MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-21

REDES SEM FIO *WI-FI* DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2012

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

TECNOLOGIA DA INFORMAÇÃO

ICA 7-21

REDES SEM FIO WI-FI DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2012

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

PORTARIA DECEA Nº 110/DGCEA, DE 11 DE SETEMBRO DE 2012.

Aprova a edição da Instrução para Redes sem Fio *Wi-Fi* do Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o art. 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1.049/GC3, de 11 de novembro de 2009, e o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 369/GC3, de 9 de junho de 2010, resolve:

Art.1º Aprovar a edição da ICA 7-21 "Redes sem Fio *Wi-Fi* do Departamento de Controle do Espaço Aéreo", que com esta baixa.

Art. 2º Esta Instrução entra em vigor na data de sua publicação.

(a)Ten Brig Ar MARCO AURÉLIO GONÇALVES MENDES
Diretor-Geral do DECEA

(Publicado no BCA nº 187, de 28 de setembro de 2012)

SUMÁRIO

PREFÁCIO

As Redes sem Fio ou Redes *Wireless* IEEE 802.11, também denominadas *Wi-Fi,* são grupos de nós de rede não cabeadas dentro de uma área geográfica limitada. Essas redes são geralmente implantadas como extensões das redes cabeadas existentes para fornecer a mobilidade, melhorando o acesso às mesmas. Embora sejam muito convenientes e extremamente populares, sua instalação e operação requer atenção do ponto de vista de segurança da informação.

As Organizações Militares que empregam o *Wi-Fi* devem estar cientes da sua segurança limitada e fraca e devem implantar controles de segurança da informação para proteger as comunicações. Essas redes são particularmente suscetíveis à perda de confidencialidade, integridade e disponibilidade. Os usuários mal-intencionados ou atacantes podem ter acesso a falhas bem documentadas de segurança e comprometer facilmente os sistemas de informação que são acessados por essa rede. Essas ações podem corromper os dados da Organização Militar, consumir largura de banda, degradar o desempenho e permitir ataques que limitem o acesso de usuários autorizados.

Esta Instrução do Comando da Aeronáutica apresenta cuidados que devem ser tomados pelos administradores na instalação, configuração e administração segura dessas redes.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar as normativas de Segurança da Informação que regulamentam e orientam a utilização de Rede *Wireless Wi-Fi* para o Departamento de Controle do Espaço Aéreo e suas Organizações Militares subordinadas.

1.2 ÂMBITO E GRAU DE SIGILO

Esta Instrução se aplica ao DECEA e a todas as suas Organizações Militares subordinadas, sendo considerado ostensivo o seu grau de sigilo.

1.3 ABREVIATURAS

ASSICEA – Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo

DECEA – Departamento de Controle do Espaço Aéreo

DT – Divisão Técnica

OM – Organização Militar

SDTE – Subdepartamento Técnico do DECEA

SSSI – Seção de Segurança de Sistemas de Informação

1.4 CONCEITUAÇÃO

Os conceitos e definições estão listados na MCA 7-1 - GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO DO DECEA.

Para efeito desta Instrução do Comando da Aeronáutica, entende-se por:

1.4.1 ACCESS POINT

Access Point ou AP é um dispositivo de Rede sem Fio que realiza a interconexão entre todos os dispositivos móveis. Em geral se conecta a uma rede cabeada servindo de ponto de acesso para outra rede, como, por exemplo, a INTERNET.

1.4.2 HOTSPOT

É o nome dado ao local onde a tecnologia de redes sem fio está disponível. Onde é possível conectar-se à INTERNET, ou a qualquer outro tipo de rede, utilizando um equipamento portátil que esteja preparado para se comunicar em uma Rede sem Fio.

1.4.3 MAC

É o endereço físico de 48 bits da estação, ou, mais especificamente, da interface de rede. O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet.

1.4.4 SSID

Service Set IDentifier é um conjunto único de caracteres que identifica uma Rede sem Fio. O SSID funciona como um identificador semelhante ao documento de identificação pessoal. Diferencia uma Rede sem Fio de outra, e um cliente normalmente só pode se conectar a uma Rede sem Fio se puder fornecer o SSID correto. Existem programas que detectam o SSID das redes sem fio automaticamente; se estas estiverem desprotegidas, podem sofrer invasões ou permitir que alguém possa usar a conexão de forma indevida.

1.4.5 REDES *AD HOC*

Em telecomunicações, as redes *ad hoc* são uma especificação de rede que não possui um nó ou terminal especial, geralmente designado como ponto de acesso, para o qual todas as comunicações convergem de onde são encaminhadas aos respectivos destinos. Assim, uma rede de computadores *ad hoc* é aquela na qual todos os terminais funcionam como roteadores, encaminhando de forma comunitária as comunicações advindas dos terminais vizinhos.

1.4.6 REDE SEM FIO (*WIRELESS*)

Uma Rede sem Fio é tipicamente uma extensão de uma rede local convencional cabeada, criando-se o conceito de uma rede local sem fio (*Wireless Local Area Network* – WLAN). Uma WLAN converte pacotes de dados em onda de rádio ou infravermelho e os envia para outro equipamento *wireless* ou para um ponto de acesso que serve como uma conexão para uma LAN. Assim, uma Rede *Wireless* é um sistema que interliga vários equipamentos fixos ou móveis utilizando o ar como meio de transmissão.

1.4.7 ROGUE ACCESS POINT

Um *Rogue Access Point* (*Rogue* AP) é um ponto de acesso *wireless* que foi instalado em uma rede sem autorização explícita do administrador da rede local. O *Rogue* AP pode ter sido instalado por um usuário legítimo que desconheça as implicações desta conduta ou deliberadamente instalado por alguém com o intuito de atacar a Rede sem Fio. Em qualquer caso, um *rogue* AP representa uma séria ameaça à segurança da rede.

1.4.8 SNMP

Simple Network Management Protocol – Protocolo Simples de Gerência de Rede é um protocolo de gerência típica de redes UDP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores (*switches*). O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, fornecer informações para o planejamento de sua expansão, dentre outras.

1.4.9 TCO

Total cost of ownership ou custo total da posse é uma estimativa financeira projetada para consumidores e gerentes de empresas avaliarem os custos diretos e indiretos relacionados à compra de todo o investimento em *softwares* e *hardwares*, além do gasto inerente para mantê-los em funcionamento, ou seja, os gastos para que se continue proprietário daquilo que foi adquirido.

