Segurança em Redes Locais de Computadores das Bases Aéreas

Ranulfo Acir de Oliveira Resende, Ten Cel Av
Quarto Comando Aéreo Regional – Av. D. Pedro I, 100, São Paulo – SP
e-mail: acir_r@yahoo.com.br

***Resumo* — As redes locais de computadores constituem um valioso repositório de informações sobre as atividades cotidianas das Bases Aéreas. A preocupação com a segurança dos dados trafegados nas redes foi explicitada inicialmente pela antiga NSMA 7-3, Segurança de Dados no Ministério da Aeronáutica, que vigeu experimentalmente apenas no ano de 1999. A presente pesquisa levantou a real situação da segurança das redes de computadores das Bases Aéreas, com o objetivo de auxiliar na elaboração das políticas de segurança destas organizações. Ficou evidenciado que as redes não são seguras, apresentando falhas na implementação de itens críticos de segurança. Os dados estão atualizados até agosto de 2005.**

***Palavras-chaves* — segurança de dados, redes de computadores, Bases Aéreas, Tecnologia da Informação.**

I. INTRODUÇÃO

O assunto segurança em redes de computadores reveste-se de grande interesse nos meios civil e militar. As mais recentes publicações na área alertam para as crescentes ameaças aos sistemas informatizados[1]. Em especial, como será descrito nas Seções posteriores, as Bases Aéreas possuem nas redes locais um importante instrumento de suporte às suas atividades administrativas. O funcionamento das redes de computadores das Bases Aéreas necessita, portanto, garantir a segurança de que as informações veiculadas nas redes estarão protegidas de ações adversas.

O presente trabalho investiga a questão da segurança no contexto das redes locais de computadores das Bases Aéreas, buscando levantar dados que indiquem o quão sensíveis estão estas redes diante das principais ameaças conhecidas.

A delimitação da pesquisa especificamente no contexto das Bases Aéreas objetiva explorar as peculiaridades e as semelhanças destas Organizações e, com isto, obter resultados consistentes e de aplicação prática como instrumento de auxílio na elaboração das políticas de segurança de dados. A importância do trabalho está exatamente nisto, ou seja, na possibilidade dos resultados levantados virem, em associação com trabalhos futuros, a fundamentar procedimentos padronizados que deverão ser inseridos nos documentos de políticas de segurança de dados das Bases Aéreas.

Como embasamento teórico adotou-se a norma *NBR ISO/IEC 17799:2001*, [1], principal referência no meio civil na área de segurança da informação, e a publicação *Melhores práticas para gerência de redes de computadores* [2].

Este trabalho tem a intenção de, por meio de uma pesquisa exploratória simples, responder à pergunta: quais os principais fatores adversos que podem comprometer a segurança das redes locais de computadores das Bases Aéreas?

A busca de resposta para a pergunta acima origina os seguintes objetivos específicos da pesquisa:

1. Determinar os fatores necessários para avaliação de desempenho de uma rede local de uma Base Aérea;
2. Identificar as principais ameaças que podem levar tais fatores a saírem dos parâmetros normais; e
3. Identificar como os principais procedimentos de segurança consagrados pela literatura estão implementados nas Bases Aéreas.

Abordou-se o problema por meio do método hipotético-dedutivo, assumindo-se a hipótese de que as redes locais de computadores das Bases Aéreas não estão seguras diante das principais ameaças conhecidas.

O trabalho constituiu-se de uma pesquisa bibliográfica com a finalidade de determinar as respostas aos objetivos específicos 1 e 2. O objetivo 3 foi verificado por um questionário que foi enviado aos chefes das Seções de Informática das Bases Aéreas.

