PSI – Política de Segurança da Informação.

Documento de Diretrizes e Normas Administrativas.

Versão 1.0.1

Índice

Conceitos e Definições

Acesso Remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário;

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

Assinatura digital: permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada;

Atacante: pessoa responsável pela realização de um ataque;

Ataque: qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede;

Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

Ativo de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Auditoria: verificação e avaliação dos sistemas e procedimentos internos com o objetivo de reduzir fraudes, erros, práticas ineficientes ou ineficazes;

Bloqueio de acesso: processo que tem por finalidade suspender temporariamente ou definitivamente o acesso;

Cavalo de troia (*trojan* ou *trojan-horse*): é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

Classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

Comissão Gestora de Proteção de Dados: equipe formada para atender à Lei Geral de Processamento de Dados Pessoais (LGPD).

Cópia de Segurança (*Backup*): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

Correio Eletrônico: é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

Credenciais ou contas de acesso: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou

organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

Criptografia: é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta");

Dado: representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

Deep Web: se refere a todo aquele conteúdo que não pode ser indexado pelos sites de busca e, dessa forma, não está disponível diretamente para quem navega na Internet;

Departamento de TI: departamento de tecnologia da informação;

Diretriz: descrição que orienta o que deve ser feito, e como, para se alcançar os objetivos estabelecidos nas políticas;

Download **(Baixar):** copiar arquivos de um servidor (sítio) na Internet para um computador pessoal;

EMPRO: Empresa Municipal de Processamento de Dados de São José do Rio Preto.

Espelhamento: sistema de proteção de dados onde o conteúdo é espelhado em tempo real. Todos os dados são duplicados entre as áreas de armazenamento disponíveis.

Firewall**:** é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo por regras de filtragens que alguns pacotes autorizados passem e outros sejam bloqueados.

FTP (*File Transfer Protocol*) (Protocolo de Transferência de Arquivo): é um protocolo da Internet para transferência de arquivos;

Gestão de Risco: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

Gestão de Segurança da Informação e Comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

Hardware: é a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, como a máquina em si, placas, impressora, teclado e outros;

Incidente de Segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

Informações Críticas: são as informações de extrema importância para a sobrevivência da instituição;

Informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

***Instant Messenger* (Mensageiro instantâneo):** é uma aplicação que permite o envio e o recebimento de mensagens em tempo real;

Interceptação de tráfego: técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de ***sniffers***;

Internet: rede mundial de computadores;

***Internet Protocol* (Protocolo de Internet):** é um protocolo de comunicação usado entre duas ou mais máquinas em rede para encaminhamento dos dados;

Intranet: rede de computadores privada que faz uso dos mesmos protocolos da Internet. Pode ser entendida como rede interna de alguma instituição em que geralmente o acesso ao seu conteúdo é restrito;

Invasão: ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador;

Invasor: pessoa responsável pela realização de uma invasão (comprometimento);

LGPD: sigla para Lei Geral de Processamento de Dados Pessoais;

***Log*:** é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para reestabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais;

***On line* (Estar disponível ao vivo):** no contexto da Internet significa estar disponível para acesso imediato, em tempo real;

***Peer-to-peer* (P2P) (Ponto a ponto):** permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

***Phishing* (*phishing scam* ou *phishing*/*scam*):** tipo de golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social;

Política de Segurança da Informação (PSI): documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

Protocolo: convenção ou padrão que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. Método padrão que permite a comunicação entre processos, conjunto de regras e procedimentos para emitir e receber dados numa rede;

Proxy **(Servidor de Cache)**: é um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas;

Rede Corporativa: conjunto de todas as redes locais sob a gestão da instituição;

Rede Pública: rede de acesso a todos;

Roteador: equipamento responsável pela troca de informações entre redes;

Scam**:** esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras;

Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Servidor de Rede: recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;

Servidor - pessoa legalmente investida em cargo público;

Sistemas de Informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

Sistema de Segurança da Informação: proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

Sniffer: dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia;

Software**:** são todos os programas existentes em um computador, como sistema operacional, aplicativos, entre outros;

***Spam*:** é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

***Spyware*:** tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. *Keylogger*, *screenlogger* e adware são alguns tipos específicos de *spyware*.