1.4.10 *WI-FI*

Wi-fi é uma marca registrada da *Wi-Fi Alliance,* que é utilizada por produtos e equipamentos utilizados em redes locais sem fio, também conhecidas como WLAN, que são baseados no padrão IEEE 802.11.

1.4.11 WPA2

O WPA2 ou 802.11i foi uma substituição da *Wi-Fi Alliance* em 2004 à tecnologia WPA, pois, embora fosse bem segura em relação ao padrão anterior WEP, a *Wi-fi Alliance* teve a intenção de fazer um novo certificado para redes sem fio mais confiável e também necessitava continuar o investimento inicial realizado sobre o WPA. O principal objetivo do WPA2 é suportar as características adicionais de segurança do padrão 802.11i que não estão incluídas nos produtos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem fio.

1.5 DOCUMENTOS DE REFERÊNCIA

a) DCA 7-2 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO DECEA, de 2010;

b) PCA 7-11 – PLANO DIRETOR DE SEGURANÇA DA INFORMAÇÃO DO DECEA, de 2010;

c) NSCA 7-13 – SEGURANÇA DE SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO NO COMANDO DA AERONÁUTICA, de 2006;

d) ICA 200-5 – GERENCIAMENTO DE PLANO DE SEGURANÇA ORGÂNICA DO COMANDO DA AERONÁUTICA, de 2009; e

e) ABNT NBR ISO/IEC 27001 SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO, de 2006.

2 RESPONSABILIDADES

2.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

2.1.1 Estabelecer normas, padrões e metodologias relativas à segurança da informação, que estejam em conformidade com a legislação brasileira e com os padrões aceitos internacionalmente.

2.1.2 Estabelecer normas, padrões e metodologias que regularizem o emprego de controles de segurança da informação em *Redes Wireless*.

2.1.3 Estabelecer planejamento de auditoria de segurança da informação para verificar a implantação das diretrizes desta Intrução.

2.1.4 Elaborar parecer quanto à solicitação de instalação de uma Rede sem Fio nas Organizações Militares.

2.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

2.2.1 As Seções de Segurança de Sistemas da Informação (SSSI), das Organizações Militares subordinadas ao DECEA, deverão supervisionar a utilização dos procedimentos e instruções de segurança da informação previstas nesta Instrução.

2.3 EQUIPE DE TI LOCAL

2.3.1 Implantar e manter os controles de segurança da informação previstos nesta Instrução.

2.3.2 Administrar a Rede *Wireless* em conformidade com as boas práticas de segurança da informação presentes nesta Instrução

3 AUTORIZAÇÃO PARA INSTALAÇÃO DE UMA REDE SEM FIO

3.1 Conforme preconizado na NSCA 7-13 - SEGURANÇA DE SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA, o emprego de redes sem fio, para estabelecer conectividade entre estações ou entre redes que integram a INTRAER, só poderá ser efetivado com autorização do Órgão Central do Sistema de Tecnologia da Informação.

3.2 O emprego de redes sem fio como solução técnica de Tecnologia da Informação para atender a atividades ou sistemas de interesse do COMAER só poderá ser efetivado com autorização do Órgão Central do STI, mesmo que essas atividades ou sistemas estejam isolados da INTRAER e que sua operação tenha caráter temporário.

3.3 As Organizações Militares devem enviar documentação formal de pedido de instalação de uma Rede *Wireless* juntamente com oprojeto básico de instalação para análise e parecer do Subdepartamento Técnico do DECEA, o qual será encaminhado posteriormente para apreciação do Órgão Central do Sistema de Tecnologia da Informação.

3.4 A utilização de redes sem fio será permitida, após aprovação, somente para tráfego de informações de classificação ostensiva das Organizações Militares subordinadas ao DECEA. Para a transmissão de informações classificadas, deve-se utilizar a Rede Mercúrio, conforme preconizado no RCA 205-1 - REGULAMENTO PARA SALVAGUARDA DE ASSUNTOS SIGILOSOS DA AERONÁUTICA.

4 REQUISITOS MÍNIMOS DE *HARDWARE* E *SOFTWARE* PARA UTILIZAÇÃO DE REDE SEM FIO

Para a implantação dos controles essenciais de segurança da informação, a fim de garantir a proteção da Rede *Wireless,* é necessária a utilização de equipamentos compatíveis com as recomedações contidas nesta Instrução.

4.1 REQUISITOS MÍNIMOS DE *HARDWARE* E *SOFTWARE*

4.1.1 Existem várias questões importantes que devem ser consideradas na definição e configuração de um *Access Point* (AP), detalhadas a seguir, e que estabelecem os requisitos mínimos para equipamentos *wireless* nas Organizações Militares subordinadas ao DECEA.

4.1.2 Considerações na escolha: na escolha de um modelo de AP é importante determinar quais recursos serão suportados para criptografia e autenticação. É mandatório que os equipamentos suportem criptografia WPA2 ou superior.

4.1.3 O *Access Point* deverá possibilitar atualização de *firmware*, a fim de incorporar novos padrões e eventuais correções lançadas pelo fabricante.

4.1.4 Alteração de configurações padrão: o *Access Point* é adquirido com a configuração padrão, que é de conhecimento público. Assim é extremamente importante que todas as configurações originais sejam alteradas pelo administrador antes de tornar operacional o AP, incluindo:

a) senhas;

b) SSID;

c) chaves; e

d) SNMP *communities*.

4.1.5 Alguns AP possuem uma opção de *reset* físico com a finalidade de permitir que a configuração original seja restabelecida. Assim, é importante que o AP seja instalado em um local com acesso físico controlado.

4.1.6 Atualização: a atualização de *softwares* do Access Point é importante para mitigar ameaças e vulnerabilidades, portanto somente é mandatória a utilização de equipamento que suporte a atualização de *firmware* e/ou *software*.

4.1.7 Modos de configuração: a maioria dos AP permite vários protocolos de configuração: HTTP, SNMP, *telnet* etc. Assim, sempre que possível, é importante desabilitar os protocolos que não serão necessários e optar por um modo de configuração que não seja pela própria Rede *Wireless*, mas sim pela rede cabeada ou ainda via conexão serial. Isso minimiza as chances de que a sessão de configuração com o AP seja capturada imediatamente utilizando um cliente *Wireless*.

4.1.8 *Broadcast* de SSID: uma recomendação útil é desabilitar o *broadcast* de SSID pelo AP. Embora seja uma medida simples, pode dificultar o uso de programas de mapeamento de Redes *Wireless*.

