INSTRUÇÃO NORMATIVA STI - Nº. 018/2012

Versão: 01
Aprovação em: 21/11/2012
Ato de aprovação: Resolução 012/2012
Unidade Responsável: Sistema Tecnologia da Informação

I – FINALIDADE

Dispor sobre as normas gerais e procedimentos no tocante à segurança física e lógica dos equipamentos, sistemas, dados e informações da Câmara Municipal de Primavera do Leste/MT.

II – ABRANGÊNCIA

Abrange a Coordenadoria de Administração - CAD enquanto unidade responsável e todas as unidades da estrutura organizacional, definida na Resolução nº 010/2011, como unidades executoras, em especial, a Divisão de Operação e Manutenção de Programas – DOMPR.

III – CONCEITOS

1 Informação: É todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

2 Tecnologia da Informação - TI: É a área de conhecimento responsável por criar, administrar e manter a gestão da informação através de dispositivos e equipamentos para acesso, operação e armazenamento dos dados, de forma a gerar informações para tomada de decisão.

3 Segurança da Informação: Está relacionada com a proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade das Informações supostas.

4 Segurança Física: É a segurança em nível das infra-estruturas materiais. Abrange todo o ambiente onde os sistemas de informação estão instalados.

- **Ameaças Físicas:** Incêndios, desabamentos, relâmpagos, alagamentos, acesso indevido de pessoas, forma inadequada de tratamento e manuseio do Material,
- **Mecanismos de Segurança Física:** Portas, trancas, paredes, revestimento em equipamento, blindagem, guardas, extintores, saída de emergência; etc;
- **Controle de Acesso:** Tudo aquilo que rege os recursos e autorizações e as suas restrições de acessos aos ativos de informações e acesso à internet.

5 Segurança Lógica: É a forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação.

- **Ameaças Lógicas:** Vírus acessos remotos à rede, backup desatualizados, violação de senhas, etc.
- **Mecanismos de segurança Lógica:** Detectores de intrusões, anti-vírus, firewalls, firewalls locais, filtro anti-spam, fuzzers, analisadores de código, etc.
- **Ameaças a Perda da Confidencialidade:** Quando houver a perda ou quebra do sigilo de uma determinada informação sendo por sua vez senha, logins, e acessos remotos;
- **Ameaças a Perda da Integridade:** Sendo quando a exposição de uma determinada informação por alguma pessoa ou individuo não autorizado perante os setores;
- **Ameaças a Perda de Disponibilidade:** Este acontece quando a informação deixa de estar acessível por quem necessita dela.

6 Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou dados corrompidos ou equipamentos danificados.

7 Usuário: Pessoa física cadastrada em um ou mais sistemas informatizados para acesso a informações.

8 Cadastro: Procedimento de criação de usuário (Login/ID) para acesso aos sistemas informatizados.

9 Senha: Conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e a permitir seu acesso aos dados, programas e sistemas não disponíveis ao público, de uso pessoal e intransferível.

IV – BASE LEGAL E REGULAMENTAR

A presente Instrução Normativa integra o conjunto de ações, de responsabilidade do Chefe do Poder Legislativo, no sentido de atendimento aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, dispostos no Artigo 37 da Constituição Federal.

Amparado nos artigos 31, 70 e 74 da Constituição Federal, bem como no projeto de Lei da Câmara dos Deputados nº 1.713, de 1996 – que dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores, na Norma Internacional de Segurança da Informação ISO/IEC 17799:2000, na Versão Aplicada aos países da língua portuguesa NBR

ISSO/IEC 17799, além de outras normas que venham assegurar o cumprimento dos princípios inerentes, bem como Legislação Municipal e disposições do Tribunal de Contas do Estado.

V – RESPONSABILIDADES

1 Da Coordenadoria de Administração – CAD

a) Promover a divulgação e a implantação desta Instrução Normativa, mantendo-a atualizada;

b) Efetuar o acompanhamento sobre a efetiva observância das instruções normativas ao Sistema de Segurança da Informação está sujeito;

c) Promover discussões técnicas com o setor de Tecnologia da Informação, visando aprimoramento das instruções normativas;

d) Manter a Instrução Normativa à disposição de todos os servidores relacionados ao setor de T.I. – Tecnologia da Informação.

