- Decreto Nº. 4.829, de 3 de setembro de 2003 da Presidência da República, disponível em http://www.cg.org.br;
- Resolução Nº. 001/2005, de dia 05 de dezembro de 2005 do Comitê Gestor da Internet no Brasil, disponível em http://www.cg.org.br;
- Resolução Nº. 002/2005, de dia 05 de dezembro de 2005 do Comitê Gestor da Internet no Brasil, disponível em http://www.cg.org.br;
- Decreto Nº. 316/99, de 08 de julho de 1999, que institui a INFOVIA-MT;
- Política de Segurança da Informação para a Rede INFOVIA-MT;
- Política de Uso Aceitável para a Rede INFOVIA-MT.

4. Definições

Termos, definições e conceitos essenciais à compreensão desta política encontram-se nas páginas na Internet do Comitê Gestor da Internet no Brasil (http://www.cg.org.br) e do Registro.br (http://registro.br).

5. Princípios

5.1 Autoridade e Responsabilidade:

A atribuição, registro e controle dos nomes de sub-domínio Internet associados ao domínio "mt.gov.br" de uma entidade da administração pública Estadual ou Municipal, é de responsabilidade do CEPROMAT.

É de responsabilidade e arbítrio de cada órgão ou entidade usuária a atribuição do nome relativo ao hospedeiro (host) de sua rede do órgão.

5.2 A Aplicabilidade:

Essa estrutura de formação de nomes de sub-domínio Internet aplica-se a toda entidade pública governamental que desejar usar um nome de sub-domínio Internet associado ao domínio "mt.gov.br".

5.3 Descrição da estrutura adotada:

O nome de sub-domínio Internet das entidades usuárias será implementado abaixo do domínio principal do Governo do Estado "mt.gov.br".

Para possibilitar o gerenciamento centralizado e autonomia operacional das entidades usuárias é adotado o conceito de sub-domínio, que será incorporado ao domínio principal "mt.gov.br", e para o qual recomenda-se a utilização do nome da entidade, seguindo o formato (entidade.mt.gov.br).

Contudo dá-se a liberdade ao órgão usuário de utilizar a sigla que melhor a caracterize, desde que não fira os interesses órgão usuário ou do Governo do Estado de Mato Grosso. Por exemplo: cepromat.mt.gov.br, planejamento.mt.gov.br, seplan.mt.gov.br.

A atribuição do nome de hospedeiro (host) dentro do sub-domínio ficará a critério de cada administrador de rede da entidade usuária. Exemplos: www.cepromat.mt.gov.br, smtp.cepromat.com.br, www.sefaz.mt.gov.br.

Recomenda-se que nome atribuído a cada hospedeiro (host) possa caracterizá-lo de acordo com os padrões de nomenclatura de hospedeiro (host) de cada entidade, evitando o uso de nomes considerados ofensivos, abusivos, preconceituosos ou fora dos interesses do Governo do Estado de Mato Grosso.

Os hospedeiros (hosts) que respondem pelos serviços web do Governo do Estado de Mato Grosso, estarão diretamente ligados ao domínio "mt.gov.br". Exemplo: www.mt.gov.br, smtp.mt.gov.br.

Os sub-domínios que se referem aos municípios matogrossenses serão criados seguindo o formato <município>.mt.gov.br. Por exemplo: cuiaba.mt.gov.br , rondonopolis.mt.gov.br, sinop.mt.gov.br. Adicionando-se o nome de hospedeiros (hosts), teremos, por exemplo: www.cuiaba.mt.gov.br, www.rondonopolis.mt.gov.br, ftp.sinop.mt.gov.br, etc..

5.4 Divulgação e atualização:

É de responsabilidade do CEPROMAT encaminhar para publicação no Diário Oficial do Estado todo novo sub-domínio que venha a ser incluído ao domínio "mt.gov.br",
bem como a relação completa de todos os sub-domínios registrados.

