- 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

da informação e regras estabelecidas pelo Conselho Superior de Informação e da Tecnologia da Informação – COSINT no Estado de Mato Grosso.

2. Público-alvo

Esta norma aplica-se a todas as entidades do Governo do Estão de Mato Grosso, que estejam interligadas à Rede Infovia-MT ou que queiram fazer uso da mesma.

3. Referências

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

- Norma Técnica ABNT NBR ISO/IEC 17799;
- Norma Técnica ABNT NBT ISO/IEC 27001:2005;
- 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 norma encontram-se na Internet na página do Centro de Processamento de Dados do Estado de Mato Grosso – CEPROMAT (www.cepromat.mt.gov.br).

5. Características Técnicas

5.1 São características padrões do sistema de segurança – *Firewall de Perímetro*:

5.1.1 Deve suportar uma política de configuração do tipo "***negar todos os serviços, exceto aqueles expressamente permitidos***", mesmo que esta não seja a política usada;

5.1.2 Deve ser flexível; de modo a acomodar novos serviços e necessidades se a política de segurança da organização sofrer alterações;

5.1.3 Deve conter medidas de autenticação avançadas ou os hooks para instalação dessas medidas;

5.1.4 Deve usar técnicas de filtragem que permitam ou neguem serviços para hosts e/ou redes específicas e/ou protocolos, conforme necessário;

5.1.5 A linguagem de filtragem de IP deve ser flexível, de programação amigável e deve filtrar tantos atributos quanto possível, inclusive endereço IP de origem e de destino, tipo de protocolo, porta TCP/UDP de origem e de destino, e interface interna e externa;

5.1.6 Deve suportar Proxy para serviços como FTP e TELNET, de forma que possam ser empregadas e centralizadas no firewall as medidas de autenticação avançadas. Se forem necessários serviços como NTP, HTTP ou Gopher, o firewall deve conter os serviços Proxy correspondentes;

5.1.7 Deve suportar a capacidade de centralizar acesso SMTP para reduzir conexões diretas SMTP entre os sistemas de site e remoto. Isto resulta em processamento centralizado de e-mail de site;

5.1.8 Deve acomodar o acesso público ao site, de maneira que os servidores públicos de informações possam ser protegidos pelo Sistema de Firewall, mas sejam separados de sistemas de site que não exijam acesso público;

5.1.9 Deve conter mecanismos de registro de tráfego e atividades suspeitas, além de mecanismos para redução de registros de forma que os registros sejam legíveis e compreensíveis;

5.1.10 O Sistema de Firewall e/ou qualquer sistema operacional correspondente devem ser atualizados com correções e outros concertos de bugs, conforme necessário.

5.2 As seguintes características para segurança de acesso lógico devem ser implementadas sempre que tecnicamente disponíveis no sistema de firewall de perímetro:

5.2.1 As contas administrativas do Sistema de Firewall devem ter senhas de difícil dedução (senhas fortes);

5.2.2 O monitoramento e gerenciamento do Sistema de Firewall através do protocolo SNMP devem ser evitados. Caso haja necessidade de utilização deste protocolo, os seguintes requisitos devem ser atendidos:

5.2.2.1 A versão do SNMP utilizada deve ser, no mínimo, a 2.x;

5.2.2.2 A comunidade de leitura deve ter um nome de difícil dedução;

5.2.2.3 A comunidade de escrita deve ser desabilitada;

5.2.2.4 Informações de gerenciamento SNMP devem ser fornecidas apenas aos hosts cadastrados;

5.2.3 Um limite para tentativas de autenticação mal sucedidas deve ser implementado no Sistema de Firewall, a fim de evitar ataques de força bruta;

5.2.4 As falhas de autenticação de usuários devem ser registradas e seus registros devem ser verificados periodicamente de forma pró-ativa;

5.2.5 As autenticações bem sucedidas dos usuários com direito de acesso à console de gerenciamento do Sistema de Firewall devem ser registradas e seus registros devem ser verificados periodicamente de forma pró-ativa;

5.2.6 O gerenciamento remoto do Sistema de Firewall deve ser permitido apenas a partir de estações autorizadas, a fim de evitar que *hosts* não permitidos conectem-se à console do Sistema de Firewall para tentativas de acesso indevido;

5.2.7 A senha de administração do Sistema de Firewall deve ser diferente da senha de autenticação utilizada no equipamento de gerência onde a console está instalada;

5.2.8 Os direitos e permissões de acesso ao equipamento do Sistema de Firewall devem ser regularmente revistos e atualizados;

