede definido neste padrão é chamado RSN (Robust Security Network), que permite meios de comunicação mais seguros que os difundidos atualmente. Está inserido neste padrão também o protocolo WPA, que foi desenhado para prover soluções de segurança mais robustas, em relação ao padrão WEP, além do WPA2, que tem por principal característica o uso do algoritmo criptográfico AES (Advanced Encryption Standard).

2.3.6.5 - 802.11n

Também conhecido como WWiSE (World Wide Spectruan Efficiency), este é una padrão em desenvolvimento, cujo foco principal é o aumento da velocidade (cerca de 100 a 500 Mbps). Paralelamente, deseja-se aumento da área de cobertura. Em relação aos padrões atuais há poucas mudanças. A mais significativa delas diz respeito a uma modificação de OFDM, conhecida como MIMO-OFDM (Multiple Input, Multiple Output -OFDM). Outra característica deste padrão é a compatibilidade retroativa com os padrões vigentes atualmente. O 802.11n pode trabalhar com canais de 40 MHz e, também, manter compatibilidade com os de 20 MHz atuais, mas neste caso as velocidades máximas oscilam em torno de 135 Mbps.

2.3.6.6 - 802.1x

Mesmo não sendo projetado para redes sem fio (até por ter sido definido anteriormente a esses padrões), o 802.1x possui características que são complementares a essas redes, pois

permite autenticação baseada em métodos já consolidados, como o RADIUS (Remote Authentication Dial-In User Sevice), de forma escalável e expansível. Desta maneira é possível promover um único padrão de autenticação, independentemente da tecnologia (vários padrões de redes sem fio, usuários de redes cabeadas e discados etc.), e manter a base de usuários em um repositório único, quer seja em banco de dados convencional, LDAP ou qualquer outro reconhecido pelo servidor de autenticação.

É importante notar que para esta infra-estrutura funcionar, basta que os componentes - concentrador, servidor RADIUS e outros opcionais, como: LDAP, Active Directory, banco de dados convencionais etc. - estejam interligados por meio de uma rede. A localização física de cada elemento tem pouca importância.

Este padrão pressupõe a presença de um elemento autenticador, tipicamente um servidor RADIUS, e um requerente, ou seja, o elemento que requer autenticação, no caso o equipamento cliente. Essa autenticação é feita antes de qualquer outro serviço de rede estar disponível ao usuário requerente. Este, primeiramente, solicita autenticação ao autenticador, que verifica em sua base de dados as credenciais apresentadas pelo cliente, e conforme a validade ou não dessas credencias (normalmente o binômio usuário/senha), permite ou não o acesso a estas. Uma autenticação bem-sucedida irá deflagrar todos os outros processos para permitir ao usuário acesso aos recursos da rede, o que pode incluir receber um endereço via DHCP ou outro protocolo de atribuição de endereços IP, com informações de roteamento, servidores DNS, liberar roteamento na porta pelo switch, etc.

Para redes sem fio somente estará apto a fazer uso dos serviços da rede o cliente que estiver devidamente autenticado no servidor RADIUS. O 802.1x pode utilizar vários métodos de autenticação no modelo EAP (Extensible Authentication Protocol), que define formas de autenticação baseadas em usuário e senha, senhas descartáveis (One Time Password), algoritmos unidirecionais (hash) e outros que envolvam algoritmos criptográficos.

3 SEGURANÇA EM REDES SEM FIO

3.1 TÉCNICAS DE SEGURANÇA

Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando que seja modificada ou até mesmo apagada.

Desde a inserção do computador, na década de 40, como dispositivo auxiliar nas mais variadas atividades, até os dias atuais, observou-se uma grande evolução nos modelos computacionais e tecnologias usadas para manipular, armazenar e apresentar informações. Verificou-se uma migração de grandes centros de processamento de dados para ambientes de computação distribuída, este fenômeno, também ocorre dentro do Senado Federal brasileiro, objeto de estudo nesta monografia.

Segurança da informação compreende um conjunto de medidas que visam proteger e preservar informações e sistemas de informações, assegurando-lhes *integridade*, *disponibilidade*, e *confidencialidade*. Esses elementos constituem os três pilares da segurança da informação e, portanto, são essenciais para assegurar a integridade e confiabilidade dos sistemas.

A confidencialidade irá garantir que terminais não autorizados “escutem” as informações que estão trafegando na rede. A integridade irá garantir que a informação transmitida não foi alterada e que o destinatário realmente recebeu na íntegra o que o remetente enviou. A disponibilidade estabelece que o sistema estará disponível para qualquer estação autorizada em qualquer momento que ela solicite.

Deve-se considerar que no caso do Senado Federal os aspectos relacionados com a segurança da informação são de extrema importância. Vale ressaltar a grande quantidade de

tentativas de ataques que diariamente são desferidos contra a rede do Senado, administrada pelo Prodasen – Secretaria Especial de Informática.

Os prejuízos causados em um ataque sofrido podem possuir várias dimensões. Por exemplo, quando uma rede é atacada pode-se perder apenas tempo, ou seja, o tempo de baixar um backup, re-organizar ou re-indexar alguns dados. No entanto, pode-se perder ou se permitir o vazamento de informações de extrema importância, como aquelas contidas em reuniões secretas das comissões parlamentares de inquérito, neste caso, os prejuízos serão incalculáveis, pois poderão envolver o destino da nação.

A proteção de redes sem fios abrange muitos fatores, e é necessário ter-se um conhecimento razoável de todos os padrões disponíveis e o que eles têm a oferecer e, de acordo com sua aplicação, objetivo e política de segurança, implementar o nível correto. Possuir o último padrão desenvolvido e disponível não garante que a segurança será eficiente e que ele será o mais seguro, tudo vai depender da configuração completa do sistema. Os principais fatores envolvidos na segurança de redes sem fio são apresentados a seguir:

3.1.1 – WEP - Wired Equivalent Privacy

O WEP é um protocolo de criptografia bastante comum que pretende impedir que intrusos consigam ler os dados transmitidos, modificar estes dados e que tenham acesso à rede sem fio.

Este protocolo provê três serviços básicos:

- Confidencialidade: serviço opcional que quando ativado garante que apenas pessoas autorizadas tenham acesso à informação transmitida através de uma chave secreta que cada estação possui;
- Integridade: garante que o receptor receberá os dados corretos, sem alterações, inclusões ou remoções de informações;
- Autenticidade: garante o gerenciamento de quem está executando que ação na rede sem fio;

A chave secreta utilizada no WEP é compartilhada apenas com o ponto de acesso e a única forma de distribuição possível é a manual.

Um algoritmo RC4 é a base da criptografia da chave secreta. Ele é um algoritmo de fluxo, ou seja, criptografa os dados ao mesmo tempo em que são transmitidos.

Um vetor de inicialização (IV – Initialization Vector) de 24 bits é utilizado junto a chave secreta de 40 ou 104 bits para gerar a informação criptografada. Esse IV é enviado junto a mensagem cifrada formando uma chave de 64 ou 128 bits para que o receptor possa reverter o processo de criptografia.

Além disso, o WEP utiliza CRC-32 (*Cyclic Redundance Check 32*) para calcular o *checksum* da mensagem, que é incluso no quadro, para garantir a integridade dos dados. Dessa forma, o receptor recalcula o *checksum* para garantir que a mensagem não foi alterada.

A segurança do WEP é composta de dois elementos básicos: uma chave estática, que deve ser a mesma em todos os equipamentos da rede, e um componente dinâmico, que, juntos, irão formar a chave usada para cifrar o tráfego. O protocolo não define de que forma essa chave deve ser distribuída, portanto a solução convencional é também a mais trabalhosa, em que a chave é cadastrada manualmente em todos os equipamentos.

Em um segundo momento, após o estabelecimento da conexão, essa chave estática sofre uma operação matemática para gerar quatro novas chaves: uma destas será escolhida para cifrar as informações em trânsito. Essa chave será fixa e somente trocada se a chave estática original mudar. Portanto, essa nova chave gerada é fixa e susceptível a ataque de dicionário e força bruta. Pode ter tamanho de 40 a 104 bits, e o padrão ainda é 104, mas já existem várias implementações com valores maiores.

Para tentar evitar esses tipos de ataque, adiciona-se um segundo elemento que consiste em um conjunto de 24 bits geridos por uma função pseudoaleatória que será concatenada às chaves fixas (40 ou 104), vendida, respectivamente, como 64 ou 128 bits. Entretanto, os 24 bits passam em claro pela rede, já que esta foi a forma encontrada para dar conhecimento desse valor, possibilitando que os elementos da rede estabeleçam a comunicação cifrada. Normalmente, esse procedimento é realizado pelo concentrador que, então, distribui a informação para os elementos participantes da rede.

É importante notar que esta noção de equivalência (Wired Equivalent Privacy) faz supor que, como não existe proteção ao conteúdo em redes cabeadas (toda proteção deve ser feita por software ou firmware), se pensou em um mecanismo que tivesse dificuldade de quebra compatível a um acesso físico. Porém, após terem sido expostas várias fragilidade do WEP, esse conceito de equivalência não se sustenta. Mas a despeito disso, o WEP ainda provê segurança adequada a vários tipos de cenários.

3.1.2 – Endereço MAC (Media Access Control)

Trata-se de um endereço dado pelo fabricante à sua placa de rede, ou seja, antes de sair da fábrica, o fabricante do hardware atribui um endereço físico a cada placa de rede. Esse endereço é programado em um chip na placa. Como o endereço MAC está localizado na placa de rede, se esta for substituída em um computador, o endereço físico deste mudaria para o novo endereço MAC.

O endereço MAC possui tamanho de 48 bits, expressos com doze dígitos hexadecimais. Eles são utilizados para identificar unicamente uma placa de rede. Os primeiros seis dígitos são administrados pelo consórcio IEEE e identificam o fabricante ou fornecedor da placa de rede; os seis últimos são uma identificação da placa.

Não existem duas placas com o mesmo endereço MAC, ou seja, este endereço é único para cada placa de rede em cada computador. Os endereços MAC geralmente são gravados na memória ROM e copiados para a memória RAM quando a placa de rede é iniciada.

Uma das formas encontradas para restringir o acesso a uma determinada rede sem fio é mediante o cadastramento prévio dos dispositivos participantes. Como o endereço MAC identifica cada interface de rede, apenas os dispositivos cadastrados de antemão terão acesso permitido. Esse mecanismo exigirá sempre alguma manutenção, que será maior ou menor, de acordo com o fluxo de usuários e interfaces que entram e saem do cadastro, porém não deixa de ser uma boa solução para pequenas redes e ambientes com poucas mudanças. Mas é importante lembrar que esse tipo de autenticação pode, no melhor dos casos, identificar o equipamento e não o usuário. Particularmente, isso é importante em computadores compartilhados ou vulneráveis a acessos não autorizados, quer sejam acessos físicos, quer remotos.

3.1.3 – WPA – Wi-Fi Protected Access Equivalent Privacy

O WPA, também chamado de WEP2, surgiu da necessidade em se aumentar o nível de segurança das redes sem fios, combatendo algumas vulnerabilidades do WEP. O propósito

deste protocolo é a mudança constante da chave de encriptação dificultando a invasão ou descoberta da chave.

O protocolo WPA é compatível com o padrão de redes sem fio 802.11i e realiza melhorias na encriptação de dados e na autenticação do usuário, porém requer um *upgrade* de *software*. Ele pode ser utilizado numa rede híbrida que tenha WEP instalado.

A vantagem do WPA sobre o WEP é a melhoria na criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP – *Temporal Key Integrity Protocol*) que possibilita a criação de chaves por quadro, um mecanismo de distribuição de chaves e um vetor de inicialização de 48 bits, ao invés de 24 bits como era no protocolo WEP. Além disso, uma outra vantagem é a melhora na autenticação de usuários. Essa autenticação se utiliza do 802.1x e do EAP (*Extensible Authentication Protocol*), que faz a autenticação de cada usuário antes de entrar na rede.

Basicamente o WPA utiliza-se de:

- Autenticação: através do EAP faz a validação do usuário;
- Autorização: assegura acesso a serviços autorizados;
- Confidencialidade: melhora na criptografia dos dados com a utilização do TKIP;
- Integridade: Usando o MIC (*Message Integrity Code*) faz a validação dos usuários.

No WPA a autenticação 802.1x é obrigatória; no padrão 802.11 era opcional. A autenticação com WPA é uma combinação de sistema aberto e autenticação 802.1x que utiliza duas fases: a primeira utiliza a autenticação de sistema aberto e indica ao usuário da rede sem fio que ele pode enviar quadros para o ponto de acesso sem fio e a segunda fase utiliza o 802.1x para realizar a autenticação do usuário.

Em ambientes domésticos, onde não existe um servidor de autenticação (servidor RADIUS – *Remote Authentication Dial-In User Service*), o WPA provê um outro método de autenticação chamado PSK (*Pre-Shared Key*), que permite que o usuário digite chaves e senhas manualmente.

