

ORDEM DE SERVIÇO Nº 007, DE 3 DE JULHO DE 2018.

Regulamenta e uniformiza a utilização dos recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito da Administração Municipal.

Considerando a necessidade de uniformizar e regulamentar a utilização dos recursos de Tecnologia da Informação e Comunicação (TIC), no âmbito da Administração Municipal,

D E T E R M I N O:

Seção I Das Disposições Gerais

Art. 1º Fica regulamentada e uniformizada a utilização dos recursos de Tecnologia da Informação e Comunicação (TIC), no âmbito da Administração Municipal da Prefeitura Municipal de Porto Alegre (PMPA).

Parágrafo único. Os recursos de Tecnologia da Informação e Comunicação (TIC) compõem-se de equipamentos e sistemas de informática, independentemente de sua propriedade, sujeitando-se a sua utilização ao disposto nesta Ordem de Serviço e nos respectivos normativos complementares.

Art. 2º Para efeito do disposto nesta Ordem de Serviço, considera-se:

I – *hardware*: um componente ou conjunto de componentes físicos de um computador, tais como: componentes eletrônicos, circuitos integrados e placas, ou de seus periféricos, como monitores, *mouse*, teclado, impressoras, *scanners*, estabilizadores, *no-breaks*, *webcams* e outros;

II – *software*: são os componentes que não fazem parte do equipamento físico propriamente dito e que incluem o conjunto de um ou mais programas, bem como os dados a eles associados, empregados durante a utilização dos sistemas;

III – rede: a infraestrutura de interconexão, como cabeamento, roteadores, *switches* e *access-points*; e os elementos por ela interconectados, tais como microcomputadores, impressoras, telefones e câmeras de vídeo; que trocam informações e compartilham recursos através de protocolos pré-definidos;

IV – *internet*: rede de computadores interligados de abrangência global, que se comunicam utilizando o protocolo TCP/IP e UDP/IP;

V – *intranet*: uma rede privada de computadores interligados de abrangência restrita, que se comunicam utilizando os protocolos da *internet*, porém cujos recursos usualmente não estão diretamente visíveis a público em geral e outros computadores na *internet*;

VI – rede municipal de informática, ou rede PMPA: conjunto de equipamentos (*hardware*) e programas (*software*) interligados e utilizados na Administração Municipal;

VII – *intranet* PMPA: segmento privado da rede PMPA destinado ao uso exclusivo por usuários autorizados e estritamente através de equipamentos e *software* previamente homologados;

VIII – *backup*: cópias de segurança dos dados, realizadas periodicamente em um dispositivo de armazenamento (óptico ou magnético), permitindo o resgate das informações no caso de falha no meio onde estão armazenados ou perda das informações por apagamentos acidentais;

IX – licença de uso de *software*: o contrato de licença de uso que determina as ações autorizadas ou proibidas pelo seu desenvolvedor e que devem ser cumpridas pelo usuário da licença;

X – SPAM: termo em inglês (*spiced ham*) que passou a ser utilizado para designar as mensagens eletrônicas não solicitadas e enviadas para um grande número de pessoas;

XI – sistema operacional: programa (s) que gerenciam os recursos do computador, fornecendo ao usuário um meio amigável de interagir com o equipamento;

XII – navegador: programa de computador utilizado para acessar e interagir com documentos de hipertexto localizados na *internet* ou *intranet*, também conhecidos como páginas *web* ou *sites*;

XIII – processador de texto: programa utilizado para escrever e desenvolver textos no computador;

XIV – planilha eletrônica: programa de computador que utiliza abas contendo tabelas em forma de grade compostas de linhas e colunas para realização de cálculos e apresentação de resultados;

XV – correio eletrônico: serviço que possibilita a troca de mensagens por meio de recursos disponíveis na *internet*;

XXVI – *site*: conjunto de documentos de hipertexto acessível pela rede mundial (*web*) disponibilizado por um indivíduo, empresa ou instituição, contendo um endereço específico da rede *internet* (URL: *Uniform Resource Locator*), podendo ser subdividido em outras páginas com endereços específicos e próprios;

XXVII – suporte: serviço prestado por pessoal especializado, visando a identificar e solucionar problemas encontrados nos recursos de TIC;

XXVIII – *download*: a transferência ou a cópia de um arquivo originalmente armazenado em um servidor ou computador remoto para o computador local;

XXIX – usuários: aqueles que estão autorizados a utilizar os recursos de TIC;

XX – sistema: todos os *software* utilizados na rede do Município;

XXI – programa de código malicioso (*malware*): *software* projetado especificamente para atentar contra a segurança dos recursos de TIC (ex.: vírus, *spyware* etc.);

XXII – *spyware*: mensagem de *e-mail* forjada, que busca imitar um conteúdo legítimo, e que tem como objetivo induzir ao usuário executar alguma operação que comprometa a segurança de seus dados ou dos recursos de TIC aos quais ele tem acesso, sendo frequentemente utilizadas para roubo de senhas e fraudes financeiras;

XXIII – *software* livre: programa de computador que pode ser usado, copiado, estudado, modificado e redistribuído, de acordo com uma licença de autorização;

XXIV – Política de Segurança da Informação (PSI): documento(s) que contém um conjunto de normas, métodos e procedimentos cujo objetivo é garantir a manutenção da confidencialidade, integridade e disponibilidade da informação sob custódia do Município;

XXV – autorizador de TIC: representante de um determinado órgão do Município, responsável pelos esclarecimentos e decisões relativas ao uso dos recursos de TI amparadas nesta Ordem de Serviço, limitado a 4 (quatro) servidores; e

XXVI – autorizador de Desenvolvidores de Sistemas e Consultorias junto à PROCEMPA: representante de um determinado órgão do Município, responsável pelas demandas junto ao CTIC, limitado a 5 (cinco) servidores.

