DECRETO N.º 552 DE 04 DE OUTUBRO DE 2007.

Dispõe sobre a Política de Segurança de Informações do Município de Petrópolis e dá outras providências.

CONSIDERANDO a infra-estrutura de informática e conectividade implantada com recursos do PMAT – Programa de Modernização Administrativa e Tributária do BNDES;

CONSIDERANDO a implantação de um Sistema Integrado de Gestão do Município, interligando as atividades tributárias, administrativas e financeiras;

CONSIDERANDO a necessidade de estabelecer uma política de uso e de acesso à informação no âmbito da Administração Direta do Município;

CONSIDERANDO a importância de tratar a informação da administração pública de forma segura e confiável, para melhor atender ao cidadão.

O Prefeito no uso das atribuições que lhe são conferidas pela legislação em vigor,

DECRETA

C A P Í T U L O I

D I S P O S I Ç Õ E S I N I C I A I S

Art. 1º. Fica estabelecida a Política de Segurança de Informações para o Município que tem como objetivo reduzir riscos de ocorrência de perdas e alterações indevidas nos dados, preservando a confidencialidade, a integridade e a disponibilidade das informações armazenadas digitalmente nos órgãos da Administração Pública, bem como assegurar a continuidade das atividades, evitando acesso e utilização indevidos.

Art. 2º. A Secretaria de Controle Interno e a Secretaria de Planejamento e Desenvolvimento Econômico através do Departamento de Tecnologia da Informação - DETEC, proporão as regras básicas e os controles de segurança a fim de estabelecer um nível aceitável de proteção das informações.

Art. 3º. As diretrizes da Política de Segurança de Informações serão auditadas, periodicamente, pela Secretaria de Controle Interno.

C A P Í T U L O I I
D O S P R I N C Í P I O S D A S E G U R A N Ç A

Art. 4º. Com relação ao tratamento de informações:

I.As informações são de propriedade do Município, e como tal, devem ser tomadas as medidas necessárias para protegê-las de alteração, destruição ou divulgação não autorizadas, quer seja acidental ou intencional.

II.Toda informação deve ter um gestor que definirá a sua classificação, a autorização de acessos e o cancelamento dos mesmos. A Secretaria de Controle Interno e o SPE/DETEC proverão o suporte necessário aos gestores para a definição da classificação das informações.

III. As informações devem ser classificadas, quanto a confidencialidade, integridade e disponibilidade, e identificadas de forma a serem adequadamente acessadas, manipuladas, armazenadas, transportadas e descartadas.

IV.Funcionários públicos e prestadores de serviço devem garantir o sigilo das informações a que tiverem acesso, tomando o cuidado necessário quanto a sua divulgação interna e externa, avaliando o seu respectivo nível estratégico. Esta ação deve ser formalizada através da assinatura de um Termo de Sigilo e Confidencialidade no ato da sua respectiva contratação, junto ao Departamento de Recursos Humanos da Secretaria de Administração.

V.Todos os processamentos executados nos Sistemas de Informação do Município de Petrópolis deverão ter suas responsabilidades conhecidas e distribuídas de forma a não serem concentrados em um mesmo grupo ou pessoas.

Art. 5º. No tocante ao controle de acesso:

I. Todo funcionário público ou pessoa autorizada deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida através dela.

II. A concessão de autorização de acesso deverá ser restrita aos recursos mínimos necessários para que os usuários desenvolvam suas atividades.

III. Prestadores de Serviço devem possuir acesso com prazo limitado à execução de suas atividades.

IV. Quando do desligamento de um funcionário, o DETEC deve ser informado pelo seu superior para que sua identificação deva ser automaticamente desativada, de tal modo que o mesmo não tenha mais acesso aos sistemas, e uma cópia de seus dados deverá ser realizada e mantida por um período de 01 mês, após o qual os mesmos serão definitivamente removidos.

V. Quando ocorrer a alteração de função de um usuário, e esta levar a alguma alteração no nível de acesso aos sistemas, tal alteração deve ser devidamente autorizada e documentada antes de entrar em vigor, através do Formulário de Solicitação de Acesso (anexo III).

