

GUIA DE BOAS PRÁTICAS EM TECNOLOGIA DA INFORMAÇÃO

“Segurança da informação e comunicação um compromisso de todos”.

“Simples atitudes podem evitar grandes problemas”.



Sumário

INTRODUÇÃO.....	3
SOFTWARE LIVRE.....	3
POLÍTICAS DE USO DOS COMPUTADORES.....	3
Para que serve uma política de uso?.....	3
Quais recursos computacionais devem seguir a política de uso?.....	3
Quais recursos computacionais devem seguir a política de uso?.....	3
O que posso instalar no computador?.....	3
Que tipo de sítios posso acessar?.....	4
Cuidados para utilização dos equipamentos de informática.....	4
Como utilizar de forma segura o sistema operacional e aplicativos.....	5
Da utilização dos Laboratórios de Informática.....	7
Da utilização de equipamentos de informática nos auditórios.....	7
SERVIÇOS DISPONÍVEIS AOS USUÁRIOS.....	8
Como solicitar acesso a rede?.....	8
Como solicitar o desenvolvimento de um novo sistema?.....	8
Como acessar o servidor de arquivos?.....	8
Como solicitar a recuperação de um arquivo perdido?.....	9
Como solicitar um equipamento?.....	9
Como solicitar um suporte técnico?.....	9
Como acompanhar uma solicitação de suporte técnico?.....	9
SEGURANÇA DA INFORMAÇÃO.....	10
SEGURANÇA DA INFORMAÇÃO.....	10
O que pode ocorrer com um computador vulnerável?.....	10
Senhas.....	10
Como alterar minha senha?.....	10
Minha senha foi bloqueada, o que eu faço?.....	10
Esqueci minha senha, o que eu faço?.....	10
Como utilizar minha senha com segurança?.....	10
Quais os riscos ao navegar na internet?.....	11
Programas Maliciosos.....	11
O antivírus protege contra programas maliciosos?.....	11
Recebi um e-mail solicitando minha senha, devo responder?.....	11
Recebi um e-mail solicitando divulgação de um fato, o que faço?.....	12
Como verifico se um arquivo está com vírus?.....	12
Como verifico se um arquivo está com vírus?.....	12
Como “limpar” meu computador?.....	12
Existe alguma rotina automática para limpar meu Computador?.....	12
Preciso fazer backup dos meus dados?.....	12
REDE SEM FIO.....	12
Quais os riscos em utilizar rede sem fio?.....	13
Como acessar a rede sem fio?.....	13
Quais áreas que possuem cobertura da rede sem fio?.....	13
A QUEM PROCURAR EM CASO DE PROBLEMAS?.....	13
OS 10 MANDAMENDOS DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO.....	13

1 INTRODUÇÃO

A tecnologia faz parte da vida das pessoas, empresas privadas e setor público. Do aluno da rede pública de ensino aos grandes centros de pesquisa, da dona de casa ao executivo, todos interagem de alguma forma com recursos de TI. Para que toda a informação que circula possa servir somente ao seu propósito, que é o de informar, sem prejudicar quaisquer pessoas ou instituições, é necessária a gestão segura dos recursos disponíveis em tecnologia da informação.

Na Prefeitura Municipal de Murici não é diferente. Aliás, deve-se sempre adotar os procedimentos padrões, de modo a contribuir de forma positiva com a disponibilidade, integridade, confidencialidade e autenticidade da informação.

O desafio de fomentar a Segurança da Informação e Comunicações é grande, afinal, são muitos computadores, servidores e usuários distribuídos em vários pontos e instâncias. Mas está longe de ser impossível, pois depende principalmente da atenção e da atitude das pessoas sobre as boas práticas de TI.

A partir de agora você tem acesso a informações fundamentais para um serviço público eficiente para o seu dia a dia e adaptado aos novos tempos.

2

SOFTWARE LIVRE

O setor de tecnologia passou a adotar uma ação de reusabilidade de software, quando alguma subunidade solicita uma aplicação, a primeira tarefa a ser realizada é uma busca no cenário nacional por algum software livre que sirva de solução para a demanda, atualmente o Governo Federal disponibiliza o Portal do Software Público Brasileiro, caso a solução não seja adequada novas fontes são procuradas até que se encontre um software capaz de dar uma resposta ao usuário. Quando não há realmente uma solução baseada em software livre, o setor de tecnologia passa para demanda proprietária que precisa ser licenciada para ser utilizada.

