Teresina, 15 de fevereiro de 2006

REGULAMENTO

Estabelece as normas de uso e segurança de recursos de Tecnologia da Informação no âmbito da Secretaria da Fazenda do Estado do Piauí.

Art. 1º As normas dispostas neste Regulamento têm o escopo de proteger os recursos de Tecnologia de Informação das ameaças de:

I. Divulgação não autorizada de informações;

II. Modificações e despersonalização das informações;

III. Indisponibilidade dos recursos;

IV. Armazenamento de conteúdo ilegal;

V. Recebimento de conteúdo malicioso (vírus, cavalos-de-tróia e documentos contendo macros perigosas);

VI. Mensagens-bombas (mensagens que provocam congestionamento do sistema - SPAM);

VII. Invasões externas;

VIII. Invasões à rede interna e demais recursos compartilhados.

Art. 2º Este Regulamento rege os procedimentos de todos os usuários de recursos de Tecnologia de Informação da SEFAZ-PI, inclusive estagiários, contratados e fornecedores, que seguirão às normas de uso geral.

Parágrafo único. São normas de uso geral:

I. Os usuários devem conhecer o Regulamento Geral de Segurança da Informação da SEFAZ.

II. Somente pessoal autorizado deve utilizar os recursos de informática. O seu uso deve ser limitado exclusivamente aos interesses da organização e aderentes às funções de cada colaborador/contratado/estagiário.

III. O usuário é responsável pelas informações armazenadas nos equipamentos dos quais faz uso. Nos casos de equipamentos de utilização coletiva, o superior imediato é o responsável ou pessoal por ele delegado.

IV. O usuário deve manter sigilo sobre as informações consideradas estratégicas e/ou confidenciais.

V. O usuário deve informar ao seu superior imediato quando informações ou aplicações consideradas estratégicas e/ou confidenciais forem encontradas sem tratamento de segurança correto. O superior imediato deve informar a ocorrência ao Grupo Segurança da Informação prontamente.

VI. As informações consideradas estratégicas e/ou confidenciais devem ser armazenadas nos servidores de arquivos, em diretórios (pastas) devidamente protegidos, em caso de anexos em mensagens de correio eletrônico, os mesmos deverão ser desanexados e armazenados nos servidores.

VII. A transferência de grandes volumes de informações consideradas estratégicas e/ou confidenciais deve ser feita através da rede em diretórios (pastas) específicos para este fim.

VIII. Documentos impressos de conteúdo estratégico e/ou confidencial devem ser resguardados contra acessos não autorizados.

IX. O usuário deve encerrar sua sessão (*logoff*) na estação de trabalho ao

término de suas atividades. Ao final do expediente, a estação de trabalho deverá ser desligada.

X. Em casos de ausência do usuário por menores períodos (ex.: intervalo do almoço), deve ser ativada a proteção de tela com senha (*screen saver*) em sua estação de trabalho. O período de tempo

XI. configurado para que a proteção de tela seja automaticamente acionada não deve exceder a 10 (dez) minutos.

XII. Os diretórios (pastas) de trabalho das estações não podem ser compartilhados.

XIII. O gestor do contrato e o usuário prestador de serviço são os responsáveis pelo uso indevido das informações contidas nos equipamentos de prestadores de serviço.

XIV. Cabe à área de Tecnologia de Informação - TI autorizar a conexão de equipamentos de prestadores de serviço na rede corporativa da SEFAZ.

XV. Usuários que utilizem *notebooks* devem assinar um Termo de Custódia.

XVI. A entrada e saída de pessoas não pertencentes aos ambientes críticos de TI (salas de servidores, centrais de monitoramento, etc.) não é permitida. Necessidades específicas devem ser autorizadas pelos gestores das áreas e serão registradas.

XVII. O usuário deve zelar pelo bom uso do equipamento. Problemas de manutenção em função de líquidos, restos de comida, etc., serão de responsabilidade do usuário.

XVIII. O usuário é responsável pela guarda do equipamento. Em caso de roubo dentro do ambiente de trabalho, o usuário deverá informar à SEFAZ. Em caso de roubo fora do ambiente de trabalho, o usuário deverá tomar as providências cabíveis com a polícia ou órgãos competentes e notificar a SEFAZ.

XIX. Respeitar a integridade dos recursos de tecnologia de informação da

SEFAZ. Os usuários, a menos que tenham uma autorização específica para esse fim, não podem tentar, permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na SEFAZ, de sua propriedade ou de qualquer outra pessoa ou instituição.

XX. Não ligar ou desligar fisicamente ou eletricamente a um recurso de tecnologia de informação da SEFAZ, nenhum componente externo, como cabos, impressoras, discos ou sistemas de vídeo, sem uma autorização específica.