No WEP a integridade dos dados é garantida com um ICV (*Integrity Check Value*) de 32 bits, já no WPA existe um método conhecido como Michel que especifica um novo algoritmo, calculando um MIC (código de integridade da mensagem) e anexando-o ao ICV.

O TKIP utiliza um vetor de inicialização de 48 bits, ao invés de 24 bits utilizado no WEP. Assim, WPA as chaves são de 128 bits.

3.1.4 – VPN - Virtual Private Network

Um Rede Privada Virtual – VPN, é uma rede privativa (com acesso restrito) construída sobre a infra-estrutura de uma rede pública, geralmente a Internet".

A VPN utiliza uma técnica chamada de tunelamento, onde pacotes são transmitidos na rede compartilhada em um túnel privado que simula uma conexão ponto-a-ponto (enlace dedicado).

Esta tecnologia possibilita que o tráfego de várias fontes trafegue via diferentes túneis sobre a mesma infra-estrutura. Permite que diferentes protocolos de rede se comuniquem através de uma infra-estrutura incompatível e também possibilita diferenciar o tráfego de várias fontes, permitindo distintas rotas de destino e qualidade de serviço.

A característica mais importante para as redes sem fio é o fato de uma VPN criar canais privados de comunicação, onde os dados viajam criptografados, aumentando consideravelmente a segurança dos dados.

Uma VPN provê uma conexão segura através de um conjunto de três serviços:

- Autenticação: implementada através de senhas e identificação dos usuários, estabelece a identificação do remetente e do receptor da informação;
- Encriptação: Implementada através de algoritmo de criptografia aplicado sobre a mensagem de texto aumentando a dificuldade para decriptografá-la;
- Encapsulamento: a mensagem criptografada é encapsulada pela VPN em pacotes com o seu próprio endereço como origem. Este processo é conhecido também como tunelamento.

Uma das grandes vantagens das Redes Privadas Virtuais é que elas tendem a apresentar custos muito menores de implementação do que aqueles obtidos com as Redes Privadas.

3.2 VULNERABILIDADES EM REDES SEM FIO

3.2.1 – Vulnerabilidade nos Protocolos

3.2.1.1 – Vulnerabilidade no WEP

Uma das vulnerabilidades do WEP está no vetor de inicialização (IV). Como as chaves de encriptação são utilizadas por longo período de tempo, recomenda-se que o vetor de inicialização seja alterado a cada quadro enviado. No geral, este vetor inicia em 0 e vai sendo acrescido em 1 a cada nova utilização.

Dois problemas podem ser verificados nesse sistema: Um deles reside no fato de que em algum momento o vetor de inicialização (IV) se repetirá e sendo uma cadeia cíclica, o tráfego poderá ser facilmente monitorado. O outro problema está na freqüente remoção e reinserção dos dispositivos de rede sem fio, retornando a contagem do vetor de inicialização à 0, fazendo com que os quadros com valores baixos de IV sejam comuns.

Grande parte dos problemas do protocolo WEP vinculam-se ao fato de que o padrão foi definido em uma época em que havia restrições dos Estados Unidos referentes à exportação de criptografia com chaves maiores que 40 bits.

Hoje, alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algum tempo.

Outra grande vulnerabilidade do protocolo WEP é quanto ao método de criptografia que utiliza o RC4. O RC4 é simétrico, ou seja, a mesma chave utilizada para a criptografia também é utilizada para a decriptografia.

Teoricamente, conhecer o vetor sem conhecer a chave é inútil, porém existem situações que, na prática, contradizem essa afirmação. Em virtude do pequeno tamanho do vetor, este se repete várias vezes durante um dia de tráfego, pois com 24 bits são possíveis 16.777.216 valores diferentes. Como uma rede com tráfego intenso transmite em torno de 600 a 700 pacotes, mesmo que todos os valores sejam usados sem repetição, o mesmo valor será utilizado novamente ao final de 7 horas, assim um atacante poderá observar passivamente o tráfego e identificar quando o mesmo valor será usado novamente. Essa reutilização do vetor irá, em algum momento, revelar a chave (os outros 104 bits), pois alguns pacotes têm

conteúdo previsível, como "username", "login", "password", vários espaços em branco em mensagens de e-mail, etc.

Ataques completamente passivos podem não obter um padrão de pacote que permita descobrir a chave, então o atacante poderá atuar de forma mais ativa e forçar uma resposta conhecida enviando, por exemplo, um ping para algum equipamento da rede-alvo. Devido ao pacote ICMP de resposta ter seu conteúdo conhecido, nesse momento a chave será revelada. Essa descoberta é possível por meio de uma simples operação matemática, conhecida como XOR, que diz que de posse de três informações complementares é possível deduzir a quarta, Neste caso são conhecidos a mensagem cifrada, a chave cifrada e o pacote em claro, portanto por uma operação de regra de 3 pode se chegar à informação desejada: a chave em claro.

Para piorar este cenário, algumas implementações utilizam a mesma seqüência de vetores desde o momento em que o equipamento é ligado, facilitando ainda mais a descoberta do segredo. Outro problema com o WEP relaciona-se à forma de armazenamento das chaves no cliente. Como o protocolo não define nenhum método para cifragem na guarda da chave, esta é armazenada de forma legível, o que torna um ambiente com chaves de melhor qualidade mais difícil de ser quebrado, vulnerável caso um cliente que compõe a rede seja comprometido.

3.2.1.2 – Vulnerabilidade no WPA

O WPA foi criado exatamente para sanar as vulnerabilidades do protocolo WEP, mas ele também apresenta algumas falhas que devem ser conhecidas para evitar possíveis problemas. No entanto, não há muitas ferramentas disponíveis que promovam ataques ao WPA.

No mais, a maior vulnerabilidade, que não é específica a este protocolo, é o uso de senhas pequenas ou de fácil adivinhação. Porém esta falha pode deixar a rede sujeita a ataques, onde o suposto invasor testa seqüências de senhas e/ou palavras comuns.

No caso do WPA, senhas com menos de 20 caracteres são mais susceptíveis a esse tipo de ataque. É muito comum fabricantes usarem senhas pequenas (de 8 a 10 posições) imaginando que o administrador irá modificá-las quando colocar o equipamento em atividade, porém isso não ocorre na prática, o que torna redes com WPA tão ou mais vulneráveis do que aquelas que utilizam WEP.

3.2.2 – Vulnerabilidades Físicas

Em redes Wireless a segurança está relacionada também à parte física dos equipamentos. Diferentemente das redes cabeadas, nas redes sem fio esse aspecto é muito mais relevante, visto que a área de abrangência aumenta substancialmente. Muitos pontos, antes nas redes cabeadas, que eram irrelevantes devem ser cuidadosamente tratados nas redes sem fios como, por exemplo, o posicionamento dos *hardwares* utilizados entre, outros.

O acesso aos equipamentos, que há algum tempo, era estabelecido e controlado exclusivamente via portaria e/ou recepção, ou mesmo a necessidade de obter um ponto de rede cabeada, ou acesso a um computador da rede, agora devem ser pensados em termos de dezenas ou centenas de metros ao redor do ambiente da empresa. Aspectos antes irrelevantes (sob o ponto de vista de performance e segurança), como posicionamento de determinados componentes de rede, agora devem ser cuidadosamente estudados, sob o risco de comprometer o bom funcionamento da rede e, principalmente, facilitar o acesso não autorizado e outros tipos de ataques.

Alguns itens relevantes que devem ser levados em consideração no momento de avaliar a área de abrangência de uma rede sem fio são:

- O alcance atingido pelo padrão a ser adotado;
- A potência dos equipamentos que serão utilizados. Em geral, concentradores têm potência máxima de 32 mW (15 dbm) - alguns equipamentos atualmente chegam a 300 mW (24,8 dbm) - e a maioria dos concentradores permite selecionar valores intermediários, caso o administrador ache conveniente, em função da área efetiva a ser coberta por um determinado equipamento;

Deve-se sempre considerar que antenas mais potentes ampliam a distância de recepção. Portanto, para garantir que o sinal não será capturado a uma determinada distância, não é suficiente percorrer os limites da instalação para verificar até onde o sinal chega, já que um atacante munido de uma interface de maior potência, ou de uma antena que lhe permita estar a uma distância tão grande deste limite quanto for a potência da antena ou interface por ele utilizada, poderá receber sinal a uma distância não prevista pelos testes. Desta forma, um teste de propagação do sinal não deve ser o único fator de prevenção a ataques, visto que o

atacante pode utilizar um equipamento mais moderno ou com características distintas daqueles utilizados nos testes e, desta maneira, conseguir sinal onde os testes não obtiveram.

As vulnerabilidades físicas incluem aquelas configurações onde o administrador mantém o mesmo "*setup*" sugerido pelo fabricante. Alguns equipamentos que são fornecidos para a elaboração de uma rede, muitas vezes, possuem ferramentas de segurança, mas nem sempre estas ferramentas já vêm habilitadas de fábrica (por várias razões, como incompatibilidade com equipamentos de outros fornecedores, facilidade de instalação etc.). Este fato faz com que os administradores com pouca experiência em redes sem fio ou com os prazos de implantação vencidos coloquem os equipamentos em produção sem qualquer mudança (ou com mudanças mínimas, suficientes para que o ambiente funcione). É certo que equipamentos com configurações de fábrica em que os mecanismos de segurança não forem habilitados, serão alvos fáceis de ataques.

Praticamente todos os equipamentos saem de fabrica com senhas de administração e endereço IP padrão. Caso estes não sejam trocados, poderão permitir a um atacante que se utilize delas em uma rede-alvo e tenha condições de identificar todas as configurações feitas, podendo até mesmo modificá-las. Redes que estejam usando métodos de segurança como WEP- que pode ser adequada em algumas circunstâncias - estarão completamente vulneráveis caso o equipamento venha com as chaves WEP configuradas e estas não sejam mudadas pelo administrador. Essas informações constam nos manuais e documentos públicos, portanto qualquer possível atacante poderá acessá-las.

O gerente de tecnologia da informação deve considerar que qualquer informação pode ser útil a um atacante. Se alguma informação de fábrica, que permita acesso ou presuma detalhes que possam ser usados em ataques, estiver disponível, certamente será utilizada em algum momento. Portanto, contas administrativas devem ser trocadas, bem como as chaves WEP ou WPA, e o SSID deve ser modificado de modo a não permitir identificar a rede, empresa ou qualquer outra característica pela qual possa interessar-se um atacante.

Um fato nem sempre lembrado é que a maioria dos concentradores vêm com o serviço SNMP habilitado, o qual é responsável por prover informações gerenciais sobre o equipamento e o tráfego e, em alguns casos, permite até mesmo a configuração de alguns parâmetros remotamente, podendo perfeitamente ser usado por um atacante, pois revela uma vasta gama de informações sobre a rede em questão.

Mesmo o pessoal de TI com grande vivência em redes cabeadas vêm encontrando dificuldades em configurar de forma segura seu ambiente Wi-Fi. Por mais semelhanças que

existam em relação a proteção de serviços, sistemas, aplicações, atualizações etc., há vários outros pontos que são novidade absoluta e, portanto, necessitam de tempo e disposição pura ter desembaraço nas novas questões de segurança em ambientes de rede sem fio. Quanto a esse aspecto, os equipamentos que vêm com todas as possibilidades de conexão habilitadas e, por outro lado, sem nenhum mecanismo para garantir a segurança do equipamento e do ambiente ativo não colaboram para que, em um primeiro momento, o administrador possa montar uma rede simultaneamente utilizável e segura.

Ao se estabelecer uma analogia com sistemas operacionais, observa-se que, ao longo do tempo, as configurações de segurança têm sido uma preocupação crescente dos fornecedores. Se no passado os sistemas saíam de fábrica com falhas de segurança e exigiam um tempo dispendioso para estabelecimento de uma configuração de segurança que o administrador considerasse adequada, atualmente os fornecedores estão bem mais rigorosos em termos de serviços habilitados, usuários ativos, permissões de arquivos, diretórios e demais áreas do sistema. Assim, imagina-se que à medida que alguns padrões de segurança forte estejam consolidados, os equipamentos devam ser entregues com mais recursos de segurança habilitados. Mas até que isso aconteça, o administrador deve estar atento que é precisamente após o sistema estar funcionando que o trabalho maior começa. Ele não deve de forma alguma deixar de utilizar ao máximo o que os equipamentos adquiridos possuírem em termos de mecanismos de segurança.

Devido à falta de conhecimento de muito administradores na forma de configuração dos dispositivos para redes sem fios há uma grande possibilidade deste dispositivo mal configurado se associar a outro dispositivo, sem consentimento ou mesmo conhecimento do usuário, neste caso ocorre o que é denominado de *Associação Acidental* .