3 POLÍTICAS DE USO DOS COMPUTADORES

3.1 Para que serve uma política de uso?

Para estabelecer padrões e procedimentos que busquem a segurança, estabilidade e disponibilidade dos serviços computacionais.

3.2 Quais recursos computacionais devem seguir a política de uso?

Quaisquer equipamentos, programas, meios físicos de tráfego e sistemas de armazenamento digital inseridos no ambiente da Prefeitura Municipal de Murici, incluindo notebooks, tablets, smartfone, pen drives, HD externos, impressoras, além das estações de trabalho.



Então, por razões de padronização e segurança, o usuário não pode instalar aplicativos e programas sem intervenção do setor de Tecnologia. Em caso de necessidade específica de algum programa ou sistema, deve-se entrar em contato com a Divisão de Tecnologia da Prefeitura para averiguar o possível licenciamento ou instalação caso seja software livre.

3.3 Que tipo de sites posso acessar?

Por motivos de segurança e disponibilidade do link de dados, o acesso aos sites está sendo filtrado para inibir acessos a conteúdos indevidos ou inadequados ao ambiente de trabalho. Em caso de necessidade de acesso a um site que esteja bloqueado, consulte a Divisão de Tecnologia sobre a possibilidade de liberação.

3.4 Cuidados para utilização dos equipamentos de informática

- Não ligar o computador, impressora, fax, escâner, bebedouro, etc, na mesma tomada, seja usando extensões, no breaks, estabilizadores ou adaptadores elétricos. Caso isso ocorra será gerada uma sobrecarga elétrica podendo queimar um ou mais equipamentos e ocasionar princípio de incêndio;
- Quando se perceber alterações na rede elétrica, deve-se salvar os documentos e por medida de segurança desligar os equipamentos por um período, até que a rede elétrica volte ao normal. As principais características de alterações na rede elétrica são: lâmpadas piscando ou com luminosidade fraca, constantes bips de no breaks ou estabilizador, várias interrupções no fornecimento de energia por um curto período de tempo;
- Quando não for mais utilizar os equipamentos desligar normalmente e após isso retirar o plugue da tomada;
- Ao ligar uma impressora aguarda o tempo necessário para o que o sistema de impressão seja carregado, o tempo médio é de 3 minutos, só após esse tempo se deve mandar os documentos para impressão;
- O abastecimento da impressora com excesso de papel, pode causar o problema na tração dos roletes uma vez que podem se puxados mais de uma folha ao mesmo tempo, este mesmo problema pode ocorrer em caso de folhas úmidas, sempre que for abastecer com folhas verifique se as mesmas estão soltas;
- Quando a impressora estiver por muito tempo sem uso, antes da impressão solte as folhas com a mão deixando-as separadas;
- Quando ocorrer de uma folha ficar presa dentro da impressora, primeiro cancele o processo de impressão e desligue-a da rede elétrica antes de tentar remover a folha. Caso a remoção esteja exigindo muita força solicite a presença do técnico, remover uma folha pode causar desalinhamento em peças internas;



