

INSTRUÇÃO NORMATIVA STI Nº. 001

UCCI - Unidade Central de Controle Interno

STI – Sistema de Tecnologia e Informação

Versão: 1.0

Aprovada em: 30/12/2011

Unidade Responsável: Gabinete do Prefeito

I - FINALIDADE

A presente instrução normativa tem por objetivo disciplinar os procedimentos administrativos do Sistema de Tecnologia da Informação quanto a segurança física e lógica dos equipamentos, sistemas, dados e informações, contra acessos não autorizados, acidentes naturais e danos intencionais.

II - ABRANGÊNCIA

A presente Instrução Normativa abrange todos os setores das Unidades da Administração Direta e Indireta do Poder Executivo.

III - CONCEITOS

Tecnologia da Informação

Entende-se como Tecnologia da Informação o conjunto de recursos tecnológicos e computacionais para geração e uso da informação. Para os fins da presente instrução normativa, o termo designa o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, bem como, o modo como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas.

Recursos Computacionais

Para os efeitos desta instrução, Recursos Computacionais se refere a todos os equipamentos, as instalações ou banco de dados direta ou indiretamente administrados, mantidos ou operados pelas Unidades Administrativas, compreendendo: Computadores de qualquer espécie, incluídos seus equipamentos acessórios; Impressoras, *Plotters* e equipamentos multifuncionais conectados ao computador; Redes de computadores e de transmissão de dados; Banco de dados ou documentos residentes em disco, fita magnética ou outros meios; Leitoras de códigos de barra, Scanners, equipamentos digitalizadores e afins; *Patch Panel*, *Switches*, *Hubs*, e outros equipamentos de rede; Softwares, sistemas e programas adquiridos ou desenvolvidos pela Administração.

Usuário

É todo servidor público municipal ou prestador de serviço que necessite de acesso à rede corporativa ou utilize algum recurso computacional da rede pública municipal.

Unidade Usuária

Corresponde a qualquer unidade administrativa integrante da estrutura municipal, que utilize os recursos computacionais da Prefeitura Municipal.

Segurança Física

A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. A segurança física deve se basear em perímetros predefinidos nas imediações dos recursos computacionais, podendo ser explícita como uma sala-cofre, ou implícita, como áreas de acesso restrito. A segurança física pode ser compreendida em dois aspectos: a) Segurança de acesso - trata das medidas de proteção contra o acesso físico não autorizado; b) Segurança ambiental – trata da prevenção de danos por causas naturais.

Segurança Lógica

A segurança lógica é um processo pelo qual um sujeito ativo deseja acessar um objeto passivo. O sujeito é um usuário ou um processo da rede e o objeto pode ser um arquivo ou outro recurso de rede (estação de trabalho, impressora, etc). A segurança lógica compreende um conjunto de medida e procedimentos, adotados pela empresa ou intrínsecos aos sistemas utilizados. O objetivo é proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas. Na segurança lógica, pretende-se proteger recursos e informações referentes a: Aplicativos (Programas fonte e objeto); Arquivos de dados; Utilitários e Sistema Operacional; Arquivos de senha; Arquivos de log.

Sistema

Para os efeitos desta instrução normativa, a palavra sistema terá o seguinte conceito: “Um conjunto organizado de componentes para coletar, transmitir, armazenar e processar dados de modo a fornecer informação para ação.” (Zwass; 1998).

Dados e Informações

De acordo com o Dicionário Contemporâneo da Língua Portuguesa, informação vem do latim informativo, onis, ("delinear, conceber idéia"), ou seja, dar forma ou moldar na mente, como em educação, instrução ou treinamento. Para esta instrução normativa, informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação

(quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe. As palavras informação e dados são intercambiáveis em muitos contextos. Porém, não são sinônimos. Por exemplo, de acordo com a observação de Adam M. Gadomski (1993), dados é tudo que pode ser processado e as informações são dados que descrevem um domínio físico ou abstrato.