Art. 6º. Constituem faltas graves o mau uso de informações, pertencentes ao Município de Petrópolis, e de seus recursos de processamento, ou o não cumprimento de normas que visem protegê-los, bem como o mau uso da identificação pessoal, por parte do servidor público ou qualquer outro, sob pena de aplicação das sanções administrativas aplicáveis ao caso concreto, previstas na Lei Municipal n.º 3.884, de 15.07.1977 (Estatuto dos Funcionários Municipais), sem prejuízo das sanções cíveis e penais aplicáveis.

Art. 7º. Quanto à capacitação:

I. Os servidores públicos e prestadores de serviço deverão possuir conhecimento mínimo para a execução de suas tarefas, conhecer a Política de Segurança de Informações do Município de Petrópolis, e serem devidamente treinados para o uso da rede e controle dos recursos de informática, antes de terem acesso aos mesmos.

II. A divulgação da Política de Segurança de Informações e a disseminação da cultura de segurança serão efetuadas em conjunto pela Secretaria de Controle Interno e a SPE/DETEC, gerentes e chefes das divisões de informática.

Art. 8º. Quanto à estabilidade do ambiente:

I. A disponibilização de recursos de informática somente será permitida após atendimento às recomendações desta Política e homologação pela área de Informática e a autorização do responsável pelos respectivos recursos. Estes recursos deverão ser identificados de forma individual, inventariados, preservados, protegidos contra acessos indevidos, serem submetidos à manutenção preventiva periódica, estar com documentação atualizada e aprovada pelo setor responsável, e de acordo com as cláusulas contratuais pactuadas com fornecedores e com a legislação em vigor.

II. Os recursos de informática compartilhados deverão ser usados de forma que outros usuários não sejam afetados, e desde que previamente pactuado.

III. Os recursos portáteis, por suas características, devem ser configurados, acondicionados e transportados atendendo às regras de segurança. O usuário do recurso portátil obriga-se à assinatura de Termo de Custódia, a ser elaborado pelo setor competente, que determinará os direitos e deveres quanto à utilização, posse e guarda do recurso e das informações nele armazenadas, junto ao DETEC.

IV. A entrada e saída de qualquer recurso de informática deve ser documentada e aprovada pelo responsável da área de informática local ou pelo Chefe do Núcleo Administrativo de cada secretaria.

V. Os equipamentos de terceiros ou alugados deverão ser identificados junto ao DETEC, e o seu uso deverá estar em conformidade com o disposto na Política de Segurança de Informações. A retirada destes equipamentos deverá ser realizada em conformidade com os procedimentos internos.

VI. Os microcomputadores e impressoras instalados nas diversas secretarias, de forma alguma podem ter alteradas as suas configurações, removidos ou trocados os seus componentes internos e terem instalados programas não autorizados pelo DETEC.

VII. Toda a aquisição de equipamentos e programas de informática deve ser submetida à análise do DETEC, visando atender aos padrões definidos de certificação dos fornecedores, compatibilidade tecnológica adequada à prática do mercado de bens de informática, prazos de garantia, serviços de instalação e configuração, etc.

Art. 9º. Os recursos considerados críticos à atividade fim devem estar resguardados por um plano de contingência que garanta a continuidade dos serviços, previna e solucione situações de anormalidade. O referido plano deve ser documentado e, periodicamente, testado, revisado e sempre que necessário atualizado para atender as modificações ocorridas no ambiente, evitando a indisponibilidade e, conseqüentemente, impacto nas atividades dos usuários internos e externos.

C A P Í T U L O I I I
D A S A T R I B U I Ç Õ E S E D A S R E S P O N S A B I L I D A D E S

Art. 10. Caberá ao Chefe da Divisão de Informática ou Chefe do Núcleo de Apoio Administrativo das secretarias (sob a orientação do DETEC):

I.. Garantir a segurança das informações armazenadas nos equipamentos de sua área ou delegar esta atribuição a outro servidor capacitado;

II. Solicitar ao gestor do sistema a disponibilização e a exclusão das contas de acesso aos sistemas informatizados do Município;

III. Solicitar à Secretaria de Controle Interno e a SPE/DETEC a conta do usuário para o acesso à rede, à internet e de acesso para correio eletrônico dos seus diversos setores, através do Formulário de Solicitação de Acesso (anexo III);

IV. Efetuar o back-up local de acordo com as orientações estabelecidas pelo DETEC;

V. Solicitar ao DETEC o remanejamento ou a inclusão de um novo ponto de rede;

VI. Manter atualizado o antivírus instalado nos equipamentos que compõem o seu ambiente informatizado;

VII. Solicitar suporte técnico ao DETEC sempre que identificar falhas nos equipamentos ativos de rede, microcomputadores e impressoras;

VIII. Solicitar ajuda operacional na utilização dos serviços disponíveis na Intranet, inclusive quanto aos sistemas informatizados.

