

PREFEITURA DE JUIZ DE FORA	Anexo I à Portaria N°	
	SEPLAG-JF	SSTI
TECNOLOGIA DA INFORMAÇÃO		
PSI/N.0003 - Norma de Gerenciamento de Acesso Remoto à Rede Corporativa da Prefeitura de Juiz de Fora		
Versão: 1	Vigor em: / /2014	Pag.: 1/4

ANEXO I

1. Objetivo:

Estabelecer os critérios e procedimentos para os usuários de Tecnologia da Informação e prestadores de serviço que necessitem acessar remotamente o ambiente da rede corporativa da PJJ.

2. Abrangência:

Aplica-se a todos os usuários de informática e prestadores de serviços que necessitem acessar remotamente o ambiente corporativo da PJJ.

3. Terminologia e Abreviações:

3.1. Acesso remoto - Acesso realizado, a partir de um computador remoto, aos equipamentos servidores, estações de trabalho ou serviços de rede disponibilizados pela SSTI.

3.2. IP (Internet Protocol) - Protocolo responsável pelo endereçamento dos dados que são transmitidos pelos computadores.

3.3. Patches (hotfixes) - Atualizações de segurança do sistema operacional.

3.4. P2P (Peer-to-Peer - Ponto a ponto) - É uma arquitetura de sistemas distribuídos caracterizada pela descentralização das funções na rede, em que cada equipamento realiza tanto funções de servidor quanto de cliente. Muito utilizado em aplicativos de troca de arquivos.

3.5. SPAM - Mensagem de correio eletrônico não solicitada, enviada em grande quantidade para uma lista de e-mails, fóruns ou grupos de discussão.

3.6. VPN (Virtual Private Network - Rede Privada Virtual) - É uma rede privada que usa a estrutura de uma rede pública (como por exemplo, a Internet) para transferir dados, permitindo a implementação de protocolos de segurança na transmissão.

4. Documentos complementares:

PSI/N.0002 - Norma de Homologação de Estação de Trabalho.

5. Regras e Diretrizes:

5.1. Somente terão direito ao acesso remoto à rede corporativa da PJJ, os usuários e prestadores de serviços que comprovadamente, necessitem do recurso para desempenho de atividades do interesse da PJJ.

5.2. O cadastramento do funcionário deverá ser solicitado formalmente à SEPLAG-JF/SSTI, através do envio de memorando e preenchimento do formulário contido no ANEXO II, em que serão relacionados os serviços, sistemas e equipamentos servidores que serão acessados, bem como as justificativas pertinentes.

5.3. O usuário deve sempre garantir a autenticidade e veracidade de todos os dados que informar através de preenchimento do formulário, mantendo permanentemente atualizadas as informações fornecidas à PJJ, sendo o único responsável pelas declarações falsas ou inexatas que prestar e que vierem a causar prejuízos à Prefeitura ou a terceiros.

5.4. A liberação para acesso remoto será analisada pela SEPLAG-JF/SSTI e somente será liberado caso não comprometa, de forma alguma, a segurança da rede corporativa da PJJ.

5.5. O acesso remoto à rede corporativa da PJJ deve ser realizado por meio de endereço de IP fixo e válido na Internet.

5.6. O usuário ou prestador de serviços poderá ser auditado pela PJJ, durante todo o acesso remoto.

5.7. O código de acesso fornecido pela SEPLAG-JF/SSTI ao usuário para acesso remoto é pessoal e intransferível.

6. Equipamento Utilizado para Acesso Remoto:

6.1. O equipamento que será utilizado no acesso remoto deverá estar atualizado com todos os *patches* de correção e de segurança fornecidos pelo fabricante, devidamente aplicados.

6.2. O equipamento deve possuir software antivírus homologado pela PJJ, conforme estabelecido no ANEXO III da Norma PSI-N.0002 - Homologação de Estação de Trabalho.

6.3. As estações deverão estar livres de *malware* (vírus, *trojans*, *worms*, *keyloggers* e códigos maliciosos) antes de estabelecer a conexão remota com a rede corporativa da PJJ.