Seção II Da Finalidade

Art. 3º Os recursos de TIC têm como finalidade permitir aos usuários a prática de atividades relacionadas:

- I – ao desempenho de suas funções administrativas e profissionais;
- II – à pesquisa autorizada e ao aperfeiçoamento profissional visando qualificar o serviço prestado internamente e aos cidadãos; e
- III – ao acesso e à disseminação de informações de interesse da Administração Municipal.

Seção III Do CTIC:

Art. 4º O Comitê de Tecnologia de Informação e Comunicação (CTIC) instituído por meio do Decreto n.º 18.977, de 18 de março de 2015, é a instância maior, no âmbito da Administração Municipal, para determinar e ratificar políticas institucionais de uso de recursos de TIC e de Políticas de Segurança da Informação (PSI), sendo responsável por decidir, normatizar e regulamentar sobre quaisquer casos omissos nesta Ordem de Serviço ou na política de TIC vigente.

Seção IV Dos Usuários

Art. 5º Ficam autorizados à utilização dos recursos de TIC todos os servidores e estagiários em efetivo exercício nos órgãos da Administração Municipal.

§ 1º O acesso à rede municipal está condicionado à concordância do usuário com as normas desta Ordem de Serviço e os respectivos normativos complementares.

§ 2º A concordância poderá ser expressa tanto pela assinatura de termo aditivo ao contrato de trabalho disponibilizado pelo órgão ao qual o usuário está vinculado, quanto por meio de formulário eletrônico disponibilizado pela Companhia de Processamento de Dados de Porto Alegre (PROCEMPA), mediante uso de sua credencial de rede PMPA.

Art. 6º Para habilitação do acesso do usuário aos recursos de TIC, este receberá uma credencial de rede PMPA, a qual é pessoal, única por CPF, e intransferível, sendo de responsabilidade do usuário toda e qualquer ação executada por meio de sua credencial pessoal.

§ 1º A credencial de rede PMPA é composta por *login*, senha pessoal e endereço de *e-mail* institucional;

§ 2º Cada servidor deve possuir uma única credencial de rede PMPA, a qual estará vinculada ao órgão em que estiver exercendo suas atividades, independentemente do seu órgão de origem.

§ 3º Informações relevantes referentes ao uso dos recursos de TIC e aos demais normativos vigentes poderão ser enviados a qualquer momento para o endereço de *e-mail* institucional do usuário;

§ 4º Em caso de necessidade de endereço de *e-mail* adicional, a sua criação deverá ser motivada e encaminhada a PROCEMPA pelo respectivo autorizador de TIC do respectivo órgão, sendo o endereço de *e-mail* adicional vinculado à credencial, e a caixa de correio, já existente.

Art. 7º A criação de credenciais de rede, ou seu cancelamento definitivo, mesmo que por remoção ou transferência de servidores e estagiários entre setores ou órgãos, será procedido pela PROCEMPA, mediante requerimento do setor responsável pelos recursos humanos dos respectivos órgãos ou autorizador de TIC, a ser enviado através da ferramenta designada pela PROCEMPA.

§ 1º A credencial de rede PMPA possibilita, por padrão, acesso somente aos equipamentos de informática e *software* necessários para a consecução das tarefas do usuário, e utilização de serviços de telemática e de impressões, a navegação na *web* através dos *sites* institucionais e governamentais oficiais, que sejam relevantes para o desempenho das suas atividades funcionais, conforme perfil básico definido.

§ 2º Permissões adicionais poderão ser concedidas, ou restrições especiais aplicadas, mediante normativa aprovada pelo CTIC, para aplicação pela PROCEMPA no escopo global da PMPA ou no escopo específico de alguma secretaria ou autarquia.

§ 3º As necessidades especiais de uso, observando o sigilo às informações e as características da atividade funcional desempenhada pelo usuário, deverão ser solicitadas e motivadas pela chefia responsável ao autorizador de TIC do respectivo órgão, e providenciadas pela PROCEMPA, mediante prévia avaliação da viabilidade de configuração, e sujeitam-se a revisão anual, sem a qual poderão ser revogadas.

Art. 8º A permissão de acesso como administrador de rede é prerrogativa exclusiva da PROCEMPA.

§ 1º A permissão de acesso como administrador local para membros de TI dos Órgãos será regulamentada em instrução normativa específica.

§ 2º Aos usuários finais será concedida permissão comum de usuário de rede, observando-se os casos de necessidades especiais onde poderá ser atribuída permissão local com nível de acesso mais elevado na estação de trabalho do usuário.

Art. 9º As credenciais de rede serão desativadas pela PROCEMPA por critério de inatividade, em decorrência imediata do encerramento do vínculo funcional do usuário, ou mediante notificação enviada pelo setor de recursos humanos ou autorizador do TIC do respectivo órgão à PROCEMPA.