Processamento de Dados

Conceitua-se como Processamento de Dados uma série de atividades ordenadamente realizadas, que resultará em uma espécie de arranjo de informações, pois no início da atividade é feita a coleta de informações, ou dados, que passam por uma organização onde no final será passada para o usuário o dado pertinente a sua busca.

IV - BASE LEGAL E REGULAMENTAR

1 - Constituição Federal;

V - RESPONSABILIDADES

1 - Unidade Responsável pela Instrução Normativa

1.1 - Promover a divulgação da Instrução Normativa, mantendo-a atualizada; Orientar as áreas executoras e supervisionar sua aplicação;

1.2 - Promover discussões técnicas com as unidades executoras e com a unidade responsável pela coordenação do controle interno, para definir as Rotinas de trabalho e os respectivos procedimentos de controle que devem ser objeto de alteração, atualização ou expansão.

2 - Unidades Executoras

2.1 - Atender as solicitações da unidade responsável pela Instrução Normativa (Assistência Social), quanto ao fornecimento de informações e à participação no processo de atualização;

2.2 - Alertar a unidade responsável pela Instrução Normativa sobre as alterações que se fizerem necessárias nas rotinas de trabalho, objetivando a sua otimização, tendo em vista, principalmente, o aprimoramento dos procedimentos de controle e o aumento da eficiência operacional;

2.3 - Manter a Instrução Normativa à disposição de todos os funcionários da unidade, velando pelo fiel cumprimento da mesma;

2.4 - Cumprir fielmente as determinações da Instrução Normativa, em especial quanto aos procedimentos de controle e quanto à padronização dos procedimentos na geração de documentos, dados e informações.

3 - Unidade Responsável pela Coordenação do Controle Interno

3.1 - Prestar apoio técnico por ocasião das atualizações da Instrução Normativa, em especial no que tange à identificação e avaliação dos pontos de controle e respectivos procedimentos de controle;

3.2 - Através da atividade de auditoria interna, avaliar a eficácia dos procedimentos de controle inerentes ao STI, propondo alterações na Instrução Normativa para aprimoramento dos controles.

VI - PROCEDIMENTOS

1 - Obrigações e Permissões dos Usuários

1.1 - Para utilizar os computadores e obter acesso ao correio eletrônico, Internet da rede corporativa do Município, software, aplicativos e pastas em geral, o usuário deverá solicitar com antecedência, ao Secretário da Unidade Administrativa, a abertura de uma conta de acesso (login) e senha;

1.2 - Toda conta de acesso é atribuída a uma única pessoa e será de responsabilidade e uso exclusivo de seu titular, não podendo esse permitir ou colaborar com o acesso aos recursos computacionais por parte de pessoas não autorizadas e nem compartilhar com outros usuários;

1.3 - O perfil de acesso dos usuários aos aplicativos e sistemas será o necessário para o desempenho de suas atividades;

1.4 - O usuário será responsável pela segurança de sua conta de acesso e senha, pelas informações armazenadas nos equipamentos dos quais faz uso e por qualquer atividade neles desenvolvida;

1.5 - As contas inativas por mais de 30 (trinta) dias serão desabilitadas. O usuário que pretende preservar seus dados deverá comunicar ao secretário da pasta seu afastamento com antecedência;

1.6 - Em caso de demissão, licença ou transferência, esta deverá ser comunicada com antecedência ao departamento de TI pelo secretário da pasta.

1.7 - As contas de acesso dos prestadores de serviços e servidores temporários deverão ser automaticamente bloqueadas na data do término do contrato.

2 - Estações de Trabalho e Componentes

2.1 - O usuário deverá executar somente tarefas e aplicações que estejam dentro do escopo de trabalho de seu Setor, utilizando os programas e equipamentos com zelo e responsabilidade;

2.2 - Caberá aos usuários comunicar imediatamente a Administração quaisquer problemas que venham ocorrer, bem como relatar qualquer suspeita de uso inadequado dos recursos computacionais;

2.3 - Não será permitido aos usuários alterar, configurar ou remanejar estações de trabalho e periféricos de seus locais de instalação sem o conhecimento da TI.