A relação de todos sub-domínios registrados deverá estar disponível para consulta na home page do CEPROMAT "www.cepromat.mt.gov.br".

6. Disposições finais

A solicitação de registro de subdomínios "entidade.mt.gov.br" deve ser feita oficialmente pelo interessado ao Centro de Processamento de Dados do Estado de Mato Grosso – CEPROMAT, órgão que administra o DNS (*Domain Name System*) central do Governo do Estado de Mato Grosso.

Em nenhuma hipótese serão registrados nomes considerados ofensivos, de baixo calão, preconceituosos ou manifestamente desvinculados dos objetivos e propósitos do Governo do Estado de Mato Grosso.

Atender a esta resolução serão intimados a fazê-lo, com prazo de até 6 (seis) meses para conviver em paralelo com o endereço antigo.

Para as aplicações disponibilizadas abaixo do domínio "mt.gov.br" ou de qualquer sub-domínio "entidade.mt.gov.br", recomenda-se que o nome da aplicação seja inserido após o domínio ou sub-domínio, por exemplo: www.sad.mt.gov.br/sigp, www.sad.mt.gov.br/contratos, www.sefaz.mt.gov.br/tributário, etc. Nos casos não aplicáveis, recomenda-se que o nome da aplicação seja um hospedeiro (host) do domínio ou sub-domínio, por exemplo: direto.mt.gov.br, isosystem.sad.mt.gov.br, etc..

Os nomes de domínios atualmente registrados serão revisados e os que deixarem de atender a esta resolução serão intimados a fazê-lo, com prazo de até 6 (seis) meses para conviver em paralelo com o endereço antigo.

A entidade usuária é responsável pelas atividades de seus usuários e pelo conteúdo das informações contidas em suas páginas web.

Governo do Estado de Mato Grosso
Secretaria de Estado de Planejamento e Coordenação Geral
Conselho Superior do Sistema Estadual de Informação e Tecnologia da Informação

RESOLUÇÃO Nº. 003/2007

Dispõe sobre as políticas e diretrizes para implementação, manutenção e o uso de redes locais sem fio (Wireless) no âmbito do Estado de Mato Grosso.

O CONSELHO SUPERIOR DO SISTEMA ESTADUAL DE INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO, no uso das competências que lhe são conferidas pela Lei Nº 8.199 de 11 de novembro de 2004 e regulamentadas pelo Decreto Nº 6.300 de 31 de agosto de 2005;

CONSIDERANDO a necessidade de estabelecer políticas e diretrizes para nortearem a implementação, manutenção e o uso de Redes Locais Sem Fio (Wireless) interligadas a Rede Infovia-MT;

CONSIDERANDO a necessidade de políticas e diretrizes para prover confiabilidade e continuidade dos serviços que se deseja disponibilizar para o cidadão;

RESOLVE:

Art.1º - Apresentar as recomendações para instalação das redes locais sem fio (Wireless) de forma padronizada, permitindo a sua conexão à Infovia-MT,conforme o especificado no anexo "Norma de Padronização das Redes Locais Sem Fio (Wireless).

Art.2º - Caberá ao Centro de Processamento de Dados do Estado de Mato Grosso-CEPROMAT como gestor da Rede INFOVIA-MT a responsabilidade pela avaliação e aceitação da ligação destas redes locais sem fio (Wireless) à Infovia-MT obedecendo os procedimentos do Anexo desta Resolução.

Art.3º-Esta Resolução entrará em vigor na data de sua publicação.

CUMPRA-SE

Conselho Superior do Sistema Estadual de Informação e Tecnologia da Informação, em 04 de abril de 2007.