5.2.9 O Sistema de Firewall deve estar logicamente localizado entre duas ou mais redes que devem ser protegidas de acessos indevidos e que necessitem que seu fluxo de dados seja controlado;

5.2.10 A primeira regra para controle de acesso a ser criada deve bloquear toda comunicação destinada ao equipamento do Sistema de Firewall, permitindo apenas que a máquina de gerência cadastrada possa estabelecer uma conexão com o mesmo;

5.2.11 O Sistema de Firewall deve ser instalado em um equipamento servidor dedicado e com sua capacidade de hardware monitorada constantemente;

5.2.12 Que o número de regras criadas no Sistema de Firewall seja inferior a 100 (cem), a fim de evitar que o fluxo de dados declarados nas regras fique confuso;

5.2.13 Que a data e hora do sistema onde o Firewall está instalado seja sincronizada com outros dispositivos de proteção da rede (roteadores, sistemas de IDS, etc) através do protocolo NTP;

5.2.14 Que a data e hora de outros equipamentos sincronizados com o Sistema de Firewall sejam monitoradas constantemente, a fim de manter a compatibilidade entre os mesmos;

5.2.15 O envio de alertas no caso de eventos de segurança que requerem ação imediata deve ser configurado no Sistema de Firewall;

5.2.16 As regras do Sistema de Firewall devem ser configuradas de forma a registrar os eventos relevantes para a segurança, garantindo assim a rastreabilidade dos incidentes quando os mesmos ocorrerem;

5.2.17 Todas as regras no Sistema de Firewall devem possuir uma breve descrição de sua funcionalidade e quem foi o criador das mesmas;

5.2.18 Que a comunicação entre o módulo do Sistema de Firewall e o servidor de autenticação onde são mantidas as informações de usuários seja criptografada com chaves de no mínimo 128bits;

5.2.19 Recomenda-se que o recurso "*Anti-Spoofing*" deve ser habilitado nas interfaces de rede do Sistema de Firewall, a fim de evitar que ataques externos utilizem do recurso de falsificação de endereços para criar incidentes de segurança;

5.2.20 O Sistema de Firewall deve ser configurado de forma a amenizar ataques do tipo "*Syn Flood*", para manter a disponibilidade dos sistemas ou evitar a exploração de vulnerabilidades que utilizam este recurso;

5.2.21 Os *patchs* de segurança do Sistema de Firewall devem estar atualizados, conforme recomendação do fabricante;

5.2.22 Os *patchs* de segurança do Sistema de Firewall devem ser homologados em um ambiente de teste antes de serem disponibilizados em produção.

5.3 São características para segurança de acesso físico:

5.3.1 O acesso físico ao Sistema de Firewall deve ser permitido apenas para usuários autorizados e devidamente identificados;

5.3.2 O Sistema de Firewall deve estar fisicamente protegido contra ameaças à sua segurança (ex. incêndio, enchente, arrombamento e etc.);

5.3.3 O ambiente em que se encontra o Sistema de Firewall deve conter controles de temperatura e umidade, a fim de evitar um dano físico à máquina onde o Sistema de Firewall se encontra instalado.

5.4 São requisitos padrões dos órgãos usuários da INFOVIA-MT que possua sistema de proteção – *firewall de perímetro*:

5.4.1 O órgão deve possuir profissional certificado no produto, o qual realizará a instalação, configurações, implantação de políticas de segurança e testes de vulnerabilidade; ou ainda podendo terceirizar este serviço;

5.4.2 A certificação que trata o item anterior, deve ser a oficial e obtida junto ao fabricante do Sistema de Firewall em centro de treinamento/certificação devidamente homologado pelo fabricante do Sistema de Firewall;

5.4.3 O órgão deve implementar mecanismo que permita estabelecer base de regras que defina quais máquinas da sua Intranet acessam quais endereços da INFOVIA-MT e vice-versa;

5.4.4 O órgão deve se submeter a testes de análise de vulnerabilidade e comprovação que a política adotada é segura, após implantação da política de segurança do sistema de proteção – firewall de perímetro, a serem conduzidos pela administração da INFOVIA-MT. E em caso de alguma vulnerabilidade ser verificada, o órgão deverá efetuar correções, de forma a eliminar a vulnerabilidade;

5.4.5 A política de segurança do sistema de proteção – firewall de perímetro da INFOVIA-MT deverá ser implantada em conjunto com a equipe técnica de administração da INFOVIA-MT e equipe da técnica do órgão;

5.4.6 Fica a critério do Órgão a escolha do Sistema de Firewall para a sua Intranet, seguindo as normas acima citadas, possibilitando assim a integração com o Sistema de Central Firewall da INFOVIA-MT;

5.5 O Sistema de Firewall Central deve contemplar as seguintes características e necessidades:

5.5.1 É baseado em roteamento, totalmente aberto, e não requer mudanças de software em sistemas clientes;

5.5.2 Permite ou nega acesso às redes conectadas, baseado em autentificação dos usuários, autentificação do cliente e autentificação de sessão.