Na Seção 2 são discutidas as características das redes locais das Bases Aéreas e os seus parâmetros de funcionamento. A seguir, na Seção 3, é abordada a questão da segurança propriamente dita, com o detalhamento das suas dimensões, das principais ameaças e defesas. Por último, no Seção 4, são apresentadas considerações sobre o questionário e é discutido o significado dos resultados levantados para se inferir a realidade atual quanto à implementação dos principais itens de segurança nas redes de computadores das Bases Aéreas.

II. A REDE LOCAL DE UMA BASE AÉREA

No organograma generalizado de uma Base Aérea, de acordo com o Regulamento de Base Aérea, RMA 21-5 [3], observa-se um total de 14 divisões administrativas que usualmente são transpostas para grupos de usuários em uma rede local. Adicionalmente, o servidor de arquivos é estruturado em pastas de forma a atender os grupos de usuários destas divisões administrativas.

Na área de Intendência, a rede local dá suporte às consultas ao SIAFI e ao Programa Automatizado de Gestão, que controla os Pedidos de Aquisição de Material e Serviços.

Na parte de pessoal tem-se o suporte ao SIGPES como função de maior relevância.

[1] NAKAMURA, Emílio Tissato e outros. Segurança de Redes em Ambientes Cooperativos

Semelhantemente, cada setor de uma Base Aérea possui no funcionamento da rede local o suporte para importantes funções administrativas e, como resultado, informações preciosas, mesmo que não classificadas, circulam pelas redes locais de computadores das Bases Aéreas.
Do exposto, conclui-se que, no atual estágio de informatização das Bases Aéreas, a área administrativa sofre intensamente as conseqüências da interrupção dos serviços das redes locais de computadores. Assim sendo, torna-se imperioso conhecer os parâmetros de funcionamento normal das redes locais para buscar a maior segurança na sua operação.

A. Parâmetros de Funcionamento de uma Rede Local

Para estudar o funcionamento das redes locais de computadores convém conhecer os principais indicadores que permitem aferir a qualidade do tráfego de dados entre os equipamentos.

1) Taxa de Erros: Verificada nos nos enlaces ópticos ou metálicos, as taxas de erros devem ser normalmente muito próximas de zero. Em enlaces metálicos aceita-se, no pior caso, 1 erro a cada 10^9 bits transmitidos e, em enlaces ópticos, 1 erro a cada 10^{12} bits transmitidos.
2) Taxa de Colisões: Normalmente verificada nos repetidores e comutadores, a taxa de colisões deve ser sempre inferior a 10%.
3) Taxa de Utilização da CPU: A taxa de utilização da CPU deve ser verificada nos servidores e deve estar necessariamente abaixo de 75% para um funcionamento normal da máquina.
4) Taxa Utilização da Memória: A taxa de utilização da memória também deve ser verificada nos servidores e deve estar, necessariamente, abaixo de 75% para um funcionamento normal da máquina.
5) Tráfego de Difusão (Multicast e Broadcast): o endereçamento IP [4] possibilita a cada computador uma identificação única na rede. Existem, contudo, endereçamentos coletivos que permitem enviar mensagens (pacotes) para mais de uma máquina, na chamada difusão do tipo Multicast, e para todas as máquinas de uma rede, na difusão do tipo Broadcast.
O que é relevante é que para o funcionamento normal da rede o tráfego de difusão, ou seja, de pacotes Multicast e Broadcast, deve ser necessariamente baixo.
6) Tempo de PING e de TRACEROUTE[1] para computadores internos: Durante a utilização dos comandos PING e TRACEROUTE, tendo-se como alvos computadores (normalmente servidores) internos da rede, devem ser observados tempos de retorno inferiores a 1 ms.
Os parâmetros apresentados servem como indicadores para o monitoramento das redes locais e como comprovação de que o funcionamento da rede pode estar apresentando algum problema. O fato dos indicadores estarem dentro dos padrões normais sugere que não há problemas com a rede. Contudo, a indicação anormal de um ou mais parâmetros permite concluir que há um problema que necessita ser investigado.