XXI. Comunicar ao Administrador de Sistemas e Rede local ou a Equipe de Segurança da informação qualquer evidência de violação das normas em vigor, não podendo acobertar, esconder ou ajudar a esconder violações de terceiros, de qualquer natureza.

Art. 3º As informações importantes e relacionadas às atividades de trabalho na SEFAZ devem ser armazenadas nos servidores de rede específicos para este fim.

Art. 4º A cópia de segurança das informações existentes nas estações de trabalho é responsabilidade de cada usuário.

Art. 5º O controle de acesso aos recursos de Tecnologia de Informação será de responsabilidade de cada usuário, obedecendo ao seguinte:

I. Os atos e acessos do usuário aos dados e sistemas devem ser realizados através de sua identificação única no ambiente informatizado.

II. É vedada a inclusão de usuários na rede fora do processo normal de inclusão de usuários estabelecido pela área de TI.

III. O tamanho de caracteres para formação da senha não pode ser menor que 6 (seis).

IV. Não devem ser utilizadas senhas óbvias, como datas, nomes próprios e siglas.

V. Considerando 4 (quatro) tipos de caracteres (letras minúsculas, letras

maiúsculas, números e símbolos), a senha deve ser composta de pelo menos 3 (três) tipos.

VI. O número máximo de tentativas de autenticação nos sistemas (*logon*) é 3 (três). No caso deste número ser ultrapassado, a conta do usuário irá permanecer bloqueada, sendo a liberação efetuada apenas por solicitação formal do gerente ou coordenador.

VII. É obrigatória a troca de senha no primeiro acesso do usuário.

VIII. A senha corporativa de rede terá uma validade de 90 (noventa) dias, sendo requisitada automaticamente a sua troca para o usuário.

IX. O usuário não poderá reutilizar as suas últimas 3 senhas.

X. A troca de senha deve ser de responsabilidade do usuário.

XI. É proibido o compartilhamento de senhas/usuários e, em caso de suspeita de perda de sigilo, o usuário deve trocar a sua senha.

XII. O usuário será responsabilizado por tentar "quebrar" a segurança do sistema, inclusive com tentativas de descobrir a senha de outros usuários.

XIII. O perfil de acesso dos usuários aos aplicativos e sistemas será o mínimo necessário para o desempenho de suas atividades.

XIV. O gestor da área e a área de Recursos Humanos são os únicos setores que podem autorizar a criação ou revogação das contas de acesso dos usuários aos aplicativos e sistemas da SEFAZ.

XV. O gestor de contrato de prestadores de serviço é o único que pode solicitar a criação das contas de acesso aos seus prestadores de serviço. O mesmo será responsável por informar quando houver saída ou troca de prestadores de serviço.

XVI. Prestadores de serviço devem ter identificação diferenciada e única, com prazo de validade temporário, de acordo com o contrato estabelecido, não podendo ser superior a 6 (seis) meses, podendo ser prorrogado.

XVII. É proibido o uso de recursos computacionais por usuários desligados da SEFAZ. Os mesmos terão seus privilégios (conta na rede e em qualquer sistema desta Secretaria, uso de e-mail, acesso à Internet, etc.) imediatamente revogados na data de desligamento.

XVIII. Utilizar qualquer Recurso de tecnologia de informação da SEFAZ somente após obter uma autorização por escrito e assinar o Termo de Responsabilidade, no qual declara conhecer as políticas e normas em vigor e se compromete a cumpri-las.

XIX. Exibir a comprovação de vínculo com a SEFAZ ou autorização especial ao pessoal responsável, sempre que solicitado durante a utilização dos recursos, sob pena de imediata suspensão da conexão, sem prejuízo das disposições legais pertinentes.

XX. O usuário deverá respeitar a integridade e limites de sua autorização de acesso ou conta.

XXI. A segurança de suas contas e de suas senhas - a conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas sem a autorização expressa e por escrito da UNITEC.

XXII. Informar imediatamente a Equipe de Segurança de Recursos de tecnologia de informação da SEFAZ qualquer suspeita de tentativa de violação de segurança, em qualquer nível.

XXIII. Não permitir ou colaborar com o acesso aos Recursos de tecnologia de informações da SEFAZ por parte de pessoas não autorizadas, sob pena de ser co-responsabilizado pelos eventuais problemas que esses acessos vierem a causar.

Art. 6º O procedimento de descarte de informações seguirá as seguintes premissas:

I. Devem ser removidos da rede e das estações de trabalho os arquivos que não sejam mais necessários ou que não se refiram a assuntos de trabalho.

II. Os arquivos que não sofrerem acesso por um período de 1 (um) ano

serão removidos da rede, à exceção daqueles protegidos por prazos legais.