§ 1º A notificação do encerramento de vínculo poderá ser substituída por uma revisão periódica dos vínculos ativos, desde que acordado com a PROCEMPA e que a mesma seja realizada em intervalos não superiores a 3 (três) meses.

§ 2º Credenciais inativas (sem *login* em estações de trabalho ou no *webmail*) há mais de 3 (três) meses, e sem orientação específica preexistente em contrário, serão bloqueadas pela PROCEMPA, com posterior notificação ao autorizador de TIC do respectivo órgão, deixando de receber e-mails a partir da data do bloqueio; porém preservando o conteúdo já existente na caixa de *e-mail* do usuário e podendo ser reativadas por solicitação do autorizador de TIC.

§ 3º Credenciais inativas há mais de 12 (doze) meses serão removidas pela PROCEMPA, com a perda de todo o conteúdo associado àquela conta, incluso, mas não restrito a mensagens existentes na caixa de *e-mail* do usuário, com notificação prévia de 1 (uma) semana ao autorizador de TIC do respectivo órgão, sobre a alteração a ser realizada.

§ 4º Quando houver a necessidade de manutenção do acesso à conta em casos de afastamentos legais, por período superior a 3 (três) meses, o setor responsável pelos recursos humanos do órgão ou o autorizador de TIC do respectivo órgão, deverão notificar previamente a PROCEMPA, de forma que a conta não seja suspensa, nem removida.

§ 5º Os prazos de inatividade, formas de notificação e demais informações, processos e procedimentos relacionados à desativação das credenciais de usuários da rede PMPA constarão em norma complementar publicada pelo CTIC.

Art. 10. As disposições desta Ordem de Serviço aplicam-se, no que couber, aos prestadores de serviço, que mediante prévia autorização formal da autoridade responsável pela contratação, e anuência do autorizador de TIC do respectivo órgão, recebam acesso a qualquer dos recursos de TIC da PMPA.

Parágrafo único. A autorização a prestadores de serviço está condicionada a definição do escopo estrito de utilização e será por prazo determinado, não superior a 12 (doze) meses, podendo ser renovado havendo interesse do órgão, sinalizado à PROCEMPA pelo autorizador de TIC do respectivo órgão, e limitado ao período de contratação.

Seção V **Dos Equipamentos de TIC**

Art. 11. Compõem os equipamentos de TIC:

I – os equipamentos de informática (*hardware*) adquiridos ou disponibilizados pelo Município;

II – os equipamentos de informática doados registrados como patrimônio do Município.

Parágrafo único. Os equipamentos de informática deverão ser previamente registrados pela Área de Patrimônio e homologados pela PROCEMPA, antes de serem conectados a rede PMPA.

Art. 12. A instalação de equipamentos, adição ou a substituição de peças, periféricos ou outros elementos físicos de informática, que integram o patrimônio do Município, deverá ser efetuada pelos responsáveis de TI dos respectivos órgãos, observados os padrões previamente determinados, com auxílio da PROCEMPA, se necessário.

Art. 13. A utilização de equipamentos particulares deverá ser motivada e previamente autorizada pelos responsáveis de TI dos respectivos órgãos e homologada pela PROCEMPA.

§ 1º O uso dos equipamentos particulares autorizados está limitado por padrão a rede *wireless* “Porto Alegre Livre”, ou rede visitante equivalente que esteja logicamente isolada da *intranet* PMPA.

§ 2º Necessidades especiais de uso dentro da *intranet* PMPA deverão ser previamente avaliadas e homologadas pela PROCEMPA, e os equipamentos autorizados deverão sofrer adequação para uso na *intranet* da PMPA, procedimento que envolve, mas não está limitado a:

I – remoção de programas proibidos, ou incompatíveis com os normativos vigentes;

II – instalação de programas e controles de segurança obrigatórios; e

III – configuração de acesso remoto pelos administradores de rede da PROCEM-PA, de forma a permitir auditar a conformidade das configurações e os acessos realizados dentro da *intranet* PMPA, sempre que necessário.

Art. 14. É prerrogativa da PROCEMPA, vetar a utilização dentro da *intranet* PMPA de equipamentos patrimoniados ou particulares que não estejam em conformidade com os normativos vigentes da informação, ou que representem riscos físicos ou lógicos à rede PMPA, incluindo, mas não restrito a:

I – computadores doados cujo sistema operacional está descontinuado e não recebe mais atualizações de segurança do fabricante;

II – computadores cujo sistema operacional não esteja homologado para instalação da solução anti-*malware* utilizada na rede PMPA;

III – computadores cujo *software* instalado possua restrições de licenciamento incompatíveis com o uso profissional ou corporativo na rede da PMPA.

Art. 15. Cabe a PROCEMPA aplicar os controles que julgar oportunos tecnicamente viáveis de forma a coibir o uso de dispositivos não autorizados, ou fora de conformidade, dentro da rede PMPA, tais como:

I – bloqueio, sem aviso prévio ao usuário e com notificação posterior ao autorizador de TIC do respectivo órgão, do dispositivo ou da credencial do usuário na rede PMPA; e

II – exigência de autenticação de usuário e ou respectivo dispositivo para conectividade à rede PMPA.