Art. 11. Caberá ao Gestor do Sistema:

I. Identificar e atribuir os acessos permitidos às funcionalidades dos sistemas informatizados sob sua gestão;

II. Solicitar oficialmente à Secretaria de Controle Interno e a SPE/DETEC, administradores gerais do sistema integrado, o cadastramento e o cancelamento dos usuários e suas permissões por função, através do Formulário de Solicitação de Acesso (anexo III);

III. Participar dos testes paralelos, homologar e autorizar a implantação efetiva dos sistemas sob sua gestão.

Parágrafo Único: Gestor do Sistema deve ser designado em conjunto pela titular da Secretaria de Controle Interno e a SPE/DETEC, levando-se em conta suas atribuições diretamente relacionadas às funcionalidades dos módulos do sistema integrado.

Art. 12. Caberá aos responsáveis no DETEC:

I. Estabelecer condições para uma eficiente, segura e controlada execução de aplicações e armazenamento de informações sob sua custódia;

II. Verificar com regularidade os logs de acesso (registros dos acessos) à Internet e manter os mecanismos de filtros necessários para impossibilitar os acessos indesejáveis;

III. Analisar e homologar os treinamentos necessários para a correta e eficiente utilização dos recursos informatizados;

IV. Autorizar o uso de equipamentos de informática, bem como a conexão de equipamento particular nas redes internas;

V. Solicitar a aquisição e homologar equipamentos e programas utilizados pela Administração;

VI. Instalar programas e sistemas adquiridos ou desenvolvidos pela Administração e configurar as estações de trabalho;

VII. Realizar atualizações tecnológicas e manutenção do ambiente informatizado, segundo os quesitos especificados na Política de Segurança;

VIII. Autorizar a entrada e saída de recursos de sua área ou sob sua custódia, ou delegar essa autoridade a outro servidor;

IX. Garantir a integridade e disponibilidade das informações e dos recursos do ambiente informatizado, segundo os controles estabelecidos;

X. Efetuar backup e guarda das informações e dos códigos-fonte dos sistemas informatizados e em desenvolvimento, bem como autorizar a restauração das

cópias de segurança;

XI. Efetuar backup e guarda das informações referentes aos serviços disponíveis na Intranet;

XII. Manter-se atualizado quanto as possíveis ameaças as quais o ambiente está sujeito, bem como manter-se atualizado sobre novas técnicas que podem ser aplicadas para um melhor funcionamento dos sistemas e ambiente computacional;

XIII. Verificar o cumprimento desta Política e realizar revisões periódicas em conjunto com a Secretaria de Controle Interno.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 13. É responsabilidade de todo servidor público e dos prestadores de serviço deste Município observar desvios dos procedimentos estabelecidos, e informar esses desvios ao responsável imediato.

Art. 14. Estas diretrizes deverão ser revisadas e atualizadas em conjunto pela Secretaria de Controle Interno e a SPE/DETEC, à medida que se agreguem novos valores às atividades da Administração Pública, ou dentro do intervalo de 2 (dois) anos.

Art. 15. Constituem partes integrantes desta portaria os Anexos:

I - Normas Gerais para Usuários;

II - Glossário de Termos Técnicos;

III – Formulário de Solicitação de Acesso.

Art. 16. Este Decreto entrará em vigor na data de sua publicação**.**

Gabinete do Prefeito Municipal de Petrópolis, em 04 de outubro de 2007.

Rubens Bomtempo
Prefeito

Almir Schmidt
Secretário de Planejamento e Desenvolvimento Econômico

ANEXO I

NORMAS GERAIS PARA USUÁRIOS

1. As normas gerais para usuários são um conjunto de regras que determinam a conduta adequada dos servidores públicos e prestadores de serviços, em relação à informação e aos recursos que as suportam, a fim de promover a segurança de informações.

