DECRETO Nº 5.597, DE 23 DE JANEIRO DE 2024.

Normatizar o uso de recursos da Tecnologia da Informação disponibilizados pela Prefeitura do Município de Matão, e institui a Política de Segurança da Informação.

CONSIDERANDO a necessidade de normatizar o uso apropriado dos recursos da tecnologia da informação no âmbito da Prefeitura do Município de Matão, promovendo a proteção dos usuários, dos equipamentos, dos softwares, dos dados dos contribuintes e da própria Administração Pública;

CONSIDERANDO a necessidade de garantir a segurança das informações geradas, adquiridas, processadas, armazenadas e transmitidas no âmbito da Administração Municipal, de forma a atender aos princípios da confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

CONSIDERANDO que os servidores públicos devem zelar pelas informações que lhes são confiadas no exercício de suas funções;

CONSIDERANDO que as ações de segurança da informação reduzem custos e riscos e aumentam os benefícios prestados aos cidadãos, ao permitir a oferta de processos, produtos e serviços suportados por sistemas de informações mais seguros; **DECRETA:**

Art. 1º - Fica instituída a Política de Segurança da Informação no âmbito da Prefeitura do Município de Matão.

§ 1º - A Política de Segurança da Informação constitui um conjunto de diretrizes e normas que estabelecem o princípio de proteção, controle e monitoramento das informações processadas, armazenadas e custodiadas pela Administração Municipal, aplicando-se a todos os órgãos do Poder Executivo Municipal.

§ 2º - Compete à Secretaria de Administração e Finanças a coordenação das políticas de gestão da segurança da informação no Município.

Art. 2º – Este Decreto entra em vigor na data de sua publicação.

Palácio da Independência, aos 23 de janeiro de 2024

APARECIDO FERRARI
Prefeito Municipal

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PREFEITURA MUNICIPAL DE MATÃO

SUMÁRIO

1 – APRESENTAÇÃO

A Segurança da Informação é um tema em permanente discussão no âmbito das instituições. Na Prefeitura Municipal de Matão as questões estratégicas da área de Tecnologia da Informação são tratadas e discutidas constantemente de maneira a aprimorar os mecanismos de gestão governamental, visando a melhoria contínua da qualidade dos processos internos e serviços prestados ao cidadão.

A elaboração da Política de Segurança da Informação visa estabelecer diretrizes, normas, procedimentos e padrões a serem observados e seguidos por todas as pessoas que utilizarem a infraestrutura da Prefeitura Municipal de Matão, tendo como propósito definir, difundir, manter e aprimorar os procedimentos de segurança da informação no âmbito da instituição, bem como evitar e gerenciar os riscos e ameaças à segurança da informação.

2 – OBJETIVOS

Este documento tem por objetivo principal estabelecer diretrizes de Tecnologia da Informação para proteção legal da Prefeitura Municipal de Matão, adequando as necessidades de negócio, em consonância com: a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018; o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014; e com as boas práticas de Segurança da Informação, preservando as informações no tocante a:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Dessa forma, busca-se desenvolver um comportamento ético e profissional, para que todos possam utilizar da melhor forma as ferramentas de Tecnologia da Informação e as informações por elas geradas, ao mesmo tempo, busca-se reduzir ameaças através da adoção de medidas preventivas para evitar possíveis incidentes que tragam prejuízos à instituição.

3 – INTRODUÇÃO

A Política de Segurança da Informação baseia-se em padrões internacionais e nacionais na área de Segurança de Informação e, principalmente, na série normativa Série normativa ABNT ISO 27000. A política versa sobre práticas a serem seguidas na Prefeitura Municipal de Matão.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da instituição poderão ser monitorados e gravados conforme previsto nas leis brasileiras. É também obrigação de cada colaborador se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu superior e do Departamento de Tecnologia da Informação, sempre que não estiver seguro quanto à aquisição, uso ou descarte de informações.

Esta política será atualizada no prazo máximo de 4 anos. Deve ser reavaliada periodicamente sempre que o Departamento de Tecnologia da Informação julgar necessário ou identificar ameaças e riscos para garantir que a Instituição esteja efetivamente protegida.

4 – DIRETRIZES GERAIS

O uso correto e responsável dos recursos de Tecnologia da Informação deve ser aplicado a todos os colaboradores da instituição, incluindo qualquer indivíduo ou organização que possua vínculo com este órgão, tais como funcionários, ex-funcionários, prestadores de serviço, ex-prestadores de serviço, estagiários, ex-estagiários, que possuíram, possuem ou virão a possuir acesso às informações da Prefeitura Municipal de Matão e/ou fizeram, fazem ou farão uso da informação e recursos computacionais compreendidos na infraestrutura disponível. Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelo usuário, no âmbito da infraestrutura de Tecnologia da Informação, ficando os transgressores sujeitos à Lei Penal, Civil e Administrativa, na medida da conduta, dolosa ou culposa, que praticarem.