2 Da Divisão de Operação e Manutenção de Programas – DOMPR

a) Classificar as informações;

b) Gerenciar identidade e controle de acesso lógico;

c) Controlar o acesso Físico;

d) Controlar o acesso à internet, através de monitoramentos;

e) Verificar formas de utilização do e-mail, enviar, receber e baixar;

f) Configurar e instalar o sistema operacional e demais softwares em todos os

computadores portáteis e estações de trabalho;

g) Orientar sobre as formas de utilização dos equipamentos de Tecnologia da Informação;

h) Orientar sobre utilização de programas e aplicativos;

i) Zelar pelo armazenamento das informações geradas;

j) Gerenciar as contingências e garantir a continuidade do processo de trabalho da rede;

k) Coordenar as ações necessárias na ocorrência de incidentes de segurança e do meio físico;

l) Coordenar ações em determinadas ocorrências de acidentes com hardware e lógico;

m) Recepcionar e conferir a documentação necessária ao cadastro, suspensão e exclusão de usuários, à habilitação e inabilitação de módulos e ao fornecimento de senhas.

3 Dos Usuários

a) Assinar Termo de Responsabilidade (Anexo II), formalizando a ciência e o aceite da Normativa, bem como estar ciente sobre a responsabilidade do seu cumprimento;

b) Comunicar imediatamente a área de Tecnologia da Informação – T.I. qualquer descumprimento ou violação desta Normativa e seus procedimentos;

c) Zelar pela ordem das instalações do local e do equipamento disposto. Surgindo qualquer necessidade de manutenção a equipe técnica deve ser informada do fato e do ato ocorrido;

d) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

e) Não manusear alimentos e bebidas próximo aos equipamentos de Informática;

f) Assumir atitude pró-ativa no que diz respeito à proteção das informações da entidade;

g) Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades de cada setor.

4 Da Unidade de Controle Interno – UCI

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

b) Através da atividade de auditoria interna avaliar o cumprimento e a eficácia dos procedimentos de controle desta Instrução Normativa, para aprimoramento da mesma.

VI – PROCEDIMENTOS

1 Do Cadastro e Acesso dos Usuários

1.1 As solicitações de habilitação ou inabilitação de usuários aos sistemas informatizados serão processados, exclusivamente, pela Divisão de Operação e Manutenção de Programas – DOMPR.

1.2 O pedido de cadastro dos usuários, bem como alteração, exclusão, bloqueio e desbloqueio, será realizado através do preenchimento do formulário "Controle de Acesso aos Sistemas" (Anexo I), que deve ser devidamente preenchido e assinado pelo superior imediato do servidor.

1.3 O acesso do usuário aos sistemas informatizados é feito mediante uso de senha pessoal e intransferível e sua autorização de uso não implica direito de acesso imotivado aos sistemas e informações.

1.4 O formulário "Controle de Acesso aos Sistemas" (Anexo I), será emitido em 2 (duas) vias, sendo uma via arquivada no setor de Tecnologia da Informação e outra para arquivo do solicitante.

2 Do Backup

2 - Processos Administrativos e Sindicâncias

2.1 A execução dos backups e respectiva verificação é de responsabilidade da área de Tecnologia da Informação.

2.2 Os Backups do banco de dados dos sistemas administrativos (Sistema de Administração Publica-SIAP.4000 Folha, Compras, Almoxarifado, Orçamentário, Financeiro e Patrimônio,) entre outros.

2.3 Os Backups de estações de trabalho e computadores portáteis serão realizados sempre que houver necessidade de manutenção e/ou conserto dos equipamentos ou por outras circunstâncias que representem alguma ameaça ou risco à base de dados.

2.4 Cópia fiel das informações serão armazenadas em unidade externa, em DVD ou CD, em outra máquina da rede ou em Pen-drive.

2.5 A responsabilidade pela segurança e integridade dos backups é da área de Tecnologia da Informação.

2.6 Preferencialmente, as cópias e geração dos Backups serão realizadas utilizando software livre, ou quando for o caso, manualmente através do recurso CTRL + C do hardware.

3 Da Política de Login / Senhas

3.1 A criação do login e senha aos usuários serão processadas nos termos do item 1 – Do cadastro e acesso dos usuários – desta Instrução Normativa, pela área de T.I.

