Política de controle de acesso à Internet

1 Apresentação

Este documento descreve uma política que visa assegurar o uso apropriado da Internet pelos usuários na Prefeitura do Município de Quatá. Por usuário, entende-se todos aqueles que utilizam Internet na prefeitura, compreendendo: funcionários, estagiários e prestadores de serviço.

2 Objetivos

Definir regras a serem seguidas no âmbito da Prefeitura do Município de Quatá relativas ao acesso a sites e serviços da Internet.

Melhorar a estabilidade e a disponibilidade de recursos de Internet.

Termo de Ciência de Uso

1. Os usuários podem ser servidores públicos municipais (em caráter efetivo, contrato ou comissionado), bem como estagiários ou prestadores de serviços, desde que vinculados à Prefeitura do Município de Quatá.

2. O acesso à Internet é um direito concedido a cada usuário por meio de credencial (*login* e senha) pessoal e intransferível.

3. O usuário deverá assinar um termo de ciência e entregar ao Analista de TIC ou a pessoa por ele autorizada para obter sua credencial de acesso à Internet.

4. Cada usuário é o único e total responsável por sua credencial, assim como por todas as ações realizadas por este código. O usuário terá direito de acesso à Internet enquanto tiver vínculo com a Prefeitura do Município de Quatá.

5. Antes de ausentar-se do seu local de trabalho, recomenda-se ao usuário desconectar-se de sua credencial ou bloquear o acesso ao computador por meio de senha.

6. O acesso à Internet é permanentemente monitorado e pode ser auditado. A princípio, as informações só podem ser acessadas pelo Setor de Tecnologia da Informação. Superiores de cada secretaria poderão solicitar, por escrito, relatórios de utilização. Ainda cabe ressaltar que os relatórios serão fornecidos mediante ordem judicial.

7. O superior de cada secretaria poderá definir quais conteúdos devem ser liberados ou bloqueados para cada usuário de sua pasta.

8. É permanentemente proibido utilizar a Internet disponibilizada pela Prefeitura do Município de Quatá para:

   a) constranger, assediar, prejudicar ou ameaçar qualquer pessoa;

   b) fazer-se passar por outra pessoa ou camuflar sua identidade quando utilizar os recursos computacionais com a finalidade de enganar outras pessoas;

   c) tentar obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como *cracking*). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;

d) tentar interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques de negação de serviço (DDoS, do inglês *Distributed Denial of Service*), provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;

e) acessar sites de conteúdo impróprio, tais como:

i. apologia ao uso de drogas;

ii. apologia à violência e ao terrorismo;

iii. conteúdo ofensivo, preconceituoso ou discriminatório;

iv. pornografia, em especial pedofila e

v. violação de direitos autorais.

9. O acesso a sites e serviços disponíveis na Internet será controlado por filtros de conteúdo e reguladores de tráfego implementados nos dispositivos de segurança de rede.

10. O Setor de Tecnologia da Informação utilizar-se-á da tecnologia disponível para bloquear o acesso a sites de conteúdo impróprios.

11. O Setor de Tecnologia da Informação utilizar-se-á da tecnologia disponível para bloquear o acesso a serviços que estejam realizando um alto consumo de banda e assim, comprometendo a utilização de Internet dos demais usuários.

12. O Setor de Tecnologia da Informação receberá solicitações do superior de cada secretaria e poderá liberar ou bloquear serviços de acordo com a necessidade apresentada.

13. O Setor de Tecnologia da Informação utilizar-se-á da tecnologia disponível para controlar a banda e a velocidade de acesso à Internet para cada usuário a fim de garantir uma maior estabilidade e disponibilidade de recursos de Internet a todos.

14. Periodicamente, a lista de serviços e sites bloqueados será analisada e poderá ser alterada.

Eu, _____, portador do CPF _____, declaro, nesta data, ter ciência e estar de

acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los.

____/____/_____, Quatá-SP

_____

Assinatura