5 – DIRETRIZES ESPECÍFICAS

5.1 – POLÍTICA DE SENHAS

O envolvimento do usuário é importante no processo da segurança dos recursos de TI, pois é na adequada utilização destes recursos, como instrumento de trabalho, que se inicia a formação de uma sólida cultura de segurança da informação. Desta forma, recomenda-se aos usuários a adoção das seguintes práticas:

- A conta de acesso é o instrumento para identificação do usuário na rede da Prefeitura Municipal de Matão e caracteriza-se por ser de uso individual e intransferível. Para o cadastramento de uma nova conta de usuário o responsável pelo departamento deve solicitar a criação por e-mail, identificando o funcionário e o cargo que ocupa, utilizando formulário disponível no ANEXO I. No caso de desligamento, o mesmo processo deve ser efetuado, evitando assim que usuários que não façam mais parte do departamento tenham acesso aos arquivos e sistemas.
- A formação da nomenclatura da credencial de login de acesso à Internet é composta pelo prenome e as letras iniciais do(s) sobrenome(s) do funcionário.
- O usuário deve utilizar senhas que contenham, pelo menos, oito caracteres, compostos de letras minúsculas e maiúsculas, números e símbolos, evitando o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com o usuário ou palavras constantes em dicionários. A senha nova não pode ser a mesma das últimas cadastradas. É obrigatória a troca de senha no primeiro acesso.
- O usuário deve alterar periodicamente suas senhas. A senha expira a cada 90 dias mas o usuário pode trocá-la a qualquer momento.
- O usuário nunca deve anotar senhas em locais de fácil acesso e não salvar senhas nos computadores corporativos.
- O usuário nunca deve divulgar sua senha a terceiros ou permitir o uso por terceiros de recursos autorizados por intermédio de sua senha.
- Sempre que se ausentar da estação de trabalho, o usuário deve remover sua credencial de acesso, desautenticando-se, pois qualquer utilização por meio da

identificação e da senha de acesso é de responsabilidade do usuário aos quais as informações estão vinculadas.

- Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos nos sistemas de Tecnologia da Informação deve ser imediatamente comunicada ao Departamento de Tecnologia da Informação.
- As contas com alto privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente conforme as responsabilidades e necessidades atribuídas. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos técnicos do Departamento de Tecnologia da Informação.
- Em caso de comprometimento comprovado da segurança do ambiente de Tecnologia da Informação por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.
- A base de dados de senhas deve ser armazenada com criptografia.
- Caso o usuário esqueça a sua senha, ele ou seu superior, deverá requisitar por e-mail a troca por uma nova.

5.2 – ACESSO À INTERNET

O acesso à Internet e Intranet da Prefeitura Municipal de Matão segue em consonância com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018 e o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014. Desta forma, os usuários devem ficar atentos às seguintes recomendações:

- O acesso será restrito e liberado somente mediante a utilização de credencial de acesso.
- O acesso à Internet contará com filtros e monitoramento por meio do registro de logs vinculados à credencial de cada usuário. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso.
- Toda a informação acessada, recebida, produzida e/ou transmitida através do acesso à Internet fornecido pela Prefeitura Municipal de Matão está sujeita a monitoramento, não havendo por parte do usuário quaisquer expectativas de privacidade, podendo ser utilizadas, sem qualquer notificação ou aviso, por

pessoas autorizadas para finalidades oficiais, incluindo investigações, toda a informação trafegada, seja originada da rede interna e destinada a redes externas ou o contrário.

- Sites e serviços bloqueados poderão ser liberados ao usuário mediante solicitação devidamente justificada através de ofício encaminhado ao Secretário de Administração de Finanças.
- Os gestores das unidades, gestores de contratos, supervisores de estágio e o Setor de Pessoal deverão sempre informar imediatamente ao Departamento de Tecnologia da Informação, através de e-mail, o desligamento de algum usuário, seja qual for o motivo, para que seja realizado o bloqueio de acesso.
- É vedado utilizar à Internet da instituição para incitar violência, difamação ou promover quaisquer outras ações vedadas no estatuto do servidor público ou tipificadas como crime pela legislação brasileira.
- A utilização da rede sem fio acontecerá mediante a utilização de usuário e senha e a liberação dos dispositivos devem ser solicitadas pelo responsável pelo departamento.
- É vedado realizar a instalação de qualquer equipamento que permita a criação de ponto de acesso sem fio ou a expansão do sinal sem prévia autorização do Departamento de Tecnologia da Informação. Os pontos de acesso da rede sem fio só podem ser instalados, registrados e configurados pelo Departamento de Tecnologia da Informação.
- O usuário deve certificar-se da procedência do site e a utilização de conexões seguras (criptografadas) ao realizar transações via web.
- O usuário deve verificar se o certificado do site ao qual se deseja acessar, esta íntegro e corresponde realmente aquele sítio, observando ainda, se o mesmo está dentro do prazo de validade.
- O usuário deve certificar que o endereço apresentado no navegador corresponde ao site que realmente se quer acessar, antes de realizar qualquer ação ou transação.
- Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino.

