

PREFEITURA MUNICIPAL DE RONDONÓPOLIS	DATA VIGÊNCIA 20/12/2011
NORMA INTERNA: N.º STI 01/2011	Versão I
ASSUNTO: PROCEDIMENTOS PARA SEGURANÇA FÍSICA E LÓGICA DOS EQUIPAMENTOS, SISTEMAS, DADOS E INFORMAÇÕES	
SETORES ENVOLVIDOS: TODAS AS UNIDADES ADMINISTRATIVAS	
<p>1) OBJETIVOS:</p> <p>1.1. Estabelecer procedimentos para a utilização relativa ao cadastro, suspensão e exclusão de acesso aos recursos disponíveis relativos a computadores, Internet, Intranet / rede interna e utilização de e-mails, no âmbito da Prefeitura Municipal de Rondonópolis-MT.</p>	
<p>2) Consideram-se para os efeitos desta Instrução Normativa:</p> <p>2.1. Usuário: os servidores pertencentes ao quadro de pessoal do município de Rondonópolis-MT, devidamente autorizados a acessar a internet, e-mails e computadores da rede corporativa municipal;</p> <p>2.2. Cadastro: procedimento de criação de usuário para acesso a rede corporativa, computadores, Internet e/ou ter direito a utilização de e-mail corporativo;</p> <p>2.3. Senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e permitir seu acesso aos dados, programas e sistemas não disponíveis ao público, de uso pessoal e intransferível;</p> <p>2.4. Caixa-postal: caixa de correio para envio e recebimento de correspondências (e-mails);</p> <p>2.5. Id de usuário ou login: identificação única do usuário;</p> <p>3. Entende-se como rede corporativa municipal, todas as redes e/ou computadores de domínio público municipal.</p> <p>4. Compete ao Departamento de Tecnologia da Informação, recepcionar e conferir a documentação necessária ao cadastro, suspensão e exclusão de usuários, além do fornecimento de senha provisória.</p> <p>5. O cadastro de usuário para acesso a rede corporativa, computadores, Internet e/ou utilização de e-mail corporativo, depende do prévio encaminhamento ao Departamento de Tecnologia de Informação dos formulários “SARC - SOLICITAÇÃO DE ACESSO A REDE CORPORATIVA”, “REC – REQUERIMENTO DE EMAIL CORPORATIVO”, “RSE – REQUERIMENTO DE SITES ESPECÍFICOS”, “TERMO DE RESPONSABILIDADE”, constante no Anexo II, III, IV e V desta instrução.</p> <p>6. Ao usuário será fornecido o “id de usuário” após o mesmo ter tomado ciência e assinado o Termo de Responsabilidade de Acesso a rede corporativa, computadores, Internet / E-mail – Anexo V desta Instrução.</p> <p>7. O e-mail deve ser única e exclusivamente utilizado para o trato de questões de interesse administrativos da Prefeitura Municipal de Rondonópolis e suas unidades administrativas;</p>	