Sítio (Site): conjunto de páginas virtuais dinâmicas ou estáticas, que tem como principal objetivo fazer a divulgação da instituição;

***Streaming*:** transferência de dados (normalmente áudio e vídeo) em fluxo contínuo por meio da Internet;

Switches: um switch de rede é um equipamento eletrônico de comutação que funciona como um nó central numa rede no formato estrela, armazenando em memória o endereço físico de todos os computadores conectados a ele, relacionando cada endereço físico a uma de suas portas e permitindo assim a interligação entre os dispositivos conectados;

Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

Trilhas de Auditoria: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados;

Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública;

Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

Wireless (rede sem fio): rede que permite a conexão entre computadores e outros dispositivos através da transmissão e recepção de sinais de rádio.

Worm: tipo de código malicioso. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores.

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Câmara Municipal de São José do Rio Preto para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país, principalmente à Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709 de agosto de 2018.

Objetivos

Estabelecer diretrizes que permitam aos colaboradores, prestadores de serviços, estagiários e afins da Câmara Municipal de São José do Rio Preto seguir padrões de comportamento desejáveis e aceitáveis relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da instituição e do indivíduo, a fim de mitigar riscos técnicos e jurídicos.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento e que obedeçam à LGPD.

Garantir a continuidade das atividades da Câmara Municipal, protegendo os processos críticos contra falhas ou desastres.

Minimizar os riscos de danos, perdas financeiras ou qualquer outro impacto negativo à Câmara Municipal resultante de uma falha na segurança da informação.

Atender aos requisitos legais, regulamentares e contratuais pertinentes às atividades realizadas na Câmara Municipal.

Enfatizar as obrigações das pessoas relacionadas à segurança da informação de sua área de atuação.

Garantir a clareza na definição de todas as responsabilidades da segurança da informação.

Empregar medidas técnicas e organizacionais adequadas no tratamento de dados pessoais e empregar esforços para a proteção destes dados contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras.

Preservar as informações da Câmara Municipal de São José do Rio Preto quanto à:

- **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.
- **Autenticidade:** garantia da identidade de um usuário, sistema ou site.
- **Não-repúdio ou irretratabilidade:** garantia que não seja possível negar uma ação.

Aplicações da PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, estagiários, prestadores de serviço e afins, e se aplicam à informação em qualquer meio ou suporte.

Esta PSI dá ciência a cada colaborador de que os ambientes, sistemas, computadores e rede da instituição poderão ser monitorados e gravados, com prévia autorização, conforme previsto nas leis brasileiras.

Esta política responsabiliza cada colaborador a se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação da Comissão Gestora de Proteção de Dados sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Princípios da PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Câmara Municipal de São José do Rio Preto pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

Respeitar a privacidade de todos os colaboradores, estagiários, prestadores de serviço e afins, agindo de forma ética e obedecendo aos princípios da LGPD.

A Câmara Municipal, por meio do Departamento de TI, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas, pautando-se na ética e na legalidade.

Requisitos da PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores, prestadores de serviço, estagiários e afins da Câmara Municipal de São José do Rio Preto a fim de que a política seja cumprida dentro e fora da instituição.

Todo incidente que afete a segurança da informação deverá ser comunicado à Comissão Gestora de Proteção de Dados e, se julgar necessário, deverá encaminhar posteriormente ao Departamento de TI e à Diretoria Geral para análise e realizar as devidas providências.

Poderão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à Internet, no correio eletrônico, nos sistemas desenvolvidos pela Câmara Municipal ou por terceiros.

Caso tenha alguma determinação superior ou de razões tecnológicas que impossibilitem a aplicação desta política, ou ainda o uso apropriado de controle mínimos adequados à garantia da segurança da informação, o solicitante deverá informar imediatamente à Comissão Gestora de Proteção de Dados através de e-mail ou de forma escrita. Desta forma será possível a análise para a adoção de alternativas para minimizar os riscos e organizar um plano de ação para o tratamento da informação.

A Câmara Municipal exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na instituição.

