Elaborado pela DSTI

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
MATO GROSSO

Normas e manuais das redes administrativas

Sumário de Informações do Documento		
Tipo do Documento: Normas e manuais das redes administrativas		
Responsável: DSTI		
Resumo: Este documento é destinado a descrever as normas e mais das redes administrativas		
Versão	**Data**	**Mudanças**
1.0	15/12/2018	Documento – Recursos de tecnologia da informação no IFMT elaborado por Clayton R. Franceschetto

Diretrizes

Todos os dispositivos conectados à rede IFMT, pertencerem à instituição ou não, devem estar em conformidade com a Política de Segurança da Informação (PSI) do IFMT, Decisão Nº 028/2012 do CONSUP.

As credenciais de acesso à rede do IFMT para a comunidade interna e informação de usuário e senha para visitantes - são de uso individual e não podem ser compartilhados com terceiros, sob pena de suspensão ou cancelamento dos privilégios de acesso. As credenciais de visitantes somente podem ser compartilhadas quando forem criadas especificamente para este fim.

A guarda das credenciais de acesso são de total responsabilidade de cada usuário, bem como todas as atividades e acessos efetuados através da respectiva conta.

Dispositivos contaminados com vírus podem ter seu acesso automaticamente bloqueado pelos sistemas de segurança da instituição.

É dever dos usuários o respeito à propriedade intelectual e direitos autorais, bem como a toda legislação que se aplique direta ou indiretamente à atividade de navegação na Internet.

No caso de violação de quaisquer regras em vigor, o usuário fica sujeito à perda do privilégio de acesso ao serviço, sem prejuízo das demais sanções cabíveis.

Não é permitido

Acessar computadores, softwares, dados, informações ou outros recursos de informação, em redes locais ou externas, sem a devida autorização ou, intencionalmente, habilitar outros a fazerem isso.

Utilizar programas e recursos que causem ou tentem causar a indisponibilidade de serviços de rede ou que prejudiquem de alguma forma as atividades de outros usuários.

Efetuar ações que possam ser caracterizadas como violação da segurança computacional (utilização de sniffers, efetuar varreduras na rede, quebrar a senha de outras contas, etc).

Utilizar recursos de comunicação (como e-mail, instant messengers ou sistemas com funções similares) para o envio de mensagens fraudulentas, hostis, obscenas, ameaçadoras ou outras mensagens que violem as leis federais, estaduais ou outras leis ou políticas do Instituto.

Utilizar programas de compartilhamento de arquivos do tipo peer-to-peer (p2p), tais como Vuze, eMule, LimeWire, BitTorrent, etc. O objetivo desta restrição é otimizar o uso da rede e estabelecer ações de combate à pirataria.