1.1 DO TRATAMENTO DA INFORMAÇÃO

1.1.1. Os recursos da informação não públicos deverão somente ser utilizados por pessoas devidamente autorizadas, sendo o seu uso limitado aos interesses da Administração Pública e para os fins previstos.

1.1.2. Deverá ser mantido sigilo sobre as informações consideradas estratégicas e confidenciais, e mantido informado somente o responsável imediato quando informações ou aplicações críticas forem encontradas sem tratamento de segurança correto.

1.1.3. As informações confidenciais ou críticas à atividade da Administração devem ser armazenadas de forma protegida.

1.1.4. O usuário deverá sempre ter sua sessão de trabalho encerrada e desligados os equipamentos ao se ausentar do ambiente de trabalho. Proteção de tela padronizada deverá sempre ser ativada após 5 minutos sem utilização do equipamento.

1.1.5. O usuário não deve fornecer suas senhas, pois são pessoais e intransferíveis.

1.1.6. É vedada a utilização de recursos de informação não autorizados ou não homologados pela área de informática, cabendo a aplicação de punições previstas na Lei Municipal n.º 3.384 de 15/07/1977 (Estatuto dos Funcionários Municipais), e demais pertinentes à matéria.

1.1.7. Os sistemas e banco de dados somente poderão ser acessados a partir de estações internas ao ambiente e configuradas pela área de informática responsável.

1.1.8. No equipamento servidor das Secretarias e do Centro de Dados, estarão armazenados os documentos de texto, planilhas e qualquer informação que necessite de backup, porém as secretarias que possuírem um banco de imagens (fotos, projetos, mapas, etc.) devem solicitar ao DETEC uma solução específica para o caso.

2 . D O S O F T W A R E

2.1. É terminantemente proibida a utilização de cópias de programas não licenciados, ou qualquer software não autorizado e homologado pela área de informática, nos equipamentos de informática do Município. A Divisão de Informática Setorial ou, na falta desta, o Núcleo de Apoio Administrativo da Secretaria será responsabilizado pela existência deste tipo de software.

2.2. É proibida a cessão, sem autorização formal do responsável da área de informática, de cópia de software adquirido ou desenvolvido pelo Município de Petrópolis para benefício próprio ou de terceiros.

2.3. A cópia de softwares adquiridos ou desenvolvidos pelo Município, para utilização fora do ambiente do mesmo somente poderá ser realizada após concessão formal do Gabinete do Prefeito.

> (2) - Lei 9.609/98 – Estabelece que a violação de direitos autorais é crime, pena de detenção de 6 a 4 anos e multa, além de ser passível de ação cível indenizatória por parte da empresa proprietária do software (Governo Digital – www.codin.rn.gov.br)

3 . H A R D W A R E

3.1. A utilização de equipamentos é restrita àqueles autorizados pela área de informática.

3.2. A conexão de equipamentos particulares nas redes internas deverá ser autorizada pelo responsável da área de informática. Estes equipamentos deverão seguir os padrões de segurança previamente definidos.

4 . I N T E R N E T

4.1. Não são permitidos os acessos a sites em desconformidade com os interesses da Administração Pública.

4.2. A Internet só poderá ser disponibilizada através de uma única porta administrada pelo DETEC, o controle de acesso será baseado no endereço da máquina e na identificação de cada usuário.

4.3. Aos acessos à Internet que burlem estes mecanismos de controle caberá além da aplicação de punição prevista em Lei, a suspensão temporária do seu acesso e em caso de reincidência o seu cancelamento.

4.4. A permissão de download de arquivos, sempre que se fizer necessária será avaliada pelo DETEC.

5 . C O R R E I O E L E T R Ô N I C O

5.1. As mensagens enviadas através da identificação de correio eletrônico do usuário são de sua responsabilidade.

5.2. A utilização do correio eletrônico deve ser realizada em conformidade com os interesses da Administração Pública.

5.3. O usuário deverá sempre remover as mensagens obsoletas e não mais necessárias às suas atividades, em atendimento às cotas de espaço pré-estabelecidas pelo DETEC.

5.4. Todas as mensagens recebidas e a serem enviadas passarão internamente por um filtro antispam e antivírus.

5.5. O usuário deve evitar ao máximo a proliferação e o envio de mensagens não solicitadas (spam), cartões comemorativos, correntes, etc.