III A QUESTÃO DA SEGURANÇA

O funcionamento de uma Base Aérea, conforme definido em [3], implica interações internas entre seus diversos setores e externas com as demais Organizações da Força Aérea Brasileira.
A norma [5], emitida experimentalmente no ano de 1999, já orientava que os dados armazenados nas redes locais deveriam ser protegidos por um Plano de Ação e por um Plano de Contingência de Dados. No meio civil, [1] constitui uma referência para as empresas que desejam implantar controles visando à segurança de informações.
Numa avaliação prévia, observa-se que o simples atendimento [5], anterior, portanto, à correspondente civil [1], colocaria as Organizações Militares num patamar de segurança superior ao exigido pela norma da ABNT. Infelizmente a [5] não foi reeditada e não possui substituta no Comando da Aeronáutica, ficando o assunto a cargo dos respectivos Chefes das Seções de Informática.
A segurança de informações no contexto das redes locais de computadores das Bases Aéreas se reveste de grande preocupação em virtude dos incidentes reportados pelo CERT-BR (Computer Emergency Response Team), conforme mostra a figura 6, terem crescimento superior a 500% no período de 2001 a 2004[2].

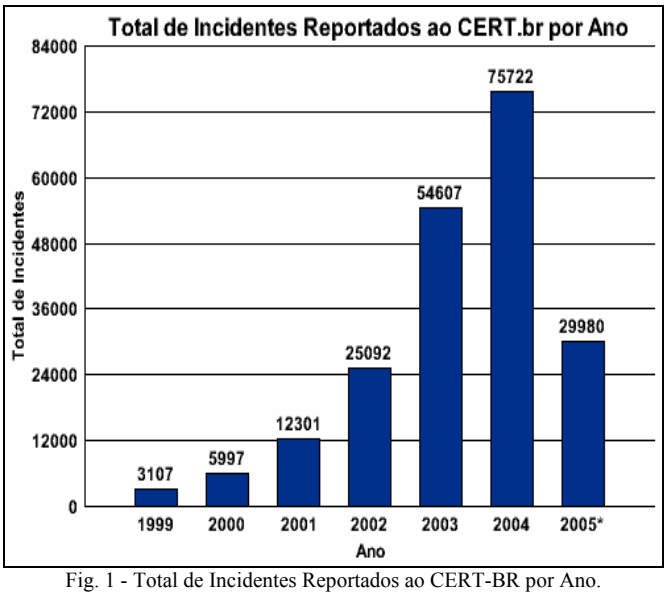

Fig. 1 - Total de Incidentes Reportados ao CERT-BR por Ano.

Na figura 1, para o ano de 2005, tem-se um valor parcial dos incidentes ocorridos no início do ano.
Este trabalho utilizou o princípio de Pareto[3] [6] para levantar as principais ameaças à segurança das redes locais de dados das Bases Aéreas.

A. As Dimensões da Segurança, Ameaças e Defesas

Em [1] adota-se o conceito de segurança da informação por meio de três dimensões:

- confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas;

1 Ping e Traceroute (ou tracert no Linux) são conhecidas funcionalidades do Sistema Operacional para monitoramento da rede de dados.

2 Fonte: http://www.nbso.nic.br/stats/incidentes/#2005, acesso em 21/08/2005.

3 O princípio de Pareto, conforme [6], pág. 170, assume a hipótese que em um fenômeno 20% das causas são responsáveis por 80% dos resultados.

- integridade: garantia de que a informação é completa e exata, ou seja, que não foi indevidamente alterada;
- disponibilidade: garantia de que os usuários autorizados terão o acesso à informação sempre que necessário.

É imperativo, portanto, conhecer as ameaças que podem comprometer pelo menos uma destas dimensões.

Adotando-se como fonte de dados estatísticos os incidentes reportados ao CERT.BR no ano de 2004, destacam-se as seguintes ameaças: worm, ataque ao usuário final, DOS, invasão, ataque ao servidor WEB, scan e fraude. Os dados sobre estes ataques estão condensados na Tabela 1.