Seção VI **Do Uso dos Sistemas de Informática**

Art. 16. Compõem os sistemas de informática:

I – as licenças de uso de aplicativos adquiridos pelo Município;

II – as licenças de uso doadas para o Município; e

III – *software* e respectivos códigos fonte desenvolvidos ou adquiridos para atender às necessidades do Município.

Art. 17. A instalação de *software* deverá ser solicitada pelos responsáveis de TI dos respectivos órgãos, e realizada pela PROCEMPA, devendo ser rigorosamente observadas as condições de uso e de instalação dos aplicativos, estabelecidas pelos fabricantes.

Art. 18. A Administração Municipal poderá adotar o uso de *software* livre em quaisquer áreas, seguindo padrão autorizado pelo CTIC, após análise técnica da PROCEMPA.

Parágrafo único. A instalação de software pela PROCEMPA não implica a aquisição automática e implícita de novas licenças pela PROCEMPA, devendo a licença apropriada ser providenciada pelo respectivo órgão no caso de novas instalações.

Art. 19. Compõem o conjunto básico de aplicativos dos computadores do Município:

I – sistema operacional de uso difundido;

II – navegador para uso da *internet* e acesso ao correio eletrônico institucional;

III – sistema de detecção e mitigação de *malwares*;

IV – pacote base de aplicativos de escritório de uso gratuito (editor de textos e planilha eletrônica); e

V – programa leitor de *Portable Document Format* (PDF), quando não incluso no próprio sistema operacional.

Art. 20. Outros *software* somente poderão ser instalados, dependendo da necessidade determinada pela atividade desempenhada pelo usuário na PMPA, desde que previamente autorizado pelo autorizador de TIC do respectivo órgão, e homologado pela PROCEMPA, mesmo que o usuário possua licença para a sua instalação ou uso.

Parágrafo único. O usuário será responsável pela observância das normas atinentes ao uso de aplicativos não autorizados, bem como pelas implicações legais decorrentes dessa instalação ou uso desse *software*.

Art. 21. O uso de aplicativos ou serviços na nuvem está sujeito ao mesmo regimento e trâmite adotado para *software* instalados localmente, estando condicionado a anuência do autorizador de TIC e homologação prévia pela PROCEMPA.

Art. 22. É prerrogativa da PROCEMPA vetar a instalação ou uso, bloquear o acesso ou remover, sem aviso prévio e com notificação posterior ao autorizador de TIC, qualquer software que viole os normativos vigentes ou que represente riscos físicos ou lógicos aos recursos de TIC, incluso mas não restrito a software não licenciado ou cuja licença seja sabidamente

incompatível com o uso corporativo, ou cujo uso interfira ou prejudique a operação de outros sistemas da rede PMPA.

Seção VII **Do Uso da *internet***

Art. 23. O acesso à *internet* deverá ser utilizado primariamente para o desempenho das atribuições funcionais.

§ 1º Será admitido o uso eventual da *internet*, por curtos períodos, para fins pessoais, desde que tais usos não comprometam o desempenho, pelo usuário, das suas atribuições funcionais e desde que esteja em conformidade com os demais termos desta Ordem de Serviço e suas respectivas normas complementares.

§ 2º A PROCEMPA poderá aplicar controles de forma a limitar ou bloquear operações acesso à *internet* para fins pessoais que impliquem grande consumo do canal de acesso à *internet*, tais como o *download* ou upload de grandes arquivos, o acesso a vídeos e demais conteúdos de streaming, ou VoIP, de forma a preservar os recursos da rede PMPA para as atividades primordiais da Administração Municipal.

§ 3º A resolução de problemas relativos a acessos à *internet* realizados para fins pessoais, será realizada pela PROCEMPA em política de melhor esforço, não sendo oferecidas quaisquer garantias estritas de solução efetiva ou de nível de serviço nesses casos.

Art. 24. Fica vedado o acesso por qualquer usuário a recursos que contenham:

I – informações inadequadas ou não relacionadas às atividades exercidas pelo usuário;

II – material atentatório à dignidade e à integridade da pessoa;

III – material pornográfico, pedófilo e assemelhados;

IV – material que faça apologia, incite ou facilite atividades criminosas, bem como apologia ao uso da violência;

V – jogos de azar;

VI – material inadequado ou inconveniente ao ambiente de trabalho, cujo conteúdo cause constrangimento ou desconforto aos demais; e

VII – material cujo acesso represente violação de propriedade intelectual ou de direitos autorais, ou de outra forma ilícitos segundo a legislação vigente.

Art. 25. Não poderão ser acessados *sites* que tragam aos equipamentos e às redes códigos maliciosos, artifícios de violação ou quaisquer outros elementos que possam vir a alterar ou danificar a rede, os equipamentos, os sistemas e os bancos de dados da Administração Municipal.

Art. 26. O *download* de arquivos via *internet* está restrito a assuntos relacionados às atribuições funcionais.

Art. 27. O envio ou upload, de qualquer conteúdo para a *internet*, incluso mas não restrito a utilização de serviços de *e-mail* e de armazenamento em nuvem, deverá observar os normativos vigentes, referentes aos tipos de arquivos e conteúdos autorizados, e a prevenção de evasão de dados do Município sem autorização.

Art. 28. A PROCEMPA irá aplicar os controles que julgar oportunos e tecnicamente viáveis de forma a coibir abusos no acesso à *internet* para fins pessoais, ou violações aos dispostos nessa Ordem de Serviço e demais normativos vigentes, incluso, mas não restrito a:

I – bloqueio de acesso a *sites*;

II – bloqueio de tipos de arquivos ou de categorias de conteúdos;

III – inspeção ou monitoramento, individual ou coletiva, de forma contínua ou sazonal, dos acessos à *internet*.