5.6. Não será permitido o envio ou recebimento de mensagens contendo arquivos de música, vídeo, jogos e executáveis.

5.7. Cabe ao Chefe da Divisão de Informática ou Chefe do NAA de cada Secretaria, manter atualizada a sua lista de contas de e-mail.

5.8. Após 60 (sessenta) dias de inatividade da conta de e-mail, está será desativada pelo DETEC.

6 . B A C K U P

6.1. O backup das informações armazenadas nas estações de trabalho do usuário é de sua responsabilidade, e para sua garantia deve ser efetuado periodicamente;

6.2. O DETEC manterá uma política específica para o backup dos equipamentos servidores do Centro de Processamento de Dados do Município;

6.3. As Secretarias que não se encontram dentro da abrangência física do Anel de Fibra Óptica terão o backup das informações armazenados, localmente, no servidor de arquivos da mesma, cuja responsabilidade de guarda será do Chefe da Divisão de Informática ou do Chefe do NAA, que deverá organizar e classificar as informações para cópia, identificando as informações críticas, de acordo com as orientações do DETEC.

6.4. O Gestor do Sistema deverá solicitar à área de informática a restauração da cópia de segurança das informações armazenadas nos servidores, que, em caso de tratar-se de informações críticas.

7. CONTROLE DE ACESSO

7.1. Os atos e acessos do usuário às informações e aos sistemas deverão ser realizados através de sua identificação pessoal. Diante a suspeita de perda de sigilo de sua senha, o usuário deverá efetuar a troca da mesma e informar à área de informática e ao chefe imediato.

7.2. O tamanho mínimo da senha será de 06 (seis) caracteres alfanuméricos e, no primeiro acesso após a habilitação, o usuário terá, obrigatoriamente, que substituir por uma senha.

7.3. É proibida a adoção de senhas frágeis pelos usuários, tais como nomes próprios, palavras de vocabulário, siglas, nomes de fabricantes, datas comemorativas, dentre outras.

7.4. O Usuário deverá alterar sua senha a cada 60 (sessenta) dias e não utilizar senhas repetidas.

7.5. Considera-se fraude a tentativa, por um usuário não autorizado, de quebrar a segurança do sistema ou descobrir a senha de outros usuários, e será aplicada punição prevista em lei.

7.6. Os usuários terão direito apenas aos privilégios necessários para o desempenho de suas atividades, os quais deverão ser solicitados pelos gestores do sistema ou responsáveis imediatos.

7.7. Terceiros, ou prestadores de serviços, deverão ter identificação com prazo de validade temporário, de acordo com o projeto ou contrato estabelecido.

8. DESCARTE DE INFORMAÇÕES

8.1. Os arquivos e informações que não sejam mais necessários deverão ser removidos do ambiente operacional de forma segura e irrecuperável.

8.2. Informações críticas ou confidenciais deverão ser descartadas com a destruição irrecuperável da mesma.

9. PADRONIZAÇÃO

9.1. É proibido alterar a configuração da estação de trabalho sem autorização da área de

informática. Os usuários devem respeitar os padrões de hardware e software implementados.

9.2. Somente o responsável pela área de informática, ou alguém designado por ele, poderá realizar atualizações tecnológicas no ambiente informatizado.

10. COMBATE A VÍRUS

10.1. As estações de trabalho deverão, obrigatoriamente, ter o antivírus padrão instalado, configurado, ativado e atualizado.

10.2. O usuário deverá informar imediatamente à área de informática e ao responsável imediato em caso de ocorrência de vírus.

11. ATENDIMENTO AO USUÁRIO

11.1. O usuário deverá acompanhar os técnicos de informática quando ocorrer a manutenção corretiva nos equipamentos sob sua responsabilidade ou nas suas estações de trabalho.

11.2. A prioridade de atendimento será concedida aos equipamentos e aplicações críticas às atividades da Administração.

12. SEGURANÇA FÍSICA

12.1. A entrada e saída de pessoas não pertencentes aos ambientes críticos deverão ser registradas, bem como prestadores de serviço deverão estar devidamente identificados através do uso de crachás, os quais deverão estar sempre visíveis.

12.2. A sala de servidores, ou Centro de Dados, tem o acesso restrito aos seus administradores ou pessoas autorizadas e acompanhadas por eles.

12.3. É proibido alimentar-se e fumar próximo aos equipamentos de informática.