- Não retirar e colocar de maneira brusca o t ner/cartucho da impressora, pode haver derramamento do p /tinta de impress o ocasionando ac mulo de sujeira dentro do equipamento;
- Toda impressora possui um tempo de espera para que o documento seja totalmente carregado em sua mem ria, somente ap s esse procedimento   que ser  impresso. Ent o o usu rio deve enviar o arquivo para impress o e aguarda ele ser impresso, n o adianta mandar duas ou tr s vezes o mesmo documento que ele n o ser  impresso mais r pido, e sim consumir mais papel e t ner da impressora, caso o tempo de espera ultrapasse 2 minutos ai sim poder  ser considerado um problema e deve-se verificar: papel na impressora, t ner e papel preso, caso nenhum desses seja o problema procurar o setor de tecnologia para averigua o;
- N o deixar os cabos que conectam a impressora, esc ner ou o computador muito esticados ou mal encaixados;
- Deixe o computador limpo, livre de poeira e umidade;
- Em casos de rel mpagos, desligue o equipamento da tomada;
- Evite fazer refei es na frente do computador;
- N o conecte ou desconecte nenhum cabo com o computador ligado, exceto os cabos de rede e USB;
- N o bata, empurre ou mude de lugar o computador com ele ligado, isso pode prejudicar o hardware do computador;
- N o deixar materiais pesados em cima dos gabinetes e monitores;
- Nunca use aqueles famosos CDs para limpar o leitor de CD/DVD, muitos (se n o todos) s o feitos com um produto que oxida, riscam e enchem de poeira; Mantenha o gabinete e o local onde o computador est  sempre muito bem arejado;
- N o ligue e desligue o computador diversas vezes consecutivas, voc  pode danificar algum componente;

3.6 Como utilizar de forma segura o sistema operacional e aplicativos

- Quando utilizar um pendrive, c meras digitais, celulares ou outros dispositivos conectados ao computador, a primeira coisa a fazer   uma varredura com o antiv rus para eliminar programas maliciosos. Uma simples abertura do dispositivo sem os cuidados necess rios   suficiente para infectar o computador com programas maliciosos, corromper arquivos e pastas do sistema deixando o computador inutiliz vel at  os devidos reparos;



- Não deixar que usuários não autorizados ou que não sejam do setor administrativo da Prefeitura utilizem os computadores e impressoras, pois se eles não possuírem conhecimentos para prevenir contaminação por vírus de computador ou manuseio de impressoras, poderão danificar os equipamentos ou o sistema operacional e acessar sites de conteúdo nocivos ao computador como: jogos, pornografia, download de filmes e músicas. Prejudicando a utilização da rede de computadores para tarefas administrativas e acadêmicas;
- Sempre fazer o backup de seus arquivos pessoais ou de trabalho pelo ao menos uma vez por semana;
- Nunca desligar o computador diretamente na tomada elétrica ou no botão de desligar, sempre utilizar o método tradicional do sistema operacional;
- Não Clique em Links desconhecidos que você recebe pelas Redes/E-mail etc;
- Em suas senhas combine letras, números e caracteres especiais;
- Nunca forneça suas senhas a ninguém;
- Não clique em *link* recebido através de redes sociais, pois estes podem apontar para *malwares* e sites de *phishing*. Principalmente se este *link* vier de alguém desconhecido;
- Nunca utilize senhas baseadas em informações pessoais;
- Jamais clique em programas recebidos por e-mail cuja origem você desconhece;
- Verifique com antivírus atualizado os arquivos recebidos por e-mail antes de executá-los;
- A menos que você solicite, bancos nunca entram em contato com clientes através de e-mail, muito menos operadoras de cartões de crédito;
- Desconfie de todas as mensagens recebidas por e-mail cujo conteúdo solicite informações ou atualizações de dados pessoais;
- Não clique em URL de bancos recebidas por e-mail. Elas normalmente direcionam usuários para sites fraudulentos;
- Acostume-se a sempre digitar manualmente no seu navegador o endereço (URL) do seu banco;
- Em acessos a páginas da Internet que peçam login e senha. sempre verifique a presença do cadeado fechado no canto inferior direito do seu navegador.



- Quando houver cursos, palestras e reuniões que será necessário utilizar o equipamento de videoconferência, informar com antecedência o setor de tecnologia para que a instalação seja realizada;

videoconferência, é de inteira responsabilizada do setor de tecnologia a instalação e configuração do equipamento;

- Ao utilizar as dependências dos auditórios os Funcionários, técnicos e administrativos devem zelar pelos equipamentos de tecnologia;

4 SERVIÇOS DISPONÍVEIS AOS USUÁRIOS

O setor de tecnologia disponibiliza vários serviços para todo o parque computacional da Prefeitura Municipal de Murici para que tudo funcione corretamente é necessário a contribuição do usuário final seguindo as normas aqui estabelecidas, como principais serviços temos:

- Acesso a rede sem fio
- Servidor de compartilhamento de arquivos, permitindo interação mais rápida entre as subunidades;
- Serviço de atualização automática de computadores, diminuindo o tráfego de dados e melhorando a conexão de internet
- Filtro de conteúdo, melhorando a qualidade de acesso à internet;
- Sistema de atendimento em Tecnologia e Infraestrutura, velocidade em detecção e resolução de problemas técnicos e de infraestrutura predial;

4.1 Como solicitar acesso a rede Prefeitura?

Para servidores, os passos são:

- A chefia imediata solicita a criação de login e senha através do sistema de atendimento;
- Aguardar o atendimento e informações através do sistema;
- Realizar a primeira autenticação com as informações passadas através do sistema e alterar a senha padrão;
- Seguir as normas de segurança e políticas de uso dos computadores;

4.2 Como solicitar o desenvolvimento de um novo sistema?

- Se for necessário desenvolver um novo sistema de informação, o responsável da área deve encaminhar o pedido ao setor de tecnologia, por meio de memorando;
- A solicitação será analisada, caso haja a possibilidade de utilização de um sistema baseado em software livre, este terá prioridade na implantação;
- Todo desenvolvimento de software deverá respeitar a disponibilidade de pessoal e conhecimento técnico do setor de tecnologia;

4.3 Como acessar o servidor de arquivos?

- Toda subunidade tem um espaço no servidor de armazenamento de dados para guardar



arquivos. Durante o processo de autenticação da rede, o sistema mapeia automaticamente uma letra associada ao espaço correspondente ao seu setor. Esse espaço é exclusivo para alocar arquivos que fazem parte do trabalho. Não se deve armazenar, nesse local, arquivos de cunho particular ou arquivos do tipo, imagem, vídeos ou áudio. Necessidades específicas de armazenamento devem ser solicitadas junto ao setor de tecnologia, que será analisada a possibilidade de atendimento

- e liberação de acesso ao respectivo compartilhamento.

4.4 Como solicitar a recuperação de um arquivo perdido?

- Caso algum arquivo tenha sido excluído indevidamente do servidor de rede, é necessário solicitar a restauração através do sistema. É preciso informar o caminho completo do arquivo ou da pasta que se deseja recuperar;
- A política de backup do servidor de arquivos é feita diariamente, portanto se o arquivo excluído foi criado no mesmo dia, é necessário uma ação de recuperação até as 22 horas do dia corrente, caso ultrapasse o tempo o arquivo poderá ser perdido completamente.

4.5 Como solicitar um equipamento?

- Para solicitar equipamentos de informática, o responsável pela subunidade deve encaminhar memorando com o pedido para o setor de tecnologia.
- A solicitação deve ser detalhada para que o setor de tecnologia avalie a melhor configuração a ser utilizada.

4.6 Como solicitar um suporte técnico?

- Todo atendimento de tecnologia da informação respeitará a ordem de solicitações feitas no sistema;
- Qualquer solicitação feita fora do sistema dependerá da disponibilidade técnica dos servidores de TI;
- Toda a troca de informações sobre o suporte técnico será feita através do sistema, via inserção de comentários;
- É de responsabilidade do usuário acompanhar o andamento de sua solicitação e fornecer informações quando solicitado;

4.7 Como acompanhar uma solicitação de suporte técnico?

Toda solicitação feita dentro do regimento e precisa ser acompanhada pelo usuário até que termine o atendimento, é através desse monitoramento que haverá a troca de informações entre o setor de tecnologia e o usuário.



5 SEGURANÇA DA INFORMAÇÃO

5.1 O que pode ocorrer com um computador vulnerável?

Entre outras coisas, pode ocorrer:

- Roubo de informação;
- Perda de dados;
- Redução de desempenho;
- Uso do computador para atacar servidores e outros computadores.

Por isso, os cuidados com a segurança são importantes.

5.2 Senhas

Na Prefeitura são utilizadas senhas para:

- Acesso a rede;
- Acesso a internet;
- Sistema;

Além dessas, podem ser necessárias outras para acessar aplicativos específicos.