(Original Assinado)
YÊNES JESUS DE MAGALHÃES
Presidente do Conselho e
Secretário de Estado de Planejamento e Coordenação Geral

(Original Assinado)
WALDIR JÚLIO TEIS
Secretário de Estado de Fazenda
Membro do Conselho

(Original Assinado)
SÍRIO PINHEIRO DA SILVA
Auditor Geral do Estado
Membro do Conselho

(Original Assinado)
GERALDO A DE VITTO JUNIOR
Secretário de Estado de Administração
Membro do Conselho

(Original Assinado)
JOÃO VIRGILIO DO N SOBRINHO
Procurador Geral do Estado
Membro do Conselho

(Original Assinado)
ADRIANO NIEHUES
Diretor Presidente do Cepromat
Membro do Conselho

ANEXO I – RESOLUÇÃO Nº. 003/2007

NORMA DE PADRONIZAÇÃO DAS REDES LOCAIS SEM FIO (WIRELESS) PARA A INFOVIA-MT

1. Objetivo

Este documento tem como objetivo estabelecer políticas e diretrizes para o uso adequado do serviço de comunicação de dados usando redes locais sem fio, Redes Wireless, com a tecnologia Wi-Fi, nos órgãos de governo do Estado de Mato Grosso, tendo em vista os objetivos definidos da rede INFOVIA-MT.

2. Público-alvo

Esta norma aplica-se ao ambiente de redes locais sem fio (Redes Wireless), com uso da tecnologia Wi-Fi, dos órgãos de governo do Estado de Mato Grosso. E deve ser observada pelos gestores de TI, administradores de ativos de TI, administradores de infra-estrutura de redes, projetistas de redes, e usuários da Rede INFOVIA-MT.

3. Referências

Para a elaboração do presente documento, foram consideradas as seguintes referências:

- Norma Técnica ABNT NBR ISO/IEC 17799;
- Norma Técnica ABNT NBR ISO/IEC 27001:2005;
- Norma IEEE Standard 802.11x, que normatiza a comunicação em rede local sem fio WLAN;
- Decreto Nº 316/99, de 08 de julho de 1999, que institui a INFOVIA-MT;
- Política de Segurança da Informação para a Rede INFOVIA-MT;
- Política de Uso Aceitável para a Rede INFOVIA-MT.

4. Definições

Além dos conceitos apresentados a seguir, alguns termos, definições e conceitos essenciais à compreensão desta política encontram-se no documento denominado "Termos, Definições e Conceitos referentes à INFOVIA-MT".

4.1. Redes sem fio Wireless Fidelity

Wireless Fidelity ou Wi-Fi, é um padrão de Wireless LAN desenvolvido pelo The Institute of Electrical and Electronics Engineers, Inc. – IEEE sob o código de padrão da família **Erro! A referência de hyperlink não é válida.**. O padrão IEEE **Erro! A referência de hyperlink não é válida.** define as camadas Física e Link de dados (media access control (MAC) sublayer).

4.1.1. Rádio-freqüência:

Normatizada pelo IEEE, nos grupos do comitê 802, especificamente:

- 802.11 – Normatiza a comunicação em rede local sem fio WLAN;
- 802.15 – Redes locais pessoais WPAN e sua interoperabilidade com WLAN;
- 802.16 – Redes metropolitanas de acesso sem fio WMAN;
- 802.20 – Redes de acesso sem fio com usuários móveis – proposta.

4.1.2. Principais Padrões do IEEE 802.11:

Na família IEEE 802.11 temos os principais padrões:

- IEEE 802.11 a: Padrão WI-FI para freqüência 5Ghz com capacidade teórica de 24Mbps;
- IEEE 802.11 b: Padrão WI-FI para freqüência 2,4 Ghz com capacidade teórica de 11Mbps; Este padrão utiliza o recurso denominado DSSS (Direct Sequency Spread Spectrum – Seqüência Direta de Espalhamento de Espectro) para diminuição de interferência;
- IEEE 802.11 g: Padrão WI-FI para freqüência 2,4 Ghz com capacidade teórica de 54Mbps; Alguns fabricantes já disponibilizam a capacidade de 108 Mbps;
- IEEE 802.11 i: Wi-Fi Protected Access (WPA e WPA 2) padrão de segurança instituído para substituir padrão WEP (Wired Equivalent Privacy) na qual possuía falhas graves de segurança, possibilitando que um hacker pudesse quebrar a chave de criptografia após monitorar algumas horas de comunicação.