4.1.9 Filtragem por endereço MAC: alguns AP possuem o recurso de filtragem de clientes *wireless* por endereço MAC. Embora endereços MAC possam ser forjados e muitas vezes não seja prático manter uma lista dos clientes autorizados (e em alguns casos seja inviável, como

em seminários), o administrador pode considerar o uso desse recurso como uma camada adicional de segurança da informação do seu ambiente *Wireless*.

4.1.10 Auditoria: o *Access Point* deve ter suporte para geração de eventos de segurança da informação, mediante a criação de *logs* de eventos.

4.1.11 Acesso remoto: o *Access Point* deve ter suporte para a utilização de SNMP v3, que possui recursos avançados de segurança da informação em relação aos seus antecessores.

5 VISÃO GERAL DOS PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO PARA A REDE SEM FIO

5.1 Os princípios de segurança da informação para a Redes *Wireless* estão descritos abaixo:

a) confidencialidade: garantir que a comunicação não possa ser acessada por pessoas não autorizadas;

b) integridade: detectar quaisquer alterações intencionais ou não nos dados que trafegam na rede;

c) disponibilidade: garantir que os dispositivos e os indivíduos possam acessar uma Rede sem Fio e seus recursos sempre que necessário; e

d) controle de acesso: restringir os direitos de dispositivos ou indivíduos em acessar uma rede ou recursos dentro desta.

5.2 Os princípios de segurança da informação para a Rede sem Fio e para as redes cabeadas são os mesmos, assim como as principais categorias de alto nível de ameaças que elas enfrentam.

5.2.1 Os principais ataques que podem acarretar prejuízo para os princípios da Rede *Wireless* são os seguintes:

a) *denial of service(DOS)*: o ataque de negação de serviço é uma tentativa em tornar os recursos da rede indisponível;

b) *eavesdropping:*: atacante passivamente monitora comunicações de rede de dados, incluindo credenciais de autenticação;

c) *man-in-the-middle*: é um ataque sofisticado e usualmente praticado em redes sem fio, pois não há a necessidade do atacante estar conectado a uma rede cabeada. Permite ainda ao atacante interceptar as comunicações entre um AP e um cliente, obtendo assim as credenciais de autenticação e dados;

d) *masquerading*: o atacante se faz passar por um usuário autorizado para obter acesso a privilégios não autorizados;

e) modificação de mensagem: atacante altera uma mensagem legítima, excluindo, adicionando ou alterando-a;

f) reprodução de mensagem: atacante monitora passivamente transmissões e retransmissões de mensagens, agindo como se o atacante fosse um usuário legítimo;

g) apropriação inadequada: atacante se apropria ou utiliza indevidamente um serviço; e

h) análise de tráfego: atacante monitora passivamente transmissões para identificar padrões de comunicação e de comportamento do usuário.

6 PROCEDIMENTO DE SEGURANÇA DA INFORMAÇÃO DE USO DE REDES SEM FIO

O DECEA e suas Organizações Militares subordinadas devem mitigar os riscos para a utilização de Redes *Wireless* mediante a aplicação de controles de segurança da informação para enfrentar as ameaças e vulnerabilidades específicas na utilização desta. A seguir serão apresentados os procedimentos de segurança na correta utilização da Rede *Wireless*. Esses itens estão agrupados em categoria para melhorar o seu entendimento.

6.1 PROCEDIMENTO DE SEGURANÇA

6.1.1 As Organizações Militares devem elaborar procedimento de segurança da informação especificando para qual finalidade será utilizada a rede, quais usuários estão autorizados a utilizar, e especificar os recursos de informação que devem estar disponíveis para os usuários, por exemplo: permitir que um funcionário de empresa terceirizada utilize a conexão de *Internet*, mas sem poder acessar a rede interna.

6.1.2 No procedimento de segurança da informação deve constar que a utilização de equipamentos *wireless*, em áreas que armazenam e processam informações classificadas, deve ser proibida. Equipamentos da Rede sem Fio, em áreas que armazenam e processam informações sensíveis, podem se tornar uma ameaça para a disponibilidade das informações, pois dispositivos como telefones, *headphones*, teclados etc. podem causar interferência e consequentemente tornar as informações processadas em áreas sigilosas indisponíveis. Por esse motivo, no documento do procedimento de segurança da informação deve-se recomendar a proibição da utilização de equipamentos *wireless* em áreas que armazenam e processam informações reservadas.

6.1.3 No procedimento de segurança da informação deve constar que a utilização de *hotspots,* pelas estações que armazenam ou tenham acesso a informações reservadas, deve ser proibida. A utilização de *hotspots* pelas estações que armazenam ou tenham acesso a informações reservadas representa uma ameaça à perda de confidencialidade das informações, ocasionando o impacto de vazamento de informações. Usuários mal-intencionados ou atacantes podem capturar essas informações que trafegam pela rede para fins diversos.

6.1.4 No procedimento de segurança da informação deve constar que a utilização de redes *ad hoc* deve ser proibida quando possível. A utilização destas pode ocasionar uma ameaça aos controles de segurança da informação da Rede sem Fio, permitindo que os clientes se comuniquem diretamente sem proteção ou restrição. Adicionalmente, permite ainda o acesso de clientes indevidos à rede.

6.1.5 O procedimento de segurança da informação deve informar ao usuário sobre políticas de segurança da informação que a Organização Militar está obrigada a cumprir e sobre o uso adequado de equipamentos de propriedade da Organização Militar.

6.1.6 As Organizações Militares devem padronizar os sistemas operacionais e aplicações utilizadas na Rede *Wireless*. Embora normalmente exista a necessidade de utilização de sistemas heterogêneos nos ambientes de Tecnologia da Informação atuais, deve-se buscar o máximo de padronização possível em relação ao uso de marcas, modelos e fabricantes de equipamentos, e de sistemas operacionais instalados na Rede *Wireless*. Isso facilita a administração do *Wi-Fi*, reduzindo o *Total Cost of Ownership* e possibilita uma gestão eficiente da segurança da informação.

6.2 ARQUITETURA DA REDE

6.2.1 A Rede *Wireless* deve ser separada da rede cabeada da Organização Militar por meio de uma DMZ ou VLAN. O equipamento de rede não deve ser utilizado como uma ponte (*bridge*) que conecta diretamente a Rede *Wireless* e a rede interna. Caso contrário, se o equipamento de rede for comprometido por um atacante, toda a rede, inclusive a rede interna, estará vulnerável, podendo permitir o acesso indevido às informações classificadas e recursos.