3.2 A senha deverá conter, no mínimo, 6 (seis) caracteres alfanuméricos, ou seja, composta por letras e números.

3.3 Recomenda-se que as senhas sejam alteradas, no mínimo, uma vez por ano e sempre que o usuário perceber que a mesma pode ser de conhecimento de outrem.
3.4 Em face do seu caráter de pessoalidade, a senha é intransferível, não podendo ser compartilhada, divulgada a outra pessoa, anotada em papel ou em sistema visível, ou de acesso não protegido.

4 Das Configurações de Rede

4.1 É proibido aos usuários realizar alterações nas configurações de rede e de inicialização das máquinas, sendo estas atribuições exclusivas do setor de T.I.
4.2 Não é permitido fazer Download e/ou instalar software de gerenciamento de download para efetuar baixas de músicas e filmes sem autorização da equipe de T.I. – Tecnologia da Informação.

5 Da utilização de equipamentos de informática particulares

5.1 A utilização de equipamentos de informática particulares fica condicionada à prévia comunicação à equipe de T.I., mediante encaminhamento de autorização formal do superior imediato do servidor.
5.2 A responsabilidade por esses equipamentos é única e exclusivamente do usuário/proprietário. Da mesma forma, a responsabilidade por qualquer

manutenção, recuperação de informação, de suporte especializado ou fornecimento de quaisquer acessórios são de responsabilidade e ônus do usuário/proprietário, e, portanto, não serão realizados pelos técnicos na Câmara e em horário de expediente.

6 Da segurança e acesso aos recursos de tecnologia

6.1 O acesso aos ativos centrais da entidade e ao ambiente informatizado, rack, servidores, central telefônica, firewall e sala de manutenção, deve ser motivado por necessidade de serviço, devendo ser controlado e restrito às pessoas autorizadas.

6.2 A utilização dos recursos de tecnologia da informação será monitorada, com a finalidade de detectar divergência entre as normas que integram a Política de Segurança da Informação e os registros de eventos monitorados, fornecendo evidências nos casos incidentes de segurança.

6.3 As permissões de acesso devem ser graduadas de acordo com as atribuições, renovadas periodicamente conforme instrução específica que receberão da área técnica.

6.4 Os novos usuários deverão ser orientados quanto às normas e procedimentos de acesso e utilização dos recursos de Tecnologia da Informação.

6.5 Arquivos de origem desconhecida nunca devem ser abertos, muito menos executados.

7 Do uso da Internet

7.1 A Câmara Municipal de Primavera do Leste não se responsabiliza pela segurança de transações eletrônicas, incluindo comércio eletrônico e internet banking, realizadas pelos usuários internos por meio dos recursos de Tecnologia da Informação disponibilizados pela Instituição.

7.2 Não são permitidas conexões por meio de placas, equipamentos de fax-modem, ou outras tecnologias móveis.

7.3 A Câmara Municipal poderá monitorar os acessos às páginas da Internet com o intuito de identificar, bloquear e notificar formalmente os usuários internos ou colaboradores sobre as páginas com conteúdo impróprio para o ambiente de trabalho e casos detectados de queda de produtividade em função do uso abusivo desta ferramenta.

7.4 Não são autorizados acessos a páginas de conteúdo impróprio ao ambiente de trabalho, como por exemplo: pornografia, downloads, youtube, vídeos, jogos, músicas entre outros.

7.5 O Departamento de T.I. deverá manter arquivo do monitoramento do uso da Internet e encaminhar as situações que estiverem em desacordo com a presente instrução normativa ao Coordenador de Administração e também à Coordenadoria de Controle Interno.

8 Termo de Responsabilidade

8.1 O descumprimento do Termo de Responsabilidade – Anexo II caracteriza infração funcional, podendo ocasionar a responsabilização civil, administrativa e penal do infrator.

9 Do recadastramento

9.1 Todos os acessos criados para os sistemas até a data da publicação desta Instrução Normativa terão um prazo de 60 (sessenta) dias para serem recadastrados.

9.1.1 O processo de recadastramento obedecerá aos procedimentos estabelecidos neste instrumento e a solicitação do recadastramento ficará a cargo do órgão ao qual o usuário está lotado.

9.1.2 Vencido o prazo, o acesso será cancelado pela Divisão de Operação e Manutenção de Programas – DOMPR.

V – CONSIDERAÇÕES FINAIS

1- Os Procedimentos contidos nesta Instrução Normativa não eximem a observância das demais normas aplicáveis ao assunto.

2- O descumprimento do previsto nos procedimentos aqui definidos será passível de instauração de Processo Administrativo para apuração de responsabilidade.