5.3 Como alterar minha senha?

Para alterar suas senhas, veja os passos descritos a seguir para cada tipo de acesso:

- **Acesso a rede e a internet**
 1. Pressione a combinação de teclas ctrl+alt+del;
 2. Clique em “Alterar uma senha”;
 3. Forneça a senha atual, nova senha e confirme a nova senha.

5.4 Minha senha foi bloqueada, o que eu faço?

Por razões de segurança, quando o sistema de monitoramento detecta algum tipo de atividade suspeita com o perfil de usuário, automaticamente o perfil é bloqueado. Neste caso, você deve ligar para o setor de Tecnologia e solicitar a liberação.

Importante: somente o próprio usuário pode solicitar a liberação do acesso ou uma nova senha.

5.5 Esqueci minha senha, o que eu faço?

É necessário abrir uma solicitação de suporte técnico, para isso poderá solicitar junto a sua subunidade para alguém que possua o perfil de acesso.

5.6 Como utilizar minha senha com segurança?

- Jamais compartilhe senhas com outras pessoas. Lembre-se que, a princípio, você é o



responsável por tudo que ocorre com o uso de sua senha.

- Se você não consegue memorizar suas senhas e precisa anotar em algum lugar, dificulte o acesso das pessoas aos seus lembretes. Não deixe suas senhas anotadas em locais visíveis, de fácil acesso, expostas em cadernos, pastas ou marcadores em sua mesa de trabalho.
- A senha existe para evitar acessos não autorizados por outras pessoas a ambientes e sistemas que exigem segurança e controle, por isso, bloqueie sempre o seu computador em suas ausências, evitando o acesso indevido a informações sob sua responsabilidade. No Windows, utilize o conjunto de teclas <Ctrl> + <Alt> + ou <Windows> + <L> para bloquear rapidamente o computador.
- Utilize senhas também em celulares e notebooks, protegendo suas informações em caso de extravio, furto ou roubo do equipamento.
- Sempre que possível diversifique as senhas que possui, evitando que a descoberta de uma delas dê acesso a outras informações protegidas.

5.7 Quais os riscos ao navegar na internet?

Alguns sítios exploram vulnerabilidades dos navegadores e acabam instalando programas maliciosos no computador do usuário. Por isso, é importante manter os aplicativos atualizados e não fazer download de arquivos em sites desconhecidos.

5.8 Programas Maliciosos

São programas criados para executar ações maliciosas no computador, como captura de senhas e danificação de arquivos e programas. Os mais comuns são:

Vírus – programa que infecta o computador utilizando-se de diversos meios. É replicado pela ação do computador infectado.

Cavalo de troia – programa invasor que pode ler, copiar, apagar e alterar dados do sistema sem o conhecimento do usuário.

Backdoors – programa que tenta obter controle de uma máquina aproveitando-se uma falha de segurança em um programa de computador ou sistema operacional, abrindo uma porta para seu invasor controlar o computador remotamente.

Keylogger – programa capaz de capturar e armazenar as teclas digitadas pelo usuário.

5.9 O antivírus protege contra programas maliciosos?

Em geral, o antivírus detecta programas maliciosos oriundos de e-mails, CDs, cartões de memória, pen drives etc. Contudo, é sempre bom tomar cuidado com todas as mídias que recebe. Verifique sempre se o antivírus está funcionando e atualizado.

Evite também executar programas ou abrir arquivos de origem duvidosa. Lembre-se que, por exemplo, joguinhos de computador aparentemente inofensivos, ao serem executados, poderão conter e instalar programas maliciosos, que poderão ocasionar danos irreversíveis aos seus arquivos, mau funcionamento do seu equipamento ou até mesmo furtar suas senhas. Muitas vezes, esses arquivos podem vir de amigos ou colegas de trabalho que desconhecem que seus arquivos possuem essa ameaça.

5.10 Recebi um e-mail solicitando minha senha, devo responder?

Não! Nunca se deve informar senhas e dados pessoais por e-mail. Há uma prática maliciosa conhecida como “phishing”, que consiste em solicitar informações ou ações do



usuário. Cuidado, como essas mensagens se assemelham a e-mails verdadeiros, é possível o recebimento de algum e, por isso, deve-se estar sempre atento.