5.5.3 Suporta os seguintes padrões: Telnet, HTTP, POP, NNTP, SMTP, Gopher.

5.5.4 Suporta aplicações multimídia.

5.5.5 Suportar conexões VPN.

5.5.6 Capaz de fornecer um acesso seguro aos serviços disponíveis na Internet, evitando conexões não autorizadas à mesma.

5.5.7 Suporta servidores de autentificação.

5.5.8 Permite tradução de endereços (NAT) de redes privadas conforme RFC 1597, em endereços de Internet válidos.

5.5.9 Suporta esquema de criptografia manual IPSEC, algoritmos de criptografia tipo DES e algoritmos de autentificação tipo MD5 e Secure ID.

5.5.10 Possui algoritmos de criptografia FWZ-1 e RC4.

5.5.11 Suporta algoritmos de autentificação SHA-1, 3-DES e CBC DES.

5.5.12 Implementa mecanismo "anti-spoofing".

5.5.13 Grava em arquivo LOG, o registro, com data e hora e verificação de todos os eventos relativos ao tráfego monitorado, em particular às tentativas de violação da política de segurança estabelecida.

5.5.14 Gera a partir do LOG, arquivo que possa ser lido por qualquer software de geração de relatórios.
5.5.15 Suporta os seguintes sistemas operacionais: Solaris, Família Windows, HP - UX / AIX, Linux.
5.5.16 Implementa filtros de segurança para a aplicação de FTP, de modo que seja possível autenticar o usuário.
5.5.17 Efetua controle bidirecional de Correio Eletrônico.
5.5.18 Permite bloqueio e/ou controle de applets JAVA e de objeto ACTIVEX.
5.5.19 Disponibiliza interface gráfica para auditoria, com dados históricos do arquivo de LOG de toda tentativa de comunicação e de conexão válida.
5.5.20 Possui interface para customização e mecanismo de criação de serviços TCP/IP.
5.5.21 Disponibiliza mecanismo que envia mensagens de notificação para o administrador, a cada tentativa de acesso não autorizado.
5.5.22 Permite a implantação de filtros de tráfego, baseados em endereço IP de origem ou de destino.
5.5.23 Suporta módulo de criptografia que permite criptografia Firewall-Firewall, e cliente Firewall.
5.5.24 É uma plataforma aberta possibilitando integração com produtos de segurança de outros fabricantes.
5.5.25 Dispõe de interface gráfica para a implementação da política de segurança.
5.5.26 Suporta as seguintes topologias de Rede: Ethernet, Fast-Ethernet, FDDI, Token Ring, ISDN, GIGABIT e ATM.
5.5.27 Suporta topologia T1 e T3.
5.5.28 Suporta protocolos UDP e ICMP.

6. Disposições finais

Outros itens referentes ao uso, administração e gerenciamento de sistema de proteção – *firewall de perímetro* – 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. 005/2007

Dispõe sobre a instituição dos Padrões para elaboração de Propostas, Projetos e Planos de Projetos de Tecnologia da Informação de Tecnologia, no âmbito do Poder Executivo 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 padronizar as normas para elaboração de Propostas e Planos de Projetos de Tecnologia da Informação a Administração Pública Estadual;

RESOLVE:

Art. 1º - Determinar que sejam obedecidos os procedimentos constantes nos Anexos I e II da presente Resolução.