3.2.3 – Vulnerabilidades Espaciais

Neste caso existe vulnerabilidade relativa ao espaço onde se encontram instalados os equipamentos da rede. Um ataque a uma rede sem fio deve começar pelo mapeamento da área onde se encontram as instalações-alvo. Neste caso o atacante irá promover um mapeamento do ambiente. Esse procedimento possibilita obter o maior número de informações sobre uma determinada rede, permitindo conhecer detalhes que lhe permitam lançar ataques de forma mais precisa e com menos riscos de ser identificado. Tal ação pode ter maior ou menor grau de êxito, dependendo dos mecanismos de proteção existentes na rede-alvo.

Existem métodos que permitem ao atacante mapear componentes e atividades da rede-alvo e, ainda assim, passar despercebido, por meio do mapeamento passivo. Ferramentas tradicionais em rede cabeada, como o p0f, podem executar esse trabalho, basta ao atacante estar posicionado em uma área coberta pelo sinal da rede-alvo, não sendo nem preciso estar associado ao concentrador.

De posse dessas informações, o atacante pode selecionar equipamentos de interesse ou que estejam vulneráveis, sem correr o risco de ser descoberto antes de um ataque direto, o que pode aumentar as chances de êxito, visto que de outra forma ele poderia ter sido bloqueado ainda nas tentativas preliminares.

Também pode ocorrer de o atacante se utilizar de programas, que mesmo não o mantendo despercebido pela rede, facilitem o acesso aos dados que irão lhe permitir planejar o ataque, neste caso trata-se de um mapeamento ativo. Como exemplo pode-se capturar o endereço MAC, o qual está associado ao fornecedor do equipamento, portanto isso já pode ser suficiente para que, caso exista alguma vulnerabilidade conhecida para esse determinado equipamento, esta venha a ser usada.

Alguns gestores de tecnologia da informação ocultam a presença do equipamento na rede através da filtragem do envio/recebimento de pacotes ICMP REPLY (resposta ao ping). Essa estratégia pode funcionar em muitos casos e até evitar alguns ataques de negação de serviço, mas é ineficiente para esconder a existência de um equipamento, pois se o serviço está ativo e acessível, poderá ser localizado.

3.3 FERRAMENTAS PARA TESTE DE VULNERABILIDADES EM REDES SEM FIO

3.3.1 – AIRCRACK

O Aircrck é uma suíte de ferramentas que consegue descobrir a chave do WEP, permitindo que o teste de invasão seja realizado.

Dentro do Aircrack podemos encontrar diversas ferramentas, como o airmon, que identifica a interface wireless, o chipsete e o driver utilizado, conforme ilustrado na figura:

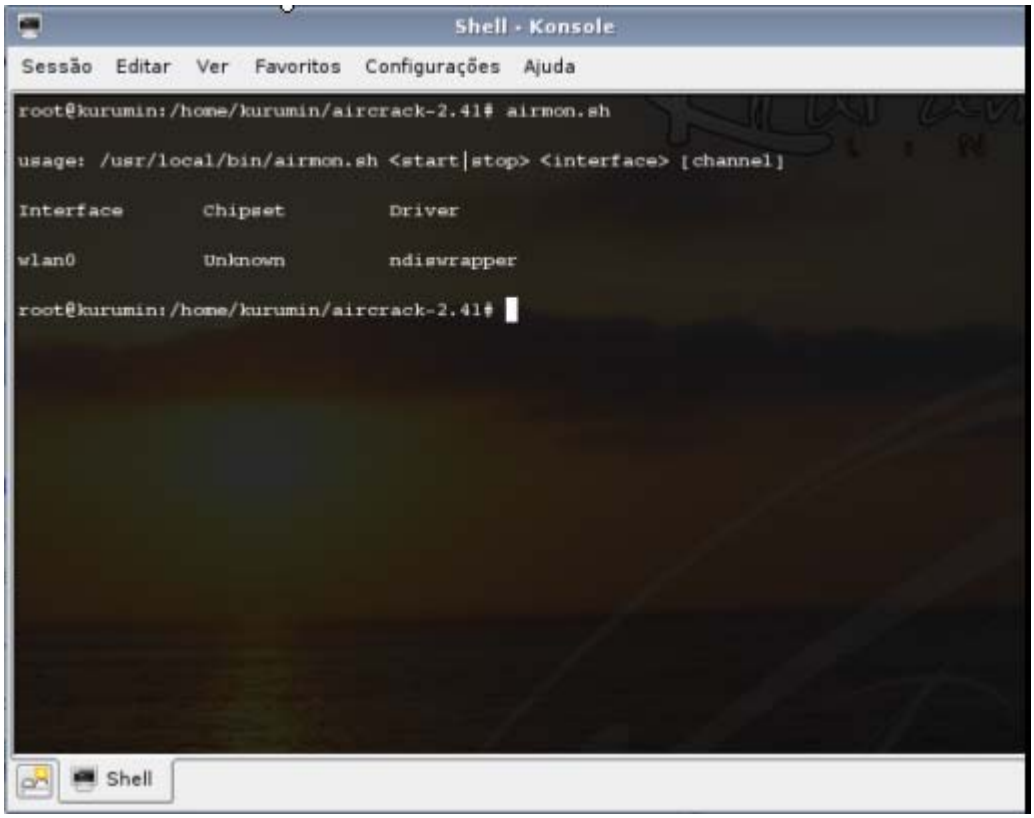

Figura 3.11 – Tela do Airmon.

Observamos que na figura foi identificada a interface ***wlan0***, já o chipset não foi identificado devido ao uso do ndiswrapper, o qual emula uma placa de rede para a qual ainda não existam drivers disponíveis para Linux.

Já o Airodump é a ferramenta que permite a captura do tráfego da rede. O Airodump deverá ser utilizado para capturar o tráfego porque é possível determinar qual será a rede monitorada. Ou seja, caso existam redes wireless de outras empresas próximas àquela que se deseja monitorar, a utilização do Airodum permitirá o monitoramento apenas do tráfego desejado.

3.4 TÉCNICAS DE ATAQUES A REDES SEM FIO

Para garantirmos a segurança em uma rede qualquer é necessário que, primeiramente se conheçam os tipos de ataque que poderão ser desferidos contra esta rede. Basicamente podemos fazer a seguinte classificação para os meios de intromissão:

- Interrupção: é o tipo de ataque em que o intruso interrompe o fluxo dos dados para que os mesmos não cheguem ao seu destino.
- Intersecção: ocorre quando o intruso captura o tráfego da rede, Essa técnica consiste em colocar um computador entre dois computadores que se comunicam via rede; em seguida, o computador intermediário se faz passar por um dos computadores originais. Essa técnica permite que o computador intermediário obtenha uma conexão funcional com os computadores originais e tenha a capacidade de ler ou modificar mensagens trocadas entre os computadores originais, enquanto os usuários desses computadores crêem estar comunicando entre si.

3.4.1 – MAC SPOFFING:

Uma das formas de se gerenciar o acesso a uma rede sem fio é mantendo uma lista com todos os endereços MAC das máquinas que terão permissão de acesso.

Entretanto, é possível que se realize a troca do endereço físico. Desta maneira, qualquer atacante mal intencionado pode capturar, através de técnicas de Eavesdrooping & Espionage, um endereço MAC válido de um cliente, efetuar a troca de seu próprio endereço pelo do cliente e utilizar a rede como um usuário autorizado.

Os ataques que forjam um endereço MAC podem ter diversos objetivos, dentre eles o de ocultar a presença do atacante na rede. Em virtude de a maioria dos detectores de ataque (IDS) não examinarem as camadas mais baixas do protocolo TCP/IP (normalmente analisam até a camada 3), o atacante pode utilizar-se de um ataque de força bruta, mudando sucessivamente o endereço MAC, buscando encontrar um que esteja autorizado no controle de acesso do concentrador e que por conseqüência, permita o acesso. Desta maneira, o atacante pode construir uma lista de endereços MAC válidos para uma determinada rede, utilizando de acordo com a sua conveniência e disponibilidade, por exemplo, endereços pouco utilizados para evitar choque com usuários legítimos.

3.4.2 – NEGAÇÃO DE SERVIÇO (*DoS)*

Na negação de serviço – *Denial of Service DoS*- o ataque consiste em se deixar indisponíveis os serviços da rede.

Para as redes sem fio, que utilizam a freqüência *ISM*, na faixa de 2,4 GHz, existe um mecanismo relativamente simples de se prover um ataque do tipo *DoS*, trata-se de ligar um aparelho qualquer que trabalhe na mesma faixa de freqüência daquela da rede. Aparelhos domésticos como telefones celulares, forno de microondas, telefones sem-fio e aparelhos de monitoramento infantil trabalham nesta faixa de frequência e podem ser utilizados para provocar *DoS* em uma rede.

Os ataques também podem ser realizados a partir do processo de o atacante se fazer passar pelo ponto de acesso. Assim, eles se utilizam do mesmo ESSID e endereço MAC do ponto de acesso da rede e a inundam com solicitações de dissociação.

Os pedidos de dissociação obrigam os *hosts* a se desassociarem e se re-associarem à rede. Se estas dissociações são realizadas em intervalos curtos de tempo, teremos um DoS, pois os clientes não conseguirão permanecer conectados por muito tempo.

Outra maneira de causar uma negação de serviço é inundar a rede com tráfego aleatório.

Além disso, ataques de DoS podem ocorrer sem que haja intenção maliciosa com redes vizinhas, já que, geralmente, cada fabricante utiliza o mesmo canal *default* para os seus equipamentos. Assim, uma rede pode interferir na outra, mesmo de forma não intencional.

3.4.3 – ASSOCIAÇÃO MALICIOSA:

Neste tipo de ataque o atacante se faz passar por um ponto de acesso, assim os membros da rede irão enganar-se acreditando estarem conectados à rede real.

A falha no sistema que está por trás da associação maliciosa está no fato de o ponto de acesso não poder ser identificado de forma inequívoca.

Uma das ferramentas que são comumentemente utilizadas para a associação maliciosa é o FakeAp. O FakeAp possui características que podem levar o cliente a imaginar que está conectado ao ponto de acesso correto, dentre estas características, podemos destacar:

- Pode receber conexões em um canal específico.
- Pode utilizar ESSID específico.

- Pode utilizar um endereço MAC específico ou o padrão de um determinado fabricante.
- Pode utilizar uma chave WEP determinada pelo usuário.
- Permite a configuração manual da potência de saída.

3.4.4 – ACESSO NÃO AUTORIZADO:

Devido à constante redução nos preços dos equipamentos necessários para a construção de uma rede sem fio, fica cada vez mais simples para usuários não autorizados entrarem em uma rede.

Desta forma ele pode criar um ponto de acesso com sinal mais forte que os demais pontos da rede, tendo prioridade na conexão e tornando-se uma rede de captura de senhas, ESSDI ou quaisquer outras informações que possam ser posteriormente decriptadas.

3.4.5 – WARDRIVING:

Wardriving é uma forma de ataque que foi difundida entre os hackers dos Estados Unidos e Europa, e mais recentemente no Brasil. Esta técnica de ataque consiste em se dirigir um veículo à procura de redes sem fio abertas, as quais estejam passíveis de serem invadidas.

Utilizando-se de um notebook e alguma antena caseira, que pode ser posicionada dentro ou fora do veículo o processo de captação da rede passa a ser mais simples.

Os atacantes buscam falhas nos protocolos, ou de redes de empresas que não mantém nenhum tipo de criptografia em suas redes. Normalmente, são descobertas falhas na rede e consegue-se estabelecer a conexão. Alguns ataques são realizados por verdadeiras gangues que picham os muros próximos à localização da rede e descrevem os dados da mesma (como o ESSID e a chave WEP).

A prática é tão conhecida que em 3 de novembro de 2001 foi criado o Dia Mundial do Wardriving. No Brasil, existem sites que vendem camisetas e propagam símbolos próprios adequados à este tipo de ataque.

A propagação deste tipo de simbologia é conhecida como *Warchalking* , que é uma forma de comunicação inventado nos Estados Unidos, há aproximadamente 70 anos, durante a época da depressão. O warchalking era uma forma de comunicação utilizada pelos "Hobos" (andarilhos desempregados). Através de símbolos próprios os Hobos conseguiam se comunicar, informando, por exemplo, se em determinada residência havia um médico que não cobraria por uma consulta ou a existência de um lugar seguro para se fazer uma refeição.

Os símbolos básicos do Warchalking são apresentados na figura a seguir:

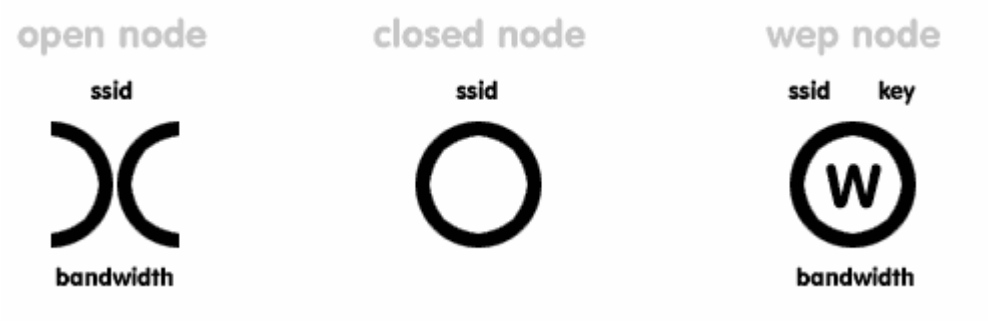

Figura 3.12 – Símbolos empregados no Warchalking.