6.2.2 As conexões da rede com outras redes externas devem ser protegidas por *firewalls*. Se a Rede *Wireless* for conectada diretamente a outras redes internas ou à Internet sem a instalação de *firewall*, poderá acarretar em risco elevado de acesso indevido aos serviços e às informações internas por parte de usuários não autorizados, sobretudo se houver uma conexão não monitorada com a Internet.

6.2.3 A Rede *Wireless* deve ser segregada em uma *virtual lan* (VLAN), de modo a permitir a aplicação de controles de acesso que identifiquem os protocolos e serviços autorizados a trafegar.

6.2.4 Deve-se realizar um levantamento local na Organização Militar para determinar a localização adequada de instalação do *Access Point*. A potência de transmissão não deve, sempre que possível, permitir a cobertura eletromagnética além dos limites físicos das instalações da Organização Militar.

6.2.5 As Organizações Militares devem considerar a segurança física como parte da arquitetura de Rede *Wireless*. Os equipamentos devem ser fisicamente seguros ou protegidos por um alarme para evitar a violação ou roubo. Usuários podem ser treinados em segurança física para proteção de equipamentos *Wireless*, a fim de evitar o comprometimento ou roubo de estações que acessam a Rede *Wireless*, conforme a ICA 200-5 - GERENCIAMENTO DE PLANO DE SEGURANÇA ORGÂNICA DO COMANDO DA AERONÁUTICA, de 2009.

6.3 CRIPTOGRAFIA E AUTENTICAÇÃO

6.3.1 O tráfego de administração remota do *Access Point* através da rede deve ser protegido por meio de criptografia. Alguns modelos de *Access Point* permitem administração remota via *browser*, tanto na rede local quanto pela Rede *Wireless*. Em muitas implantações, esse tráfego passa em claro pela rede. O objetivo desse controle é evitar o acesso indevido ao tráfego de administração, que pode conter senhas de acesso e outras informações sigilosas.

6.3.2 O WPA2 (*wi-fi* protected access 2) deve ser habilitado no *Access Point*. A aplicação desse controle de segurança da informação torna redes sem fio tão seguras quanto redes cabeadas. O WPA2 permite a implantação de um sistema completo e seguro, ainda que compatível com sistemas anteriores.

6.3.3 As chaves simétricas compartilhadas pelos equipamentos que utilizam o WPA2 devem utilizar a mesma metodologia de senha forte, ou seja, devem ter no mínimo 16 caracteres, entre letras maiúsculas, minúsculas, número e caracteres especiais.

6.3.4 Um *banner* de advertência para *login* na interface de administração do *Access Point* deve ser implantado. A exibição de uma mensagem de advertência durante o *logon* na interface de administração do AP tem como propósito informar que o equipamento em questão pertence à Organização Militar e é de uso restrito para usuários autorizados, e que os acessos eventualmente estarão sendo auditados.

6.3.5 Um mecanismo para ocultar o esquema de endereçamento IP utilizado na rede interna deve ser implantado. O conhecimento da arquitetura e dos endereços IP utilizados pelos equipamentos da rede interna (servidores, estações etc.) facilita o planejamento de ataques. Por esse motivo, recomenda-se introduzir mecanismos que permitam ocultar estas informações de usuários não autorizados, evitando que as mesmas possam ser mapeadas remotamente por algum atacante.

6.3.6 Deve ser implantada, na Rede Wireless, solução segura de autenticação para permitir que somente usuários autorizados possam acessar a rede. Soluções de autenticação incluem o uso de nomes de usuários e senhas, cartões inteligentes, biometria, PKI, ou uma combinação de soluções (por exemplo, cartões inteligentes com PKI). Mecanismos de autenticação podem ser integrados em uma solução *Wireless* para aumentar a segurança do sistema. Por exemplo, se uma VPN está sendo usada para garantir a confidencialidade e integridade de proteção para a Rede *Wireless* de comunicação, a VPN pode ser configurada para exigir autenticação do usuário.

6.3.7 Os mecanismos de identificação automática de equipamentos de Rede *Wireless* devem ser utilizados para autenticar conexões. Uma identificação automática deve ser usada caso haja necessidade que a comunicação somente seja iniciada de um local ou equipamento específico. Nesse caso, além da autenticação do usuário remoto, o identificador no equipamento deve ser usado para indicar se possui permissão para conectar-se à rede. Adicionalmente, métodos de identificação automática de equipamentos auxiliam nos processos investigativos, uma vez que garantem a origem dos acessos realizados.

6.4 PROTEÇÃO AOS CLIENTES *WIRELESS*

6.4.1 É recomendado instalar um *firewall* na máquina local, devendo também ser instalado e configurado para todos os usuários que utilizam a Rede *Wireless*. A utilização de *firewall* nas máquinas locais adiciona uma camada extra de segurança da informação nos sistemas de informação, protegendo-os de ataques hostis e configurações incorretas. Associado à existência de *firewall*, protegendo o perímetro da rede interna e a rede DMZ, é recomendável a instalação e configuração de um *firewall* nas máquinas locais. Caso algum atacante invada uma máquina local, será mais difícil utilizá-la para realizar novos ataques na Rede *Wireless*.

6.4.2 A utilização de equipamentos *wireless* que não sejam de propriedade da Organização Militar deve ser proibida. A utilização de equipamentos *wireless* de propriedade pessoal dos usuários e que não pertençam à Organização Militar pode acarretar vazamento de informações e dificultar a rastreabilidade caso ocorra algum incidente de segurança da informação. Nos casos de seminários, worshop, etc, de caráter temporário e provisório, o usuário deve solicitar à equipe de TI local o acesso à rede, sendo que esta deverá documentar e monitorar os acessos desse usuário durante o período de utilização da rede.

6.4.3 Os clientes *wireless* devem ser configurados de modo a não permitir a conexão automática na Rede *Wireless*. Permitir tais conexões automáticas aumenta o risco de ataque malicioso à rede.

6.4.4 Os clientes w*ireless* devem ser desativados quando não estiverem em uso.

6.4.5 As máquinas clientes que acessam a Rede *Wireless* devem ter um *software antivírus* instalado e atualizado. O *software antivírus* identificará, removerá e prevenirá a propagação de vírus, *worms* e outros *malwares* entre os equipamentos de *wireless*. Assim, estações de

usuários estão em risco de ameaças de *malware* conhecidas e devem ter um *software antivírus* instalado e sempre atualizado.