- É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:
  - Pornografia, pedofilia, preconceitos, vandalismo, entre outros;
  - Acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede da Prefeitura Municipal de Matão;
  - Uso recreativo da internet em horário de expediente;
  - Uso de proxy anônimo, VPN e tuneladores;
  - Acesso a rádio e TV em tempo real (serviços de streaming) em horário de expediente;
  - Acesso a jogos;
  - Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;
  - Envio externo de qualquer software licenciado à Prefeitura Municipal de Matão ou dados de sua propriedade ou de seus usuários;
  - Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do Departamento de Tecnologia da Informação;
  - Utilização de softwares de compartilhamento de conteúdo na modalidade peer-to-peer (P2P).
- Caso o Departamento de Tecnologia da Informação julgue necessário, haverá bloqueios de acesso a arquivos e sites não autorizados que comprometam o uso de banda da rede, o desempenho e produtividade das atividades do usuário, bem como, que exponham a rede a riscos de segurança.
- É proibido utilizar os recursos do município para fazer o download ou distribuição de software ou dados não legalizados.
- Haverá auditoria dos sites acessados por usuário para verificação da adequação à política vigente.
- Comprovada a utilização irregular, o usuário envolvido poderá ter o seu acesso à Internet bloqueado, sendo comunicado o fato à chefia imediata, podendo

incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

5.3 – UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

Todos os dados e arquivos relativos às atividades da Prefeitura Municipal de Matão devem ser mantidos no servidor de rede, onde existe sistema de cópia de segurança realizado diariamente em arquivamento em nuvem e de forma confiável.

- O sistema de arquivos compreende o conjunto de pastas compartilhadas que são armazenados nos servidores e mapeadas nas estações de trabalho.
- As pastas de rede compartilhadas são organizadas em três tipos:
  - a) pastas do departamento: acesso compartilhado somente entre os usuários do mesmo departamento;
  - b) pasta pessoal "Meus Documentos Seguros": pasta individual para cada usuário para armazenar informações, documentos e materiais sigilosos no âmbito da Administração Pública Municipal;
  - c) pasta pública: acesso compartilhado entre todos os usuários. Os usuários têm acesso para ler os documentos públicos, porém a alteração ou inserção desses arquivos devem ser solicitadas ao Departamento de Tecnologia da Informação.
- É de responsabilidade do usuário armazenar os arquivos nas pastas de rede apropriadas.
- Não armazenar documentos que desrespeitem às leis e regulamentações, notadamente àquelas referentes aos crimes de delitos informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade.
- Não armazenar documentos protegidos pelos direitos autorais, inclusive músicas, textos, documentos digitalizados e qualquer conteúdo encontrado em revistas, livros ou quaisquer outras fontes protegidas por direitos autorais. No caso de detecção desses arquivos, os mesmos serão excluídos sem prévio aviso ao usuário.

- Fazer cópias de documentos pessoais e e-mails salvos localmente no computador, pen-drive ou drive externo, pois no caso de perda desses arquivos o Departamento de Tecnologia da Informação não se responsabilizará pela recuperação dos mesmos.
- Toda informação gerada pelos usuários, utilizando integralmente ou parcialmente recursos da Prefeitura Municipal de Matão, são de propriedade do município.
- O usuário nunca deve fornecer dados a terceiros, exceto os de natureza pública ou mediante autorização da autoridade competente.
- O usuário nunca deve utilizar recurso da entidade pública para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza.

5.4 – UTILIZAÇÃO DE E-MAIL

- A concessão das contas de correio eletrônico depende de solicitação formal via e-mail da chefia imediata do colaborador e endereçada ao Departamento de Tecnologia da Informação.
- Todas as mensagens enviadas por correio eletrônico com o endereço profissional devem ser usadas para assuntos de interesse do município e não se deve manter qualquer expectativa de privacidade de seus conteúdos. É vedado o envio de mensagens com conteúdo eleitoral, difamatório, ofensivo, preconceituoso, obsceno, pornográfico ou que dê margem a interpretação de discriminação racial, sexual, religiosa ou política e para a disseminação de qualquer prática ilícita.
- É vedado a utilização de serviços de e-mail que não sejam o oficial (@matao.sp.gov.br), como por exemplo: Gmail, Hotmail e Yahoo.
- A comunicação corporativa interna, a comunicação com cidadãos e a comunicação com outras instituições deverá ser realizada com e-mail oficial.
- É vedado o envio de *spams*, correntes e quaisquer outros assuntos que não sejam de interesse institucional.

- O uso do e-mail é estritamente corporativo, sendo vedado utilizar em redes sociais, *e-commerce*, serviços de *streaming* e outros.
- É vedado compartilhar credenciais de acesso do e-mail a usuário não autorizado.
- O usuário não deve abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus.
- O usuário deve efetuar a manutenção de sua caixa postal, evitando ultrapassar o limite de armazenamento e garantindo o seu funcionamento contínuo.

5.5 – UTILIZAÇÃO DE PROGRAMAS

As estações de trabalho são adquiridas e entregues ao Departamento de Tecnologia da Informação, que cuidará da instalação do sistema operacional e aplicativos mínimos necessários para o desempenho de suas funções básicas.

São considerados legítimos os softwares instalados e utilizados conforme suas licenças de uso e que não contrariem as demais regras do município e a legislação. Em especial, esta norma contempla a possibilidade de uso de software livre para fins legítimos e não abusivos.