Um par de semicírculos opostos em forma de "X", significa um "open node" ou, simplesmente, um link aberto. Um círculo fechado significa um "closed node". Um círculo com um "W" significa que a conexão está protegida por chave WEP ou WPA, geralmente indicada no canto superior direito. Abaixo do símbolo deve estar a velocidade do node. O SSID ou nome do hotspot deve ficar no topo da figura.

4 SEGURANÇA DENTRO DO AMBIENTE DO SENADO FEDERAL

4.1 INTRODUÇÃO

Com o avanço cada vez maior na utilização de aparelhos portáteis, como os notebooks e os PDA's (Personal Digital Assistance), pode-se verificar a agregação de diversas facilidades a estes aparelhos.

O Senado Federal e outros órgãos federais podem tirar grande vantagem na utilização de aparelhos portáteis para fomentar seus membros com informações que, de outra forma, somente poderiam ser obtidas através de meios estáticos, demandando tempo para tal aquisição. A mobilidade dentro de um ambiente como o referido é imprescindível na medida em que os senhores parlamentares poderão receber informação em tempo real e, desta forma, agilizar a tomada de decisões em situações urgentes, basta tomar como exemplo o fato notório do uso de aparelhos celulares durante as reuniões. Tais dispositivos facilitaram a execução dos trabalhos parlamentares, pois as informações podem chegar, em tempo real, aos senhores senadores através da assessoria parlamentar, embora também tenha trazido alguns inconvenientes como o excesso de ruído sonoro causado pelos sinais de aviso e os murmúrios provocados com a utilização dos telefones móveis.

Dentro do plenário do Senado Federal já existe um sistema de transmissão sem fio utilizando a tecnologia Wi-Fi e instalado pela Secretaria Especial de Informática – Prodasen, do Senado Federal. Este sistema fomenta os *tablets* instalados para cada um dos senadores, permitindo que os mesmos possam realizar consultas à intranet (como consultas à pauta do dia – onde são definidas todas as votações que serão realizadas) e também consultas à Internet.

Figura 4.13 – Tablets com sistema Wi-Fi instalado no plenário no Senado Federal.

Uma vez que o Senado já possui uma estrutura que garante que todos os sinais de vídeo e áudio gerados em discursos proferidos por parlamentares sejam armazenados para posterior consulta, criou-se a expectativa de que esta consulta pudesse ocorrer por meio de acesso como os PDA`s, ou seja, através da transmissão de streaming de áudio ou vídeo após a consulta realizada pelo parlamentar.

Esta expectativa gerou o tema para a realização deste trabalho, pois em determinado momento o gestor de tecnologia de informação necessitará tomar decisões a respeito de como a tecnologia funciona e os passos a serem adotados para a implementação desta. Assim ele poderá tomar este trabalho como base para suas decisões.

4.2 SISTEMAS DE ARMAZENAMENTO

Todo o áudio gravado dentro do Senado Federal é armazenado pela Secretaria Técnica de Eletrônica – STEL. Este áudio engloba as sessões que ocorrem no plenário, nas oito salas de comissão e em outros eventos que envolvam a atividade parlamentar, conforme ilustrado na figura 4.2:

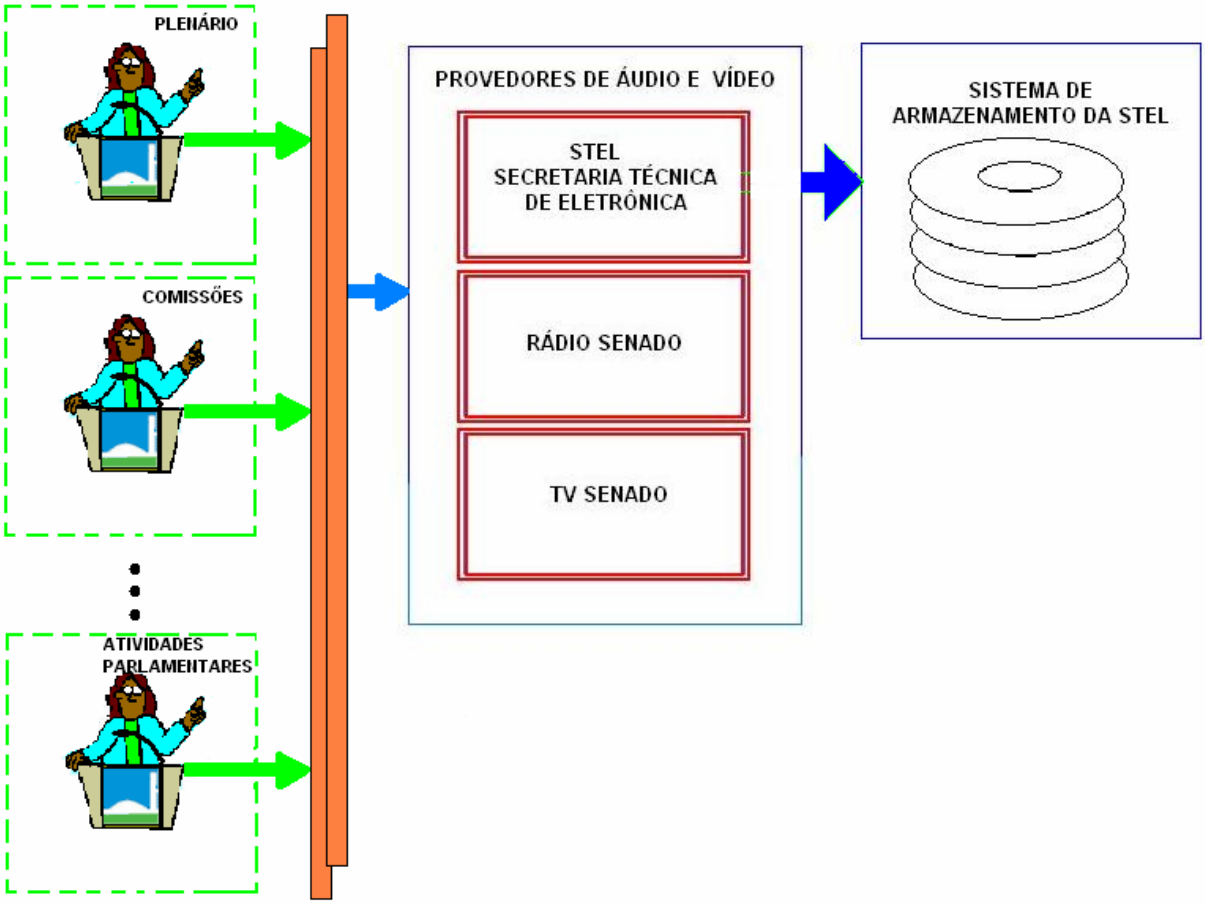

Figura 4.2 – Esquema simplificado do sistema de armazenamento do sinal de áudio no Senado Federal.

4.2.1 – Armazenamento Analógico:

Ainda há pouco tempo (cerca de 5 anos) o sinal de áudio era armazenado na forma analógica em fitas de rolo, figura.4.3:

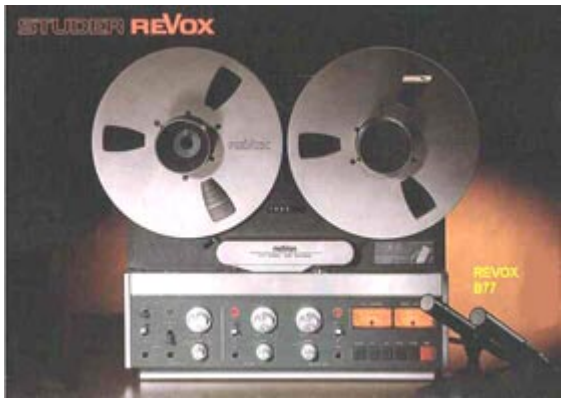

Figura 4.3 – Sistema de armazenamento analógico

Por uma decisão de TI da época em que este tipo de armazenamento era considerado como mais robusto e tecnicamente o mais viável, ele foi adotado e a aquisição de equipamentos, insumos, treinamento de pessoal, inclusive na área técnica, foi realizada. Percebe-se que foi uma decisão acertada uma vez que este sistema perdurou desde os anos 70 com a utilização dos mesmos aparelhos e das mesmas mídias. Assim não foi necessária nenhuma mudança no parque instalado mesmo com o aparecimento de novas tecnologias ou de modelos superiores de máquinas.

Sabe-se que, estruturalmente, as fitas magnéticas são formadas por uma base coberta por uma superfície de gravação — um polímero onde está disperso o pigmento magnético (como óxidos de ferro ou de cromo). Normalmente adiciona-se a esta superfície um componente lubrificante. A fita pode ter uma cobertura traseira, para proteção e redução de atrito.

Em alguns casos, a superfície de gravação não é composta de pigmentos dispersos em polímero, mas de uma finíssima camada metálica depositada diretamente sobre a base.

Um dos maiores problemas enfrentados durante o período em que se utilizou o sistema de armazenamento baseado em fita magnéticas consistiu no tamanho das mídias, uma vez que para uma gravação de 2 horas consumia-se um rolo completo de fita, gerando um volume

grande para armazenamento. Outro fator observado foi a perda de qualidade da informação com o passar do tempo.

4.2.2 – Armazenamento Digital - Minidisc:

Ainda mais recentemente, final dos anos 90, uma nova decisão de TI sugeriu que o parque de máquinas para armazenamento deveria ser substituído em decorrência dos seguintes fatores:

⇒ Chegada do formato de armazenamento digital, garantindo, dentro de certos parâmetros, a qualidade de informação.

⇒ Desgaste natural das máquinas analógicas existentes,

⇒ Dificuldades em se conseguir mídias novas no mercado brasileiro,

Com isso, a decisão no sentido do novo tipo de mídia para o armazenamento digital foi tomada favoravelmente aos aparelhos de minidisc, desenvolvido, principalmente, pela Sony.

O minidisc é um disco armazenado em um estojo similar aos disquetes de 3 ½ polegadas, conforme ilustrado na figura:

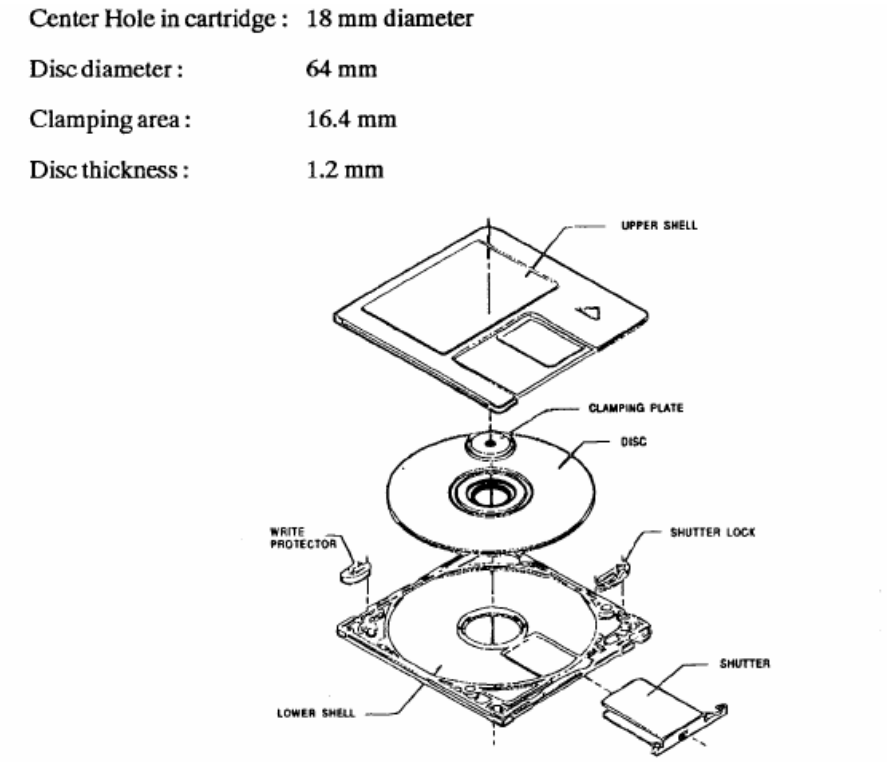

Figura 4.4 – Mídia de armazenamento do tipo minidisc.