6.5 SEGURANÇA FÍSICA

6.5.1 As Organizações Militares devem implantar controles de segurança física para a Rede *Wireless*. Essas medidas são necessárias para proteger os componentes de infraestrutura da Rede *Wireless* contra roubo, alteração ou uso indevido. A segurança física é fundamental para garantir que somente usuários autorizados tenham acesso aos equipamentos.

6.5.2 Deve-se implantar controles de segurança física sempre que a função de *reset* do equipamento *wireless* estiver habilitada. A configuração do AP é retornada para os padrões de fábrica após um evento de *reset.* Somente pessoal autorizado deve restaurar a configuração padrão de um equipamento *wireless* para garantir que os controles de segurança da informação possam ser reinseridos.

6.6 AUDITORIA E MONITORAMENTO

6.6.1 A opção de auditoria do *Access Point* deve ser habilitada e configurada de forma a registrar os eventos de segurança da informação. Os *logs* ajudam a identificar potenciais problemas de *software/hardware,* tentativas de acesso não autorizado e outros eventos relevantes, fornecendo evidências no caso de um incidente de segurança da informação.

6.6.2 As Organizações Militares devem proteger os registros de auditoria (*logs*) gerados pelo *Access Point* contra acessos indevidos. O *Access Point* deve permitir a auditoria de eventos relevantes para a segurança da informação, como, por exemplo, falhas de *login*. Embora normalmente a auditoria seja limitada em funcionalidade, recomenda-se que os *logs* sejam protegidos contra acessos indevidos, visando preservar a sua integridade.

6.6.3 As Organizações Militares devem redirecionar os *logs* do *Access Point* para um servidor de *logs*. Esses arquivos devem ser gerenciados de forma semelhante à dos sistemas Unix, via *syslog*. O redirecionamento para um servidor permite o armazenamento de uma maior quantidade de eventos, facilitando a rastreabilidade. Além disso, se o equipamento for comprometido, os *logs* poderão ser perdidos ou adulterados, caso não tenham sido redirecionados para um servidor.

6.6.4 As Organizações Militares devem verificar periodicamente os registros de auditoria gerados pelo *Access Point*. Embora necessário, o simples processo de registro dos eventos relevantes para a segurança da informação, relacionados ao funcionamento e à utilização do *Access Point*, não é suficiente. Para que os eventos de segurança da informação possam ser efetivamente rastreados (por exemplo, tentativas de acesso não autorizado) é importante que os registros sejam continuamente analisados por um administrador de Rede sem Fio ou auditor qualificado.

6.6.5 As Organizações Militares devem desenvolver procedimentos de segurança da informação de auditoria de Rede *Wireless*. Desenvolver um procedimento de auditoria ajudará a assegurar que a Organização Militar possa detectar comportamentos não autorizados e violações de segurança da informação na Rede sem Fio.

6.6.6 As Organizações Militares devem implantar um sistema de monitoramento de tráfego na Rede *Wireless*. Sistemas de monitoramento de banda permitem melhor acompanhamento do uso do *link* e consequentemente melhor planejamento de capacidade, evitando o consumo

excessivo da banda por serviços não essenciais. Além disso, a monitoração constante do tráfego permite detectar incidentes de segurança da informação.

6.7 CONFIGURAÇÕES DE SISTEMAS E APLICAÇÕES

6.7.1 As Organizações Militares devem habilitar o recurso de MAC *Address Filtering* (filtragem por MAC) no *Access Point*. O endereço MAC é um código de 12 caracteres que é único para cada placa de rede ou cartão PCMCIA, e é determinado pelo fabricante do equipamento. Alguns equipamentos de *wireless* permitem limitar o acesso dos usuários ao *Access Point* em função do endereço MAC da placa em uso. Embora em grandes redes o gerenciamento deste tipo de restrição seja complexo e existam algumas limitações (o endereço MAC pode ser forjado), é recomendável que o recurso de MAC *Address Filtering* seja implantado quando possível, pois se trata de mais uma medida de proteção contra ataques à Rede sem Fio.

6.7.2 O intervalo de envio de *broadcast* de *beacons* emitidos pelo *Access Point* deve ser o maior possível. Recomenda-se que o intervalo para a emissão de beacons seja maximizado. Isto dificultará a descoberta da rede por atacantes que estejam pesquisando redes passivamente, pois o envio de informações de configuração da Rede *Wireless* (SSID, canal de operação, taxa, criptografia *on/off*, etc.) será enviado em um intervalo maior.

6.7.3 As Organizações Militares devem configurar os *Access Points* para ignorar *probe-requests* sem SSID definido. Segundo a especificação 802.11, um dispositivo que está procurando por um *Access Point* pode enviar um *broadcast* em um determinado canal chamado *Probe-request*. Por *default*, todos os APs que estiverem no alcance da transmissão vão responder com um *Probe-response*, que contém essencialmente as mesmas informações do *beacon*. Muitas ferramentas de atacantes utilizadas em *War Driving* procuram pela existência de Rede sem Fio enviando *Probe-requests* em diversos canais e capturando as respostas dos AP. Por este motivo, é recomendável evitar que os AP respondam aos *Probe-requests* que não tenham um SSID definido.

6.7.4 As Organizações Militares devem configurar os equipamentos da Rede *Wireless* com parâmetros diferentes da configuração *default* do fabricante. Estão disponíveis na Internet informações sobre a configuração *default* de diversos tipos de equipamentos para Redes *Wireless*.

6.7.5 A potência do sinal emitido pela antena do *Access Point* e outros dispositivos da Rede *Wireless* deve ser ajustada para as condições do ambiente em análise. Por padrão, a maioria dos APs e outros equipamentos são configurados para a potência de transmissão máxima, com o objetivo de estender a propagação do sinal e reduzir a necessidade de suporte técnico em função de baixo sinal de recepção. Entretanto, em muitas situações, a potência do sinal transmitido é muito superior à que seria necessária para a Rede *Wireless*, e os sinais de *broadcast* emitidos pelo AP seriam propagados além dos limites de cobertura desejados, facilitando a detecção por atacantes e eventualmente ocasionando problemas de interferência com outras redes vizinhas. Para reduzir estes riscos, é recomendável que a potência transmitida seja ajustada para evitar o vazamento de radiofrequência.