2.4 - Não deverão ser conectados *Notebooks*, Laptops ou outros equipamentos aos computadores da administração pública municipal sem o conhecimento da Secretaria Municipal de Administração e Planejamento;

2.5 - Os usuários, a menos que tenham uma autorização específica para esse fim, não poderão tentar permitir causar qualquer alteração ou destruição de ambientes operacionais, dados ou equipamentos de processamento ou comunicações instalados na administração pública municipal;

2.6 - Com exceção das estações de trabalho, impressoras e estabilizadores, os usuários não poderão ligar desligar fisicamente ou eletricamente equipamentos da administração pública municipal sem autorização prévia da Secretaria Municipal de Administração e/ou Departamento de Tecnologia da Informação, especialmente os equipamentos de rede, como *Switches e Hubs*, servidores e *routers*;

2.7 - Não será permitida a utilização dos recursos computacionais para benefício próprio ou de terceiros, direto ou indireto sem a liberação do secretário da Unidade Administrativa, sujeitando-se o infrator a imediata suspensão de sua chave de acesso, sem prejuízo da aplicação das demais penalidades cabíveis previstas no Estatuto dos Servidores Municipais;

2.8 - Os usuários deverão manter os equipamentos nas suas perfeitas condições de uso na forma como lhes foram entregues, evitando a colagem de adesivos ou outros enfeites particulares e realizando a devida limpeza física superficial sobre os equipamentos;

2.9 - Não deverão colocar objetos sobre os equipamentos de forma a prejudicar o seu sistema de ventilação, assim como manipular líquidos, alimentos ou substâncias que possam ocasionar danos quando os estiver operando;

2.10 - O usuário deverá encerrar sua sessão (desligar ou fazer *logout*) na estação de trabalho ao término de suas atividades, devendo, no final do expediente, a estação de trabalho permanecer desligada, bem como sua impressora e demais periféricos;

3 - Programas e Softwares

3.1 - Os usuários não poderão instalar ou fazer "*upgrade*" de qualquer espécie de programas ou aplicativos nas estações de trabalho sem aprovação do secretário da pasta.

3.2 - Quaisquer instalação, após devida aprovação, deverá ser comunicada ao Departamento de Informática, que deverá ser analisada com intuito de não causar conflito com banco de dados e outros softwares;

3.3 - Não será permitido carregar e executar qualquer tipo de jogos, áudios ou vídeos bem como armazenar tais arquivos no servidor ou na estação de trabalho que não seja compatível com as atividades desenvolvidas pelo Setor;

3.4 - De forma a zelar pela segurança do seu computador, sempre que o programa de antivírus enviar mensagem informando que algum arquivo está infectado por vírus, o usuário deverá informar imediatamente ao departamento de Tecnologia da Informação- TI;

3.5 - Não será permitido o uso, para fins particulares ou de recreação, de serviços que sobrecarreguem a rede computacional tais como: rádios on-line, páginas de animação, visualização de apresentações, vídeos, jogos, conteúdo pornográfico, entre outros.

4 - Ambiente de Rede

4.1 - O Departamento de Tecnologia da Informação disponibilizará os pontos de rede necessários ao desenvolvimento das atividades dentro de seus prédios, devendo, para qualquer alteração ou criação de um ponto novo ser comunicado num tempo hábil;

4.2 - É expressamente proibido do uso de meios ilícitos de acesso aos computadores, sistemas e arquivos do ambiente de rede computacional municipal.

4.3 - É proibido o acesso remoto aos computadores da rede pública municipal sem o conhecimento ou consentimento do usuário, salvo se autorizado pelo secretário da pasta;

4.4 - Não deverá utilizar quaisquer materiais ou informações, incluindo arquivos, textos, planilhas ou imagens disponíveis na rede corporativa do Município, que não respeitem os direitos autorais, marcas registradas, patentes, sigilos comerciais ou outros direitos de propriedade intelectual de terceiros;

4.5 - Ficará proibido tentar burlar a utilização dos recursos computacionais do Município com o objetivo de obter proveito pessoal ou violar sistemas de segurança estabelecidos.