III. Arquivos com informações estratégicas e/ou confidenciais não devem ser mantidos na Lixeira do Windows.

IV. Documentos impressos de conteúdo estratégico e/ou confidencial devem ser fragmentados antes de serem jogados no lixo.

Art. 7º Quanto ao combate a vírus eletrônicos:

I. Todas as estações de trabalho devem possuir *software* antivírus padrão SEFAZ instalado, configurado, ativado e atualizado, incluindo microcomputadores e *notebooks* de terceiros que necessitam de acesso à rede da SEFAZ.

II. O usuário deve informar imediatamente ao *Help Desk* em caso de contaminação por vírus de computador.

Art. 8º Os sistemas de correio eletrônico e as informações neles contidas são pertencentes à SEFAZ e disponibilizados aos usuários como uma ferramenta de apoio às atividades do serviço público, seguindo às seguintes orientações.

§ 1º Ao utilizar os recursos, o usuário deve manter o cuidado de:

I. Utilizar o sistema exclusivamente em prol dos interesses da SEFAZ;

II. Tratar sua senha como pessoal e intransferível;

III. Identificar suas mensagens com seu nome e endereço eletrônico;

IV. Avaliar cuidadosamente o envio de mensagens para listas e grupos de usuários, para que não se transformem em mensagens-bombas;

V. Quando for necessário o envio de arquivos grandes (> 500 *kbytes*) anexos às mensagens, os mesmos devem ser compactados ("zipados");

VI. No caso de informações sigilosas enviadas por correio eletrônico para usuários internos, explicitar no cabeçalho ou no corpo da mensagem que se tratam de informações confidenciais;

VII. No caso de informações sigilosas enviadas por correio eletrônico para fora da SEFAZ, utilizar recursos auxiliares de segurança, como criptografia;

VIII. Manter o mínimo necessário de mensagens armazenadas na caixa postal.

§ 2º São inadmissíveis quanto ao uso do correio eletrônico:

I. Criar, transmitir ou armazenar material que caracterize atividade ilegal, ofensiva, discriminatória ou contrária aos interesses da SEFAZ;

II. Criar, transmitir ou armazenar material que seja atentatória a dignidade da pessoa humana;

III. Transmitir mensagens para pessoas ou sistemas não autorizados;

IV. Criar ou transmitir mensagens prejudiciais à imagem da SEFAZ;

V. Criar ou transmitir mensagens de caráter pessoal que ofendam a integridade moral dos servidores da SEFAZ;

VI. Criar, transmitir ou armazenar qualquer tipo de conteúdo malicioso, como vírus e cavalos-de-tróia;

VII. Criar ou transmitir correntes, pirâmides e outros tipos de mensagens-bombas;

VIII. Criar ou transmitir piadas e material pornográfico;

IX. Divulgar sua senha;

X. Utilizar a senha de outra pessoa;

XI. Utilizar o sistema para negócios pessoais;

XII. Sobrecarregar o sistema (neste sentido, o envio de arquivos anexos mensagens, sempre que possível, deve ser evitado);

XIII. Violar os padrões de segurança estabelecidos;

XIV. Influenciar comportamento considerado inaceitável.

§ 3º Responsabilização pelo uso do correio eletrônico:

I. Cada usuário é responsável pelo conteúdo armazenado ou enviado através do correio eletrônico;

II. Cada colaborador (funcionário ou estagiário) da SEFAZ é responsável pelas atividades de parceiros e contratados sob sua responsabilidade.

Art. 9º Sobre a privacidade das informações contidas no correio eletrônico:

I. Informações confidenciais não devem ser enviadas pelo correio eletrônico sem alguma forma de proteção contra vazamento e alteração não autorizados;

II. A SEFAZ reserva para si o direito de monitorar e interferir no tráfego de mensagens, com o propósito de verificar o cumprimento dos padrões de segurança, sempre que julgar necessário e sem aviso prévio.

Art. 10 O acesso à Internet é disponibilizado a colaboradores, parceiros e estagiários como uma ferramenta de apoio às atividades profissionais. O seu uso deve ser restrito e controlado.

§ 1º O acesso à internet deve seguir as seguintes orientações:

I. Uso da Internet restrito às atividades relacionadas com os negócios/serviços da SEFAZ. Exemplos: comunicação com os contribuintes e fornecedores, pesquisas de tópicos pertinentes e obtenção de informações úteis, no sentido de manter os níveis mais altos de produtividade, qualidade e atualização tecnológica;

II. Conduzir adequadamente o uso da Internet, respeitando direitos autorais, regras de licenciamento de *softwares*, direitos de

propriedade, privacidade e proteção de propriedade intelectual;

III. A proteção de arquivos contendo dados sensíveis ou sigilosos da SEFAZ, assim definido pela Política de Segurança, quando transferidos de qualquer forma pela Internet;