6.7.6 Na instalação de um *Access Point*, recomenda-se verificar a existência de conflitos de sinal com *Access Points* de outras redes próximas. A colisão de sinais gerados por AP de redes diferentes ocorre porque em muitas implantações, os administradores mantêm os equipamentos operando no canal *default* definido pelo fabricante. Adicionalmente, a

interferência de sinais de rádio pode ocasionar a negação de serviço (*denial of service*) em ambas as redes.

6.7.7 As Organizações Militares devem configurar corretamente a data e hora do *Access Point*. É importante que o horário esteja corretamente configurado utilizando um servidor RTP, pois a data e hora do sistema são normalmente utilizadas para geração do time *stamp* (selo de tempo) no registro de cada evento, permitindo que a auditoria possa ser realizada com exatidão.

6.7.8 O volume de tráfego gerado na Rede *Wireless* deve ser monitorado. Normalmente, durante um ataque, é gerado um elevado volume de tráfego, tentando fazer o *download* da maior quantidade possível de dados. Nesse caso, o endereço IP ou MAC *address* associado ao *Access Point* terá um pico de volume de tráfego em relação às condições de operação normais. Embora não se possa garantir que um volume de tráfego sem fio acima do normal seja um ataque, em ambientes onde o nível de segurança requerido for muito elevado, recomenda-se que o administrador faça este monitoramento como uma forma preventiva para detecção.

6.7.9 O protocolo cliente-servidor *telnet* deve ser desabilitado no *Access Point*. Este, além de transmitir dados em claro, possibilita que sejam feitos ataques de força bruta. Por esse motivo, é recomendável que a sua utilização para administração remota do *Access Point* seja evitada quando possível.

6.7.10 Um período de inatividade para encerramento de sessão, para máquinas de usuários conectados na Rede *Wireless*, deve ser estabelecido. O estabelecimento de um período de inatividade para máquinas de usuários conectados na Rede sem Fio diminui o risco de uma sessão perdida por usuários mal-intencionados ou atacantes que desejam cometer atos ilícitos com credenciais de outro usuário.

6.7.11 As Organizações Militares devem desabilitar todos os protocolos de gerenciamento inseguros e não utilizados no AP e configurar os protocolos de gestão remanescentes de menor privilégio. Desabilitar todos os protocolos de gerenciamento inseguros e não essenciais elimina os métodos potenciais que um atacante pode usar ao tentar comprometer um AP. Exemplos de protocolos de gerenciamento de senhas inseguras SNMPv1 e SNMPv2.

6.8 SERVIÇOS LOCAIS E REMOTOS

6.8.1 As Organizações Militares devem desabilitar o serviço SNMP no *Access Point*, caso seja desnecessário. Este protocolo é utilizado para o gerenciamento de dispositivos como roteadores, *Access Points*, *switches*, *firewalls* e outros equipamentos e serviços. Os pacotes SNMP, versão 1, são transmitidos em claro e podem conter informações sensíveis, como dados de configuração de ativos e nomes das comunidades utilizadas.

6.8.2 Sempre que possível, as Organizações Militares devem utilizar o SNMPv3 para gerência remota dos equipamentos da Rede *Wireless*. Esta versão inclui facilidades de segurança no protocolo, como privacidade, autenticação e controle de acesso.

6.8.3 O nome da comunidade SNMP de leitura *read only* no agente SNMP do *Access Point* deve ser de difícil dedução, evitando-se o uso do nome *default public*. O nome da comunidade funciona praticamente como uma senha no controle da comunicação entre agentes e gerenciadores SNMP *managers*. O conhecimento deste pode permitir que informações sobre as configurações do agente sejam acessadas remotamente por usuários não autorizados.

6.8.4 O nome da comunidade SNMP de escrita *read write* no agente SNMP do *Access Point* deve ser de difícil dedução, evitando-se o uso do nome *default private*. O nome da comunidade funciona praticamente como uma senha no controle da comunicação entre agentes e gerenciadores SNMP managers. O conhecimento deste pode permitir alterações nas configurações do agente remotamente via SNMP por parte de usuários não autorizados.

6.8.5 O acesso de escrita *read write* ao agente SNMP do *Access Point* deve ser removido. O acesso de escrita *read write* aos agentes monitorados via SNMP, tais como servidores, estações, roteadores, *switches, hubs, firewalls, access point* e outros dispositivos em redes IP, permite que suas configurações sejam alteradas remotamente. É recomendável que este seja concedido apenas nos casos estritamente necessários. O nome da comunidade de escrita deve ser de difícil dedução. Adicionalmente, como as mensagens do protocolo são baseadas em UDP e trafegam em claro pela rede, recomenda-se que o tráfego de gerenciamento seja isolado, se possível.

6.8.6 O agente SNMP do *Access Point* deve ser configurado para enviar *traps* somente para *hosts* de gerenciamento autorizados. Nos casos em que o uso deste protoloco é indispensável, recomenda-se que os *traps* SNMP sejam enviados somente para os *hosts* específicos onde é feito o gerenciamento, para reduzir o risco de acesso não autorizado às informações de *status* dos agentes e outros alertas.

6.9 POLÍTICA DE SENHA FORTE

6.9.1 As Organizações Militares devem substituir as senhas padrão fornecidas pelo fabricante, para acesso ao *Access Point*, por outras de política forte, ou seja, alteradas regularmente, com no mínimo 16 caracteres entre eles: letras maiúsculas e minúsculas, números e caracteres especiais. Os dados dos parâmetros *default* de vários modelos de *Access Point*, incluindo o acesso administrativo, estão disponíveis na Internet. De posse da senha de administração, um atacante pode obter controle total sobre o AP, existindo o risco de acesso indevido a informações classificadas, fraude ou indisponibilidade dos serviços.

6.10 ATUALIZAÇÃO

6.10.1 As Organizações Militares devem utilizar produtos que possam permitir a atualização de *software* ou *firmware*. Equipamentos de *wireless* requerem este suporte para que eles possam ser atualizados com os *patches* de segurança sem fio e acessórios lançados após a aquisição. Nem todos os AP suportam atualização, assim deve ser verificada a existência desta antes da aquisição.

6.10.2 Os administradores de rede devem verificar regularmente, junto aos fornecedores, a existência de novos *patches*, *upgrades* ou atualizações e aplicá-las. Além disso, muitos modelos de equipamentos de *wireless* possuem alerta de segurança, ou seja, listas de *e-mail* para informar os clientes de novas vulnerabilidades e ataques conhecidos.