6.4. O equipamento deve possuir *firewall* pessoal devidamente habilitado para proteção do acesso às informações da PJJ.

6.5. Devem ser utilizadas somente ferramentas de segurança homologadas pela SSTI para acesso remoto.

7. Responsabilidades dos Usuários Autorizados para Acesso Remoto:

7.1. Usar a conexão somente para finalidades e serviços da PJJ.

7.2. Efetuar a configuração do equipamento utilizado para acesso remoto, conforme instruções da SEPLAG-JF/SSTI.

PREFEITURA DE JUIZ DE FORA	Anexo I à Portaria N°	
	SEPLAG-JF	SSTI
TECNOLOGIA DA INFORMAÇÃO		
PSI/N.0003 - Norma de Gerenciamento de Acesso Remoto à Rede Corporativa da Prefeitura de Juiz de Fora		
Versão: 1	Vigor em: / /2014	Pag.: 2/4

7.3. Não utilizar a conexão de acesso remoto para fins de rede de compartilhamento de arquivos tipo P2P, transmissão de e-mails não solicitados ou de propaganda (spam), transmissão de softwares mal-intencionados (vírus, *trojans* - cavalos de tróia, *worms*, *spywares* e assemelhados), acesso a pornografia ou conteúdo considerado ilegal pela legislação vigente, download de softwares ou arquivos sem licença do proprietário (pirata) e ocultação da própria identidade (*Proxy*).

7.4. Nunca compartilhar o acesso à rede da PJF com usuários não autorizados, por qualquer meio, inclusive através de compartilhamento por meio físico, ou através da divulgação de nome de usuário e senha.

8. Penalidades:

8.1. A não observância de quaisquer das disposições contidas nesta norma implicará na aplicação de penalidades previstas no Estatuto Municipal e/ou na Legislação vigente.

9. Relação de Anexos:

Anexo II - Termo de Responsabilidade para Acesso Remoto à Rede Corporativa.

10. Aprovação:

Aprovado por:

Data: ____/____/____

Subsecretário de Tecnologia da Informação



PREFEITURA DE JUIZ DE FORA	Anexo II à Portaria N°	
	SEPLAG-JF	SSTI
TECNOLOGIA DA INFORMAÇÃO		
PSI/N.0003 - Norma de Gerenciamento de Acesso Remoto à Rede Corporativa da Prefeitura de Juiz de Fora		
Versão: 1	Vigor em: / /2014	Pag.: 3/4

ANEXO II

Termo de Responsabilidade para Acesso Remoto à Rede Corporativa					
<p>Solicito à SEPLAG-JF/SSTI que seja realizada a liberação do acesso remoto aos sistemas ou equipamentos servidores mencionados no item 8, do usuário, cujos dados seguem abaixo, devidamente autorizado conforme no quadro ao lado: Em: ___/___/___</p> <p style="text-align: right;">Assinatura e Carimbo do Superior Imediato ou Gestor do Contrato</p>					
1	NOME COMPLETO			2	TELEFONE/RAMAL
3	MATRÍCULA / RG	4	LOTAÇÃO/NOME DA EMPRESA		
5	CARGO/FUNÇÃO			6	LOGIN
7	E-MAIL				
8	SERVIDORES E SISTEMAS DA REDE PJF QUE DESEJA ACESSAR				
	Hostname	IP Interno	Serviço/Protocolo	Porta	IP Externo
9	TIPO DE USUÁRIO				
	<input type="checkbox"/> Administrador <input type="checkbox"/> Restrito				
10	DESCRIÇÃO DOS SERVIÇOS QUE SERÃO REALIZADOS NO AMBIENTE A SER ACESSADO REMOTAMENTE				
11	ENDEREÇO IP REAL DAS MÁQUINAS QUE IRÃO ACESSAR O AMBIENTE DA REDE PJF				
12	JUSTIFICATIVA PARA O ACESSO REMOTO				
13	REGRAS E DIRETRIZES AO USUÁRIO				
	<p>A rede interna da PJF e os equipamentos que a compõem têm como finalidade única e exclusiva permitir aos seus usuários a prática de atividades relacionadas ao trabalho e informações de interesse da PJF.</p> <p>A cada usuário é entregue um login e senha para acesso aos recursos de rede.</p> <p>Assim, cabe ao usuário observar o que segue:</p> <ul style="list-style-type: none"> • Garantir a autenticidade e veracidade de todos os dados que informar através do preenchimento de formulários, mantendo permanentemente atualizadas as informações fornecidas à PJF, sendo o único responsável pelas declarações falsas ou inexatas que prestar e que vierem a causar prejuízos à Prefeitura; • Não fornecer o código de acesso a terceiros; • Agir em conformidade com a lei, com os avisos, regulamentos de uso e instruções levados ao seu conhecimento, bem como com a ordem pública, com a moral e bons costumes geralmente aceitas; • Utilizar o serviço de acesso remoto apenas para realizar atividades relacionadas ao seu trabalho; • Não violar as regras e normas explicitadas nas Portarias que dispõem sobre a Política de Segurança de Informações da Prefeitura de Juiz de Fora. 				