ANEXO II

GLOSSÁRIO DE TERMOS TÉCNICOS

O B J E T I V O

Este manual descreve as definições dos termos e expressões constantes deste Decreto e seus anexos da Política de Segurança de Informações da Administração Direta.

D E F I N I Ç Õ E S

Acesso Físico: Trânsito (entrada ou saída) de pessoas em um ambiente seja uma sala, um cofre ou uma área.

Acesso Lógico: Procedimento através do qual é permitido a um usuário do ambiente de informática o acesso às informações armazenadas em meio magnético. Somente deverá ser liberado quando atender todos os mecanismos de proteção disponíveis na instalação.

Acesso Remoto: A capacidade de se conectar a uma rede utilizando recursos de uma localização distante. Geralmente, isso implica o uso de um computador, um modem e algum software de acesso remoto (ssh, por exemplo) para estabelecer conexão ao servidor de rede.

Administração de Dados: Responsável por garantir a integridade dos dados, nos assuntos relacionados à Administração Pública, buscando a integração e divulgação destes dados através da identificação e organização do Modelo Global.

Administrador de Rede (ou Sistemas): Pessoa cuja função principal é gerenciar, monitorar e configurar a rede, ou o sistema, e mantê-los funcionando de forma satisfatória.

Ambiente Computacional: Ambiente lógico composto de software e controlado por sistemas operacionais.

Ambiente Informatizado: Ambiente físico onde se localizam estações de trabalho, servidores de rede e equipamentos de apoio que provêem o processamento e o armazenamento das informações.

Ambiente Operacional: Ambiente onde são executados os aplicativos e sistemas da Administração.

Antivírus: *Software* que identifica e remove vírus de computador.

Aplicação Crítica: Aplicação que atualiza valores concede autorizações de acesso e/ou trata de informações classificadas como sigilosas ou vitais para a execução das atividades fim da Administração.

Aplicativo (ou **Aplicação):** Programa ou grupo de programas adquiridos ou desenvolvidos para determinado fim, tais como processador de textos, sistema de banco de dados, planilha eletrônica e sistemas específicos.

Área de Informática: Área responsável pelo processamento e armazenamento da informação. Cumpre regras especificadas pelo DETEC.

Arquivo de Log (ou simplesmente **Log):** Arquivo em que são gravados registros relativos a transações executadas em um serviço informatizado.

Backup (ou Cópia de Segurança): Um substituto ou alternativa para um recurso. O termo *backup* refere-se, usualmente, a um disco ou fita que contém uma cópia de informações.

Base de Dados: São informações organizadas, inter-relacionadas e armazenadas em meio magnético.

Chave de Acesso: Identificação do usuário (*user-id*) do ambiente computacional.

Classificação da Informação: É o grau de confidencialidade de uma informação (confidencial, restrita, pública) e a que tipo de tratamento ela está sujeita (identificação, acesso, distribuição, uso em correios e fax, reprodução, estocagem, descarte e transporte).

Correio Eletrônico (ou e-mail): Serviço de comunicação que consiste na troca de mensagens através de redes de computadores.

Download: Jargão usado para descrever a gravação de um programa no computador do usuário a partir de um site na internet. Por analogia, é usado com relação a uma página de um site, para se dizer que as informações foram exibidas na tela do usuário.

Equipamento Crítico: Dispositivo que armazena informações classificadas como críticas ou que possui sistema de emulação ou ainda que executa aplicações críticas.

Estação de Trabalho: Refere-se a qualquer computador conectado a uma rede.

Ferramenta de Segurança: Dispositivo de *hardware* ou *software* destinado a proteger e controlar os acessos ao conjunto de informações da empresa, de acordo com a política de segurança estabelecida.

Firewall: Dispositivo de segurança que, uma vez instalado, controla e autoriza o tráfego de informações transferidas entre redes.

Gestores do Sistema: Usuário proprietário da informação, sendo responsável pela sua criação e classificação, pelos recursos sob sua responsabilidade, pela validação, liberação e cancelamento do acesso aos recursos e aos locais restritos da sua Unidade, bem como por definir os perfis de acesso dos usuários.

Hardware: Equipamento físico ou dispositivo mecânico, elétrico ou eletrônico, que compõem os equipamentos computacionais.