A grande vantagem trazida com o sistema de gravação em minidisc consiste na diminuição da mídia de armazenamento, pois com isso consegue-se a mesma capacidade de armazenamento de áudio, cerca de duas horas, em uma mídia com cerca de 10% do tamanho da fita magnética. Assim ocorreu uma redução importante do espaço necessário para a estocagem do material digitalizado, além vantagem da manutenção da qualidade por um tempo estimado de 25 anos e, portanto muito superior ao da fita magnética analógica.

A grande desvantagem apresentada por este tipo de mídia consiste em se tratar de um sistema proprietário da empresa Sony, que utiliza um padrão de codificação digital conhecido como ATRAC (semelhante ao MP3). Com isto é dificultada a entrada de empresas fornecedores na competição pelo fornecimento de insumos o que acarreta grandes desvantagens, principalmente para o serviço público, onde o processo de aquisição de quaisquer bens prioriza a concorrência por meio das licitações.

4.2.3 – Armazenamento Digital - PetaSite:

A mais recente decisão em gerenciamento de tecnologia da informação ocorreu no sentido de se retirar o armazenamento digital em mídias de minidisc e adotar-se o armazenamento em uma solução de *storage* do tipo robô de fitas.

Tal solução baseou-se no estudo das tendências das tecnologias atuais, viabilidade de compra para o serviço público e tempo de armazenamento.

Com esta solução pretende-se garantir o armazenamento de todo o áudio e vídeo produzido dentro do Senado Federal envolvendo as atividades parlamentares. Deve-se observar que o sistema ainda está em fase de montagem e a capacidade de armazenamento em fitas, hoje adquirida é de 1,5 PetaBytes.

O sistema de armazenamento opera da seguinte forma:

O sinal de áudio é digitalizado nas estações utilizando software proprietário. As estações possuem 1 Terabytes de capacidade de armazenamento. A digitalização é feita no formato mp3 à taxa de 128 Kbps. Após a catalogação inicial o arquivo é transferido para servidores. Estes são compostos de diversos HDs que utilizam tecnologia RAID totalizando 3,44 Terabytes de capacidade de armazenamento. A estação é apresentada na figura abaixo:

Figura 4.5 – Estação de captura de áudio e vídeo

Os arquivo armazenados nos servidores são automaticamente transferidos para o robô e recuperados quando necessários.

Um robô de fitas opera da seguinte forma. Um braço mecânico corre sobre um trilho movimentando as fitas de um slot para o drive de leitura/gravação. As fitas são identificadas por códigos de barras, possuem capacidade 500 GB e empregam tecnologia S-AIT (Super Advanced Intelligent Tape).

O robô Petasite é apresentado na figura a seguir.

Figura 4.6 - Petasite

O processo de digitalização de todo o acervo audiovisual do Senado Federal ocorrerá de forma gradual. O acervo atual é de aproximadamente 20.000 horas de vídeo e 18.000 horas de áudio. A taxa de armazenamento do vídeo será de 25 Mbps e o áudio a 128 Kbps.

4.3 STREAMING DE ÁUDIO

Emprega-se a tecnologia de *streaming* para tornar mais leve e rápido o download e a execução de áudio e video na internet, uma vez que com esta técnica, pode-se executar a reprodução dos arquivos de áudio ou do vídeo enquanto ainda se esta´realizando o download.

Caso não fosse empregada a técnica do *streaming*, para mostrar um conteúdo multimídia, o arquivo inteiro teria de ser primeiramente descarregado, como em um download, e mais tarde executá-lo, para finalmente ver e/ou ouvir o conteúdo do arquivo. Entretanto, o *streaming* permite que esta tarefa seja realizada de uma maneira mais rápida para o usuário.

O termo *streaming* deriva da palavra stream, ou seja, fluxo contínuo, pois os pacotes são enviados na forma de uma corrente que ao chegar ao seu destino permite que estes sejam remontados. Este tipo de armazenamento é denominado *buferização*.

Assim, neste processo, o computador do cliente conecta-se ao servidor e este, começa a lhe mandar o arquivo. O cliente começa a receber o arquivo e constrói um buffer onde começa a salvar a informação. Quando se enche o buffer com uma pequena parte do arquivo, o cliente começa a executar o arquivo ao mesmo tempo em que o download continua a ser executado. O sistema é sincronizado de tal forma que arquivo possa ser executado ao mesmo tempo em que o download é processado, assim, quando o download for concluído a execução do mesmo também o será. Caso ocorra de a conexão sofrer alterações na velocidade, a informação armazenada durante o processo de *bufferização* será utilizada, garantindo, desta forma, a execução do arquivo sem travamentos. Caso a conexão seja totalmente perdida, o buffer se esvaziará e a execução do arquivo será perdida.

4.3.1 – Ferramentas para Streaming:

Na verdade, o processo de streaming pode ser observado com freqüência em nossos computadores. É o que fazem aplicativos como o Real Player ou o Windows Media Player,

programas que se instalam como plug-ins nos navegadores para receber e mostrar conteúdos multimídia por streaming.

Quando pretendemos incluir áudio ou vídeo nas páginas o melhor então, é utilizar a tecnologia de streaming. Para isso simplesmente temos que salvar os arquivos multimídia com o formato de um dos programas de streaming e seguir umas pequenas normas na hora de subi-los à Internet e colocá-los na página. As normas para seguir são próprias de cada sistema e não as veremos aqui.

Para converter os arquivos de áudio e vídeo ao formato de cada programa de streaming são utilizados programas especiais que podem ser baixados das páginas de cada tecnologia. Por exemplo, o programa para converter ao formato para o Real Player é o Real Producer.

Na hora de desenvolver o web com conteúdos multimídia será necessário tomara a decisão relativa à tecnologia de streaming que será empregada.

As principais ferramentas para streaming são:

Real Media: é possivelmente a mais popular. Também é a empresa com mais experiência no setor e desenvolve muitos produtos orientados à distribuição de arquivos multimídia.

Windows Media: é a aposta da Microsoft. Já possui uma cota de usuários muito importante e certamente aumentará com rapidez já que Microsoft inclui o plug-in na instalação típica dos seus sistemas operacionais.

Quick Time: trata-se da ferramenta da Apple, possui a menor percentagem de usuários.

4.3.2 – Servidores de Streaming:

Á princípio não é necessário contar com um servidor especial para colocar arquivos de áudio ou vídeo para download via streaming. Qualquer servidor pode mandar a informação e é o cliente quem se encarrega de processá-la para poder executá-la na medida em que for sendo recebida.

Entretanto, existem servidores especiais preparados para transmitir streaming. Embora em muitas ocasiões não seja necessária sua utilização, eles podem trazer alguns benefícios

para o cliente, como a verificação da velocidade da conexão para determinar a taxa de transmissão e conseqüentemente a qualidade na execução do arquivo.

Em determinados casos, como para transmissões de rádios ou a transmissão de um evento ao vivo, será imprescindível a utilização de um servidor específico.

4.4 SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DO SENADO FEDERAL.

Após o processo de armazenamento de dados digitais no Petasite é preciso garantir os pilares da segurança da informação. Mesmo para informações completamente públicas, sem nenhuma restrição de acessibilidade, deverá ser garantido um mínimo de segurança. Por exemplo, impedir que um usuário não autorizado possa alterar o conteúdo ou subescrever uma informação de áudio, vídeo ou texto.

Segundo a Norma NBR 17799 [27], a segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, procurando assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos.

A aplicação dos quesitos desta norma procura preservar os três atributos básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

i. A Confidencialidade que deverá garantir que a informação será acessada somente por pessoas autorizadas. O grau de acesso poderá ser dividido em diversos níveis dependendo do conteúdo da informação.

ii. A Integridade que deverá garantir a exatidão da informação e dos métodos de processamento.

iii. A disponibilidade que deverá garantir que somente os usuários autorizados, em seus diversos níveis, obtenham acesso à informação, sempre que necessário.

Apesar da maioria dos documentos do Senado Federal apresentarem certo grau de publicidade dependendo do tipo de informação é preciso garantir que a informação armazenada possua requisitos confiáveis de segurança.

É necessário planejar e implementar um programa de gerenciamento arquivístico de documentos eletrônicos de maneira a garantir a confiabilidade desses registros. Os mecanismos de arquivo consideram que a confiabilidade possui duas dimensões qualitativas: fidedignidade e autenticidade.

Fidedignidade significa que o documento é capaz de representar os fatos que atesta, enquanto autenticidade significa que o documento é o que diz ser.

Ao dar acesso aos documentos arquivísticos, mesmo que eles sejam de conteúdo público, é necessário garantir que o sistema não seja vulnerável a alterações e que tenha mecanismos de auditoria e de segurança [30]. O gestor deverá prever no sistema de controle da informação, o nível de acesso permitido para cada usuário e registrar o acesso completo ou a tentativa de acesso às informações sigilosas.

O Petasite não armazenará apenas documentos públicos. Haverá o conteúdo de produções específicas da TV Senado, bem como conteúdos de outras instituições que poderão ser anexados por convênio ou por compra. Por exemplo, o convênio com a Rádio Nacional. Nele, a digitalização será efetuada por conta do Senado Federal com a condição de que o conteúdo poderá ser então utilizado nas produções da TV e da Rádio Senado. Nesse caso, os conteúdos estarão disponíveis no Petasite, mas nem todos os usuários poderão utilizá-los. Por conta disso, será previsto, nos requisitos do sistema, a utilização de credenciais de segurança e perfis específicos para os diversos grupos de usuários, bem como, controles específicos para gerenciamento das questões referentes ao Direito Autoral.

O Senado Federal, atualmente possui uma Comissão Permanente de Acesso a Documentos, que está estudando e elaborando um ATO dispondo sobre o sigilo dos dados, das informações e dos documentos de interesse da segurança da sociedade e do Estado, no âmbito do Senado. O ATO, ainda em fase de estudo por parte da Comissão Permanente, foi baseado no decreto N° 4553 [31]. Este decreto está apresentado no Anexo I.

O ATO em seu artigo 1° estabelece os diversos graus de sigilo, que deverão ser obedecidos na classificação dos documentos produzidos pelo Senado Federal, em qualquer suporte, que digam respeito à segurança da sociedade e do Estado e à intimidade do indivíduo. O ATO regula ainda o acesso aos documentos públicos de natureza sigilosa, bem como disciplina, no âmbito do Senado Federal, os procedimentos relativos à preservação e à

salvaguarda de documentos, dados, informações, materiais, comunicações, sistemas, áreas e instalações sigilosas.

O ATO em seu artigo 6° estabelece que os dados, as informações e os documentos sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos.

i. Os dados ultra-secretos são as informações e os documentos, referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

ii. Os dados secretos são as informações e os documentos, referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

iii. Os dados confidenciais são as informações e os documentos, que, no interesse do Poder Legislativo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

iv. Os dados reservados são as informações e os documentos, cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

O ATO em seu artigo 32° estabelece que a Comissão Permanente de Acesso a Documentos deverá efetuar os seguintes procedimentos:

i. Regular o acesso e a salvaguarda aos dados, informações e documentos do Senado Federal e Congresso Nacional;

ii. Fixar as categorias de sigilo dos documentos;

iii. Classificar os documentos, segundo as categorias pré-fixadas;

iv. Regular a reprodução dos documentos sigilosos.

O Gestor de TI deverá prever um sistema de gerenciamento de arquivos digitais – (SGAD) com controles de segurança da informação, preferencialmente, basedos no modelo de requisitos para a gestão de arquivos eletrônicos (MoReq) [28], que enumera de forma

genérica os requisitos funcionais que um sistema deve possuir para o gerenciamento de arquivos digitais. O SGAD é um software especializado consistindo de pacotes integrados que dependem da natureza da organização em estudo.

O SGAD deverá controlar quem está autorizado a acessar os documentos e em que circunstâncias o acesso será permitido, visto que os documentos podem conter informações sigilosas. Os acessos aos documentos digitais devem ser registrados nas rotinas de auditoria para garantir a admissibilidade jurídica e auxiliar na recuperação da informação. Uma rotina de auditoria deverá possuir os registros de procedimentos executados pelo SGAD. Estes procedimentos incluem ações empreendidas pelos usuários e as iniciadas automaticamente em conseqüência de parâmetros do sistema [29]. O SGAD deverá estar munido de controles integrados para proporcionar o backup freqüente dos documentos digitais juntamente com os metadados relacionados, além de permitir restaurar rapidamente o backup em caso de problemas devido a falhas do sistema, contingência, quebra de segurança, etc. Em alguns casos específicos é necessário limitar o acesso do usuário à informação, utilizando um plano de categorias de segurança e credenciais de segurança. Estas credenciais de segurança prevalecem sobre quaisquer direitos que possam ser atribuídos aos usuários do sistema. Isto pode ser obtido através da atribuição de uma ou mais “Categorias de Segurança” a classes, arquivos digitais ou documentos digitais. Em seguida, pode-se atribuir aos usuários uma ou mais credenciais de segurança que impeçam o acesso a todas as classes, arquivos digitais e documentos digitais em categorias de segurança superiores [29].