6.10.3 As Organizações Militares devem testar os *patches* e atualizações de *software* regularmente. Estes também devem ser testados antes da sua implementação para garantir que funcionem corretamente.

6.10.4 As Organizações Militares devem atualizar a versão do *firmware* do *Access Point* para a última versão disponível considerada estável pelo fabricante. Novas versões de *firmware* frequentemente corrigem falhas de segurança que podem comprometer a disponibilidade ou a segurança do *Access Point*.

6.11 TREINAMENTO DE USUÁRIO

6.11.1 As Organizações Militares devem elaborar uma campanha de conscientização de usuários no uso seguro das Redes *Wireless*. A ausência desta na Organização Militar permite que usuários não tenham conhecimento de como utilizar a rede de forma segura, podendo acarretar no uso inadequado dos recursos. Conscientização e treinamento em segurança da informação auxiliam os usuários na utilização de boas práticas, evitando invasões acidentais ou maliciosas em sistemas de informação.

6.12 TRATAMENTO DE INCIDENTES NA REDE *WIRELESS*

6.12.1 As Organizações Militares devem elaborar um procedimento de segurança da informação de resposta a incidentes para a Rede *Wireless*. No caso de algum ataque local ou remoto ser bem-sucedido e ocasionar o comprometimento de sistemas de informação internos, é importante que a Seção de Segurança de Sistemas da Informação esteja treinada para responder ao incidente de forma adequada.

6.12.2 As Organizações Militares devem implantar um Sistema de Prevenção de Intrusos W*ireless* (WIPS). OWIPS monitora o espectro de radiofrequências para detectar a presença de acesso não autorizado de r*ogue access points* e de ferramentas de ataque em redes sem fio. O sistema monitora o espectro de rádio utilizado pela Rede sem Fio e imediatamente alerta o administrador quando um *rogue access point* é detectado. Além disso, um WIPS também inclui funcionalidades de prevenção automática de ataques.

6.12.3 A Rede *Wireless* também deve ser monitorada por meio de uma console de *software antivírus*. A utilização de uma solução para distribuição de atualizações e novas versões de *software antivírus* que permita a monitoração centralizada de possíveis infecções é fundamental para a gerência e resposta aos incidentes relacionados com a contaminação do ambiente da rede interna por códigos maliciosos ou vírus.

6.13 POLÍTICA DE *BACKUP*

6.13.1 As Organizações Militares devem executar um procedimento de segurança da informação de cópias de segurança periódico para os arquivos de configuração dos *Access Points*. Uma cópia de segurança do arquivo de configuração deve ser gerada após cada alteração relevante. A existência de uma cópia (*backup*) deste arquivo ajuda a reduzir o tempo de indisponibilidade quando da ocorrência de eventos que requeiram a sua reinstalação ou reconfiguração, como, por exemplo, falhas inesperadas de *software* ou *hardware*. O armazenamento de cópias de segurança atualizadas também permite que seja realizado um histórico das alterações efetuadas.

6.14 AVALIAÇÕES DE SEGURANÇA DA REDE *WIRELESS*

6.14.1 As Organizações Militares devem executar um procedimento de segurança da informação de verificação periódica de servidores DHCP maliciosos na Rede *Wireless*. A inclusão deste serviço na Rede sem Fio pode expor os clientes a diversos tipos de ataques sem que os mesmos tenham conhecimento. Por exemplo, caso um servidor DHCP malicioso seja configurado de forma a inserir o endereço de um servidor DNS nas configurações de rede das máquinas dos usuários, as consultas realizadas por eles retornarão respostas incorretas e com isso suas informações poderão se interceptadas por usuários maliciosos. Por esse motivo, recomenda-se que um procedimento de verificação periódica deste serviço seja implantado.

6.14.2 As Organizações Militares devem executar um procedimento de segurança da informação para mapeamento de portas e serviços não autorizados. A existência destas dentro de uma rede permite ataques a sistemas desconhecidos pelos administradores, ou indicam máquinas que foram invadidas e que tiveram serviços adicionais instalados. O mapeamento periódico de portas e serviços é importante para que o administrador da rede identifique proativamente quais serviços não autorizados estão em uso na rede e possa desabilitá-los antes que eventos de segurança da informação possam ocorrer, ou então para identificar máquinas que já foram comprometidas.

6.14.3 As Organizações Militares devem executar periodicamente um procedimento de segurança da informação para identificação de vulnerabilidades. Atualmente, é frequente a criação de programas com códigos maliciosos e a descoberta de novas falhas em sistemas de informação. A operação estável depende diretamente da atualização dos *patches* que eliminam ou minimizam essas vulnerabilidades, e das configurações dos sistemas de informação que restringem o acesso e tornam o sistema mais seguro.

6.14.4 As Organizações Militares devem executar periodicamente um procedimento de segurança da informação de verificação de pontos de acesso não autorizados na Rede *Wireless*. A inclusão destes pontos na rede criam portas de entrada para usuários não autorizados e expõem as máquinas a diversos tipos de ataques sem que os mesmos tenham conhecimento. Outro fator importante é que muitas vezes estes não possuem configurações de segurança para controlar acesso ao dispositivo, assim, qualquer pessoa que tenha acesso à área de cobertura do mesmo pode acessar a rede interna.

6.14.5 As Organizações Militares devem designar um grupo ou responsável técnico para pesquisar as vulnerabilidades de equipamentos *wireless*. Atribuir a responsabilidade para rastrear problemas de segurança em redes sem fio ajuda a garantir a continuidade da administração segura.

6.15 INVENTÁRIOS DE ATIVOS DE INFORMAÇÃO

6.15.1 As Organizações Militares devem elaborar um inventário dos equipamentos de Rede *Wireless*. É necessário ter controle de quais equipamentos são utilizados em suas instalações (estações, servidores etc.) para assegurar que as proteções estão sendo feitas e ter gerência patrimonial sobre seus ativos.

6.15.2 O inventário de ativos de informação da Rede *Wireless* deve conter os seguintes elementos: AP, máquina dos usuários, servidor de autenticação etc. Além disso, devem estar descritos: endereços IP, canais utilizados, algoritmo de criptografia usado, SSID, fabricante, número do modelo e de série, a localização do equipamento e atribuído utilizador.

