

Instrução Normativa SCI nº. 01/2018

DISPÕE SOBRE A REGULAMENTAÇÃO DA UTILIZAÇÃO DOS RECURSOS DE INFORMÁTICA E REDES DA PREFEITURA MUNICIPAL DE SANTA HELENA (SC), VISANDO ESTABELECEER UMA POLÍTICA DE SEGURANÇA DOS DADOS E INFORMAÇÕES DA INSTITUIÇÃO E A PRIVACIDADE EFETIVA DOS USUÁRIOS.

Marcelo Campagnaro, Controlador Interno do Município de Santa Helena, Estado de Santa Catarina, no uso de suas atribuições legais, e visando estabelecer uma política de segurança dos dados e informações da Prefeitura e a privacidade efetiva dos seus usuários, resolve expedir a seguinte Instrução Normativa:

CAPÍTULO I DA UTILIZAÇÃO

Art. 1º A presente Normativa visa estabelecer a política de segurança e racionalização na utilização dos recursos computacionais no âmbito da Prefeitura.

Parágrafo único. A utilização destes recursos está relacionada às funções dos usuários e à prestação de serviços das Unidades Administrativas.

Art. 2º Para obter o acesso à rede e recursos de informática, o servidor público deverá utilizar seu login e senha exclusivos, obtidos junto ao Setor de TI da prefeitura.

Parágrafo único. Ao adotar e utilizar os recursos, o servidor manifesta conhecimento, concordância e comprometimento de acatar este regulamento e demais normas referentes ao uso da informática.

CAPÍTULO II DOS USUÁRIOS

Art. 3º São considerados usuários autorizados para utilização dos sistemas de informações e das redes de computadores da Prefeitura todos os servidores municipais.

Parágrafo único. Compete ao Setor de Tecnologia da Informação a concessão de autorizações de acesso ao que se refere o "caput" deste artigo, mesmo àquelas de caráter especial ou por tempo determinado, desde que esta utilização esteja de acordo com as determinações deste regulamento.

CAPÍTULO III

DAS RESPONSABILIDADES INDIVIDUAIS

Art. 4º Nenhum usuário poderá ter acesso, copiar, alterar ou remover arquivos de terceiros sem autorização explícita do usuário a quem os arquivos pertençam.

Parágrafo único. Ressalvam-se do dispositivo previsto no "caput" deste artigo, os casos especiais protegidos por lei ou regulamento.

Art. 5º O usuário é responsável por sua identificação na rede corporativa (login) e deverá protegê-lo de acessos de terceiros através de senhas secretas e procedimentos de segurança.

Art. 6º O usuário é inteiramente responsável pelo uso de sua conta de acesso à rede, senha e outros tipos de autorização, que são de uso individual e intransferível, e não podem ser compartilhados com terceiros.

Art. 7º É vedado ao usuário autorizar acesso de terceiros aos recursos de informática ou rede da Prefeitura, executando, instalando ou modificando a configuração de software ou hardware, sem a prévia autorização do Setor de Tecnologia da Informação.

Art. 8º O usuário é responsável pela manutenção de senhas seguras, devendo seguir normas e procedimentos padronizados e divulgados pelo Setor de Tecnologia da Informação.

Art. 9º O usuário é totalmente responsável por ações indevidas que venham a ser efetuadas a partir de sua conta de acesso à rede, caso alguém obtenha o acesso à sua conta devido à não utilização de senhas seguras.

Art. 10. O usuário tem o dever de respeitar a propriedade intelectual e os direitos autorais, sob as penas previstas em lei.

Art. 11. Nenhum usuário pode, sob quaisquer circunstâncias, usar computadores e redes da Prefeitura para difamar, caluniar ou molestar outras pessoas.

Parágrafo único. Fica expressamente proibido a utilização de logins considerados *fakes* para ações previstas no "caput" deste parágrafo.

Art. 12. Entende-se por molestamento o uso intencional dos recursos de informática ou redes para:

I - perturbar, amedrontar, ameaçar ou ofender pessoas usando linguagem ou qualquer outro mecanismo ou material que comprometam a integridade física ou moral do receptor ou de sua família;

II - contatar alguém várias vezes com a intenção de perturbá-la, enviando ou não mensagens, seja quando não existe uma proposta de comunicação ou quando o receptor expressa o desejo de finalizar a comunicação;

III - não disponibilizar recursos computacionais de forma intencional;

IV - invadir a privacidade da Prefeitura, seus usuários ou de terceiros.

