



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

ANEXO **x** - RESOLUÇÃO N°.xxx/2010

GOVERNO DO ESTADO DE MATO GROSSO

**Norma de Segurança Estadual
para
Uso da Internet**

PLUSQUAM



Governo do Estado de Mato Grosso

Conselho Superior do Sistema Estadual de Informação e Tecnologia da informação – COSINT
Norma de Segurança Estadual para Uso da Internet

ANEXO I – RESOLUÇÃO 010/2011

Norma de Segurança Estadual para uso da Internet

PROPOSTA

SETEMBRO / 2011



Governo do Estado de Mato Grosso

Conselho Superior do Sistema Estadual de Informação e Tecnologia da informação – COSINT
Norma de Segurança Estadual para Uso da Internet

FRANCISCO TARQUINIO DALTRO
Presidente do Conselho e
Vice Governador do Estado de Mato Grosso

JOSÉ GONÇALVES BOTELHO DO PRADO
Membro do Conselho e
Secretário de Estado de Planejamento e Coordenação Geral

EDMILSON JOSÉ DOS SANTOS
Membro do Conselho
Secretário de Estado de Fazenda

JOSÉ ALVES PEREIRA FILHO
Membro do Conselho
Auditor Geral do Estado

CESAR ROBERTO ZILIO
Membro do Conselho
Secretário de Estado de Administração

WILSON CELSO TEIXEIRA
Membro do Conselho
Diretor Presidente do CEPROMAT

PROPOSTA

ÍNDICE

1.	INTRODUÇÃO.....	5
2.	OBJETIVOS.....	5
3.	REFERÊNCIAS.....	5
4.	DEFINIÇÕES.....	5



Governo do Estado de Mato Grosso

Conselho Superior do Sistema Estadual de Informação e Tecnologia da informação – COSINT
Norma de Segurança Estadual para Uso da Internet

5.	DISPOSIÇÕES GERAIS	6
5.1.	DISPONIBILIZAÇÃO DE ACESSOS	6
5.2.	RESTRICÇÕES DE ACESSO.....	7
5.3.	INFORMAÇÕES.....	8
5.4.	MONITORAMENTO / AUDITORIA.....	8
5.5.	RECURSOS TECNOLÓGICOS	8
6.	DISPOSIÇÕES FINAIS	8

PROPOSTA

1. Introdução

Esta norma faz parte dos instrumentos normativos de Segurança da Informação das entidades governamentais do Poder Executivo do Estado de Mato Grosso. Neste documento constam orientações e regras de conduta que devem ser observados por todas as entidades governamentais e seus agentes públicos e prestadores de serviço, de forma a garantir o uso responsável da Internet através dos recursos disponibilizados pela Administração Pública do Poder Executivo Estadual.

2. Objetivos

Estabelecer normas aplicáveis aos agentes públicos e prestadores de serviço, aqui denominados de usuários, quando utilizando recursos da Administração Pública no âmbito do Poder Executivo Estadual para acesso à rede mundial de computadores – Internet.

3. Referências

- Políticas e Diretrizes de Segurança da Informação Estadual
- NBR/ISO/IEC 27001:2005 de 30/04/2006 - Código de prática para gestão da segurança da informação.
- Decreto Lei 3.505, de 13/06/00 que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Decreto Lei 4.553, de 27/12/2002 que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.
- Políticas e Diretrizes do SEITI.
- Norma de Segurança da Informação para uso de Internet - SEFAZ/MT.

4. Definições

- **Agente Público:** Toda e qualquer pessoa que exerce uma atribuição pública em sentido lato, seja estagiário, ocupante de função, cargo ou de emprego público.
- **Autenticação:** Verificação da identidade de um usuário, de um dispositivo, ou de outra entidade em um sistema computadorizado, freqüentemente como um pré-requisito a permitir o acesso aos recursos em um sistema.
- **Browser:** um navegador, também conhecido pelos termos ingleses web browser ou simplesmente browser, é um programa de computador que habilita seus usuários a interagirem com documentos virtuais da Internet, também conhecidos

como páginas HTML, que estão hospedadas num servidor Web. Exemplos de browser.: Internet Explorer, Mozilla Firefox, Opera, Safari e Chrome.

- **Código Malicioso:** Também conhecido por *malware*, é um programa desenvolvido especificamente para executar ações danosas em um computador.
- **Download:** (significa descarregar ou baixar, em português) é a transferência de dados de um computador remoto para um computador local.
- **Entidade Governamental:** Incluem-se entre as entidades governamentais do poder executivo, para fins deste documento, as agências, auditorias, autarquias, empresas, federações, fundações, governadoria, procuradorias, secretarias e unidades desconcentradas.
- **Internet:** é a rede mundial de computadores interconectados. A Internet é um conglomerado de redes em escala mundial de milhões de computadores interligados pelo Protocolo de Internet que permite o acesso a informações e todo tipo de transferência de dados.
- **MP3:** é uma abreviação de MPEG-1 Audio Layer 3 e é um formato de áudio digital codificado.
- **Página web:** também conhecida pelo equivalente inglês webpage, é uma "página" na *world wide web*, geralmente em formato HTML e com ligações de hipertexto que permitem a navegação de uma página, ou secção, para outra.
- **Recurso:** além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento.
- **Upload:** é a transferência de dados de um computador local para um servidor. Caso ambos estejam em rede, pode-se usar um servidor de FTP, HTTP ou qualquer outro protocolo que permita a transferência. É parecido com Download, só que em vez de carregar arquivos para a sua máquina, você os envia para o servidor.
- **Usuário:** quem utiliza de forma autorizada recursos de informação da Administração Pública no âmbito do Poder Executivo do Estado de Mato Grosso.
- **Vírus:** É um programa ou parte de um programa, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos do computador.