6.16 DOCUMENTAÇÃO

6.16.1 As Organizações Militares devem documentar os procedimentos de instalação e configuração dos ativos da Rede *Wireless*. A existência de uma documentação da instalação, configuração e manutenção destes equipamentos ajuda a evitar erros de operação, permite a verificação de conformidade da configuração em relação a políticas e também facilita a recuperação do sistema em caso de falhas de *software* ou *hardware*.

6.16.2 As Organizações Militares devem documentar a arquitetura da Rede *Wireless*, o que ajuda a evitar erros de operação, permite a verificação de conformidade da configuração em relação a políticas e também torna possível uma reconfiguração mais rápida do ambiente,

reduzindo o tempo de indisponibilidade (*downtime*) no caso de necessidade de reinstalação dos sistemas.

6.16.3 As Organizações Militares devem manter atualizada a documentação da arquitetura da Rede *Wireless*. Expansões da rede, redistribuição de equipamentos, mudanças de endereçamento e outras alterações geralmente são feitas sem a devida atualização dos documentos da Rede sem Fio. Uma documentação desatualizada provoca erros, retrabalhos e, na ocorrência de incidentes de segurança da informação, pode aumentar o tempo de indisponibilidade dos serviços afetados.

6.17 DESCARTE DE EQUIPAMENTOS

6.17.1 As Organizações Militares devem remover todas as informações nos equipamentos da Rede *Wireless*, incluindo chaves pré-compartilhadas e senhas de equipamento. Os atacantes podem usar informações confidenciais em equipamentos de rede descartados para conduzir ataques subsequentes em redes da Organização Militar. As organizações devem utilizar utilitários de limpeza de disco em equipamentos que possuam discos rígidos. Outra opção é excluir as configurações manualmente, utilizando a interface de gerenciamento.

6.17.2 As Organizações Militares, ao descartar um equipamento da Rede *Wireless*, devem assegurar que seus registros de *log* de auditoria estão mantidos conforme necessário para atender aos requisitos legais. As informações contidas nos registros de auditoria podem ser necessárias, mesmo após o equipamento de Rede sem Fio ser descartado, como, por exemplo, para uma investigação de um incidente de segurança da informação.

7 FASES DO CICLO DE VIDA DE UMA REDE SEM FIO

7.1 GARANTIA DA IMPLANTAÇÃO DAS FASES DO CICLO DE VIDA

7.1.1 As Organizações Militares subordinadas ao DECEA devem assegurar que as considerações de segurança da informação de Rede sem Fio estão incorporadas em cada fase do ciclo de vida de sua implantação, configuração e administração.

7.2 OBJETIVO DESTA SEÇÃO

7.2.1 Esta seção da Norma apresenta orientações sobre planejamento e implantação de uma Rede sem Fio. Ela descreve um modelo de ciclo de vida para a rede *Wi-Fi* e apresenta recomendações de melhores práticas relacionadas com a segurança da informação para cada fase do ciclo de vida.

7.3 FASES DE CICLO DE VIDA DE UMA REDE SEM FIO

7.3.1 Fase 1: Iniciação. Esta fase inclui as tarefas que a Organização Militar deve realizar antes de começar a projetar sua solução de Rede *Wireless*. Estas incluem o fornecimento de uma visão global de como a Rede sem Fio irá apoiar a missão da Organização Militar, criando uma estratégia para a sua implantação, elaborando um procedimento de segurança da informação em conformidade com esta Instrução, e especificação de requisitos de negócios e funcional para a solução.

7.3.2 Fase 2: Aquisição/Desenvolvimento. A fase de aquisição/desenvolvimento é dividida da seguinte forma:

a) Planejamento e *Design*. Nesta fase, os administradores de Rede *Wireless* devem especificar as características técnicas da rede, tais como: métodos de autenticação, componentes de rede relacionados, listas de controle de acesso e conjuntos de regras de *firewall*. Os administradores também devem realizar um levantamento do local para ajudar a determinar a arquitetura da solução e como a rede deve ser integrada com a infraestrutura de autenticação existente; e

b) Aquisições: Esta fase envolve a especificação do número e tipo de componentes de Rede *Wireless* que devem ser comprados, os conjuntos de recursos que devem suportar (por exemplo, módulos válidos de encriptação) e o que as certificações devem manter (por exemplo, WPA2).

7.3.3 Fase 3: Implementação. Nesta fase, com o equipamento adquirido, primeiro se realiza a configuração adequada para atender aos requisitos de segurança da informação operacional e, em seguida, instalado e ativado em uma Rede *Wireless* em operação. A implantação inclui os controles de segurança da informação, tais como registro de eventos de segurança da informação, gerenciamento de rede, integração com o servidor de autenticação e criptografia.

7.3.4 Fase 4: Operação/Manutenção. Esta fase inclui tarefas relacionadas à segurança da informação que a Organização Militar deve executar em uma base contínua, uma vez que a Rede *Wireless* encontra-se operacional, incluindo análise e avaliação de segurança da informação periódica, revisões de *log* e tratamento de incidentes de segurança da informação.

7.3.5 Fase 5: Descarte. Esta fase engloba tarefas que ocorrem depois que a Rede *Wireless* e seus componentes foram retirados, incluindo a preservação de informações para atender aos

requisitos legais, mídias que podem conter material sensível e o descarte seguro de equipamentos.

8 DISPOSIÇÕES FINAIS

8.1 A presente Instrução é de caráter geral e deve ser revisada periodicamente a cada 24 (vinte e quatro) meses.

8.2 Esta Instrução contém boas práticas de segurança da informação para Rede sem Fio genérica. Como os procedimentos de configuração variam com relação à marca e ao modelo, para obter informações sobre os detalhes da implementação é necessário consultar a documentação fornecida pelo fabricante.

8.3 As Organizações Militares nas quais a Rede sem Fio já está em operação têm o prazo de até 18 meses para a adequação às diretrizes constante desta ICA. A sua não observância implicará que os riscos e as consequências foram assumidos pela referida OM

8.4 Esta Instrução de Comando da Aeronáutica deverá estar em conformidade com as Diretrizes da DTI – Órgão Central do Sistema de Tecnologia da Aeronáutica –, e será revisada e atualizada sempre que forem atualizadas ou aprovadas Normas relativas ao assunto pela Diretoria de Tecnologia da Informação do Comando da Aeronáutica.

8.5 Casos não previstos nesta Instrução deverão ser levados à apreciação do Exmo Sr Diretor-Geral do DECEA.