Não é permitida a instalação nos equipamentos do município de qualquer software, gratuito ou não, sem as devidas licenças para uso comercial do município. A instalação dos softwares licenciados deve ser feita por um técnico do Departamento de Tecnologia da Informação, remotamente ou presencialmente, dependendo do caso.

Em todos os equipamentos utilizados na rede de informática da Prefeitura será instalado software de acesso remoto, permitindo que os técnicos do Departamento de Tecnologia da Informação possam dar suporte ao usuário sem precisar se deslocar até o departamento do mesmo, agilizando o atendimento.

O uso ou instalação de software sem licença de uso ou em nome de outros sem autorização caracteriza crime de pirataria, ficando o usuário e o instalador sujeitos às sanções administrativas, legais e penais da legislação.

Ocasionalmente, serão realizadas verificações no inventário dos equipamentos, com relação a hardware e software, permitindo identificar desvios das normas.

5.6 – UTILIZAÇÃO DOS EQUIPAMENTOS

Os recursos computacionais somente devem ser utilizados para a execução de atividades de interesse da Prefeitura Municipal de Matão.

Cada estação de trabalho possui controle de IP (Protocolo Internet), o qual permite que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que ausentar do ambiente de trabalho o usuário deve bloquear a estação de trabalho.

Em todas as estações de trabalho e notebooks deve estar instalado, ativo e atualizado o antivírus corporativo indicado pelo Departamento de Tecnologia da Informação.

O usuário não deve impedir a operação e atualização do antivírus sem autorização e conhecimento da equipe do Departamento de Tecnologia da Informação.

Constatado qualquer problema com o antivírus, o usuário deverá comunicar aos responsáveis do Departamento de Tecnologia da Informação, que tomarão as providências cabíveis.

Os usuários devem evitar comer ou beber próximo aos equipamentos de TI a fim de evitar danos.

É proibida a abertura física dos computadores para qualquer tipo de finalidade, caso seja necessário reparo, o mesmo deverá ser solicitado via abertura de chamado, ao Departamento de Tecnologia da Informação.

Equipamentos pessoais ou de terceiros não devem ser ligados diretamente na rede do município. Somente estação de trabalho e equipamentos devidamente registrados e configurados pelo Departamento de Tecnologia da Informação terão acesso à rede local.

O remanejamento de equipamentos só deverá ser feito pelos técnicos do Departamento de Tecnologia da Informação.

Em caso de eventos no ambiente da Prefeitura Municipal de Matão, que necessitem utilizar os recursos de Tecnologia da Informação, tais como: seminários, licitações, etc. deverá ser solicitado com antecedência mínima de 5 dias úteis ao Departamento de Tecnologia da Informação.

Em caso de dano, inutilização ou extravio do equipamento o colaborador deverá comunicar imediatamente ao Departamento de Tecnologia da Informação, que deverá adotar as providências cabíveis.

Em caso de furto ou roubo, deverá providenciar Boletim de Ocorrência junto à autoridade policial e entregá-lo na Secretaria de Administração e Finanças, com cópia ao Departamento de Tecnologia da Informação, os quais deverão adotar as providências necessárias.

É proibido colar adesivos com ímãs nos equipamentos.

É dever do usuário zelar pela integridade do equipamento estritamente como instrumento de trabalho, com os acessórios que foram utilizados.

Não é permitido retirar ou transportar qualquer equipamento de informática da Prefeitura Municipal de Matão sem autorização prévia do Departamento de Tecnologia da Informação.

É vedado retirar e/ou danificar placas identificadoras de patrimônio, travas e lacres de segurança dos equipamentos de informática.

5.7 – SISTEMAS E APLICAÇÕES

Os sistemas deverão gerar registros (logs) de eventos de segurança. Devem ser utilizados para este fim recursos do sistema operacional, recursos de banco de dados e recursos da aplicação. Os registros deverão conter ao menos as seguintes informações: identificação da aplicação e função, momento da ocorrência (timestamp), informações que identifiquem a máquina ou local da ocorrência e os dados relevantes manipulados pela aplicação.

5.8 – DATACENTER

As instalações do Datacenter serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, danos e quaisquer interferências de origem humana ou natural.

Todas as instalações de novos servidores deverão seguir procedimentos padrões e incluir pacotes, Service Packs, Hot Fixes obrigatórios.

Os acessos remotos devem ser feitos utilizando equipamentos corporativos, devidamente atualizados e com recursos de segurança.

Sistemas de proteção de acesso (firewall) devem ser utilizados para permitir apenas às redes ou máquinas alvos dos serviços o acesso aos mesmos mediante solicitação para a equipe de Tecnologia da Informação.

O acesso físico aos servidores e equipamentos de infraestrutura deve ser restrito aos funcionários do Departamento de Tecnologia da Informação. O acesso de visitantes ou terceiros ao Datacenter somente poderá ser realizado mediante agendamento prévio, com acompanhamento de um técnico da área de Tecnologia de Informação.

Os servidores e equipamentos de infraestrutura devem operar em ambiente adequado, sob condições indicadas pelo fabricante, em sala cofre, com porta com identificação de acesso e medidor de temperatura e umidade.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração dos ajudantes de limpeza.