8. A conta de e-mail é destinada aos devidos órgãos municipal e não pode ser transferida ou cedida para utilização de terceiros, sendo o usuário responsável pela sua utilização e pela manutenção de sua senha;
9. Serão criadas caixas postais (e-mail) corporativas mediante o preenchimento do formulário REC (Requerimento de E-mail Corporativo), para cada secretaria ou unidade administrativa, programas ou projetos obedecendo ao disposto a seguir:
 - 9.1. Poderão ser criadas caixas-postais para projetos ou programas, independente do tempo de vigência do projeto, sendo seu conteúdo redirecionado para o gestor do projeto ou programa ou a quem ele determinar.
 - 9.2. As caixas postais corporativas serão criadas obedecendo a sigla da unidade administrativa, sendo seu conteúdo redirecionado para o gestor da unidade ou a quem ele determinar.
10. É facultada ao Departamento de Tecnologia de Informação, a utilização de filtros de conteúdo, que atuam de forma automática, não sendo permitido o envio ou recebimento de mensagens com conteúdo não autorizado (pornografia, apologia **a drogas, pedofilia, etc.**)
11. A conta de acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail é pessoal e não pode ser transferida para terceiros, sendo o usuário responsável pela sua utilização e pela manutenção de sua senha;
12. O acesso a sites ou serviços que representem risco aos dados ou a estrutura de informação da administração municipal serão bloqueados;
13. Havendo a necessidade de acesso a sites não autorizados, o usuário deverá solicitar a liberação do acesso via formulário de “RSE - Requerimento de Sites Específicos” (ANEXO IV desta instrução), que será analisado pelo Departamento de Tecnologia de Informação;
14. A liberação de acessos prevista no artigo anterior, somente será efetuada se comprovada a necessidade para fins administrativos e dependerá da avaliação do Departamento de Tecnologia de Informação.
15. É facultada ao Departamento de Tecnologia de Informação, a utilização de filtros de acesso, que agem de forma automática, não sendo permitida a navegação e/ou acesso nos seguintes casos:
 - 15.1. Sites pornográficos;
 - 15.2. Sites de drogas;
 - 15.3. Sites de Pedofilia;
 - 15.4. Sites de façam alguma forma de apologia a algum tipo de racismo ou discriminação;
 - 15.5. Sites de relacionamento;
 - 15.6. E/ou outros que comprometam a estrutura da rede corporativa.
16. O sistema de filtros de acesso irá gerar relatórios periódicos indicando os usuários que eventualmente navegam e/ou acessam recursos da rede corporativa, computadores, Internet e/ou utilização de e-mail indevidamente.
17. O descumprimento do Termo de Responsabilidade - Anexo V caracteriza infração funcional, com prejuízo de responsabilidade penal e civil do infrator.
18. Nos casos de relocação, exoneração, aposentadoria, remoção, falecimento ou qualquer outro que implique o desligamento do servidor da Administração Pública Municipal, o superior imediato do usuário deve comunicar imediatamente o fato ao Departamento de Tecnologia de Informação, por meio do formulário “SOLICITAÇÃO DE ACESSO A REDE CORPORATIVA”, constante no Anexo II, assinalando no quadro a opção “exclusão”.

19. A não observância deste artigo anterior implica na transferência das responsabilidades de acesso do servidor para seu superior imediato.
20. O superior imediato deve solicitar a suspensão do acesso do usuário, comunicando imediatamente o fato ao Departamento de Tecnologia de Informação por meio do formulário “SOLICITAÇÃO DE ACESSO A REDE CORPORATIVA”, constante no Anexo II, assinalando a opção “Bloqueio”, nos seguintes casos:
 - 20.1. Férias;
 - 20.2. Licenças;
 - 20.3. Afastamentos;
 - 20.4. Cedências;
 - 20.5. Aposentadorias
 - 20.6. E qualquer outro motivo que afaste o usuário de suas atribuições informadas na “SOLICITAÇÃO DE ACESSO A REDE CORPORATIVA”, constante no Anexo II, no seu cadastramento.
21. No retorno à atividade do usuário afastado, seu superior imediato deve comunicar imediatamente o fato ao Departamento de Tecnologia de Informação por meio do formulário “SOLICITAÇÃO DE ACESSO A REDE CORPORATIVA”, constante no Anexo II, assinalando a opção “Desbloqueio”.
22. A Administração Municipal utiliza softwares e sistemas que podem monitorar e gravar todos os usos da rede corporativa, computadores, Internet e/ou utilização de e-mail da rede e das estações de trabalho da prefeitura, secretarias.
23. A Administração Municipal se reserva o direito de inspecionar qualquer arquivo armazenado na rede, estejam no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política.
24. O Departamento de Tecnologia de Informação fará vistorias de rotina nos computadores da rede corporativa e preencherá um laudo de conformidade, havendo desacordo com a normativa o usuário poderá ser penalizado com bloqueio, exclusão e até mesmo processo administrativo.
25. Para suporte e reparos nos computadores da Prefeitura Municipal, apenas os funcionários do Departamento de Tecnologia de Informação (técnicos em informática), estão autorizados.
26. O uso de impressão pelo servidor ou usuário somente é permitido no que tange aos serviços e necessidades da administração pública, sendo terminantemente vedada ao usuário a impressão de documentos particulares.
27. Material sexualmente explícito não pode ser acessado, exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais das redes corporativas da administração municipal.
28. O uso de qualquer recurso da Administração Municipal para atividades ilegais é motivo para instauração de Processo Administrativo, podendo este, culminar com a exoneração por justa causa do servidor municipal envolvido.
29. Nenhum usuário pode utilizar-se dos recursos da prefeitura para fazer o download ou distribuição de softwares ou dados piratas.
30. Nenhum usuário pode utilizar os recursos da prefeitura para deliberadamente propagar qualquer tipo de vírus, worms, cavalos de tróia, programas de controle de outros computadores e espionagem (Back Oriffice, Netbus, etc.).
31. Somente podem enviar qualquer tipo de correspondência ou documentos em nome da prefeitura municipal através dos meios de comunicação via a rede corporativa, computadores,

Internet e/ou utilização de e-mail, servidores devidamente autorizados, mediante termo de responsabilidade assinado.