PREFEITURA DE JUIZ DE FORA	Anexo II à Portaria N°	
	SEPLAG-JF	SSTI
TECNOLOGIA DA INFORMAÇÃO		
PSI/N.0003 - Norma de Gerenciamento de Acesso Remoto à Rede Corporativa da Prefeitura de Juiz de Fora		
Versão: 1	Vigor em: / /2014	Pag.: 4/4

14 PENALIDADES
<p>Uma vez que o usuário é responsável por qualquer atividade a partir de sua conta, o mesmo poderá responder por qualquer ação legal apresentada à PJF e que envolva a sua conta.</p> <p>No caso do não cumprimento às normas, o usuário terá seu acesso bloqueado para averiguação. Cabe à SSTI constituir uma Comissão para analisar o caso e recomendar a penalidade, que pode ser advertência verbal ou escrita, suspensão, restrição, ou o banimento do cadastro de usuários, com notificação formal ao órgão competente.</p>
15 TERMO DE REponsABILIDADE
<p>Declaro estar ciente da Norma de Gerenciamento de Acesso Remoto à Rede Corporativa da PJF e dos termos relacionados neste formulário e responderei pelos atos decorrentes da utilização da minha senha.</p> <p>Por ser verdade, firmo a presente.</p> <p>1. Declaro que tomei Conhecimento:</p> <p>a) Das Normas e Procedimentos adotados pela SEPLAG-JF/SSTI, quanto à segurança dos sistemas informatizados da PJF;</p> <p>b) Das responsabilidades decorrentes da confiança em mim depositada, como usuário detentor de informações da PJF.</p> <p>2. Assumo o compromisso de:</p> <p>a) Realizar meu trabalho cumprindo as normas e procedimentos de segurança;</p> <p>b) Usar o privilégio de acesso somente para o serviço a que fui designado;</p> <p>c) Usar o software e as informações obtidas somente para a finalidade determinada;</p> <p>d) Usar o software de empresas e entidades externas exclusivamente de acordo com os termos da licença ou contrato;</p> <p>e) Divulgar informações somente sob autorização competente;</p> <p>f) Informar ao meu gerente ou chefe imediato sobre qualquer violação das medidas de proteção do equipamento, do software e das informações;</p> <p>g) Permanecer junto ao equipamento por mim utilizado: terminal, microcomputador, impressora, ou outro periférico, até que o mesmo seja desativado ou seja bloqueada a sessão;</p> <p>h) Tratar como confidenciais as informações, dos sistemas relativas aos clientes e usuários;</p> <p>i) Impedir a divulgação e compartilhamento dos códigos de segurança atribuídos (Senhas) que são pessoais e intransferíveis.</p> <p>3. Reconheço:</p> <p>a) Estar sujeito a sanções e penalidades previstas em normas legais pelo descumprimento dos compromissos assumidos, devendo observar, especialmente, os seguintes diplomas legais:</p> <ul style="list-style-type: none">• Lei nº 9.609, de 19/02/1998, que dispõe sobre a Proteção da Propriedade Intelectual do Programa de Computador, sua comercialização no país e dá outras providências;• Lei nº 9.610, de 19/02/1998, que altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. <p>b) O direito da PJF de interromper ou negar a prestação de serviços sempre que houver comprometimento da segurança;</p> <p>c) O direito da PJF de inspecionar o equipamento e avaliar o cumprimento das normas e procedimentos sempre que for julgado necessário.</p> <p>Em ____/____/____</p> <p style="text-align: right;">Funcionário / Usuário / Contratado</p> <p>Obs.: O não preenchimento de QUALQUER dado acima, implicará na eliminação desta requisição sem aviso prévio. (Dúvidas ramal 7024)</p>
16 RESERVADO À SSTI
<p>ACESSO LIBERADO? () Não autorizado () Sim - EM: ____/____/____</p> <p>DATA DE EXPIRAÇÃO DO ACESSO: ____/____/____</p> <p style="text-align: center;">Técnico Responsável pela Liberação do Acesso Remoto</p>