§ 1º Os usuários não podem, deliberadamente, sobrecarregar os recursos computacionais ou de rede corporativa da Prefeitura.

§ 2º É vedado ao usuário conectar computadores mono e/ou multiusuário e servidores de rede ou similares de qualquer espécie, à rede de computadores da Prefeitura sem notificação e autorização dos administradores ou dos supervisores responsáveis pela rede computacional, assim como acessar a Internet por outro provedor que não seja o da Prefeitura.

Art. 13. É dever do usuário estar ciente do potencial e das possíveis consequências da manipulação de informações que acessa e/ou utiliza.

CAPÍTULO IV DO ACESSO ÀS INFORMAÇÕES

Art. 14. O acesso especial a senhas, informações ou outros privilégios só podem ser usados para o exercício de tarefas oficiais, como supervisão e administração das redes.

Art. 15. Informações obtidas por meio de direitos especiais e privilégios devem ser tratados como privativas e totalmente confidenciais pelos administradores de rede, que responderão por qualquer uso indevido.

Art. 16. Ao deixar de ser servidor da Prefeitura, ou ao ser nomeado para assumir uma nova função e/ou novas responsabilidades, o usuário não poderá fazer uso de benefícios, contas, senhas de acesso, direitos especiais ou informações aos quais não está autorizado em sua nova situação.

Parágrafo único: Privilégios especiais não são incorporados permanentemente aos direitos dos usuários.

Art. 17. O Setor de Tecnologia da Informação poderá suspender todos os privilégios de determinado usuário em relação ao uso das redes e computadores sob sua responsabilidade, por razões disciplinares ou relacionadas à segurança dos dados e informações e ao bem-estar dos servidores municipais ou da Prefeitura.

Parágrafo único: A ação de que trata este artigo será efetivada mediante comunicação e autorização do Chefe Superior do usuário infrator.

Art. 18. Todos os computadores conectados à rede da Prefeitura ou das unidades administrativas devem obedecer aos procedimentos padronizados estabelecidos pelo Setor de Tecnologia da Informação.

Art. 19 É facultado aos administradores de rede o acesso a todos os equipamentos ligados à rede, de forma a ser possível a realização de procedimentos de auditoria, controle, manutenção e segurança que se fizerem necessários.

Parágrafo único: Considerar-se-á também procedimentos de auditoria, controle, manutenção e segurança a que se refere o “caput” deste artigo, análise aos logs de eventos gerados por acessos aos servidores dedicados de rede, os quais serão armazenados durante o período máximo de 01 (uma) semana ou enquanto houver espaço físico para armazenamento dos mesmos.

CAPÍTULO V DAS PROIBIÇÕES

Art. 20. Os usuários não podem utilizar qualquer software ou outro dispositivo para interceptar ou decodificar senhas ou similares.

Art. 21. É proibida toda e qualquer tentativa deliberada de retirar o acesso à rede ou a qualquer recurso de informática da Prefeitura, ou de prejudicar o seu rendimento.

Art. 22. É proibido o encaminhamento para manutenção terceirizada de qualquer equipamento sem conhecimento e autorização do Setor de Tecnologia da Informação.

Art. 23. É proibido autorizar acesso aos equipamentos ou sistemas a qualquer pessoa sem conhecimento e autorização do Setor de Tecnologia da Informação.

CAPÍTULO VI DA CLASSIFICAÇÃO DOS PROCEDIMENTOS

Art. 24. É considerado como procedimento grave:

I - criar ou propagar quaisquer tipos de Praga Virtual;

II - danificar serviços e arquivos;

III - destruir ou danificar intencionalmente equipamentos, software ou dados pertencentes à Prefeitura ou a outros usuários;

IV - obter acesso a qualquer recurso não autorizado;

V - destituir e/ou instituir direitos para outros usuários;

VI - instalação de software não autorizado;

§ 1º É proibida a veiculação de nomes de empresas, instituições ou pessoas junto aos sistemas de informação da Prefeitura que não estejam oficialmente reconhecidas através de convênios de cooperação ou parceria acadêmica, técnica ou científica.

§ 2º É proibida a utilização dos recursos de informática e redes para fins particulares, ou em benefício de organizações que não tenham relação ou sejam do interesse da Prefeitura.