5 - Correio Eletrônico (E-Mail)

5.1 - O acesso ao sistema de correio eletrônico será disponibilizado aos usuários com necessidade manifesta de usá-lo como ferramenta de apoio às atividades profissionais, podendo ocasionalmente ser utilizado para mensagens pessoais curtas e pouco frequentes.

5.2 - Não será permitido participar, criar, ou distribuir voluntariamente mensagens indesejáveis, como circulares, manifestos políticos, correntes de cartas ou similares que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas computacionais desnecessariamente;

5.3 - Ficar  proibido utilizar os servios para envio de **SPAM**, ou seja, o envio em massa de e-mails para usu rios que n o os solicitaram de forma expl cita e com os quais o remetente n o mantenha qualquer v nculo de relacionamento profissional e cuja quantidade comprometa o bom funcionamento dos servidores de E-Mail;

5.4 - N o ser  permitido o uso de endereos de E-Mail para troca de informaoes ligadas a pr ticas que infrinjam qualquer lei nacional ou internacional;

5.5 - O usu rio n o dever  abrir E-Mails com arquivos anexados quando n o conhecer o remetente sob o risco de estar infectando com v rus seu equipamento.

6 - Internet

6.1 - O uso da Internet dever  ser controlado e restrito  s atividades profissionais, no sentido de manter os mais altos n veis de qualificaao em prol da atualizaao da informaao;

6.2 - Ser  inaceit vel utilizar-se dos servios internos de Internet do Munic pio desvirtuando sua finalidade, com o intuito de cometer fraudes;

6.3 - Ficar  expressamente proibido visualizar, criar, postar, carregar ou encaminhar quaisquer arquivos ou mensagens de conte dos abusivos, obscenos, insultuosos, sexualmente tendenciosos, pornogr ficos, ofensivos, difamat rios, agressivos, ameaadores, vulgares, racistas, de apologia ao uso de drogas, de incentivo   viol ncia ou outro material que possa violar qualquer lei aplic vel;

6.4 - N o ser  permitido acessar salas de bate-papo (*chat rooms*), exceto se o acesso for necess rio para realizaao das atividades do Setor;

6.5 - N o ser  permitido desfrutar de quaisquer ferramentas *Peer-to-Peer* para baixar m sicas, v deos ou jogos, tais como: *E-Mule, Kazaa, IMesh, Ares, AudioGalaxy, WinMX, Gnutella, LimeWire, Ares, utorrent, aceleradores de download* e outros;

6.6 - N o ser  permitido fazer download de arquivos cujo conte do n o tenha relaao com as atividades do Setor sem autorizaao do Secret rio da Unidade Administrativa e/ou suporte t cnico do Departamento de Tecnologia da Informaao;

6.7 - Ficar  vedada o download de arquivos de qualquer natureza baseados na tecnologia *Voip (skype)* salvo ser for conte do referente ao seu trabalho.

6.8 - Ficar  expressamente proibida a utilizaao de ferramentas que burle a segurana e regras de *proxy/firewall* com o intuito de usufruir de servios que n o lhes s o concebidos, como: ultrasurf;

6.9 - Não será permitida a manutenção não autorizada de páginas pessoais ou de serviços particulares envolvendo comercialização pela Internet utilizando os recursos computacionais do Município.

6.10 - Fica adotado como meio de comunicação oficial para troca de mensagens instantâneas, videoconferências e ligações *VoIP* o “*SKYPE*”.