32. A utilização da rede corporativa, computadores, Internet e/ou utilização de e-mail, será feita somente por usuários autorizados.
33. Sendo interesse da administração municipal que os seus servidores estejam bem informados, o uso de sites de notícias ou de serviços de notícias poderá ser autorizado, desde que o seu uso não comprometa o uso de banda da rede, nem perturbe o bom andamento dos trabalhos.
34. Os downloads de arquivos de extensões tipo: .exe, .mp3, .wav, .bat, .com, .sys, .scr, .ppt, .mpeg, .avi, .rmvb, .dll, e de programas de entretenimento ou jogos não pode ser efetuado através da rede corporativa, computadores, Internet e/ou de e-mail municipal. Da mesma forma, o uso de jogos contra oponentes na internet é proibido.
35. Servidores com acesso à internet não podem efetuar upload de qualquer software licenciado à prefeitura ou de dados de propriedade da prefeitura, sem expressa autorização da administração responsável pelo software ou pelos dados.
36. É proibido o uso de ferramentas P2P, P2M (ORKUT, Comunidades, MSN, kazaa, Morpheus, etc) bem como o uso de IM (Instant messengers) não homologados/autorizados pela Administração Municipal e Departamento de Tecnologia de Informação.
37. No tocante aos e-mails, fica expressamente proibido:
 - 37.1. Utilizar tal serviço para fins ilegais;
 - 37.2. Utilizar tal serviço para transmitir/divulgar material ilegal, difamatório, que viole a privacidade de terceiros, ou que seja abusivo, ameaçador, obsceno, prejudicial, vulgar, injurioso, ou de qualquer outra forma censurável;
 - 37.3. Transmitir e/ou divulgar qualquer material que viole direitos de terceiro, incluindo, mas sem limitação, direitos de propriedade intelectual de terceiros;
 - 37.4. Enviar mensagens não-solicitadas, reconhecidas como "spam", "junk mail" ou correntes de correspondência ("chain letters");
 - 37.5. Utilizar tal serviço para enviar/divulgar quaisquer tipos de vírus ou arquivos contendo quaisquer tipos de vírus ("Cavalos de Tróia") ou que possam causar danos ao seu destinatário ou a terceiros;
 - 37.6. Praticar quaisquer atos que violem qualquer lei ou regulamento local, estadual, nacional ou internacional aplicável;
 - 37.7. Não cumprir todas as leis aplicáveis com relação à transmissão de dados a partir do Brasil ou do território onde o usuário resida;
 - 37.8. Obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço;
 - 37.9. Interferir ou interromper os serviços ou os servidores ou redes conectadas ao serviço;
 - 37.10. Não cumprir todos os requerimentos, procedimentos, políticas, e regulamentos de redes conectadas ao serviço;
38. É proibido o uso de dispositivos portáteis para cópias de arquivos no âmbito da prefeitura municipal exemplo: pen-drive, cd, dvd, e qualquer outro dispositivo similares, sem autorização prévia do Departamento de Tecnologia de Informação. Caso haja a necessidade de uso, encaminhar ao Departamento de Tecnologia de Informação formulário de "RDP - REQUERIMENTO PARA USO DE DISPOSITIVOS PORTATEIS", constante no Anexo VI, que será analisado.
39. É proibido o uso de computadores de terceiros na rede corporativa da prefeitura municipal.

40. As entidades conveniadas, serviços terceirizados e ou qualquer outra empresa ou pessoa que utiliza a rede e ou sistemas da Prefeitura Municipal, deverão obedecer todas as normas ditadas nesta instrução, sob pena de restrição do convênio.
41. O Departamento de Tecnologia de Informação instalou uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um firewall, que é a primeira, mas não a única barreira entre a rede interna e a internet.
42. Qualquer tentativa de burlar ou fazer alteração dos parâmetros do firewall, por qualquer servidor, sem ser devidamente credenciado e autorizado para tal, ocasionará a instauração de Processo Administrativo.

SECRETARIA DE ADMINISTRAÇÃO

PREFEITO