Um SGAD deve possuir, no mínimo, os seguintes requisitos de controle e segurança [28]:

i. Permitir que um Administrador limite a usuários ou grupos de usuários o acesso aos documentos digitais, arquivos digitais e metadados.

ii. Permitir que o Administrador associe, aos atributos do perfil de usuário, indicação dos campos de metadados, documentos digitais ou arquivos digitais aos quais o usuário tenha acesso. Os atributos do perfil atuarão no sentido de:

- Proibir o acesso ao sistema sem a autenticação do usuário de acordo como o perfil atribuído a ele.
- Restringir o acesso do usuário a documentos e arquivos digitais específicos.
- Restringir o acesso do usuário a classes específicas do plano de classificação.

- Restringir o acesso do usuário de acordo com a credencial de segurança obtida pelo mesmo.
- Restringir o acesso do usuário a certas ações (por exemplo ler, atualizar ou eliminar campos de metadados específicos).
- Recusar o acesso posterior a uma data determinada.
- Designar o usuário para um grupo ou grupos determinados.

O CEDOC prevê a disponibilidade de documentos na internet em baixíssima resolução, com selo de segurança do Senado Federal. As solicitações dos documentos em alta resolução terão que ser feitas com base em critérios específicos e com orientações expressas para o usuário quanto à utilização do conteúdo.

Os documentos confidenciais deverão ter um tratamento diferenciado. Por exemplo, as informações originadas de uma sessão secreta não deverão ser armazenadas no Petasite. Para isso deverão ser adotados procedimentos específicos, como gravar o áudio em uma mídia particular tipo *Minidisc* e, mediante recibo, entregá-la ao Presidente ou Secretário da comissão.

5 CONCLUSÃO

Esta monografia apresentou de forma contextualizada os aspectos relativos a transmissão segura de streaming de áudio e vídeo em um ambiente seguro dentro do Senado Federal.

Seu objetivo principal foi estudar as formas de transmissão e possibilidades de invasão em uma rede sem fio utilizando o padrão Wi-Fi.

Observou-se que a grande mobilidade e produtividade adquiridas com a implantação de um sistema sem fio, até o momento, não garantem a segurança absoluta das informações.

As informações armazenadas no Petasite e originadas de fontes públicas, sem restrições quanto ao conteúdo apresentado, poderão ser disponibilizadas na rede sem fio do Senado Federal, ressalvados os requisitos mínimos de segurança, por exemplo impedindo que o usuário possa alterar os dados, garantindo assim a fidedignidade e a autenticidade das informações.

Devido aos riscos e vulnerabilidades encontrados no padrão IEEE 802.11, relativos à segurança, o mesmo ainda não pode ser aplicado em situações que exijam confidencialidade absoluta, como alguns casos encontrados dentro do Senado Federal, onde são tomadas decisões importantes para a nação.

As principais vulnerabilidades encontradas são:

- Falhas nas especificações dos padrões;
- Limitações dos equipamentos utilizados;
- Falha na configuração das redes.

Apesar de muitos usuários e administradores de rede sem fio negligenciarem a segurança, por desconhecerem o risco ou por medo de perder velocidade na transmissão dos dados, é possível tornar a rede mais segura. Para isso é necessário que o gestor tome, pelo menos, as seguintes precauções:

- Conscientize os usuários dos riscos e das vulnerabilidades das redes sem fio;
- Utilize um protocolo de criptografia;
- Utilize antivírus e firewall atualizados;
- Configure corretamente os equipamentos utilizados;

- Crie mecanismos que dificultem a operação dos atacantes limitando os equipamentos que podem acessar a rede;
- Utilize equipamentos específicos e de grande eficiência na confidencialidade dos dados.

Uma contribuição desta monografia, após o levantamento realizado dos aspectos de segurança, reside no fato de que o gestor de Tecnologia da Informação – TI, poderá utilizá-la para a tomada de decisão relativa a qual tipo de rede Wi-Fi poderá ser adquirido e os aspectos de segurança que deverão ser considerados no momento desta decisão.

As grandes dificuldades encontradas na elaboração dessa monografia residiram no fato de que o sistema de armazenamento digital ainda não está totalmente instalado e o Senado ainda não possui uma rede sem fio instalada, possibilitando a comunicação com o Centro de Documentação - CEDOC. Além disso o software de pesquisa ainda não foi totalmente desenvolvido. Com isso não foi possível a realização dos testes específicos, ficando os mesmos como sugestão para trabalhos futuros.

A sugestão de trabalhos futuros poderá também estar voltada para o levantamento de requisitos para as outras atividades do Senado Federal não diretamente relacionadas com o armazenamento e transmissão de streaming de áudio e vídeo da STEL. Entre elas podem-se incluir os requisitos de integração com a TV Senado, Rádio Senado e a Agência do Senado Federal.

Em suma, espera-se que esta monografia seja o ponto de partida para enfrentar os novos desafios propostos. Esta grande mudança de paradigma, de analógico para digital, deve ser administrada com muito rigor, já que as resistências serão enormes e a própria dinâmica da tecnologia digital vai propiciar novos aprendizados e novas rotinas para os técnicos e gestores de T.I. atuantes no Senado Federal.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] – Rufino, Nelson M. O. "*Segurança em Redes Sem Fio"*. Editora Novatec, 1ª edição, São Paulo, 2005.

[2] – Fleishman, G. "*Kit do iniciante em redes sem fio"*. Makrorn Books, 2ª edição, São Paulo, 2005.

[3] – Cátedra, Manuel F. "*Cell planning for wireless communications*". Artech House, Boston, 1999.

[4] – Saunders, Simom R. "*Antennas and propagation for wireless communication system*". John Wiley, 1999.

[5] – Tanembaum, A. S., "*Redes de Computadores*", Elsevier, 4ª edição, Rio de Janeiro, 2003.

[6] – Balanis Constantine A., "*Advanced Engineering Electromagnetics*", John Wiley, 1989.

[7] – Avila, Renato A. N., "*Streaming: crie sua própria radio web e TV digital*", Brasport, 1ª edição, Rio de Janeiro, 2004.

[8] – IEEE 802.11. "*IEEE 802.11 Specifications*", Acessado em 10/09/2006 em http:// /grouper.ieee.org/groups/802/11.

[9] – Conceição, A. F. ¸ Kon F., "*Adaptação de fluxos contínuos UDP sobre redes IEEE 802.11b,*" in Workshop de comunicação sem fio e computação móvel (WCSF),São Lourenço-MG, Brasil, Outubro 2003, pp. 91–101

[10] – Carvalho Filho, J. R. L., "*Um estudo de protocolos empregados na segurança de dados em redes sem fio – Padrão 802.11. 2005,* Monografia de Bacharelado em Ciências da Computação – Centro Universitário de João Pessoa – UNIPÊ.

[11] – Fransicatti, V. "*Segurança em Redes Sem Fio*", Monografia de Especialização em Redes de Coputadores - Universidade Estadual de Londrina, 2005.

[12] – Carrión, D. S. D., "*Implementação de um Ponto de Acesso Seguro para Redes 802.11b Baseado no Sistema Operacional Openbsd",* UFRJ, 2003.

[13] - Carrión, D. S. D., "*Avaliação de Protocolos de Autenticação em Redes Sem Fio",* Dissertação de Mestrado, UFRJ, 2005.

[14] – Velloso, P. B., "*Transmisão de Voz em Redes Ad Hoc*", Dissertação de Mestrado, UFRJ, 2003.

[15] - Lu, Cary, "*Largura de Banda",* Berkeley, 1ª edição, São Paulo, 1999.

[16] – AirDefense White Paper. "*Wireless LAN Security – What Hackers Know That You Don't***"**. Acessado em 07/06/2006, em : http://www.airdefense.net.

[17] – Maia, R.. "*Segurança em Redes Wireless***".** Acessado em 13/07/2006, em: http://www.gta.ufrj.br/seminarios/semin2003_1/rmaia/802_11i.html.

[18] - Martins, M.. "*Protegendo Redes Wireless 802.11b. White Paper***".** Acessado em 13/07/2006, em: http://www.modulo.com.br.

[19] – Silva, Adailton J. S. "*As Tecnologias de Redes Wireless***".** Acessado em: 01/07/2006, em: http://www.rnp.br/newsgen/9805/wireless.html.

[20] – Wi-Fi Alliance, Acessado em: 01/07/2006, em: http://www.rnp.br/newsgen/9805/wireless.html.

[21] - Puttini, R. S., Junior, Rafael T. S. *"Criptografia"***.** Acessado em: 15/06/2006, em: http://www.redes.unb.br/security/criptografia/cripto.html.

[22] – Kismet. Acessado em: 15/06/2006, em: http://www.kismetwireless.net.

[23] – Morimoto, C. E., *"Entendendo e Dominando o Linux"*. Acessado em: 15/06/2006, em: http://www.guiadohardware.net/ebooks/linux/index.html.

[24] - Morimoto, C. E., *"Kurumin – Desvendando seus Segreedos"*. Acessado em: 20/06/2006, em: http://www.guiadohardware.net/livros/kurumin/.

[25] – *"O Que é Streaming"*. Acessado em: 20/06/2006, em: http://www.criarweb.com/artigos/214.php.

[26] – Bonn, Carlos H. B., *"Vídeo Streaming"*. Acessado em: 20/06/2006, em: http://www.serpro.gov.br/publicacao/tematec/tematec/2004/ttec71.

[27] - Norma NBR ISO/IEC 17799 / 2000.

[28] - MOREQ - Model Requirements for the management of electronic records - Modelo de requisitos para a gestão de arquivos eletrônicos.
http://www.cornwell.co.uk/moreq.html.

[29] – Almeida, Demétrius Bicalho Félix,. Toscano, Ricardo Guedes Acioli., *"Requisitos para o Sistema de Gestão de Arquivos Audiovisuais Digitais do Senado Federal"*. Brasília, 2006.

[30] – Rondinelli, Roseli Curi., *"Gerenciamento Arquivístico de Documentos Eletrônicos"*. Editora FGV, 2ª edição, Rio de Janeiro, 2004.

[31] - DECRETO Nº 4.553, DE 27 DE DEZEMBRO DE 2002 . Acessado em: 28/09/2006, em: http://www.arquivonacional.gov.br

ANEXO I – DECRETO Nº 4.553, DE 27 DE DEZEMBRO DE 2002

Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, incisos IV e VI, alínea "a", da Constituição, e tendo em vista o disposto no art. 23 da Lei nº 8.159, de 8 de janeiro de 1991,

DECRETA:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Decreto disciplina a salvaguarda de dados, informações, documentos e materiais sigilosos, bem como das áreas e instalações onde tramitam.

Art. 2º São considerados originariamente sigilosos, e serão como tal classificados, dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco à segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.

Parágrafo único. O acesso a dados ou informações sigilosos é restrito e condicionado à necessidade de conhecer.

Art. 3º A produção, manuseio, consulta, transmissão, manutenção e guarda de dados ou informações sigilosos observarão medidas especiais de segurança.

Parágrafo único. Toda autoridade responsável pelo trato de dados ou informações sigilosos providenciará para que o pessoal sob suas ordens conheça integralmente as medidas de segurança estabelecidas, zelando pelo seu fiel cumprimento.

Art. 4º Para os efeitos deste Decreto, são estabelecidos os seguintes conceitos e definições:

I - autenticidade: asseveração de que o dado ou informação são verdadeiros e fidedignos tanto na origem quanto no destino;

II - classificação: atribuição, pela autoridade competente, de grau de sigilo a dado, informação, documento, material, área ou instalação;

III - comprometimento: perda de segurança resultante do acesso não-autorizado;

IV - credencial de segurança: certificado, concedido por autoridade competente, que habilita determinada pessoa a ter acesso a dados ou informações em diferentes graus de sigilo;

V - desclassificação: cancelamento, pela autoridade competente ou pelo transcurso de prazo, da classificação, tornando ostensivos dados ou informações;

VI - disponibilidade: facilidade de recuperação ou acessibilidade de dados e informações;

VII - grau de sigilo: gradação atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;

VIII - integridade: incolumidade de dados ou informações na origem, no trânsito ou no destino;

IX - investigação para credenciamento: averiguação sobre a existência dos requisitos indispensáveis para concessão de credencial de segurança;

X - legitimidade: asseveração de que o emissor e o receptor de dados ou informações são legítimos e fidedignos tanto na origem quanto no destino;

XI - marcação: aposição de marca assinalando o grau de sigilo;

XII - medidas especiais de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade, legitimidade e disponibilidade de dados e informações sigilosos. Também objetivam prevenir, detectar, anular e registrar ameaças reais ou potenciais a esses dados e informações;

XIII - necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa possuidora de credencial de segurança, tenha acesso a dados ou informações sigilosos;

XIV - ostensivo: sem classificação, cujo acesso pode ser franqueado;

XV - reclassificação: alteração, pela autoridade competente, da classificação de dado, informação, área ou instalação sigilosos;

XVI - sigilo: segredo; de conhecimento restrito a pessoas credenciadas; proteção contra revelação não-autorizada; e

XVII - visita: pessoa cuja entrada foi admitida, em caráter excepcional, em área sigilosa.