Não é permitida a entrada de nenhum tipo de alimento, bebida ou produto inflamável no Datacenter.

É resguardado a Prefeitura do Município de Matão o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de câmeras em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida.

5.9 - IDENTIFICAÇÃO DIGITAL

A Prefeitura do Município de Matão poderá, a seu critério exclusivo, fornecer certificados digitais para usuários que executam atividades profissionais específicas, devendo serem observadas as seguintes diretrizes:

- Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo;
- O usuário deverá informar ao seu superior hierárquico e a equipe de tecnologia

da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;

- O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela Prefeitura do Município de Matão imediatamente revogado.

5.10 – AQUISIÇÕES

Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação, a qualquer título, devem refletir esta Política de Segurança da Informação, contando sempre com o apoio do Departamento de Tecnologia da Informação.

5.11 – IMPRESSÕES

O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da Prefeitura do Município de Matão ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia:

- O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações sigilosas desta prefeitura;
- A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;
- Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações sigilosas, devendo as mesmas serem descartadas;
- A resolução de erros de impressão e/ou problemas técnicos deve ser feita através de contato com o Departamento de Tecnologia da Informação;
- Os serviços de impressão estão sujeitos a monitoramento para fins de auditoria, fiscalização e/ou investigação.

5.12 – POLÍTICA DE BACKUP

- O Departamento de Tecnologia da Informação é responsável por criar cópias de segurança e executar rotinas de backups nas pastas compartilhadas da rede.
- O armazenamento deve ser feito em nuvem, sendo acessível de qualquer local para a restauração.
- O backup é feito de forma incremental, ou seja, copiados apenas os arquivos alterados desde a última realização.
- O horário para o início do backup é as 20:00 h e é realizado diariamente.
- O departamento também é responsável pela restauração de arquivos. Nesse caso o usuário deve fazer a solicitação por e-mail, informando o nome do arquivo, o caminho nas pastas de rede onde este arquivo estava localizado e a data da versão que deve ser restaurada. O prazo para restauração é de até 24 horas após a abertura do chamado.
- O backup será feito do servidor de arquivos da Prefeitura, dos logs de acesso à internet e dos backup dos bancos de dados dos sistemas. Arquivos locais dos usuários não serão backupeados e devem ser de responsabilidade de cada usuário.

6 – RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

6.1 - INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todas as ocorrências que possam ter impacto negativo sobre a confidencialidade, integridade e/ou disponibilidade dos ativos e sistemas de informação ou recursos computacionais da Prefeitura do Município de Matão serão caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem registradas e tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos ativos afetados.

Incidentes de segurança devem ser priorizados tendo como base a criticidade dos ativos e sistemas de informação ou recursos computacionais afetados, combinada com a estimativa de impacto prevista.

Todos os incidentes de segurança da informação ou suspeitas de incidentes de segurança da informação devem ser imediatamente comunicados à área responsável pela Tecnologia da Informação na Prefeitura do Município de Matão.

Na ocorrência de um incidente de segurança da informação, ativos/serviços de informação ou recursos computacionais com suspeita de ter sua segurança comprometida, devem ser isolados do ambiente de produção, para garantir a contenção do incidente e evitar sua propagação.

A extensão dos danos do incidente de segurança da informação deve ser avaliada para, em seguida, ser identificado o melhor curso de ação para erradicação completa do incidente e restauração dos ativos de informação afetados.

Após a erradicação completa do incidente, deve ser realizada uma revisão completa da ocorrência e dos procedimentos de segurança da informação, identificando o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

Nenhum tipo de informação sobre os incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades e/ou pessoas externas à Prefeitura Municipal de Matão sem aprovação expressa e formal da direção.

ANEXO I

TERMO DE RESPONSABILIDADE E COMPROMISSO

Matão, _____ de _____ de _____

Solicito nesta data a criação dos acessos selecionados abaixo. Tenho conhecimento que o acesso às informações por meio desses é de minha inteira responsabilidade e que os sites visitados são gravados em equipamentos específicos para fins de auditoria.

Tenho conhecimento das Políticas de Segurança da Informação da Prefeitura de Matão, bem como me comprometo a observar suas futuras atualizações.

Comprometo-me a observar os seguintes procedimentos:

1º. Observar cuidados especiais com relação às minhas senhas:

- Proteger a estação de trabalho sob minha responsabilidade, não me afastando dela deixando-a ligada e desprotegida, com sessão de trabalho aberta, mesmo que não esteja conectado a nenhum sistema corporativo.
- Salvaguardar as senhas sob minha responsabilidade: não revelarei a terceiros as senhas de acesso ao microcomputador, a sistemas (Folha de Pagamento, Tributação, Contabilidade, Materiais, Protocolo), ou a serviços (correio eletrônico), que são estritamente pessoais.
- A senha para acesso à rede deverá ser alterada a cada 90 dias e você receberá um aviso para efetuar a troca 5 dias antes do vencimento.
- A nova senha não poderá ser igual a nenhuma das anteriormente utilizadas.
- Para elaborar uma senha segura consulte as recomendações anexas.