TABELA I: PRINCIPAIS TIPOS DE ATAQUES REPORTADOS AO CERT.BR NO ANO DE 2004[1].

Incidente	Quant.	%	Confid	Integrid	Dispon.
Worm	42267	55	NÃO	SIM	SIM
Ataque ao Usuário Final[2]	406	0	*	*	*
DOS[3]	104	0	Não	Não	SIM
Invasão	248	0	SIM	SIM	NÃO
Ataque ao Serv WEB	524	0	NÃO	SIM	SIM
Scan[4]	28158	37	*	*	*
Fraude	4015	5	SIM	SIM	NÃO

A tabela 1 confronta o tipo de ataque com a dimensão da segurança comprometida pelo mesmo. Nota-se a predominância de worms (55%) e de scan (37%).

Pela regra de Vilfredo Pareto, 20% das causas são responsáveis por 80% dos resultados. Logo, uma rede protegida das ameaças worm e scan eliminaria 92% dos incidentes de risco à segurança.

O scan não representa em si mesmo uma ameaça a alguma das dimensões da segurança, contudo corresponde a uma fase para que sejam lançados ataques de outro tipo, como DOS ou invasão.

Já os worms representam séria ameaça à disponibilidade e à integridade dos sistemas de TI. A defesa usual para este ataque é a conjugação do antivírus com um firewall bem configurado.

Portanto, a defesa de uma rede de computadores, nos dias atuais, pode ser otimizada nos seguintes fatores:

- antivírus atualizado nos servidores;
- antivírus atualizado nas estações de trabalho;
- firewall que feche ao mundo exterior, seja para Intranet ou Internet, todas as portas de comunicação não utilizadas pelos serviços essenciais;
- um bom serviço de back-up; e
- processo de acesso à rede (login) com criptografia de senhas.

As demais ameaças devem ser consideradas tendo-se como referência os ativos de informação que se deseja proteger.

Destacam-se, não pela freqüência, mas pela gravidade dos danos às dimensões da segurança, o DOS e a invasão. Nestes casos, as defesas recomendadas iniciam pela implementação de um Sistema de Detecção de Intrusão (IDS) e maior treinamento da equipe de gerência de redes em práticas usuais de segurança, como o exame de logs[5] e monitoramento do comportamento da rede. Nos casos críticos convém implantar um Honeypot[6].

A literatura apresenta, em especial [2], grande riqueza de detalhes que comprovam a correlação entre os parâmetros de funcionamento discutidos na Seção 2 e as ameaças aqui descritas. Como exemplo, pode-se citar os seguintes casos: o aumento no tráfego de difusão pode ser observado na ocorrência de vírus e worms que se proliferam pela rede. Adicionalmente, os aumentos da taxa de erros e de colisões, geralmente, são devidos a problemas físicos em alguma interface de rede ou porta de equipamento defeituosa.

IV LEVANTAMENTO DOS DADOS

O apêndice apresenta parte do questionário que foi elaborado para se mensurar a segurança no contexto das redes locais de computadores das Bases Aéreas.

Com algumas questões mediu-se a experiência profissional de quem está respondendo o questionário, que foi enviado aos Chefes das Seções de Informática das Bases Aéreas. Em especial, uma questão objetivou aferir a capacitação técnica dos profissionais, comprovada por intermédio de cursos na área de Tecnologia da Informação.

A última questão foi montada para levantar, numa escala de 1 a 5, o grau de implementação de dezoito itens de segurança, escolhidos com base em [1],[2], [7]-[10]. A escala adotada, apesar de numérica, não é quantitativa, mas sim qualitativa.

Conforme descrito no Apêndice, a resposta 1 indica que o pesquisado não conhece tecnicamente o item em questão. A resposta 2 significa que, na opinião do Chefe da Seção de Informática, o item seria desnecessário.