7 - Armazenamento de Documentos e Informações

7.1 - O usuário deverá manter sigilo sobre os documentos e informações considerados estratégicos, confidenciais ou de interesse particular da administração pública municipal;

7.2 - Os documentos e informações considerados estratégicos ou confidenciais deverão ser armazenados nos diretórios pessoais em pasta devidamente identificada por Secretaria;

7.3 - O usuário deverá informar ao seu superior imediato quando informações ou aplicações consideradas estratégicas ou confidenciais forem encontradas sem o tratamento de segurança correto;

7.4 - O diretório C:\ não deverá ser utilizado pelo usuário para guardar documentos importantes ou confidenciais, sob risco de perdê-los a qualquer tempo. Músicas, fotos, vídeos ou imagens também não serão permitidos;

7.5 - Os documentos e informação geradas pelos usuários referentes as rotinas de trabalho, no que diz respeito à alterações, gravações e leituras, são de inteira responsabilidade dos usuários do arquivo;

7.6 - Os arquivos do diretório C:\ poderão ser removidos sempre que não condizer com assuntos importantes da Administração, independentemente do seu conteúdo.

8 - Advertências e Penalidades

8.1 - Os usuários deverão estar cientes das regras e normas de uso dos recursos computacionais, evitando, desse modo, os procedimentos que prejudicam ou impedem outras pessoas de terem acesso a esses recursos ou de usá-los de acordo com o que é determinado;

8.2 - Todo servidor que tiver conhecimento de ato ilícito praticado no uso dos recursos computacionais, assim como qualquer comportamento considerado inaceitável ou suspeito de violação dessas normas, deverá comunicar o fato imediatamente à seu superior imediato, ao controle interno e/ou Suporte Técnico;

8.3 - A Administração se resguardará do direito de monitorar e interferir no tráfego de mensagens da administração pública municipal, sempre que julgar necessário e sem aviso prévio, com o propósito de verificar o cumprimento dos padrões de segurança, além de fiscalizar e auditar todos os equipamentos eletrônicos, ambiente de rede, Internet, contas de correio eletrônico corporativas.

9 - Responsabilidades do Departamento de Tecnologia da Informação

9.1 - Cabe ao Departamento de Tecnologia da Informação definir as pessoas que poderão ter acesso físico e lógico ao servidor da rede e tomar as medidas necessárias para inibir o acesso aos funcionários, cujas concessões, lhe foram total ou parcialmente alteradas ou canceladas;

9.2 - O Departamento de Tecnologia da Informação deverá avaliar e definir a ordem de relevância de cada aplicativo, segundo o grau de dependência da organização de cada um deles, atentando para as medidas de segurança para os mais importantes;

9.3 - Quando se fizer necessário, o Departamento de Tecnologia da Informação deverá fazer os encaminhamentos para a aplicação de penalidades, nos casos constatados de violações aos ambientes de processamento de dados e demais inobservâncias a presente instrução normativa;

9.4 - Com respeito a segurança lógica, deverá ser feita a manutenção de cópias (*Back-Up*) de segurança dos sistemas em local seguro e protegido contra sinistros, com execução de testes periódicos objetivando aferir se em caso de emergência, os arquivos disponíveis possibilitariam a retomada integral do processamento de dados;

9.5 - Orientar as áreas usuárias na definição dos arquivos (*Back-up*) operacional e de segurança, na proteção contra o acesso não autorizado aos aplicativos, para consulta e/ou atualização, em nível de diretórios, sistema, rotina/programa, arquivo ou dado;

9.6 - Definir em conjunto com as unidades geradoras de documentos e arquivos, das unidades que poderão ter acesso aos mesmos via rede, por tipo de documento ou informação e manutenção das tabelas para liberação do acesso;

9.7 - Efetuar a manutenção do funcionamento, segurança e confiabilidade da rede interna, com análise regular dos registros de sua utilização, com investigação sobre as tentativas bloqueadas de acesso;

9.8 - No tocante a segurança física, o Departamento de Tecnologia da Informação deverá definir as medidas para a proteção física do acervo de processamento de dados da Prefeitura Municipal, a serem observadas durante e fora do expediente normal, por todas as unidades usuárias;

9.9 - Orientar e monitorar as medidas de proteção contra incêndio nos locais de instalação dos equipamentos dos usuários;

9.10 - Elaborar e manter atualizado o plano de contingência, estabelecendo as ações e prioridades para a retomada do processamento de dados no caso de sinistro ou situação assemelhada.