5.11 Recebi um e-mail solicitando divulgação de um fato, o que faço?

É comum algumas mensagens do tipo “Ajude essa criança com câncer” ou “Previna-se do novo vírus” solicitando divulgação (“envie para todos da sua lista”). A maioria dessas mensagens é boato e não deve ser passada adiante. Vários vírus são disseminados por meio de links em textos ou em fotos. Não se deve, portanto, abrir anexos ou links recebidos de remetentes desconhecidos.

5.12 Como verifico se um arquivo está com vírus?

Sempre que um arquivo é acessado, a ferramenta de antivírus instalada nos computadores da Prefeitura Municipal verifica automaticamente se há vírus ou não. Caso queira verificar manualmente um arquivo, efetue os seguintes passos:

1. Clique sobre o ícone do arquivo, pasta ou unidade com o botão direito do mouse e escolha a opção “Verificar com o Microsoft Security Essentials”;
2. Aguarde enquanto a ferramenta efetua a varredura;
3. Caso algum programa malicioso seja detectado, a ferramenta tentará removê-lo automaticamente, se for necessário solicitará uma confirmação do usuário;
4. Ao terminar a verificação feche a ferramenta Microsoft Security Essentials

5.13 Como “limpar” meu computador?

Para executar uma varredura completa no computador, faça o seguinte:

1. Clique no ícone do castelo verde, localizado na barra do menu iniciar próximo ao relógio, escolha a opção “Abrir”;
2. Ao abrir a janela, no lado direito selecione o tipo de varredura, escolha a opção “Completo”;
3. Clique no botão “Verificar” e aguarde o processamento da ferramenta;
4. Com o término da varredura, clique em “Fechar”.

5.14 Existe alguma rotina automática para limpar meu Computador?

Sim. Por motivos de segurança, foi agendado para diariamente a partir das nove horas da manhã, ser executada;

5.15 Preciso fazer backup dos meus dados?

Sim. O Setor de Tecnologia é responsável pelo salvamento dos dados armazenados nos servidores. Quanto aos dados armazenados nas estações de trabalho, o próprio usuário é responsável pelo seu salvamento.

6 REDE SEM FIO

É uma rede que pode ser acessada sem a necessidade de conexões por fios metálicos. A mais comum utiliza radiofrequência na comunicação entre os computadores. Essa tecnologia é indicada quando se necessita de mobilidade, como no uso de notebooks. Embora a rede sem fio permita mobilidade, a rede com cabo é mais estável e mais rápida.



6.1 Quais os riscos em utilizar rede sem fio?

Como o acesso à rede é feito sem a necessidade de contato físico, é possível alguém acessá-la mesmo estando fora das dependências do órgão. Isso pode ser utilizado para roubo de informações.

Como forma de segurança, há tecnologias de criptografia e autenticação que garantem que apenas usuários certificados possam acessar a rede.

6.2 Como acessar a rede sem fio da Prefeitura?

Existem 4 redes disponíveis na Prefeitura, uma restrita ao TI e serviços administrativos e 3 aberta aos Funcionários Autorizados.

6.3 Quais áreas que possuem cobertura da rede sem fio?

Atualmente na sala de: TI, Chefia de gabinete e Sec. Finanças

7 A QUEM PROCURAR EM CASO DE PROBLEMAS?

Setor de Tecnologia da Prefeitura Municipal de Murici, que presta apoio a

- Suporte no uso do computador;
- Configuração de aplicativos;
- Problemas no acesso à rede;
- Acesso a sistemas.

8 OS 10 MANDAMENDOS DA SEGURANÇA DA :INFORMAÇÃO E COMUNICAÇÃO

1. Utilize senhas difíceis de serem descobertas;
2. Altere sua senha periodicamente;
3. Tome cuidado com downloads;
4. Tome cuidado com e-mails de remetentes desconhecidos;
5. Evite sítios com conteúdos duvidosos;
6. Não abra anexos de e-mails desconhecidos;
7. Tome cuidado com compras na internet;
8. Tome cuidado ao acessar sítios de bancos;
9. Não revele informações sobre você na internet;
10. Ao informar dados em sítios, verifique se a página é segura (com prefixo “https”).

Edvan Batista da Silva junior (Ró)
Suporte Técnico