CAPÍTULO II

DO SIGILO E DA SEGURANÇA

Seção I

Da Classificação Segundo o Grau de Sigilo

Art. 5º Os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos.

§ 1º São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

§ 2º São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

§ 3º São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

§ 4º São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

Art. 6º A classificação no grau ultra-secreto é de competência das seguintes autoridades:

I - Presidente da República;
II - Vice-Presidente da República;
III - Ministros de Estado e equiparados; e
IV - Comandantes da Marinha, do Exército e da Aeronáutica.
Parágrafo único. Além das autoridades estabelecidas no caput, podem atribuir grau de sigilo:
I - secreto, as autoridades que exerçam funções de direção, comando ou chefia; e
II - confidencial e reservado, os servidores civis e militares, de acordo com regulamentação específica de cada Ministério ou órgão da Presidência da República.
I - Presidente da República; (Redação dada pelo Decreto nº 5.301, de 2004)
II - Vice-Presidente da República; (Redação dada pelo Decreto nº 5.301, de 2004)
III - Ministros de Estado e autoridades com as mesmas prerrogativas; (Redação dada pelo Decreto nº 5.301, de 2004)
IV - Comandantes da Marinha, do Exército e da Aeronáutica; e (Redação dada pelo Decreto nº 5.301, de 2004)
V - Chefes de Missões Diplomáticas e Consulares permanentes no exterior. (Incluído pelo Decreto nº 5.301, de 2004)
§ 1o Excepcionalmente, a competência prevista no caput pode ser delegada pela autoridade responsável a agente público em missão no exterior. (Incluído pelo Decreto nº 5.301, de 2004)
§ 2o Além das autoridades estabelecidas no caput, podem atribuir grau de sigilo: (Renumerado do parágrafo único pelo Decreto nº 5.301, de 2004)
I - secreto: as autoridades que exerçam funções de direção, comando, chefia ou assessoramento, de acordo com regulamentação específica de cada órgão ou entidade da Administração Pública Federal; e (Redação dada pelo Decreto nº 5.301, de 2004)
II - confidencial e reservado: os servidores civis e militares, de acordo com regulamentação específica de cada órgão ou entidade da Administração Pública Federal. (Redação dada pelo Decreto nº 5.301, de 2004)

Art. 7º Os prazos de duração da classificação a que se refere este Decreto vigoram a partir da data de produção do dado ou informação e são os seguintes:

I - ultra-secreto: máximo de cinqüenta anos;
II - secreto: máximo de trinta anos;
III - confidencial: máximo de vinte anos; e
IV - reservado: máximo de dez anos.

§ 1º O prazo de duração da classificação ultra-secreto poderá ser renovado indefinidamente, de acordo com o interesse da segurança da sociedade e do Estado.
§ 2º Também considerando o interesse da segurança da sociedade e do Estado, poderá a autoridade responsável pela classificação nos graus secreto, confidencial e reservado, ou autoridade hierarquicamente superior competente para dispor sobre o assunto, renovar o prazo de duração, uma única vez, por período nunca superior aos prescritos no caput.

Art. 7o Os prazos de duração da classificação a que se refere este Decreto vigoram a partir da data de produção do dado ou informação e são os seguintes: (Redação dada pelo Decreto nº 5.301, de 2004)

I - ultra-secreto: máximo de trinta anos; (Redação dada pelo Decreto nº 5.301, de 2004)
II - secreto: máximo de vinte anos;(Redação dada pelo Decreto nº 5.301, de 2004)
III - confidencial: máximo de dez anos; e (Redação dada pelo Decreto nº 5.301, de 2004)
IV - reservado: máximo de cinco anos. (Redação dada pelo Decreto nº 5.301, de 2004)

Parágrafo único. Os prazos de classificação poderão ser prorrogados uma vez, por igual período, pela autoridade responsável pela classificação ou autoridade hierarquicamente superior competente para dispor sobre a matéria. (Incluído pelo Decreto nº 5.301, de 2004)

Seção II

Da Reclassificação e da Desclassificação

Art. 8º Dados ou informações classificados no grau de sigilo ultra-secreto somente poderão ser reclassificados ou desclassificados, mediante decisão da autoridade responsável pela sua classificação.

Art. 9º Para os graus secreto, confidencial e reservado, poderá a autoridade responsável pela classificação ou autoridade hierarquicamente superior competente para dispor sobre o assunto, respeitados os interesses da segurança da sociedade e do Estado, alterá-la ou cancelá-la, por meio de expediente hábil de reclassificação ou desclassificação dirigido ao detentor da custódia do dado ou informação sigilosos.

Parágrafo único. Na reclassificação, o prazo de duração reinicia-se a partir da data da formalização da nova classificação.
Parágrafo único. Na reclassificação, o novo prazo de duração conta-se a partir da data de produção do dado ou informação. (Redação dada pelo Decreto nº 5.301, de 2004)

Art. 10. A desclassificação de dados ou informações nos graus secreto, confidencial e reservado será automática após transcorridos os prazos previstos nos incisos II, III e IV do art. 7º, salvo no caso de renovação, quando então a desclassificação ocorrerá ao final de seu termo.
Art. 10. A desclassificação de dados ou informações nos graus ultra-secreto, confidencial e reservado será automática após transcorridos os prazos previstos nos incisos I, II, III e IV do art. 7o, salvo no caso de sua prorrogação, quando então a desclassificação ocorrerá ao final de seu termo. (Redação dada pelo Decreto nº 5.301, de 2004)

Art. 11. Dados ou informações sigilosos de guarda permanente que forem objeto de desclassificação serão encaminhados à instituição arquivística pública competente, ou ao arquivo permanente do órgão público, entidade pública ou instituição de caráter público, para fins de organização, preservação e acesso.

Parágrafo único. Consideram-se de guarda permanente os dados ou informações de valor histórico, probatório e informativo que devam ser definitivamente preservados.

Art. 12. A indicação da reclassificação ou da desclassificação de dados ou informações sigilosos deverá constar das capas, se houver, e da primeira página.

CAPÍTULO III

DA GESTÃO DE DADOS OU INFORMAÇÕES SIGILOSOS

Seção I

Dos Procedimentos para Classificação de Documentos

Art. 13. As páginas, os parágrafos, as seções, as partes componentes ou os anexos de um documento sigiloso podem merecer diferentes classificações, mas ao documento, no seu todo, será atribuído o grau de sigilo mais elevado, conferido a quaisquer de suas partes.

Art. 14. A classificação de um grupo de documentos que formem um conjunto deve ser a mesma atribuída ao documento classificado com o mais alto grau de sigilo.

Art. 15. A publicação dos atos sigilosos, se for o caso, limitar-se-á aos seus respectivos números, datas de expedição e ementas, redigidas de modo a não comprometer o sigilo.

Art. 16. Os mapas, planos-relevo, cartas e fotocartas baseados em fotografias aéreas ou em seus negativos serão classificados em razão dos detalhes que revelem e não da classificação atribuída às fotografias ou negativos que lhes deram origem ou das diretrizes baixadas para obtê-las.

Art. 17. Poderão ser elaborados extratos de documentos sigilosos, para sua divulgação ou execução, mediante consentimento expresso:

I - da autoridade classificadora, para documentos ultra-secretos;

II - da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto, para documentos secretos; e

III - da autoridade classificadora, destinatária ou autoridade hierarquicamente superior competente para dispor sobre o assunto, para documentos confidenciais e reservados, exceto quando expressamente vedado no próprio documento.

Parágrafo único. Aos extratos de que trata este artigo serão atribuídos graus de sigilo iguais ou inferiores àqueles atribuídos aos documentos que lhes deram origem, salvo quando elaborados para fins de divulgação.

Seção II

Do Documento Sigiloso Controlado

Art. 18. Documento Sigiloso Controlado (DSC) é aquele que, por sua importância, requer medidas adicionais de controle, incluindo:

I - identificação dos destinatários em protocolo e recibo próprios, quando da difusão;

II - lavratura de termo de custódia e registro em protocolo específico;

III - lavratura anual de termo de inventário, pelo órgão ou entidade expedidores e pelo órgão ou entidade receptores; e

IV - lavratura de termo de transferência, sempre que se proceder à transferência de sua custódia ou guarda.

Parágrafo único. O termo de inventário e o termo de transferência serão elaborados de acordo com os modelos constantes dos Anexos I e II deste Decreto e ficarão sob a guarda de um órgão de controle.

Art. 19. O documento ultra-secreto é, por sua natureza, considerado DSC, desde sua classificação ou reclassificação.

Parágrafo único. A critério da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto, o disposto no caput pode-se aplicar aos demais graus de sigilo.

Seção III

Da Marcação

Art. 20. A marcação, ou indicação do grau de sigilo, deverá ser feita em todas as páginas do documento e nas capas, se houver.

§ 1º As páginas serão numeradas seguidamente, devendo cada uma conter, também, indicação do total de páginas que compõem o documento.

§ 2º O DSC também expressará, nas capas, se houver, e em todas as suas páginas, a expressão "Documento Sigiloso Controlado (DSC)" e o respectivo número de controle.

Art. 21. A marcação em extratos de documentos, rascunhos, esboços e desenhos sigilosos obedecerá ao prescrito no art. 20.

Art. 22. A indicação do grau de sigilo em mapas, fotocartas, cartas, fotografias, ou em quaisquer outras imagens sigilosas obedecerá às normas complementares adotadas pelos órgãos e entidades da Administração Pública.

Art. 23. Os meios de armazenamento de dados ou informações sigilosos serão marcados com a classificação devida em local adequado.

Parágrafo único. Consideram-se meios de armazenamento documentos tradicionais, discos e fitas sonoros, magnéticos ou ópticos e qualquer outro meio capaz de armazenar dados e informações.

Seção IV

Da Expedição e da Comunicação de Documentos Sigilosos

Art. 24. Os documentos sigilosos em suas expedição e tramitação obedecerão às seguintes prescrições:

I - serão acondicionados em envelopes duplos;

II - no envelope externo não constará qualquer indicação do grau de sigilo ou do teor do documento;

III - no envelope interno serão apostos o destinatário e o grau de sigilo do documento, de modo a serem identificados logo que removido o envelope externo;

IV - o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará, necessariamente, remetente, destinatário e número ou outro indicativo que identifique o documento; e

V - sempre que o assunto for considerado de interesse exclusivo do destinatário, será inscrita a palavra pessoal no envelope contendo o documento sigiloso.

Art. 25. A expedição, condução e entrega de documento ultra-secreto, em princípio, será efetuada pessoalmente, por agente público autorizado, sendo vedada a sua postagem.

Parágrafo único. A comunicação de assunto ultra-secreto de outra forma que não a prescrita no caput só será permitida excepcionalmente e em casos extremos, que requeiram tramitação e solução imediatas, em atendimento ao princípio da oportunidade e considerados os interesses da segurança da sociedade e do Estado.

Art. 26. A expedição de documento secreto, confidencial ou reservado poderá ser feita mediante serviço postal, com opção de registro, mensageiro oficialmente designado, sistema de encomendas ou, se for o caso, mala diplomática.

Parágrafo único. A comunicação dos assuntos de que trata este artigo poderá ser feita por outros meios, desde que sejam usados recursos de criptografia compatíveis com o grau de sigilo do documento, conforme previsto no art. 42.

Seção V

Do Registro, da Tramitação e da Guarda

Art. 27. Cabe aos responsáveis pelo recebimento de documentos sigilosos:

I - verificar a integridade e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao seu superior hierárquico e ao destinatário, o qual informará imediatamente ao remetente; e

II - proceder ao registro do documento e ao controle de sua tramitação.

Art. 28. O envelope interno só será aberto pelo destinatário, seu representante autorizado ou autoridade competente hierarquicamente superior.

Parágrafo único. Envelopes contendo a marca pessoal só poderão ser abertos pelo próprio destinatário.

Art. 29. O destinatário de documento sigiloso comunicará imediatamente ao remetente qualquer indício de violação ou adulteração do documento.

Art. 30. Os documentos sigilosos serão mantidos ou guardados em condições especiais de segurança, conforme regulamento.

§ 1º Para a guarda de documentos ultra-secretos e secretos é obrigatório o uso de cofre forte ou estrutura que ofereça segurança equivalente ou superior.

§ 2º Na impossibilidade de se adotar o disposto no § 1º, os documentos ultra-secretos deverão ser mantidos sob guarda armada.

Art. 31. Os agentes responsáveis pela guarda ou custódia de documentos sigilosos os transmitirão a seus substitutos, devidamente conferidos, quando da passagem ou transferência de responsabilidade.

Parágrafo único. Aplica-se o disposto neste artigo aos responsáveis pela guarda ou custódia de material sigiloso.