4.1.3. Tipos de Rede Wireless

As redes sem fio (*Wireless*), também conhecidas como IEEE 802.11, Wi-Fi ou WLANs, são redes que utilizam sinais de rádio para a sua comunicação.

Este tipo de rede define duas formas de comunicação:

- modo infraestrutura: normalmente o mais encontrado, utiliza um concentrador de acesso (*Access Point* ou AP);
- modo ponto a ponto (*ad-hoc*): permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP.

5. Recomendações

As recomendações apresentadas a seguir descrevem procedimentos buscando garantir a autenticação, autorização e confidencialidade dos dados numa comunicação no contexto de redes Wi-Fi. Essas medidas podem ser resumidas através das seguintes recomendações de caráter geral:

- Implementar mecanismos de autenticação de usuário;
- Implementar gerenciamento centralizado de senhas, grupos e políticas de acesso.;
- Implementação de chaves de cifragem dinâmicas, baseadas na sessão;
- Implementar a autenticação mútua entre a base e o dispositivo de acesso. Isto significa que a base autentica o usuário e este autentica a base;
- Varredura (scanning) regular da rede pelos administradores em busca de dispositivos não autorizados.

5.1. Recomendações aos Administradores de Redes

Por administrador de um serviço móvel entende-se a pessoa e/ou equipe que é responsável, em seu órgão, pela instalação e configuração do equipamento de acesso, ao qual está conectada uma base de acesso Wi-Fi (AP - *Access Point*), pela configuração do AP, pelo estabelecimento e divulgação de políticas de controle de acesso entre os usuários de serviços móveis e pela distribuição física dos AP no local de uso.

Os administradores devem verificar regularmente a observância das instruções anteriormente recomendadas.

Os administradores devem notificar os casos que estejam em desacordo com a Política de Segurança da Informação da organização ou da Rede INFOVIA-MT.

Os administradores não devem disponibilizar dados de uma pessoa, por exemplo, de que possui acesso móvel ou sem fio configurado em sua sub-rede, sem o prévio consentimento desta.

5.2. Recomendações ao Usuário

Embora esse tipo de rede, Wi-Fi, seja muito conveniente, existem alguns problemas de segurança que devem ser levados em consideração pelos seus usuários:

- Estas redes utilizam sinais de rádio para a comunicação e qualquer pessoa com um mínimo de equipamento poderá interceptar os dados transmitidos por um cliente da rede sem fio (como *notebooks*, PDAs, estações de trabalho, celular, etc);
- O usuário não deve emprestar dispositivos pessoais móveis;
- O usuário não deve divulgar dados de configuração para acesso em redes sem fio a terceiros;
- Se um dispositivo for de uso coletivo (ex: laptop, notebook, PDA, etc), a lista com os usuários (cadastro) desse dispositivo deverá ser fornecida ao administrador da rede local e o responsável pelo dispositivo deverá manter um controle de quem está utilizando o dispositivo, podendo vir a ser requisitado a respeito;
- O usuário não deve configurar sistemas móveis de sua responsabilidade com informações pessoais ou trechos combinados destas.

5.3. Recomendações aplicáveis à WLAN

Vários cuidados devem ser observados quando se pretende conectar à uma rede sem fio como cliente, seja com *notebooks*, PDAs, estações de trabalho, etc. Portanto, recomenda-se:

- Instalar um *firewall* pessoal no dispositivo de acesso;
- Instalar e manter atualizado um bom programa antivírus;
- Atualizar as assinaturas do antivírus diariamente;
- Aplicar as últimas correções em seus *softwares* (sistema operacional, programas que utiliza, etc.);
- Desativar o compartilhamento desnecessário de disco, impressora, etc.;
- Desabilitar o modo *ad-hoc*. Utilize esse modo apenas se for absolutamente necessário e desligue-o assim que não precisar mais;
- Sempre que possível usar no mínimo o recurso de WEP (*Wired Equivalent Privacy*), que permite criptografar o tráfego entre o cliente e o AP. O administrador de rede deve procurar verificar se o WEP está habilitado e se a chave é diferente daquelas que acompanham a configuração padrão do equipamento. É importante ressaltar que o protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada, e utilizado apenas se os APS – Access Points disponíveis não possuírem o recurso de WPA;
- Verificar com seu administrador de rede sem fio sobre a possibilidade de usar WPA (Wi-Fi *Protected Access*) em substituição ao WEP, uma vez que este padrão pode aumentar significativamente a segurança da rede. Esta tecnologia inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário. Mesmo que seu equipamento seja mais antigo, é possível que exista uma atualização para permitir o uso de WPA;
- Considerar o uso de criptografia nas aplicações, como por exemplo, o uso de PGP para o envio de *e-mails*, SSH para conexões remotas ou ainda o uso de VPNs;
- Evitar o acesso a serviços que não utilizem conexão segura, por exemplo, se for necessário ler *e-mails* ou acessar a Intranet de sua organização, dê preferência a serviços que usem criptografia;
- No caso de redes Wireless de utilizações provisórias, habilitar a rede sem fio somente quando for usá-la e desabilitá-la após o uso. Algumas estações de trabalho e *notebooks* permitem habilitar e desabilitar o uso de redes sem fio através de comandos ou botões específicos;
- No caso de *notebooks* com cartões PCMCIA, permita a utilização apenas de cartões cadastrados.

5.4. Recomendações Aplicáveis a configuração de APs (Acess Points):

- Modificar as configurações padrões que acompanham o seu AP, por exemplo: o usuário administrador, senha, o grupo (*Server Set ID* – SSID), etc.. Devem-se observar as políticas de Identificação de Usuários e Senhas adotada na Política de Segurança da organização.
- Alterar o SSID (*Server Set ID*), buscando não utilizar um SSID que reflita as características da empresa (nome, endereço ou produtos);
- A administração de SSIDs utilizadas na implementação da rede Wireless deve ser controlada de modo centralizado e estes devem ser alteradas periodicamente;
- Desabilitar o *broadcast* de SSID no AP (se o ponto de acesso implementar essa característica);
- Utilizar APs onde é possível estabelecer uma lista de controle de acesso baseada em endereços MAC dos dispositivos de acesso da rede Wi-Fi. Se isso não for possível, recomenda-se implementar esse controle através de uma VLAN por MAC address, desde que o switch de acesso implemente essa característica;
- Verificar se seus equipamentos já suportam WPA (Wi-Fi *Protected Access*) e utilizá-lo sempre que possível. Esta tecnologia é mais recente e inclui melhorias em relação ao protocolo WEP para prover uma segurança adicional contra acesso e escuta de tráfego não autorizado. Lembre-se que atualizações para WPA estão disponíveis para a maior parte dos equipamentos mais antigos;
- Caso o WPA não esteja disponível, usar sempre que possível WEP (*Wired Equivalent Privacy*), para criptografar o tráfego entre os clientes e o AP. Vale lembrar que o protocolo WEP possui diversas fragilidades e deve ser encarado como uma camada adicional para evitar a escuta não autorizada;
- Se for utilizar WEP, trocar as chaves que acompanham a configuração padrão do equipamento. Procure usar o maior tamanho de chave possível (128 bits);
- A administração das chaves utilizadas na implementação dos protocolos de criptográfica deve ser controlada de modo centralizado e estas devem ser alteradas periodicamente;
- Colocar a rede Wireless em um subrede separada, de preferência em uma VLAN;
- Desligar seu AP quando não estiver usando sua rede;
- Se possível utilize um servidor RADIUS com a identificação do usuário, para autenticação;
- Realizar verificações regulares de análise de vulnerabilidades em determinados componentes de rede (APs - *Access Points*). O objetivo destas ferramentas é encontrar brechas de sistemas ou configurações;
- Para definição da área de cobertura, posicionar os pontos de acesso mais para o centro do prédio e menos nas proximidades das janelas, onde a energia irradiada poderá ser captada por quem estiver do lado de fora, pelo uso de uma antena direcional;
- Utilizar, quando possível, pontos de acesso com firmware em memória flash, que permitirão a sua atualização com a evolução dos padrões de segurança;
- Não utilizar DHCP do AP, quando possível, onde os dispositivos de acesso estão conectados. Preferir endereçamento estático, com o intuito de maior controle;
- Quando necessário e possível, aumentar a o nível de segurança com a implementação de túnel como IPSec;
- Pesquisar periodicamente a existência de bases não autorizadas (clandestinas) nas áreas de cobertura de interesse;
- Ao alocar as bases na rede corporativa, investigar o quanto um sinal de dentro do prédio pode ser captado pelo lado de fora, pelo uso de uma antena de alto ganho e software de captura apropriado.