Art. 2º - Esta Resolução entra em vigor na data 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. 005/2007

PROPOSTA DE PROJETO DE TECNOLOGIA DA INFORMAÇÃO

1. Informações Gerais do Projeto
1.1 Identificação
1.2 Meta proposta para o projeto
1.3 Informações do Responsável pela Proposta
1.4 Período de Execução Estimado
2. Proposta do Projeto
2.1 Definições, termos e siglas
2.2 Justificativa do Projeto
2.3 Objetivos do Projeto
2.4 Benefícios
2.5 Fatores críticos de sucesso
2.6 Aderência ao Plano Estratégico
2.7 Alternativas Estudadas e Solução Escolhida
2.8 Produto(s) do Projeto
2.9 Estrutura de Decomposição do(s) Produtos(s) do Projeto
2.10 Intervenientes
2.10.1 Beneficiário Alvo
2.10.2 Instituição que Abrigará as Ações do Projeto
2.10.3 Outras Instituições Envolvidas
2.11 Orçamento Preliminar
2.12 Cronograma Estimado
2.13 Comentários Finais
ANEXOS
I. Plano de Ação
II. Nome do Anexo II

ANEXO II RESOLUÇÃO N. 005/2007

PLANO DE PROJETO

1. Aprovação do Plano do Projeto
Identificação do Projeto
Informações do Responsável pelo Plano do Projeto
Breve Descrição do Projeto
Execução do Projeto
Recursos Alocados para o Projeto
Avaliação
Histórico de Revisões
2. Plano do Projeto
1.1 Visão Geral do Projeto
Definições, termos e siglas
Contextualização
Situação atual e necessidades a serem resolvidas pelo Projeto
Objetivo Geral
Justificativa do Projeto
Cooperação Técnica Externa Anterior ou em Andamento
2.2 Escopo do Projeto
Objetivos Específicos
Situação Esperada ao Final do Projeto
Beneficiário Alvo
Justificativa da Solução Escolhida e Procedimentos para Execução
Razões para Cooperação Técnica Externa
Estratégias do Projeto
Entregas do Projeto
Indicadores do Projeto
Contrapartida do Governo para Executar o Projeto
Gerenciamento do escopo
2.3 Organização do Projeto
Estrutura Organizacional
Matriz de Responsabilidade
2.4 Cronogramas
2.5 Orçamentos
2.6 Comunicação
2.7 Recursos Humanos
2.8 Aquisições
2.9 Riscos
2.10 Qualidade
2.11 Obrigações Prévias
2.12 Contexto Legal
2.13 Avaliação do Projeto
2.14 Considerações Adicionais
ANEXOS

MT FOMENTO

AGENCIA DE FOMENTO DO ESTADO DE MATO GROSSO S/A

EXTRATO DE TERMO DE ADESÃO

Interessada:	AGÊNCIA DE FOMENTO DO ESTADO DE MATO GROSSO S/A, ADERE ao Convênio Nº. 011/2005, firmado em 20/04/2005, entre o Estado de Mato Grosso e o Centro de Integração Empresa Escola – CIEE.				
CNPJ	**Nº. 06.284.531/0001-30**	**Inscrição Estadual**	**Isento**	**Substituto Tributário**	**CM 86257**
Instituição	CENTRO DE INTEGRAÇÃO EMPRESA ESCOLA – CIEE.				
CNPJ	**Nº. 61.600.839/0001-55**				
Objeto	O presente CONVÊNIO tem por objeto, a concessão de oportunidades de estágios ao corpo discente de ensino superior, de ensino médio, de educação profissional de nível médio ou superior ou escolas de educação especial, de diversas instituições de ensino, por intermédio do CONVENENTE, na condição de Agente de Integração.				
Prazo	Até 31 de março/2008.				
Fundamento Legal	Tendo em vista o disposto na Lei nº. 6.494, de 07 de dezembro de 1977, no Decreto nº. 87.497, de 18 de agosto de 1982, na Portaria nº. 8, de 23 de janeiro de 2001, do Ministério de Estado do Planejamento, Orçamento e Gestão, e observando, no que couber, a Lei nº. 8666, de 21 de junho de 1993 e no Decreto Estadual nº. 3.126, de 18 de maio de 2004.				
Assinam	Senhor **Éder de Moraes Dias** – Diretor Presidente da Agência de Fomento do Estado de Mato Grosso S.A – MT FOMENTO e o Senhor **Cláudio Rodrigo de Oliveira –** Gerente Regional do Centro de Integração Empresa Escola – CIEE.				

ÉDER DE MORAES DIAS
Diretor Presidente da MT FOMENTO

EVENTOS DE PESSOAL

SECRETARIAS

PROCURADORIA GERAL DO ESTADO

PORTARIA N. 03/PGE/00056/2007 DE: 14/06/2007

O Procurador Geral do Estado
no uso de suas atribuicoes que lhes sao conferidas por lei,
Resolve: DEFERIR
Evento: 110000/1104 - LICENCA PARA TRATAMENTO DE SAUDE
Processo Numr.: 112406/2007