§ 1º A PROCEMPA poderá bloquear sem aviso prévio, de forma parcial ou na integralidade, o acesso de um usuário a *internet*, caso detecte abusos ou identifique riscos a rede PMPA, com posterior notificação autorizador de TIC do respectivo órgão sobre o incidente.

§ 2º A PROCEMPA deverá zelar pela privacidade dos usuários, preservando, tanto quanto possível, o sigilo dos acessos a *internet* quando não houver evidência de violação a esta Ordem de Serviço ou a política de segurança da informação.

Seção VIII **Do Uso do Correio Eletrônico**

Art. 29. Os usuários deverão utilizar o correio eletrônico disponibilizado pela Administração Municipal como meio de receber e enviar comunicações oficiais, e informações relacionadas às atividades funcionais, tais como:

I – informações gerais de interesse funcional;

II – correspondência entre usuários;

III – envio de documentos oficiais e de arquivos de dados quando a PROCEMPA não disponibilizar alternativa mais apropriada para seu envio.

Parágrafo único. Fica vedada a utilização de *e-mail* particular para o exercício de atividade funcional, salvo no caso de indisponibilidade momentânea do *e-mail* institucional.

Art. 30. O endereço de *e-mail* institucional disponibilizado pela Administração Municipal, e a correspondente caixa postal onde as mensagens de *e-mail* são armazenadas, devem ser primariamente utilizados para fins relacionados às atribuições funcionais na PMPA.

Parágrafo único. Fica vedado o cadastro do *e-mail* institucional em *sites*, serviços de notificação ou listas de *e-mail* na *internet* não relacionados à atribuição funcional na PMPA, tais como redes sociais e *sites* de comércio eletrônico (*e-commerce*).

Art. 31. A utilização das caixas postais disponibilizadas pela Administração Municipal, em qualquer uma das suas modalidades de acesso, seja através da *internet* pelo *webmail*, seja pelo cliente de *e-mail* instalado nas estações de trabalho, ou através de aplicações, pressupõe as mesmas responsabilidades e cuidados.

Art. 32. Fica vedado o envio de mensagens pelo sistema de correio eletrônico, entre quaisquer usuários da PMPA, ou mesmo envolvendo usuários externos que contenham:

I – mensagens ou imagens atentatórias à dignidade e à integridade da pessoa humana;

II – mensagens ou imagens pornográficas, pedófilas ou assemelhadas;

III – propaganda de qualquer espécie;

IV – material que faça apologia, incite ou facilite atividades criminosas;

V – material inconveniente ou inadequado ao ambiente de trabalho, ou cujo conteúdo cause constrangimento e desconforto ao ser humano;

VI – "correntes", boatos, anedotas ou assemelhados, bem como outras mensagens não desejadas que possuam características de SPAM; e

VII – arquivos de música, vídeos, programas executáveis ou outros que não estejam relacionados às atribuições funcionais.

Art. 33. Fica vedado o envio de mensagens que tragam ao equipamento utilizado pelo destinatário, seja ele interno ou externo a rede PMPA, códigos maliciosos, artifícios de violação, vírus ou quaisquer outros elementos que possam vir a alterar ou danificar as redes, os sistemas, os dados registrados e os equipamentos pertencentes ao Município e a terceiros.

I – O usuário poderá solicitar à PROCEMPA a revisão e rastreamento de mensagem vinculada a suas atribuições funcionais e não recebida após 1 hora do suposto envio, para a qual exista a suspeita de bloqueio indevido pelo filtro de e-mail. Sendo que, para qual, deverá prover à PROCEMPA informações suficientes incluindo: endereço de *e-mail* ou domínio de origem, endereço de *e-mail* do destinatário, assunto e provável horário do envio;

II – A solicitação de rastreamento implica autorização implícita do usuário para que a PROCEMPA verifique o conteúdo completo da mensagem, de forma a identificar e corrigir a causa do eventual bloqueio indevido.

§ 1º As mensagens enviadas e recebidas serão verificadas de forma automatizada quanto à presença de conteúdos que possam representar risco a rede PMPA, tais como *malwares*, SPAM e *spyware*, e as que tiverem identificação positiva serão bloqueadas pela PROCEMPA.

§ 2º O envio de mensagens para qualquer destinatário externo a PMPA, deverá observar os normativos em vigor, referentes aos tipos de arquivos e conteúdos autorizados, e a prevenção de evasão de dados do Município sem autorização.

Art. 34. A capacidade de armazenamento das caixas postais de cada usuário (quota) é limitada e será definida considerando a disponibilidade de recursos, as políticas de TIC definidas para a PMPA, e de acordo com contrato de prestação de serviço firmado entre a Administração Municipal e a PROCEMPA.

§ 1º O usuário que atingir o limite de capacidade de armazenamento de sua caixa postal fica automaticamente impedido de enviar e receber novas mensagens, devendo, para liberação, efetuar a exclusão de mensagens.