Art. 25. É considerado conteúdo inapropriado para acesso, através da infraestrutura de informática da Prefeitura, qualquer página que contenha referências a:

I - nudez total ou parcial;

II - atos sexuais;

III – pornografia ou pedofilia;

IV - erotismo;

V - terminologia de baixo calção;

VI - violência;

VII - racismo;

VIII - satanismo e ocultismo;

IX - intolerância;

X - extremismo;

XI - material ilegal ou dados que levem a condutas ilegais;

XII - cassinos e jogos de azar;

XIII - sites de "hackers";

XIV - salas públicas de conversação on-line (chat);

XV - serviços de intermediação de navegação (navegação com IP diferente);

XVI – sites de relacionamentos;

XVII – jogos on-line;

XVIII – redes sociais.

Parágrafo único: Poderão ter acesso às categorias dos sites que se refere o "caput" deste artigo, os servidores devidamente autorizados através de solicitação formal em meio digital ou impresso, mediante solicitação devidamente justificada da chefia ou responsável.

CAPÍTULO VII DOS PROCEDIMENTOS E DAS SANÇÕES

Art. 26. Os interessados, ao se cadastrarem como usuários dos recursos de informática e redes da Prefeitura, devem preencher e assinar uma ficha cadastral, manifestando

conhecimento e concordância com as normas específicas e padrões para utilização e acesso aos recursos de cada unidade administrativa.

Art. 27. Os usuários, supervisores e administradores de rede têm o dever de denunciar qualquer desrespeito a este regulamento, tomando imediatamente as seguintes providências:

I - comunicar ao chefe imediato, à direção da unidade administrativa e ao Setor de Tecnologia da Informação;

II - manter o sigilo, para garantir a segurança e a conservação dos recursos.

Art. 28. O primeiro incidente envolvendo um usuário, será tratado a nível do Setor de Tecnologia da Informação, o qual tomará as providências previstas nesta Portaria ou em normas internas, com posterior registro da ocorrência.

Art. 29. Reincidências e incidentes considerados graves deverão ser tratados pelo Setor de Tecnologia da Informação, o qual informará o caso aos órgãos competentes, caso necessário, para determinação das sanções a serem impostas, com posterior registro da ocorrência.

CAPÍTULO VIII DAS PENALIDADES

Art. 30. Penalidades Nível I (leve): As leves serão advertidas por escrito ao usuário infrator com uma cópia ao seu superior hierárquico.

Art. 31. Penalidade Nível II (reincidências e grave): A reincidência ou a constatação de infração grave será encaminhada à Secretaria Municipal da Administração, para as providências administrativas competentes.

Art. 32. Todas as demais violações às normas, ainda que não expressas, poderão ser punidas com suspensão temporária ou permanente de privilégios de acesso aos recursos computacionais após avaliação da gravidade da infração.

§ 1º Caso as infrações às normas de segurança impliquem também em falta disciplinar, o assunto será objeto de apuração e solução mediante a aplicação das normas existentes na Prefeitura.

§ 2º As sanções impostas não isentam o infrator de outras cominações legais.

CAPÍTULO IX DAS PRÁTICAS RECOMENDADAS

Art. 33. São de orientação prática por parte do Setor de Tecnologia da Informação, visando normas de conduta quanto ao uso dos recursos tecnológicos:

I – Desligar os equipamentos corretamente, após cada término de expediente, principalmente computadores, impressoras e demais periféricos.

II – Evitar acesso a serviços de streaming, principalmente vídeos, quando não forem específicos e inerentes para a atividade profissional;

III – Procurar utilizar-se dos recursos de bate-papo de ferramentas disponíveis, em detrimento ao uso de telefone;

IV – O uso de smartphones e seus aplicativos, desde que voltados à assuntos de interesse público e profissional, e ainda, em momentos de não atendimento ao munícipe;

V – Realização de Backups rotineiros (não superiores a uma semana) dos sistemas sob sua responsabilidade.

Parágrafo Único: O que tange o item V deste artigo, buscar orientações junto ao Setor de Tecnologia da Informação, sobre a melhor forma de realização dos backups.

DAS DISPOSIÇÕES FINAIS

Art. 34. Toda estrutura administrativa deverá observar as disposições da presente Portaria, sob pena de incorrer nas penalidades previstas.

Art. 35. Casos omissos a esta Normativa serão tratados pelo Setor de Tecnologia da Informação em conjunto com os Secretários Municipais e chefe do Executivo.

Art. 36. Esta Normativa entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Santa Helena/SC, 18 de outubro de 2018.

MARCELO CAMPAGNARO
Coord. Controle Interno

LUIZ GLUITZ
Prefeito Municipal