5. Disposições Gerais

5.1. Disponibilização de Acessos

- 5.1.1. O acesso à Internet será provido aos usuários que necessitem desse recurso para o desempenho de suas funções.

- 5.1.2. Convém que a entidade governamental que disponibiliza o acesso à Internet implemente um sistema de identificação e autenticação única e inequívoca dos usuários.
- 5.1.3. Para ter acesso à Internet o usuário deve receber orientações quanto ao uso correto desse recurso para assegurar que todos estão cientes das implicações referentes à segurança.
- 5.1.4. O acesso à rede interna ou Intranet, via Internet, deve ser autenticado e criptografado.

5.2. Restrições de Acesso

- 5.2.1. É expressamente proibido utilizar a Internet de forma que possa prejudicar a imagem da Administração Pública ou de quaisquer de suas entidades, ou que prejudique o andamento dos trabalhos destas, ou que coloque em risco os ativos da rede de computadores da entidade governamental ou estadual (Infovia-MT), ou ainda nas seguintes situações, dentre outras:
 - 5.2.1.1. páginas de bate-papo, comunidades de discussão, sites de relacionamento e similares sem autorização e fora dos interesses da Administração Pública;
 - 5.2.1.2. criação de comércio eletrônico fora dos interesses da Administração Pública;
 - 5.2.1.3. acesso a sites fora dos interesses da Administração Pública, principalmente os de conteúdo pornográfico, racista, pedófilo, que façam apologia ao uso de drogas etc.;
 - 5.2.1.4. download de programas, jogos, protetores de telas, música, vídeos, imagens, streaming de vídeo e de áudio, torrent, p2p etc;
 - 5.2.1.5. participação em jogos.
- 5.2.2. As situações descritas no item anterior são consideradas legais **se e somente se** o usuário estiver no cumprimento de suas atribuições profissionais legítimas e de interesse da administração pública estadual.
- 5.2.3. **Cabe às entidades governamentais disciplinar o uso da Internet em outras situações não previstas neste documento, desde que não fira o que estabelece o item 5.2.1.**
- 5.2.4. No caso de *download* de interesse comum a várias áreas, convém que este seja realizado pela área responsável pela tecnologia da informação e disponibilizado aos interessados.
- 5.2.5. Somente os usuários devidamente autorizados e em conformidade com suas atribuições funcionais podem fazer *downloads*, seguindo os procedimentos de segurança adotados pela entidade governamental da Administração Pública.

5.2.6. Os usuários que estiverem acessando a Internet devem encerrar sua conexão após término da navegação e bloquear a estação de trabalho sempre que se afastarem dela temporariamente, a fim de evitar que um usuário execute acessos em nome de outro.

5.3. Informações

5.3.1. Toda informação originada na Internet deve ser considerada suspeita até que seja confirmada por outros meios.

5.3.2. Antes de usar qualquer programa que tenha sido copiado da Internet, este deve ser testado e homologado pela área responsável em um equipamento preparado e isolado da rede da entidade governamental.

5.3.3. Antes de baixar (download) arquivos de qualquer natureza, desde que em atendimento aos interesses da administração pública, tais como textos, imagens, vídeos e sons, deverão ser observados os direitos de uso.

5.3.4. Não é permitido upload (publicação, disponibilização) de programas ou de qualquer informação sem autorização da entidade proprietária ou custodiante de tal material.

5.4. Monitoramento / Auditoria

5.4.1. A entidade governamental, através de setor competente, se reserva o direito, a qualquer tempo e sem aviso prévio, de examinar os registros de acessos à Internet para verificação de atendimento à Política de Segurança. Tais registros podem referir-se a web sites visitados, arquivos copiados da Internet, tempo gasto nos acessos e outras informações necessárias para a otimização dos recursos de acesso e realização de auditoria.

5.5. Recursos Tecnológicos

5.5.1. Toda conexão à Internet deve passar por equipamentos de segurança garantindo o controle de acesso e a aplicação dos demais mecanismos de segurança e, em caso contrário, o equipamento deve estar isolado da rede da entidade governamental.

5.5.2. Cada dispositivo com acesso a Internet (estação de trabalho, notebook, servidor e outros) deve possuir um sistema de proteção instalado, ativado e atualizado contra vírus ou qualquer outro software malicioso.

5.5.2.1. Todo arquivo de texto, programa ou dado copiado da Internet deve ser verificado automaticamente quanto à presença de vírus ou qualquer outro software malicioso antes da sua utilização.

5.5.3. A área responsável pela Tecnologia Informação deve prover as configurações de segurança a serem implementadas no *browser* das estações de trabalho, caso necessário.

6. Disposições Finais

- Casos omissos a este documento devem ser tratados pelo Grupo Temático de Segurança da Informação.
- Não é dado ao Agente Público ou Prestador de Serviço o direito de alegar desconhecimento da presente norma.
- O não cumprimento da presente norma acarretará ao Agente Público ou Prestador de Serviço as penalidades cabíveis, previstas no âmbito administrativo, cível e criminal.

PROPOSTA