§ 2º Solicitações motivadas de alteração, provisória ou permanente, na quota de armazenamento de *e-mail* de usuários poderão ser encaminhadas pela chefia, com anuência do autorizador de TIC do respectivo órgão, para implementação pela PROCEMPA, observados os limites globais definidos no contrato de prestação de serviço e as políticas de TIC definidas para a PMPA.

Art. 35. De acordo com a disponibilidade dos recursos, dos requisitos de segurança e com as políticas de TIC para a PMPA, poderão ser impostos outros limites à utilização do serviço de correio eletrônico.

Art. 36. A PROCEMPA irá configurar os controles que julgar oportunos e tecnicamente viáveis de forma a mitigar riscos e coibir abusos no uso do correio eletrônico, e violações aos dispostos nessa Ordem de Serviço ou na política de segurança da informação, incluso, mas não restrito a:

I – limitação de tamanho ou bloqueio de caixas de correio;

II – limites de tamanho de mensagens e anexos;

III – bloqueio de anexos por tipo, extensão ou conteúdo;

IV – bloqueio de mensagens não vinculadas à atividade na PMPA, tais como campanhas de propaganda, notificações de *site* de compras individual ou coletiva;

V – restrições de envio de mensagens para listas de distribuição;

VI – inspeção manual do conteúdo de mensagens suspeitas recebidas de ou enviadas para a *internet*, para aprimoramento do filtro de SPAM e bloqueio de campanhas de *spyware* e *malwares*;

VII – monitoramento dos volumes de mensagens, individual ou coletiva, de forma contínua ou sazonal, de forma a coibir abusos e orientar sobre formas mais apropriadas de utilização do correio eletrônico.

§ 1º A PROCEMPA poderá bloquear sem aviso prévio mensagens ou o próprio acesso de um usuário ao correio eletrônico, caso detecte abusos ou identifique riscos a rede PMPA, com posterior notificação ao autorizador de TIC sobre o incidente;

§ 2º A PROCEMPA deverá zelar pela privacidade dos usuários, preservando, tanto quanto possível, o sigilo das mensagens trocadas através do sistema de correio eletrônico quando não houver evidência de violação a esta Ordem de Serviço ou a política de segurança da informação.

Seção IX Dos Deveres

Subseção I Do Usuário

Art. 37. São deveres do usuário:

I – zelar pelos equipamentos que utiliza, não sendo permitida qualquer remoção, desconexão de partes, substituição ou alteração das características físicas ou técnicas dos equipamentos integrantes da rede;

II – zelar pelo sigilo da senha de acesso à rede municipal de informática, a qual é pessoal e intransferível, respondendo pelo uso indevido de sua senha, ainda que praticado por terceiros;

III – realizar periodicamente, ou quando solicitado pela PROCEMPA, a troca de sua senha pessoal, conforme parâmetros definidos pela Política de Segurança da Informação;

IV – realizar a leitura periódica das mensagens enviadas pela PROCEMPA, ou pelo setor de TI dos respectivos órgãos, ao seu *e-mail* institucional a fim de manter-se a par das normas vigentes de uso dos recursos de TIC e também sobre alertas de Segurança da Informação;

V – comunicar imediatamente à chefia qualquer suspeita de que estejam sendo executados atos em seu nome, por meio de seu *login*;

VI – zelar pela segurança das informações do Município, ainda que fora das dependências deste;

VII – respeitar as áreas de acesso restrito, não executando tentativas de acesso a áreas ou máquinas alheias a suas permissões de uso;

VIII – manter a massa de dados sob sua responsabilidade, que tenham a caracterização de relevantes ao Município, sempre atualizados e com cópias de segurança (*backup*) nos servidores da PROCEMPA, evitando a perda de informações importantes relacionadas ao trabalho, sendo vedada a guarda de dados com essas características localmente em estações de trabalho, sejam elas de uso individual ou coletivo;

IX – zelar pela integridade física dos equipamentos de informática colocados à sua disposição, evitando submetê-los a condições de risco, mantendo-os afastados de líquidos, alimentos ou qualquer material ou utensílio que possam danificá-los, e comunicar imediatamente à chefia qualquer anormalidade ou defeito;

X – zelar pela segurança da infraestrutura tecnológica do Município, não utilizando mídias ou quaisquer outros dispositivos afins, que possam conter programas de código malicioso;

XI – solicitar liberação à chefia, justificando os motivos do pedido, acaso esteja impedido de desenvolver suas atividades por conta das restrições de acesso aos recursos de TIC; e

XII – informar o autorizador de TIC, quando houver a necessidade de manutenção do acesso à sua conta, durante períodos de afastamentos legais, superiores a 3 (três) meses.

Art. 38. Fica vedado ao usuário:

I – utilizar os equipamentos e sistemas colocados à sua disposição para finalidade diversa da relacionada às suas atividades;

II – fazer uso dos recursos de TIC para desenvolver, fomentar ou promover ações que incentivem o racismo ou que violem quaisquer outros direitos constitucionais do cidadão;

III – fazer uso dos recursos de TIC para molestar, ameaçar ou ofender os seus usuários ou terceiros, seja por meio de textos, imagens, vídeos ou correios eletrônicos, seja por qualquer outro meio;

IV – fazer uso dos recursos de TIC para veiculação de propaganda política;

V – utilizar os recursos de TIC para divulgar aos demais usuários mensagens (*e-mail*) que não sejam unicamente de interesse do Município, como propagandas, “correntes”, boatos, fotos de qualquer espécie e outros assemelhados;