Estes dois primeiros níveis da escala representam que o item, mesmo sendo considerado relevante para o autor da pesquisa, não foi considerado para implementação pelo pesquisado.

As respostas de 3 a 5 indicam uma graduação na implementação do item: a resposta 3 corresponde a um item avaliado como necessário mas que não foi implementado; a alternativa 4 significa que o item está em processo de implantação; o nível 5 é para os casos em que o item foi considerado já totalmente implementado. Como a escala é qualitativa, qualquer resposta inferior a 5 evidencia que há falha de segurança.

A. Resultados

A análise das respostas ao questionário mostrou que 75% dos pesquisados possuiam posto inferior ou igual a Tenente, e que apenas 50% já realizaram cursos na área de Tecnologia da Informação. Isto evidencia que as chefias das Seções de informática são, em geral, compostas de pessoal pouco experiente profissional e tecnicamente.

As respostas aos dezoito itens de segurança foram compiladas no gráfico da figura 2.

---

1 Fonte: dados adaptados de http://www.nbso.nic.br, acesso em 21/08/2005.

2 Os danos advindos deste tipo deste ataque são específicos para cada caso, não permitindo generalização.

3 DOS: Denial of Service (negação de serviço).

4 O *Scan* apenas não produz dano algum. No entanto, constitui uma fase para um ataque posterior que pode ser danoso.

5 Logs: registros armazenados nos servidores que permitem observar o comportamento malicioso de equipamentos e de usuários.

6 Ambiente de rede que simula uma rede operacional com o objetivo de registrar os atos do invasor, detectá-lo com precisão e subsidiar com dados um eventual processo judicial.

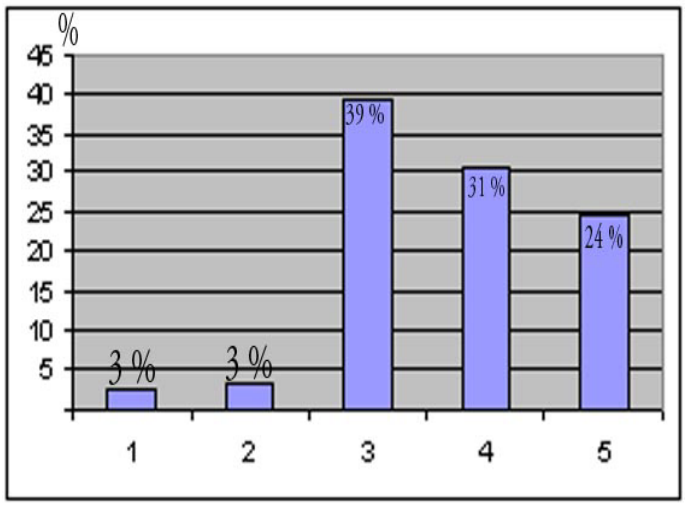

Fig. 2: Compilação das respostas aos itens de segurança

O gráfico da figura 2 mostra que 6% das respostas aos dezoito itens pesquisados correspondem aos níveis 1 e 2, na qual o item não foi considerado para implementação.
Observa-se, também, que parcela considerável das respostas (39%) correspondem ao nível 3, em que os itens foram considerados necessários mas não foram implementados e não se encontravam em processo de implantação.
Genericamente, evidenciou-se que apenas 24% das respostas corresponderam a itens de segurança totalmente implementados, ressaltando-se a elevada taxa (76%) de respostas correspondentes a itens de segurança não completamente implementados, o que caracteriza um elevado grau de falta de segurança nas redes locais de computadores das Bases Aéreas.
Em reforço da avaliação generalizada dos resultados, pode-se aprofundar a análise dos dados para considerar os itens essenciais abordados pela aplicação do princípio de Pareto realizada no Seção 2:

1. antivírus atualizado nos servidores;
2. antivírus atualizado nas estações de trabalho;
3. firewall que feche ao mundo exterior, seja para Intranet ou Internet, todas as portas de comunicação não essenciais;
4. um bom serviço de back-up; e
5. processo de acesso à rede (login) com criptografia de senhas.