2º. Observar cuidados especiais com relação ao equipamento:

- Não colar nenhum tipo de adesivo
- Não violar o lacre que garante a configuração original das máquinas.
- No caso de, durante sua observação diária, notar que o lacre esteja rompido, entrar em contato imediatamente com o Departamento de Tecnologia da Informação pelo e-mail: cpd@matao.sp.gov.br.
- O equipamento recebido possui instalados os seguintes programas: Windows, LibreOffice e Skype, que estão devidamente licenciados.
- Havendo a necessidade da instalação de outros programas, o Departamento de Tecnologia da Informação deve ser previamente consultado.
- A equipe do Departamento de Tecnologia da Informação levantará periodicamente o registro dos arquivos baixados e instalados na referida estação de trabalho, para realização de auditoria de segurança, ou seja, ocorrerá monitoramento.
- A estação de trabalho destina-se somente as atividades funcionais, razão porque não poderei considerar as medidas citadas anteriormente como invasivas à minha privacidade.

3º. Observar cuidados especiais com relação aos arquivos:

- O diretório "Meus Documentos Seguros" é uma pasta no servidor utilizada para guardar arquivos pessoais dos usuários relacionados a trabalho.

- Esta pasta será sincronizada com a pasta exclusiva do usuário no Servidor de Arquivos. Sendo assim, todos os arquivos gravados neste local estarão disponíveis no Servidor e poderão ser acessados de qualquer estação de trabalho.
- O diretório dos Grupos será uma pasta de uso do departamento em que o usuário está localizado e será utilizado para gravar arquivos com informações pertinentes ao departamento. Assim, outros usuários desse mesmo departamento poderão gravar, alterar e apagar os mesmos.
- Diariamente será realizado Backup dos arquivos localizados nos drivers mencionados anteriormente, podendo assim, serem recuperados em caso de perda acidental.
- O Departamento de Tecnologia da Informação não se responsabilizará por nenhum arquivo que não esteja gravado nos diretórios acima descritos.

4º. Observar cuidados especiais com relação ao certificado digital:

- Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo;
- O usuário deverá informar ao seu superior hierárquico e a equipe de tecnologia da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;
- O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela Prefeitura de Matão imediatamente revogado.

Assumo inteira responsabilidade pelos arquivos copiados/instalados em minha estação de trabalho, caso haja entre eles programas executáveis, pelas consequências de sua execução, tanto sobre esta estação de trabalho como sobre outros sistemas computacionais, localizados na Prefeitura de Matão ou externos à mesma.

Sou: ( ) Funcionário ( ) Estagiário

Nome completo:
RG:
CPF:
Secretaria:
Telefone para contato:
Local de Trabalho:
Cargo:

Solicito os acessos abaixo:
( ) Computador e Internet ( ) E-mail

Assinatura Funcionário/Estagiário

Assinatura do Responsável do Setor
com Carimbo ou nome legível

Secretaria:
Departamento:
Endereço:
Nome da máquina:
Patrimônio:

Técnico responsável pela configuração: _____

_____
Rubrica do Técnico
Data em que foi feita a configuração: ____/____/____

TERMO DE RECEBIMENTO E RESPONSABILIDADE

Estou recebendo neste ato o(s) seguinte(s) equipamento(s):

Descrição do Computador: Estação de Trabalho com as seguintes especificações:

Estou ciente que respondo administrativamente pela integridade do equipamento recebido.

Matão, de de .

Nome responsável: Rg:

_____
Assinatura

TERMO DE RESPONSABILIDADE E COMPROMISSO

Matão, _____ de _____ de _____

Solicito nesta data a criação dos acessos selecionados abaixo. Tenho conhecimento que o acesso às informações por meio desses é de minha inteira responsabilidade e que os sites visitados são gravados em equipamentos específicos para fins de auditoria.

Tenho conhecimento das Políticas de Segurança da Informação da Prefeitura de Matão, bem como me comprometo a observar suas futuras atualizações.

Comprometo-me a observar os seguintes procedimentos:

1º. Observar cuidados especiais com relação às minhas senhas:

a) Proteger a estação de trabalho sob minha responsabilidade, não me afastando dela deixando-a ligada e desprotegida, com sessão de trabalho aberta, mesmo que não esteja conectado a nenhum sistema corporativo.
b) Salvaguardar as senhas sob minha responsabilidade: não revelarei a terceiros as senhas de acesso ao microcomputador, a sistemas (Folha de Pagamento, Tributação, Contabilidade, Materiais, Protocolo), ou a serviços (correio eletrônico), que são estritamente pessoais.
c) A senha para acesso à rede deverá ser alterada a cada 90 dias e você receberá um aviso para efetuar a troca 5 dias antes do vencimento.
d) A nova senha não poderá ser igual a nenhuma das anteriormente utilizadas.
e) Para elaborar uma senha segura consulte as recomendações anexas.