Toda e qualquer atividade que não estejam mencionadas nesta PSI, devem ser realizados apenas após a consulta e autorização da Comissão Gestora de Proteção de Dados.

Das Responsabilidades Específicas

1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, efetivo, comissionado, estagiário ou prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Reportar imediatamente à Comissão Gestora de Proteção de Dados qualquer incidente de segurança da informação, descrita nesta política, através de um documento ou por e-mail: lgpd@riopreto.sp.leg.br.

Solicitar apoio e consultoria de segurança à Comissão Gestora de Proteção de Dados sempre que houver necessidade. Caso tenha alguma ideia, sugerir medidas que possam elevar o nível de segurança da informação da sua área de atuação para a Comissão Gestora de Proteção de Dados.

Propor modificações na PSI conforme as necessidades, atualizações nos sistemas tecnológicos e modificações dos ambientes computacionais.

Não revelar, fora do ambiente de trabalho, fatos ou informações de qualquer natureza que tenha conhecimento devido às suas atribuições, salvo em decorrência de decisão competente do superior hierárquico.

Acessar as informações pessoais de outras pessoas somente por necessidade do serviço prestado e por determinação expressa pelo superior hierárquico.

Utilizar adequadamente os equipamentos da Câmara Municipal, evitando dano físico e acessos indevidos aos ambientes computacionais, que possam comprometer a segurança da informação.

Manter cautela ao exibir informações sigilosas e confidenciais no monitor, televisão, impressoras ou outros meios eletrônicos. Sempre bloquear (atalho no teclado Windows + L) o computador ao sair do ambiente de trabalho para evitar que outras pessoas tenham acesso à sua conta de usuário.

Nunca permitir o uso de sua conta de acesso aos computadores ou sistemas da Câmara Municipal à outras pessoas, para evitar problemas administrativos ou até jurídicos, caso seja constatado alguma irregularidade realizada em sua conta.

2 - Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Câmara Municipal de São José do Rio Preto, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Câmara Municipal de São José do Rio Preto antes de conceder acesso às informações da instituição.

3 – Dos Munícipes

Fica, em regra geral, proibido a utilização de computadores da Câmara Municipal pelos munícipes.

Os munícipes poderão utilizar equipamentos móveis particulares (notebook, smartphone, televisores, etc) nas dependências da Câmara desde que não os conecte na rede local. Para isso, é disponibilizado acesso a rede sem fio “SJRioPreto”.

No caso das solicitações de uso das dependências da Câmara Municipal (Auditório e Plenário), com a requisição expressa (Ofício para o Departamento de TI) dos equipamentos de informática (computadores, notebooks e *datashow*), será permitida a utilização por munícipes. Esses deverão ser indicados pelo requerente, que responderá por qualquer dano causado ao patrimônio utilizado.

4 - Dos Custodiantes da Informação

4.1 - Da Área de Tecnologia da Informação

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, atualização de sistemas, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Câmara Municipal de São José do Rio Preto.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- **os usuários (logins) individuais de funcionários** serão de responsabilidade do próprio funcionário.

- **os usuários (logins) de terceiros** serão de responsabilidade do gestor da área contratante.

Definir as regras formais para instalação de software e hardware em ambiente de produção, exigindo o seu cumprimento dentro da Câmara Municipal.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da instituição, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Câmara Municipal.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

- ✓ Uso da capacidade instalada da rede e dos equipamentos;

- ✓ Tempo de resposta no acesso à Internet e aos sistemas críticos da Câmara Municipal;

- ✓ Períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Câmara Municipal;

- ✓ Incidentes de segurança (vírus, *trojans*, *spyware*, furtos, acessos indevidos, e assim por diante);

- ✓ Atividade de todos os colaboradores durante os acessos às redes externas, inclusive Internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

4.2 - Da Área de Segurança da Informação

Propor as metodologias e os processos específicos para a segurança da informação, como gestão de risco e sistema de classificação da informação. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Câmara Municipal.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pela Diretoria Geral.

Promover a conscientização dos colaboradores em relação à relevância da segurança da Informação para o negócio da Câmara Municipal, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar e realizar tratamento de incidentes em conjunto com a Comissão Gestora de Proteção de Dados.