Os quesitos acima foram aferidos por meio dos itens 1,2,10,13 e 15 do questionário sobre segurança.
O gráfico da figura 3 apresenta os resultados condensados para os 5 itens críticos de segurança.

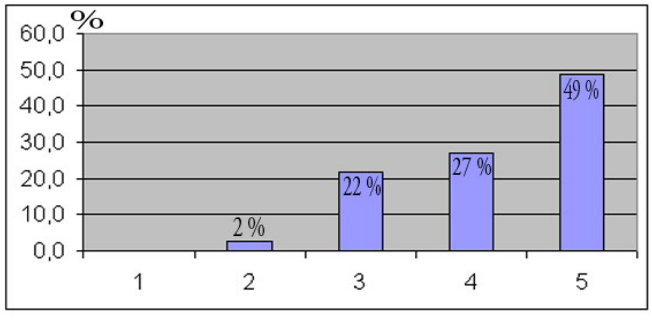

Fig. 3: Compilação das respostas ao itens de segurança críticos.

Pode-se observar que menos de 50% das respostas corresponderam a itens completamente implementados (grau 5 da escala), ratificando, mesmo na análise detalhada que considera apenas itens críticos, que as redes de computadores não estão satisfatoriamente seguras.
A hipótese inicial de que as redes não estão seguras frente às principais ameaças conhecidas fica, portanto, confirmada pelos resultados aqui apresentados.
São sumarizadas, na próxima seção, as conclusões do trabalho, abrangendo a importância do resultado no contexto da segurança de informações nas redes locais de computadores das Bases Aéreas.

IV Conclusão

Este trabalho abordou, por intermédio de uma pesquisa exploratória simples, a questão da segurança nas redes locais de computadores das Bases Aéreas.
Foi assumida inicialmente a hipótese de que as redes das Bases Aéreas não estão seguras diante das principais ameaças conhecidas.
A Seção 2 descreveu a importância das redes locais para o suporte das funções administrativas das Bases Aéreas e discutiu os parâmetros de funcionamento das redes de computadores. A questão da segurança foi criteriosamente discutida na Seção 3, onde foram apresentadas as dimensões da segurança, as ameaças e as defesas mais freqüentemente abordadas pela literatura, em especial, por [1] e [2].
Foram apresentadas na Seção 4, as diretrizes que nortearam a elaboração do questionário que foi enviado aos Chefes das Seções de Informática das Bases Aéreas. No mesmo capítulo foram analisados os dados recebidos, sendo confirmada a hipótese assumida como norteadora da pesquisa.
Verificou-se, portanto, que os dados levantados comprovaram que as redes locais de computadores das Bases Aéreas não estão seguras diante das principais ameaças apresentadas pela literatura, que atualmente são vírus, worms, o scan e o roubo de senhas de acesso.
Finalmente, recomenda-se que os itens críticos de segurança definidos pela aplicação do princípio de Pareto na Seção 2, cujas implementações nas redes das Bases Aéreas foram investigadas e detalhadamente analisadas, sejam considerados na elaboração dos documentos das políticas de segurança de dados das Bases Aéreas, com o objetivo de que tais itens sejam completamente implantados e, com isto, garantir maior segurança de informações nas redes locais de computadores.

Apêndice

Parte do questionário enviado aos Chefes das Seções de Informática das Bases Aéreas.
Usando a escala abaixo, assinale ao lado direito dos itens qual o grau de implementação (de 1 até 5) que mais se aproxima da sua opinião e da realidade, em resposta à pergunta: Como o Sr. avalia a implementação dos diversos itens relacionados à segurança da rede local de computadores de sua Base Aérea?