2º. Observar cuidados especiais com relação ao equipamento:

a) Não colar nenhum tipo de adesivo
b) Não violar o lacre que garante a configuração original das máquinas.
c) No caso de, durante sua observação diária, notar que o lacre esteja rompido, entrar em contato imediatamente com o Departamento de Tecnologia da Informação pelo e-mail: cpd@matao.sp.gov.br.
d) O equipamento recebido possui instalados os seguintes programas: Windows, LibreOffice e Skype, que estão devidamente licenciados.
e) Havendo a necessidade da instalação de outros programas, o Departamento de Tecnologia da Informação deve ser previamente consultado.
f) A equipe do Departamento de Tecnologia da Informação levantará periodicamente o registro dos arquivos baixados e instalados na referida estação de trabalho, para realização de auditoria de segurança, ou seja, ocorrerá monitoramento.
g) A estação de trabalho destina-se somente as atividades funcionais, razão porque não poderei considerar as medidas citadas anteriormente como invasivas à minha privacidade.

3º. Observar cuidados especiais com relação aos arquivos:

a) O diretório "Meus Documentos Seguros" é uma pasta no servidor utilizada para guardar arquivos pessoais dos usuários relacionados a trabalho.
b) Esta pasta será sincronizada com a pasta exclusiva do usuário no Servidor de Arquivos. Sendo assim, todos os arquivos gravados neste local estarão disponíveis no Servidor e poderão ser acessados de qualquer estação de trabalho.

c) O diretório dos Grupos será uma pasta de uso do departamento em que o usuário está localizado e será utilizado para gravar arquivos com informações pertinentes ao departamento. Assim, outros usuários desse mesmo departamento poderão gravar, alterar e apagar os mesmos.
d) Diariamente será realizado Backup dos arquivos localizados nos drivers mencionados anteriormente, podendo assim, serem recuperados em caso de perda acidental.
e) O Departamento de Tecnologia da Informação não se responsabilizará por nenhum arquivo que não esteja gravado nos diretórios acima descritos.

4º. Observar cuidados especiais com relação ao certificado digital:
a) Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo;
b) O usuário deverá informar ao seu superior hierárquico e a equipe de tecnologia da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital;
c) O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela Prefeitura de Matão imediatamente revogado.

Assumo inteira responsabilidade pelos arquivos copiados/instalados em minha estação de trabalho, caso haja entre eles programas executáveis, pelas consequências de sua execução, tanto sobre esta estação de trabalho como sobre outros sistemas computacionais, localizados na Prefeitura de Matão ou externos à mesma.

Sou: ( ) Funcionário ( ) Estagiário

Nome completo:
RG:
CPF:
Secretaria:
Telefone para contato:
Local de Trabalho:
Cargo:

Solicito os acessos abaixo:
( ) Computador e Internet ( ) E-mail

Assinatura Funcionário/Estagiário

Assinatura do Responsável do Setor
com Carimbo ou nome legível

Criando Senhas Seguras

Senhas pobres e em branco são formas mais fáceis de os atacantes invadirem o seu computador e a nossa rede. Senhas usadas por anos consecutivos, ou senhas reutilizadas frequentemente, também são prováveis de serem descobertas.

Para aumentar a proteção da sua conta na rede, é necessário que você use senhas de alta segurança quando acessar os sistemas de computadores corporativos. Será necessário que você altere a sua senha periodicamente, e que use senhas diferentes das anteriores.

Uma senha de alta segurança possui pelo menos oito caracteres e usa pelo menos de três dos seguintes grupos:

1. Letras minúsculas
2. Letras maiúsculas
3. Números (por exemplo, 1, 2, 3)
4. Símbolos (por exemplo, @, =, –, etc.)

As suas senhas também não poderão ter três ou mais letras consecutivas contidas no seu nome de conta de usuário. Será necessário que você altere a sua senha a cada 90 dias, e as suas senhas não poderão ser usadas novamente.

Quando você alterar a sua senha, a nova senha será automaticamente verificada em relação à complexidade e será comparada com as suas senhas anteriores. Isso pode parecer frustrante, e você pode ficar tentado a anotar a sua senha e colá–la na sua mesa, no monitor do computador ou em outro lugar de fácil acesso. Entretanto, no momento em que você fizer isso, estará expondo o seu computador e toda a nossa empresa a um risco tremendo, já que qualquer pessoa poderia ir ao seu computador e fazer logon na rede usando as suas credenciais. Portanto, nunca anote as suas senhas. Em vez disso, crie senhas fáceis de lembrar.

Abaixo você encontrará mais informações básicas sobre a segurança de senhas além de recomendações específicas para a criação de senhas de alta segurança que sejam fáceis de lembrar.

Use mais de uma palavra

1. Em vez de usar apenas o nome de uma pessoa conhecida, como "Amador", escolha um detalhe dessa pessoa que mais ninguém saiba, por exemplo, "UrsoAmador" ou "UrsoDodo".

Use símbolos em vez de caracteres

2. Muitas pessoas tendem a colocar os símbolos e números exigidos no fim de uma palavra, por exemplo, "Amador1234". Infelizmente, isso é relativamente fácil de ser quebrado. A palavra "Amador" encontra–se em diversos dicionários que têm nomes comuns; depois de ter descoberto o nome, o atacante tem apenas mais quatro caracteres relativamente fáceis para adivinhar. Em vez disso, substitua uma ou mais letras da palavra por símbolos que você lembre facilmente. Muitas pessoas têm suas próprias interpretações criativas da letra com que alguns símbolos e números se parecem. Por exemplo, tente substituir "A" por "@", "I" por "!", "O" por zero (0), "S" por "$" e "E" por "3". Com substituições como essas, você reconheceria "Ur$o@mador", "Ur$oAm@dor" e "Urs0Am@d0r", mas elas seriam muito difíceis de serem adivinhadas ou quebradas. Examine os símbolos do seu teclado e pense nos primeiros caracteres que lhe vêm à cabeça; pode não ser o que outra pessoa imaginaria, mas você lembrará. Use alguns desses símbolos como substituições nas suas senhas de hoje em diante.