Homologação: Análise da funcionalidade, testes e aprovações necessárias para a implantação de recursos informatizados.

Informação Confidencial: É toda informação cujo conhecimento deve ficar limitado a uma quantidade reduzida de pessoas autorizadas. Este tipo de informação requer alto grau de controle e proteção contra acessos não-autorizados.

Informação Crítica: É toda informação considerada vital para a continuidade dos processos e operações do Município, cuja perda ou indisponibilidade por um determinado período de tempo provoca prejuízos irreparáveis para a mesma.

Informação Pública: É toda informação cujo conhecimento não necessita ser limitado à determinada quantidade de pessoas, sejam elas servidores públicos municipais, prestadores de serviço ou não. São informações que tem acesso por qualquer cidadão, desde que por ele requerida.

Informação Restrita: É toda informação cujo conteúdo deve ter seu acesso limitado a quem é parte desta informação.

Integridade: Capacidade efetiva de a informação estar intacta e garantida contra perda, dano ou modificação não autorizada (indevida), realizada maliciosa ou acidentalmente.

Internet: Rede de computadores de alcance mundial conectados entre si. Considerada a "rede das redes", originalmente criada nos EUA, se tornou uma associação mundial de redes interligadas.

Intranet: Rede de computadores interna de uma empresa ou instituição que usa a tecnologia da internet.

Login (ou **log on**)**:** Procedimento para que um sistema de computador ou uma rede reconheça o usuário de tal forma que ele possa iniciar uma sessão de trabalho.

Manutenção Preventiva: Conjunto de operações para revisão, inspeção e limpeza dos recursos informatizados, objetivando corrigir, reparar pequenas falhas e manter a sua conservação.

Mídia: Dispositivos nos quais as informações podem ser armazenadas. Isto inclui *hard disks* (ou *winchester*), *floppy disks* (ou *disquetes*), CD-ROMs e fitas magnéticas. Em redes de computadores, mídia refere-se também aos cabos (ex.: cabo coaxial, fibra ótica) que interligam estações de trabalho.

Rede: Um grupo de dois ou mais sistemas de computador interligados. Quanto à disposição dos computadores, as redes podem ser classificadas como: **Local Area Network (LAN)** – os computadores estão geograficamente próximos (geralmente, no mesmo prédio); **Wide Area Network (WAN)** – os computadores estão mais distantes, uns dos outros, e são conectados através de linhas telefônicas, ondas de rádio ou via satélite.

Senha: Uma série secreta de caracteres que habilita um usuário para acesso a um arquivo, computador ou programa. A senha autentica a identidade de uma chave de acesso.

Sistema: Um conjunto de várias funções interligadas que automatiza um processo.

Sistema Operacional: É o principal programa do computador e responsável pelo controle do equipamento em si, gerenciando o uso dos dispositivos (memórias, drives) e demais programas (processadores de texto, planilhas de cálculos) e demais periféricos (impressora e scanner, discos).

Software: Conjunto de programas, procedimentos, regras e documentação referentes à operação de um sistema, armazenado eletronicamente. Ex.: sistemas aplicativos, montadores, compiladores, sub-rotinas.

Software Homologado: S*oftware* certificado tecnicamente pela Área de Informática em relação à aderência e compatibilidade com o ambiente informatizado do Município.

Software Licenciado: Refere-se, genericamente, a programas, dados e documentação de propriedade do Município e/ou protegidos por direitos autorais (*copyright*).

Spam: É o e-mail com finalidades comerciais que chega sem autorização do usuário.

Upload: O contrário de download. Transferência do computador pessoal para um servidor localizado remotamente.

Usuário: Qualquer pessoa que foi autorizada pelo Gestor, a ler, inserir ou atualizar informações.

Vírus: Um programa ou pedaço de código que é introduzido em um computador sem conhecimento do usuário e, quando executado, corrompe a operação normal do sistema. Todos os vírus de computador são fabricados. Um simples vírus que pode copiar a si próprio continuamente é relativamente fácil de produzir. Mesmo um vírus simples é perigoso porque ele pode rapidamente utilizar toda a memória disponível e levar o sistema a uma interrupção. O tipo mais perigoso de vírus é aquele capaz de reproduzir-se através da rede e burlar sistemas de segurança.

ANEXO III

Formulário de Solicitação de Acesso