3- Os esclarecimentos adicionais a respeito deste documento poderão ser obtidos junto a Coordenadoria de Administração– CAD e/ou Divisão de Operação e Manutenção de Programas – DOMPR.

4 - Esta Instrução Normativa entrará em vigor na data de sua publicação.

Primavera do Leste, 21 de novembro de 2012.

SANDRA JACOB DO CARMO
Presidente

MÔNICA C. M. CRIESE
Membro

JOAO JOSE DE ARRUDA CAMPOS
Membro

Portaria nº 060/2012 - Comissão de Elaboração das Instruções Normativas da Câmara Municipal de Primavera do Leste/MT.

De acordo:

Comissão Provisória de Implantação do Controle Interno no Legislativo, nomeada pela Portaria 059/2012 de 23 de agosto de 2012;

GLEISON FRANÇA ROSARIO
Presidente

MONICA C. M. CRIESE
Membro

REGINA CELIA DE SOUZA
Membro

MARCOS A. GAYA
Membro

GLEY A. DOURADO
Membro

ANEXO I

CONTROLE DE ACESSOS AO SISTEMA DE INFORMÁTICA E INTERNET
(__) Cadastro (__) Alteração (__) Exclusão (__) Bloqueio (__) Desbloqueio

1 – IDENTIFICAÇÃO DO SOLICITANTE

ORGÃO/SETOR		
CHEFE IMEDIATO DO SERVIDOR		MATRICULA
DATA/ASSINATURA	TELEFONE/RAMAL	E-MAIL

2 – IDENTIFICAÇÕES DO SERVIDOR

NOME COMPLETO		CPF	MATRICULA
CARGO	TIPO DE VINCULO	E-MAIL	
SOLICITO A HABILITAÇÃO DO SERVIDOR IDENTIFICADO NOS SEGUINTES MÓDULOS DO SISTEMA			
PARECER DO RESPONSAVÉL DO SETOR	**MÓDULO (SISTEMA)**		

3 – ATENDIMENTO DA SOLICITAÇÃO

Declaro estar de acordo com os perfis solicitados **Data e Assinatura**	**Declaro que nesta data o cadastramento foi efetuado** **Data e Assinatura**

ANEXO II

Eu, _____, declaro haver solicitado acesso ao (s) sistema(s) _____, comprometendo-me a:

a) Acessar o (s) sistema (s) informatizado (s) somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege os acessos a sistemas;

b) Não revelar fora do âmbito profissional fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

c) Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

d) Não me ausentar da estação de trabalho sem encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros;

e) Não revelar minha senha de acesso ao (s) sistema (s) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

f) Responder, em todas as instâncias, pelas conseqüências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Declaro, ainda, estar plenamente esclarecido e consciente que:

1º É minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade dos dados, informações contidas nos sistemas, devendo comunicar por escrito à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistemas, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

2º O acesso à informação não me garante direito sobre ela, nem me confere autoridade para liberar acesso a outras pessoas;

3º Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos dos sistemas aos quais tenho acesso para outros servidores não envolvidos nos trabalhos executados;

4º Devo alterar minha senha, sempre que obrigatório ou que tenha suposição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas;

5º Respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição (tais como direitos de acesso a arquivos, diretórios e recursos disponíveis no ambiente da instituição, etc)

6º Cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação, de suas diretrizes, bem como deste Termo de Responsabilidade.

Ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional e penal a revelação de segredo do qual me apropriei em razão do cargo. Sendo crime contra a administração pública, a divulgação a quem não seja servidor da Câmara Municipal de Primavera do Leste - MT, das informações do (s) sistema (s) ao (s) qual (is) tenho acesso, estando sujeito às penalidades previstas em lei. Sem prejuízo da responsabilidade penal e civil, e de outras infrações disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda que habilitado.

Constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da Administração Pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano, bem como modificar ou alterar o sistema de informações ou programa de informática sem autorização ou sem solicitação de autoridade competente, ficando o infrator sujeito as punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública.

Declaro, **nesta data, ter ciência e estar de acordo com os procedimentos acima descritos**, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

USUÁRIO **Primavera do Leste/MT----/----/20----** **ID do Usuário:_____** _____ Assinatura do Usuário.	Responsável técnico de Tecnologia da Informação. _____ Assinatura Setor de T.I. Tecnologia da Informação