Escolha acontecimentos ou pessoas em que você pensa

3. Para lembrar uma senha de alta segurança que deverá ser alterada em alguns meses, tente escolher um acontecimento futuro pessoal ou público. Use como uma oportunidade para lembrar de algo agradável que

está acontecendo na sua vida, ou de uma pessoa que você admira ou ama. Provavelmente você não esquecerá a senha se ela for engraçada ou carinhosa. Torne–a exclusividade sua. Certifique–se de torná–la uma frase com duas ou mais palavras e continue a usar os símbolos. Por exemplo: "F0rm@turaJ0na$".

4. **Use fonética nas palavras**
Geralmente, dicionários de senhas usados por atacantes buscam palavras contidas na sua senha. Como já foi mencionado, não hesite em usar palavras, mas certifique–se de salpicar generosamente símbolos no meio dessas palavras. Outra forma de vencer o atacante é evitar soletrar as palavras corretamente, ou usar fonéticas engraçadas que você possa lembrar. Por exemplo, "Kátia vê a galinha" poderia se transformar "KtiaVHlinh@!" ou "Kti@ V Hlinha!" Se o nome da sua gerente for Kátia, você pode até dar uma risadinha todas as manhãs na hora de digitar a senha. Se você não é bom de ortografia, já está na frente nesse jogo.

5. **Não tenha medo de criar uma senha longa**
Sua senha dever ter no mínimo 8 caracteres. Se for mais fácil para você lembrar uma frase completa, digite–a. Senhas mais longas são muito mais difíceis de serem quebradas. E mesmo se for longa, se for fácil de lembrar, provavelmente você terá muito menos dificuldade para entrar no sistema, mesmo que não seja o melhor digitador do mundo.

6. **Use as primeiras letras de uma frase**
Para criar uma senha fácil de lembrar e de alto nível, comece com uma frase que tenha as maiúsculas e a pontuação corretas, e que seja fácil de lembrar. Por exemplo: "Minha filha Laura estuda na Escola Internacional". Depois, pegue a primeira letra de cada palavra da frase, preservando as maiúsculas usadas. No exemplo acima, "MfLenEI" seria o resultado. Finalmente, substitua algumas letras da senha por caracteres não–alfanuméricos. Você pode usar um "@" para substituir um "a" ou um "!" para substituir um "L". Depois dessa substituição, a senha do exemplo acima poderia ser "Mf!enEI"; uma senha muito difícil de ser quebrada, e mesmo assim, fácil de lembrar, desde que você possa lembrar a frase na qual ela se baseou.

Faça:

- Combine letras (Maiúsculas e Minúsculas), símbolos e números de que você se lembre facilmente e que sejam difíceis para os outros adivinharem.
- Crie senhas que possam ser pronunciadas (mesmo que não sejam palavras) fáceis de lembrar, o que diminui a tentação de anotá–las.
- Tente usar as letras inicias de uma frase que você goste, especialmente se ela incluir um número ou caractere especial.
- Use duas coisas familiares e combine–as com um número ou caractere especial. Como alternativa, altere a ortografia incluindo um caractere especial. Dessa forma, você obtém algo desconhecido, o que gera uma boa senha, pois é fácil para você, e somente para você, lembrar, mas difícil para qualquer outra pessoa descobrir. Aqui estão alguns exemplos:

"Estou + 100 + dinheiro" = "Estou100dinheiro" ou "E$t0u100dinheir0"
"gato + * + Rato" = "gato*Rato" ou "gato*R@to"
"ataque + 3 + livro" = "ataque3livro" ou "@taque3livrO"

Não faça:

- Não use informações pessoais, como derivados da sua identidade de usuário, nomes de membros da família, nomes de solteira, carros, placas de automóveis, números de telefone, animais de estimação, aniversários, números de CPF, endereços ou passatempos.
- Não use palavras em qualquer idioma, soletradas de trás para frente ou de frente para trás.
- Não junte senhas ao mês, por exemplo, não use "Maioral" em maio.
- Não crie senhas novas substancialmente parecidas com as senhas usadas anteriormente.
- Não anote sua senha – Nunca guarde uma senha em papel. É bem mais seguro memorizá-la.

Fonte: www.microsoft.com/brasil

Procedimentos para Alteração de Senha

(a) Pressione CTRL+ALT+DEL;
(b) Clique em Alterar Senha;
(c) Próximo a Senha atual, digite a senha originalmente atribuída à conta;
(d) Próximo a Nova senha, digite sua senha e próximo a Confirmar nova senha é necessário digitar a senha novamente;
(e) Clique em OK e, em seguida, clique em Cancelar para retornar à sessão do usuário.