VI – agir de forma a tornar indisponível, direta ou indiretamente, os recursos de TIC;

VII – executar programas que tenham como finalidade a decodificação de senhas, a monitoração da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;

VIII – executar programas, instalar equipamentos ou executar ações que possam facilitar o acesso de terceiros não autorizados aos recursos de TIC;

IX – fazer uso de direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função dentro do Município;

X – utilizar arquivos que impliquem violação de direitos autorais, de propriedade intelectual ou de qualquer material protegido;

XI – utilizar os recursos de TIC ou permissões de acesso para divulgar, no todo ou em parte, informações a terceiros que são sigilosas ou de interesse apenas do Município;

XII – instalar, utilizar ou manter cópias de software, não autorizadas previamente pelo autorizador de TIC e homologadas pela PROCEMPA, ou não contratadas pelo Município, nos equipamentos de informática de propriedade deste;

XIII – apropriar-se, sob quaisquer meios, das chaves de ativação, *Product Keys* ou quaisquer outros códigos de *softwares* de propriedade do Município;

XIV – acessar contas de correio eletrônico de terceiros, sem a devida autorização;

XV – enviar mensagens eletrônicas com material obsceno, ilegal ou antiético, propaganda política e *hoax* (boatos, mensagens enganosas);

XVI – enviar mensagens eletrônicas ofensivas, que possam causar molestamento ou tormento;

XVII – utilizar ou divulgar material que viole direitos de propriedade intelectual de qualquer pessoa ou companhia, como marca registrada, nome comercial, segredo empresarial, domínio na *internet*, patentes, desenho industrial ou qualquer outro material não autorizado expressamente pelo autor, que viole direito de propriedade industrial, artística ou literária, bem como fazer cópia não autorizada de material protegido por direitos autorais, incluindo músicas, textos, imagens, livros ou em outras fontes protegidas por direitos autorais; e

XVIII – enviar mensagens que possam afetar de forma negativa o Município, seus servidores, fornecedores ou parceiros, inclusive no que tange às suas imagens públicas.

Subseção II **Das Chefias e dos Autorizadores de TI**

Art. 39. São deveres das chefias:

I – assegurar o cumprimento desta Ordem de Serviço, orientando e supervisionando os usuários;

II – zelar pela segurança de suas áreas;

III – controlar o acesso físico aos equipamentos sob sua responsabilidade;

IV – informar imediatamente a Área de Patrimônio do respectivo órgão, sobre o desaparecimento de equipamentos, para que seja procedida a devida busca do bem, sindicância e baixa, se for o caso;

V – não permitir que softwares licenciados para uso do Município sejam copiados por terceiros ou instalados em computadores não autorizados;

VI – manter e preservar as estruturas internas (cabearno lógico, elétrico e telefônico) de suas unidades; e

VII – informar à PROCEMPA as necessidades de manutenção dos equipamentos de informática.

Art. 40. São deveres dos Autorizadores de TI a validação da legitimidade de todas as demandas, antes de encaminhamentos e autorizações junto à PROCEMPA.

Subseção III Da PROCEMPA

Art. 41. São deveres da PROCEMPA:

I – efetuar a criação, remoção dos *logins* dos usuários na rede Municipal;

II – gerenciar o suporte e a manutenção dos recursos de informática;

III – auxiliar as chefias e os usuários, visando ao uso adequado dos recursos de TIC;

IV – realizar ações preventivas e corretivas, com a implantação de mecanismos de controle, a fim de detectar, auditar, evitar ou mitigar irregularidades;

V – instalar *software* a pedido do usuário, desde que previamente autorizados e homologados;

VI – realizar relatório técnico de auditoria, encaminhando o apurado à chefia; e

VII – zelar pela privacidade dos dados do Município, implementando Termo de Confidencialidade a todos os colaboradores que possuam privilégios de acesso administrativo as estações de trabalho, ou que possuam acesso a informações do Município hospedadas em sua infraestrutura de servidores.

Subseção IV Dos Órgãos e Autarquias da Administração Municipal

Art. 42. São deveres dos órgãos e autarquias da Administração Municipal:

I – indicar à PROCEMPA, através de seus respectivos representantes no CTIC, a lista dos responsáveis de TI do respectivo órgão, comunicando também imediatamente quando houver alterações nesses papéis;

II – noticiar à PROCEMPA, através de seus setores de recursos humanos, sobre o encerramento do vínculo funcional, sua alteração, ou afastamento de servidores, de maneira que a PROCEMPA possa adequar as suas credenciais de rede com a celeridade apropriada;

III – envolver a PROCEMPA no planejamento e implantação de qualquer solução de TI disponibilizada por terceiros, seja adquirida ou em carácter de avaliação, de forma que a mesma seja implantada respeitando as diretrizes de estruturação da rede e em conformidade com a Política de Segurança da Informação; e

IV – solicitar à PROCEMPA a orientação sobre a forma apropriada e homologada para acesso remoto por terceiros, quando tal acesso for necessário para suporte a algum sistema instalado na rede PMPA.

Subseção V Do CTIC

Art. 43. São deveres do CTIC:

I – elaborar, aprovar publicar e revisar regularmente a política de segurança da informação (PSI) do Município de Porto Alegre e os demais normativos complementares, necessários para garantir a aplicação das diretrizes estabelecidas nesta Ordem de Serviço;

II – regulamentar a seleção, alteração e publicação dos autorizadores de TIC dos órgãos que compõe a Administração Direta do Município.