IV. O uso da Internet em prol dos interesses da SEFAZ.

§ 2º São inadmissíveis quanto ao acesso à internet:

I. Utilizar a Internet para negócios pessoais;

II. Acessar ou armazenar material indevido e/ou que caracterize atividade ilegal, como pornografia e pirataria;

III. Acessar qualquer tipo de conteúdo malicioso, como vírus e cavalos-de-tróia;

IV. Acessar salas de bate-papo (*chat rooms*), exceto se o acesso for necessário para realização das atividades de trabalho;

V. Uso de softwares de comunicação instantânea, como *ICQ, IRC, Net Meeting, Instant Messenger*, etc, exceto se o acesso for necessário para realização das atividades de trabalho;

VI. Sobrecarregar o sistema;

VII. Realizar o *download* de arquivos de interesse pessoal;

VIII. Violar os padrões de segurança estabelecidos;

IX. Influenciar comportamento considerado inaceitável.

Art. 11 Modem é um recurso disponibilizado a colaboradores, parceiros e estagiários como uma ferramenta de apoio às atividades profissionais. O seu uso deve ser restrito e controlado.

§ 1º A utilização de modem deve seguir as seguintes orientações:

I. Utilizar conexão via modem exclusivamente em prol dos interesses

da SEFAZ;

II. Estar formalmente autorizado a utilizar este tipo de conexão;

III. Utilizar recursos auxiliares no cumprimento dos Padrões de Segurança, tais como assinaturas digitais e criptografia;

IV. Utilizar o mínimo necessário deste recurso;

V. Utilizar o recurso quando estiver ausente do ambiente de trabalho e fora das instalações da SEFAZ.

§ 2º São inadmissíveis quanto ao uso do modem:

I. A conexão via modem estando conectado na rede interna;

II. O compartilhamento de conexões entre colaboradores;

III. Violar os padrões de segurança estabelecidos;

IV. Influenciar comportamento considerado inaceitável.

Art. 12 A SEFAZ caracteriza como não ético e inaceitável e considera como motivo de ação disciplinar prevista em seus estatutos qualquer atividade através da qual um indivíduo:

I. Viole questões tais como direitos autorais ou proteção de patentes e autorizações da SEFAZ ou de terceiros, como também licenças de uso e outros contratos.

II. Interfira no uso correto dos recursos de informação.

III. Tente conseguir ou consiga acesso não autorizado a recursos de informação.

IV. Sem autorização, destrói, altera, desmonta, desconfigura, impede o acesso de direito ou interfere na integridade dos recursos de tecnologia de informação.

V. Sem autorização, invade a privacidade de indivíduos ou entidades que são autores, criadores, usuários ou responsáveis pelos recursos de tecnologia de informações.

VI. Remova dos recursos de tecnologia de informação da SEFAZ algum documento de sua propriedade ou por ela administrado, sem uma autorização específica.

VII. Se faça passar por outra pessoa ou esconda sua identidade na utilização dos Recursos Computacionais da SEFAZ.

VIII. Viole ou tente violar os sistemas de segurança dos recursos computacionais da SEFAZ, como quebrar ou tentar adivinhar identificação ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme.

IX. Intercepte ou tente interceptar transmissão de dados não destinados ao seu próprio acesso.

X. Tente interferir ou interfira em serviços de outros usuários ou o seu bloqueio, provocando, por exemplo, congestionamento da rede, inserindo vírus ou tentando a apropriação dos Recursos Computacionais da SEFAZ.

Art. 13 As penalidades a serem aplicadas às condutas elencadas neste Regulamento, sem prejuízo de outras penas previstas em lei ou em normas da SEFAZ, são: redução ou eliminação, temporárias ou permanentes, de privilégios de acesso, tanto aos Recursos Computacionais, quanto às redes, da UNITEC e outros serviços ou facilidades.

Art. 14 Esta Norma se aplica a qualquer funcionário, estagiário, contratados e fornecedores , quer ele esteja dentro da SEFAZ ou fora, e se refere a todos os recursos computacionais, controlados individualmente ou compartilhados, isolados ou em rede.

Art. 15 A Superintendência da Receita, as Unidades e Gerências da SEFAZ podem definir condições de uso específicas para os recursos sob seu controle, consistentes com a política geral, mas com detalhes, diretrizes e/ou restrições adicionais.

Art. 16 Cabe à SEFAZ tratar das violações de restrições adicionais de acordo com as normas internas vigentes e onde não houver estes mecanismos específicos, o exposto deste regulamento deve prevalecer.

Art. 17 No caso do uso de redes externas, as políticas envolvendo este tipo de uso também são aplicáveis e precisam ser adotadas.

Art. 18 A infração ou tentativa de infração às regras constantes neste Regulamento e demais normas sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.