6. Disposições finais

Outros itens referentes ao uso, administração e gerenciamento das redes locais sem fio não abordados neste documento ou em outros em vigor no Governo do Estado de Mato Grosso, deverão ser levados à Câmara Gerencial de Informação e Tecnologia da Informação – CGITI para estudo, proposição de soluções e providências.

Governo do Estado de Mato Grosso
Secretaria de Estado de Planejamento e Coordenação Geral
Conselho Superior do Sistema Estadual de Informação e Tecnologia da Informação

RESOLUÇÃO Nº. 004/2007

Dispõe sobre o Sistema de Proteção, firewall de perímetro, em seu ambiente de rede no âmbito do Estado de Mato Grosso.

O CONSELHO SUPERIOR DO SISTEMA ESTADUAL DE INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO, no uso das competências que lhe são conferidas pela Lei Nº 8.199 de 11 de novembro de 2004 e regulamentadas pelo Decreto Nº 6.300 de 31 de agosto de 2005;

CONSIDERANDO o Decreto Estadual nº 316/99 de 15 de setembro de 1999;

CONSIDERANDO a necessidade de normatização do sistema de proteção, firewall de perímetro no ambiente de rede no Estado de Mato Grosso;

RESOLVE:

Art.1º - Apresentar as "normas para o uso do sistema de proteção Firewall" com suas características e necessidades.

Art.2º - Determinar que todos os Órgãos participantes da Rede Infovia façam uso do sistema de proteção.

Art.3º- Esta Resolução entrará em vigor na data de sua publicação.

CUMPRA-SE

Conselho Superior do Sistema Estadual de Informação e Tecnologia da Informação, em 04 de abril de 2007.

(Original Assinado)
YÊNES JESUS DE MAGALHÃES
Presidente do Conselho e
Secretário de Estado de Planejamento e Coordenação Geral

(Original Assinado)
WALDIR JÚLIO TEIS
Secretário de Estado de Fazenda
Membro do Conselho

(Original Assinado)
SÍRIO PINHEIRO DA SILVA
Auditor Geral do Estado
Membro do Conselho

(Original Assinado)
GERALDO A DE VITTO JUNIOR
Secretário de Estado de Administração
Membro do Conselho

(Original Assinado)
JOÃO VIRGILIO DO N SOBRINHO
Procurador Geral do Estado
Membro do Conselho

(Original Assinado)
ADRIANO NIEHUES
Diretor Presidente do CEPROMAT
Membro do Conselho

ANEXO I RESOLUÇÃO N. 004/2007

NORMAS PARA O USO DE SISTEMA DE PROTEÇÃO – *FIREWALL DE PERÍMETRO* – NO ÂMBITO DA REDE INFOVIA-MT

1. Objetivo

Este documento visa estabelecer normas para o uso de sistema de proteção – firewall de perímetro, no âmbito da Rede Infovia-MT em conformidade com as normas e melhores práticas de segurança