10 - Responsabilidades das Unidades Usuárias dos Recursos Computacionais

10.1 - Cada Unidade Usuária deverá zelar pela manutenção do registro de todo o *software* básico e aplicativos instalados nos equipamentos sob sua responsabilidade;

10.2 - Supervisionar e gerenciar a execução das tarefas de tecnologia da informação, incluindo a definição das pessoas que poderão ter acesso (físico e lógico) aos equipamentos e respectivos *software* instalados na unidade.

10.3 - Definir os níveis de acesso (consulta/atualização) aos diretórios, sistemas, rotinas/programas, arquivos e dados, para todos os aplicativos de responsabilidade de sua área;

10.4 - Fazer o registro, gerenciamento da concessão e atualização, bem como, o controle sobre a utilização das senhas, com estabelecimento de procedimentos e responsabilidades dos usuários pelo sigilo das mesmas;

10.5 - Estabelecer os procedimentos e critérios para a definição de senhas e manutenção das mesmas;

10.6 - Definir a frequência do back-up operacional e da geração de cópia de segurança dos arquivos, com realização de testes periódicos;

10.7 - Conceder autorização do acesso a dados e informações, via rede, pelos diversos usuários, aos sistemas e/ou aplicativos cuja operação é de sua competência, mantendo o registro das autorizações concedidas;

10.8 - Fazer a utilização do produto de antivírus de acordo com as instruções recebidas do Departamento de Tecnologia da Informação;

10.9 - Observar todas as medidas de controle de acesso físico e de proteção contra incêndio nos locais de instalação dos equipamentos, de acordo com as definições do Departamento de Tecnologia da Informação, constantes desta Instrução Normativa;

10.10 - Comunicar ao Departamento de Tecnologia da Informação todas as situações que ensejarem manutenção da rede e dos equipamentos de processamento de dados sob sua responsabilidade.

VII - CONSIDERAÇÕES FINAIS

1 - Os termos contidos nesta Instrução Normativa, não exime a observância das demais normas competentes, que deverão ser respeitadas.

2 - Ficará a cargo da Coordenadoria de Controle Interno Municipal, unificar e encadernar, fazendo uma coletânea das instruções normativas, com a finalidade elaborar o Manual de Rotinas

Internas e Procedimentos de Controle, atualizando sempre que tiver aprovação de novas instruções normativas, ou alterações nas mesmas.

3 - Os esclarecimentos adicionais a respeito deste documento poderão ser obtidos junto a Assessoria Jurídica e Coordenadoria de Controle Interno Municipal que, por sua vez, através de procedimentos de checagem (visitas de rotinas) ou auditoria interna, aferirá a fiel observância de seus dispositivos por parte das diversas unidades da estrutura organizacional.

4 - A inobservância das normas estabelecidas nesta Instrução Normativa pelos agentes públicos acarretará instauração de processo administrativo para apurar responsabilidade conforme rege o Estatuto dos Servidores Públicos Municipais e demais sanções previstas na legislação pertinente à matéria em vigor.

5 - As publicações deveram estar de acordo com esta Instrução Normativa e os responsáveis pelas publicações devem atentar-se para o atendimento pleno das disposições contidas nesta Norma Interna.

6 - As administrações indiretas poderão utilizar o site oficial da Prefeitura para fazer suas publicações de forma eletrônica;

Esta Instrução Normativa entra em vigor a partir de sua aprovação.

Denise-MT, 30 de Dezembro de 2011.

José Pedro dos Santos Neto
Controlador Interno Interino

De acordo:

José Roberto Torres
Prefeito Municipal

Aprovada em: 30/12/2011

O conteúdo desta Instrução Normativa (ou desta nova versão) foi levado ao conhecimento do Chefe de Poder em 30/12/2011.

Publicada no Mural da Unidade Gestora e Site do Município.