Seção VI

Da Reprodução

Art. 32. A reprodução do todo ou de parte de documento sigiloso terá o mesmo grau de sigilo do documento original.

§ 1º A reprodução total ou parcial de documentos sigilosos controlados condiciona-se à autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior competente para dispor sobre o assunto.

§ 2º Eventuais cópias decorrentes de documentos sigilosos serão autenticadas pelo chefe da Comissão a que se refere o art. 35 deste Decreto, no âmbito dos órgãos e entidades públicas ou instituições de caráter público.

§ 3º Serão fornecidas certidões de documentos sigilosos que não puderem ser reproduzidos devido a seu estado de conservação, desde que necessário como prova em juízo.

Art. 33. O responsável pela produção ou reprodução de documentos sigilosos deverá providenciar a eliminação de notas manuscritas, tipos, clichês, carbonos, provas ou qualquer outro recurso, que possam dar origem a cópia não-autorizada do todo ou parte.

Art. 34. Sempre que a preparação, impressão ou, se for o caso, reprodução de documento sigiloso for efetuada em tipografias, impressoras, oficinas gráficas ou similar, essa operação deverá ser acompanhada por pessoa oficialmente designada, que será responsável pela garantia do sigilo durante a confecção do documento, observado o disposto no art. 33.

Seção VII

Da Avaliação, da Preservação e da Eliminação

Art. 35. As entidades e órgãos públicos constituirão Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS), com as seguintes atribuições:

I - analisar e avaliar periodicamente a documentação sigilosa produzida e acumulada no âmbito de sua atuação;

II - propor, à autoridade responsável pela classificação ou autoridade hierarquicamente superior competente para dispor sobre o assunto, renovação dos prazos a que se refere o art. 7º;

III - propor, à autoridade responsável pela classificação ou autoridade hierarquicamente superior competente para dispor sobre o assunto, alteração ou cancelamento da classificação sigilosa, em conformidade com o disposto no art. 9º deste Decreto;

IV - determinar o destino final da documentação tornada ostensiva, selecionando os documentos para guarda permanente; e

V - autorizar o acesso a documentos sigilosos, em atendimento ao disposto no art. 39.

Parágrafo único. Para o perfeito cumprimento de suas atribuições e responsabilidades, a CPADS poderá ser subdividida em subcomissões.

Art. 36. Os documentos permanentes de valor histórico, probatório e informativo não podem ser desfigurados ou destruídos, sob pena de responsabilidade penal, civil e administrativa, nos termos da legislação em vigor.

CAPÍTULO IV

DO ACESSO

Art. 37. O acesso a dados ou informações sigilosos em órgãos e entidades públicos e instituições de caráter público é admitido:

I - ao agente público, no exercício de cargo, função, emprego ou atividade pública, que tenham necessidade de conhecê-los; e

II - ao cidadão, naquilo que diga respeito à sua pessoa, ao seu interesse particular ou do interesse coletivo ou geral, mediante requerimento ao órgão ou entidade competente.

§ 1º Todo aquele que tiver conhecimento, nos termos deste Decreto, de assuntos sigilosos fica sujeito às sanções administrativas, civis e penais decorrentes da eventual divulgação dos mesmos.

§ 2º Os dados ou informações sigilosos exigem que os procedimentos ou processos que vierem a instruir também passem a ter grau de sigilo idêntico.

§ 3º Serão liberados à consulta pública os documentos que contenham informações pessoais, desde que previamente autorizada pelo titular ou por seus herdeiros.

Art. 38. O acesso a dados ou informações sigilosos, ressalvado o previsto no inciso II do artigo anterior, é condicionado à emissão de credencial de segurança no correspondente grau de sigilo, que pode ser limitada no tempo.

Parágrafo único. A credencial de segurança de que trata o caput deste artigo classifica-se nas categorias de ultra-secreto, secreto, confidencial e reservado.

Art. 39. O acesso a qualquer documento sigiloso resultante de acordos ou contratos com outros países atenderá às normas e recomendações de sigilo constantes destes instrumentos.

Art. 40. A negativa de autorização de acesso deverá ser justificada.

CAPÍTULO V

DOS SISTEMAS DE INFORMAÇÃO

Art. 41. A comunicação de dados e informações sigilosos por meio de sistemas de informação será feita em conformidade com o disposto nos arts. 25 e 26.

Art. 42. Ressalvado o disposto no parágrafo único do art. 44, os programas, aplicativos, sistemas e equipamentos de criptografia para uso oficial no âmbito da União são considerados sigilosos e deverão, antecipadamente, ser submetidos à certificação de conformidade da Secretaria Executiva do Conselho de Defesa Nacional.

Art. 43. Entende-se como oficial o uso de código, cifra ou sistema de criptografia no âmbito de órgãos e entidades públicos e instituições de caráter público.

Parágrafo único. É vedada a utilização para outro fim que não seja em razão do serviço.

Art. 44. Aplicam-se aos programas, aplicativos, sistemas e equipamentos de criptografia todas as medidas de segurança previstas neste Decreto para os documentos sigilosos controlados e os seguintes procedimentos:

I - realização de vistorias periódicas, com a finalidade de assegurar uma perfeita execução das operações criptográficas;

II - manutenção de inventários completos e atualizados do material de criptografia existente;

III - designação de sistemas criptográficos adequados a cada destinatário;

IV - comunicação, ao superior hierárquico ou à autoridade competente, de qualquer anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de dados ou informações criptografados; e

V - identificação de indícios de violação ou interceptação ou de irregularidades na transmissão ou recebimento de dados e informações criptografados.

Parágrafo único. Os dados e informações sigilosos, constantes de documento produzido em meio eletrônico, serão assinados e criptografados mediante o uso de certificados digitais emitidos pela Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil).

Art. 45. Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo ultra-secreto só poderão estar ligados a redes de computadores seguras, e que sejam física e logicamente isoladas de qualquer outra.

Art. 46. A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a destruição lógica, deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento.

Art. 47. Os equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo secreto, confidencial e reservado só poderão integrar redes de computadores que possuam sistemas de criptografia e segurança adequados a proteção dos documentos.

Art. 48. O armazenamento de documentos sigilosos, sempre que possível, deve ser feito em mídias removíveis que podem ser guardadas com maior facilidade.

CAPÍTULO VI

DAS ÁREAS E INSTALAÇÕES SIGILOSAS

Art. 49. A classificação de áreas e instalações será feita em razão dos dados ou informações sigilosos que contenham ou que no seu interior sejam produzidos ou tratados, em conformidade com o art. 5º.

Art. 50. Aos titulares dos órgãos e entidades públicos e das instituições de caráter público caberá a adoção de medidas que visem à definição, demarcação, sinalização, segurança e autorização de acesso às áreas sigilosas sob sua responsabilidade.

Art. 51. O acesso de visitas a áreas e instalações sigilosas será disciplinado por meio de instruções especiais dos órgãos, entidades ou instituições interessados.

Parágrafo único. Para efeito deste artigo, não é considerado visita o agente público ou o particular que oficialmente execute atividade pública diretamente vinculada à elaboração de estudo ou trabalho considerado sigiloso no interesse da segurança da sociedade e do Estado.

CAPÍTULO VII

DO MATERIAL SIGILOSO

Seção I

Das Generalidades

Art. 52. O titular de órgão ou entidade pública, responsável por projeto ou programa de pesquisa, que julgar conveniente manter sigilo sobre determinado material ou suas partes, em decorrência de aperfeiçoamento, prova, produção ou aquisição, deverá providenciar para que lhe seja atribuído o grau de sigilo adequado.

Parágrafo único. Aplica-se o disposto neste artigo ao titular de órgão ou entidade públicos ou de instituições de caráter público encarregada da fiscalização e do controle de atividades de entidade privada, para fins de produção ou exportação de material de interesse da Defesa Nacional.

Art. 53. Os titulares de órgãos ou entidades públicos encarregados da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de novo projeto, prova, produção, aquisição, armazenagem ou emprego de material sigiloso são responsáveis pela expedição das instruções adicionais que se tornarem necessárias à salvaguarda dos assuntos com eles relacionados.

Art. 54. Todos os modelos, protótipos, moldes, máquinas e outros materiais similares considerados sigilosos e que sejam objeto de contrato de qualquer natureza, como empréstimo, cessão, arrendamento ou locação, serão adequadamente marcados para indicar o seu grau de sigilo.

Art. 55. Dados ou informações sigilosos concernentes a programas técnicos ou aperfeiçoamento de material somente serão fornecidos aos que, por suas funções oficiais ou contratuais, a eles devam ter acesso.

Parágrafo único. Os órgãos e entidades públicos controlarão e coordenarão o fornecimento às pessoas físicas e jurídicas interessadas os dados e informações necessários ao desenvolvimento de programas.

Seção II

Do Transporte

Art. 56. A definição do meio de transporte a ser utilizado para deslocamento de material sigiloso é responsabilidade do detentor da custódia e deverá considerar o respectivo grau de sigilo.

§ 1º O material sigiloso poderá ser transportado por empresas para tal fim contratadas.
§ 2º As medidas necessárias para a segurança do material transportado serão estabelecidas em entendimentos prévios, por meio de cláusulas contratuais específicas, e serão de responsabilidade da empresa contratada.

Art. 57. Sempre que possível, os materiais sigilosos serão tratados segundo os critérios indicados para a expedição de documentos sigilosos.

Art. 58. A critério da autoridade competente, poderão ser empregados guardas armados, civis ou militares, para o transporte de material sigiloso.

CAPÍTULO VIII

DOS CONTRATOS

Art. 59. A celebração de contrato cujo objeto seja sigiloso, ou que sua execução implique a divulgação de desenhos, plantas, materiais, dados ou informações de natureza sigilosa, obedecerá aos seguintes requisitos:

I - o conhecimento da minuta de contrato estará condicionado à assinatura de termo de compromisso de manutenção de sigilo pelos interessados na contratação; e
II - o estabelecimento de cláusulas prevendo a:

a) possibilidade de alteração do contrato para inclusão de cláusula de segurança não estipulada por ocasião da sua assinatura;
b) obrigação de o contratado manter o sigilo relativo ao objeto contratado, bem como à sua execução;
c) obrigação de o contratado adotar as medidas de segurança adequadas, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto contratado;
d) identificação, para fins de concessão de credencial de segurança, das pessoas que, em nome do contratado, terão acesso a material, dados e informações sigilosos; e
e) responsabilidade do contratado pela segurança do objeto subcontratado, no todo ou em parte.

Art. 60. Aos órgãos e entidades públicos, bem como às instituições de caráter público, a que os contratantes estejam vinculados, cabe providenciar para que seus fiscais ou representantes adotem as medidas necessárias para a segurança dos documentos ou materiais sigilosos em poder dos contratados ou subcontratados, ou em curso de fabricação em suas instalações.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 61. O disposto neste Decreto aplica-se a material, área, instalação e sistema de informação cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

Art. 62. Os órgãos e entidades públicos e instituições de caráter público exigirão termo de compromisso de manutenção de sigilo dos seus servidores, funcionários e empregados que direta ou indiretamente tenham acesso a dados ou informações sigilosos.
Parágrafo único. Os agentes de que trata o caput deste artigo comprometem-se a, após o desligamento, não revelar ou divulgar dados ou informações sigilosos dos quais tiverem conhecimento no exercício de cargo, função ou emprego público.

Art. 63. Os agentes responsáveis pela custódia de documentos e materiais e pela segurança de áreas, instalações ou sistemas de informação de natureza sigilosa sujeitam-se às normas referentes ao sigilo profissional, em razão do ofício, e ao seu código de ética específico, sem prejuízo de sanções penais.

Art. 64. Os órgãos e entidades públicos e instituições de caráter público promoverão o treinamento, a capacitação, a reciclagem e o aperfeiçoamento de pessoal que desempenhe atividades inerentes à salvaguarda de documentos, materiais, áreas, instalações e sistemas de informação de natureza sigilosa.

Art. 65. Toda e qualquer pessoa que tome conhecimento de documento sigiloso, nos termos deste Decreto fica, automaticamente, responsável pela preservação do seu sigilo.

Art. 66. Na classificação dos documentos será utilizado, sempre que possível, o critério menos restritivo possível.

Art. 67. A critério dos órgãos e entidades do Poder Executivo Federal serão expedidas instruções complementares, que detalharão os procedimentos necessários à plena execução deste Decreto.

Art. 68. Este Decreto entra em vigor após quarenta e cinco dias da data de sua publicação.

Art. 69. Ficam revogados os Decretos nºs 2.134, de 24 de janeiro de 1997, 2.910, de 29 de dezembro de 1998, e 4.497, de 4 de dezembro de 2002.

Brasília, 27 de dezembro de 2002; 181º da Independência e 114º da República.

FERNANDO HENRIQUE CARDOSO

Pedro Parente

Alberto Mendes Cardoso
[Diário Oficial da União, de 30 de dezembro de 2002