Parágrafo único. A PROCEMPA será convidada a manifestar-se como órgão consultivo na elaboração da Política de Segurança da Informação a fim de garantir viabilidade técnica e a compatibilidade entre em regras estabelecidas e a infraestrutura tecnológica da PMPA.

Seção X Dos Controles e Penalidades

Art. 44. Detectados indícios de incidentes de segurança ou de uso inadequado dos recursos de TIC do Município, de forma a estar apta a responder em tempo hábil a ameaças de segurança, a PROCEMPA fica autorizada a auditar sem aviso prévio, em tempo real ou posteriormente ao uso, informações, tais como:

I – o uso de estações, em particular, a lista de programas em execução e de arquivos acessados, localmente e na rede, e a lista de serviços e máquinas acessadas na rede e na *internet*;

II – os cabeçalhos das mensagens de correio eletrônico, incluindo informações tais como o servidor de origem, o remetente, o destinatário e o assunto; e

III – a lista de *sites* acessados na *internet*.

§ 1º Em caso de indício forte de possível incidente de segurança, a PROCEMPA poderá auditar, em tempo real ou posteriormente ao uso, outras informações que sejam necessárias para diagnosticar e mitigar o incidente de segurança.

§ 2º Sempre que a iniciativa de intervenção da PROCEMPA que envolva acesso ao conteúdo dos arquivos e mensagens de correio do usuário não puder ser comunicada antecipadamente aos responsáveis de TI do respectivo órgão, a PROCEMPA deverá emitir um relatório posterior, no prazo de 3 (três) dias úteis, caracterizando a natureza, a motivação e o escopo da ação executada, ou em andamento, a ser enviado ao CTIC ou aos responsáveis de TI do respectivo órgão, conforme apropriado.

Art. 45. A adição, a subtração ou a substituição não autorizada de peças e equipamentos, bem como instalação de *software* não autorizados ou não homologados, constitui adulteração do patrimônio, que ensejará a adoção de medidas disciplinares, bem como a responsabilização por danos causados.

Art. 46. A PROCEMPA, mediante solicitação da chefia ou dos responsáveis de TI dos órgãos, fica autorizada a auditar estações e o acesso dos usuários à rede, por meio direto ou por aplicativos específicos, em tempo real ou posteriormente ao uso, nos moldes que entender conveniente.

Art. 47. Os responsáveis de TI poderão solicitar à PROCEMPA a suspensão liminar do *login* do usuário, comunicando-o imediatamente:

I – por questões de segurança, havendo grave risco de dano aos recursos de TIC; e

II – se constatada a inadequação na utilização dos recursos de TIC.

§ 1º A PROCEMPA poderá suspender liminarmente o *login* do usuário, comunicando imediatamente os responsáveis de TI, pelos motivos mencionados nos incs. I e II deste artigo.

§ 2º O acesso será prontamente restabelecido quando extintas as causas que motivaram a suspensão, mediante solicitação dos responsáveis de TI dos órgãos.

Art. 48. O descumprimento das disposições contidas nesta Ordem de Serviço caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, assegurando-se o contraditório e a ampla defesa dos envolvidos.

Parágrafo único. A autoridade que determinar a instauração de processo administrativo disciplinar poderá requisitar à PROCEMPA a suspensão cautelar do *login* do usuário;

Seção XI **Das Disposições Finais e Transitórias**

Art. 49. O CTIC regulamentará, por meio de instruções normativas, no mínimo, os seguintes temas relacionados à utilização de recursos de TIC:

- I – Política de Segurança da Informação (PSI) do Município;
- II – perfis de acesso aos sistemas, navegação, e quota de *e-mail*, telemática e impressões;
- III – critérios de classificação de sigilo e de criticidade de dados;
- IV – critérios para uso racional e econômico dos insumos de informática;
- V – critérios para uso e aquisição de *software* e sistemas de informática;
- VI – critérios para uso e aquisição de equipamentos de informática;
- VII – critérios para uso de equipamentos e *software* particulares;
- VIII – critérios e procedimentos para descarte de dados e equipamentos;
- IX – critérios e diretrizes para acesso remoto, por terceiros, para fins de suporte a sistemas implementados na *intranet* PMPA; e
- X – critérios para disponibilização de dados abertos.

Parágrafo único. Os normativos que comporem a PSI, complementarão e detalharão as diretrizes dispostas nessa Ordem de Serviço, com o objetivo particular de proteger os recursos e ativos de TIC considerando as propriedades de privacidade, integridade, disponibilidade, auditabilidade, assim como a adequação aos requisitos legais aplicáveis

Art. 50. Os casos omissos serão analisados pelo CTIC, mediante requerimento motivado, por escrito, da chefia das unidades administrativas, podendo o CTIC solicitar manifestação técnico-jurídica prévia, se necessário.

Art. 51. Esta Ordem de Serviço entra em vigor na data da sua publicação.

Art. 52. Fica revogada a Ordem de Serviço nº 003, de 17 de fevereiro de 2016.

PREFEITURA MUNICIPAL DE PORTO ALEGRE, 3 de julho de 2018.

Nelson Marchezan Júnior,
Prefeito de Porto Alegre.