ESCALA

1	2	3	4	5
Não sei responder	**Item desneces-sário**	**Item necessário mas ainda não implemen-tado**	**Item em processo de imple-mentação**	**Item totalmente implemen-tado**

Item	Escala
1 – Software ANTIVÍRUS nos SERVIDORES.	1( ) 2( ) 3( ) 4( ) 5( )
2 – Software ANTIVÍRUS nas estações de trabalho.	1( ) 2( ) 3( ) 4( ) 5( )
3 – Treinamento de equipe em manutenção física da rede (cabeamento estruturado).	1( ) 2( ) 3( ) 4( ) 5( )
4 – Treinamento de equipe em manutenção de microcomputadores.	1( ) 2( ) 3( ) 4( ) 5( )
5 – Treinamento de equipe em Gerência de Redes.	1( ) 2( ) 3( ) 4( ) 5( )
6 – Treinamento de equipe em segurança.	1( ) 2( ) 3( ) 4( ) 5( )
7 – Lacre nos gabinetes de todos os microcomputadores da Base Aérea.	1( ) 2( ) 3( ) 4( ) 5( )
8 – Critérios quanto ao uso de equipamentos com CD-ROM, *drive de disquetes* e portas USB disponíveis para o usuário final.	1( ) 2( ) 3( ) 4( ) 5( )
9 – Controle de licenças e combate aos softwares não licenciados (piratas).	1( ) 2( ) 3( ) 4( ) 5( )
10 – Proteção dos servidores e da rede interna por firewall.	1( ) 2( ) 3( ) 4( ) 5( )
11 – Estação de detecção de intrusos (IDS).	1( ) 2( ) 3( ) 4( ) 5( )
12 – Servidores instalados em salas específicas com controle de acesso.	1( ) 2( ) 3( ) 4( ) 5( )
13 – Controle de acesso à rede por senhas cifradas.	1( ) 2( ) 3( ) 4( ) 5( )
14 – Política de segurança definida em documento específico.	1( ) 2( ) 3( ) 4( ) 5( )
15 – Cópias diárias de segurança *(backup)* do servidor de arquivos.	1( ) 2( ) 3( ) 4( ) 5( )
16 –Cópias de segurança (backup) guardadas em prédio separado.	1( ) 2( ) 3( ) 4( ) 5( )
17 – Estação com sistema de verificação de vulnerabilidades (Ex.: Nmap ou Nessus).	1( ) 2( ) 3( ) 4( ) 5( )
18 – Estação de gerenciamento SNMP.	1( ) 2( ) 3( ) 4( ) 5( )

REFERÊNCIAS

[1] Associção Brasileira de Normas Técnicas. NBR ISO/IEC 17799: Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2000

[2] LOPES, Raquel V. et al. Melhores práticas para gerência de redes de computadores. Rio de Janeiro: Campus, 2003.

[3] BRASIL. Ministério da Aeronáutica. RMA 21-5: Regulamento de Base Aérea. Brasília, DF, 1989.

[4] COMER, E Douglas. Interligação em redes com TCP/IP. Rio de Janeiro: Campus, 1998.

[5] BRASIL. Ministério da Aeronáutica. NSMA 7-3: Segurança de Dados no Ministério da Aeronáutica, 1999.

[6] MARANHÃO, M e Madeira, M. E. B. O processo nosso de cada dia: Modelagem de processos de trabalho. Rio de Janeiro, 2004.

[7] MITNICK, Kevin D. MITNICK A Arte de Enganar. São Paulo: Pearson Makron Books, 2003.

[8] NAKAMURA, Emílio Tissato et al. Segurança de redes em ambientes cooperativos. São Paulo: Futura, 2003.

[9] TERPSTRA, John H. et al. Segurança para Linux. Rio de Janeiro: Campus, 2005.

[10] TRENT, R. Hein et al. Manual completo do Linux. São Paulo: Pearson Makron Books, 2004.