Manter comunicação efetiva com a Comissão Gestora de Proteção de Dados, Departamento de TI e Diretoria Geral sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Câmara Municipal.

Buscar alinhamento com as diretrizes corporativas da instituição.

5 – Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, a Câmara Municipal poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores de rede, correio eletrônico, conexões com à Internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do superior ou por determinação da Diretoria Geral;

- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Correio Eletrônico

O objetivo desta norma é informar aos colaboradores da Câmara Municipal quais são as atividades permitidas e proibidas quanto ao uso do sistema de correio eletrônico corporativo.

Entende-se por sistema de correio eletrônico, programas, servidores que utilizam um ou mais dos seguintes protocolos: SMTP, POP3 e IMAP.

Engloba desde o software cliente (agente) do usuário, que fará o envio e recebimento de e-mails, até os servidores de correio eletrônico disponibilizados via Internet (*WebMail*).

O uso do correio eletrônico da Câmara Municipal é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para

fins pessoais é permitida desde que feita com bom senso, não prejudique a Câmara e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da Câmara Municipal:

- Fornecer a senha de acesso para pessoas externas;
- Acessar conta de e-mail de outro usuário sem seu consentimento;
- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagens por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Câmara Municipal vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Evitar envolvimento em discussões ou polêmicas (“*flame wars*”) com outros usuários de correio eletrônico (internos e externos);
- Armazenar arquivos de conteúdo ilegal ou considerados abusivos;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer um dos usuários estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
    - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Câmara Municipal;
    - Contenha ameaças eletrônicas, como: ***spam, mail bombing, phishing,*** **vírus de computador**;
    - Contenha arquivos com código executável **(.exe, .com, .bat, .pif, .js, .vbs, .hta, .src,.cpl, .reg, .dll, .inf**) ou qualquer outra extensão que represente um risco à segurança;
    - Vise obter acesso não autorizado a outro computador, servidor ou rede;

- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Vise disseminar correntes, pirâmides, boatos e outros;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- **Nome do colaborador;**
- **Gabinete ou departamento;**
- **Câmara Municipal de São José do Rio Preto;**
- **Telefone(s);**
- **Correio eletrônico.**

Para uma utilização harmônica dos recursos de correio eletrônico, recomenda-se que o usuário evite o envio de e-mails que ocupem muito espaço de armazenamento (imagens, projetos com mapas, gráficos e outros). Para isso existem outros meios mais eficientes (Consulte o Departamento de TI). Também é recomendado que o usuário não respondesse e-mails incluindo os anexos recebidos.

O titular da conta tem total responsabilidade pelo uso da sua conta de e-mail. O mal uso de uma conta por terceiros será responsabilidade de seu titular. Também é de exclusiva responsabilidade do usuário o conteúdo de seus arquivos.

O usuário é responsável pela cópia de segurança de sua caixa postal instalada em sua estação de trabalho.

A caixa postal deve ser limpa a fim de não exceder os limites estabelecidos.

A Câmara Municipal não se responsabilizará, em nenhuma hipótese, por eventuais perdas e danos causados pela utilização dos recursos oferecidos, direta ou indiretamente.

Internet

Todas as regras atuais da Câmara Municipal visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da Internet. Embora a conexão direta e permanente da rede corporativa da instituição com a Internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na Internet está sujeita a divulgação e auditoria. Portanto, a Câmara Municipal, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

O acesso à internet através de cabeamento ou a rede Wi-fi CMSJP por qualquer dispositivo que não é propriedade da Câmara Municipal (celular, notebook, televisão e afins) é proibida, pois gera grande riscos na segurança da rede, onde há a possibilidade de invasões por vírus ou outros programas maliciosos.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/Internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Câmara, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo diretor/vereador.

A Internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse da Câmara Municipal que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Câmara Municipal para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal, a LGPD e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na Internet.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na Internet são expressamente proibidos.

Qualquer software não autorizado baixado será excluído pelo Departamento de TI.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da Câmara Municipal para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Todos os softwares e arquivos transferidos de fontes que não sejam da própria Câmara Municipal via Internet (ou qualquer outra rede Pública) devem ser examinados com o software de detecção de vírus utilizado pela instituição. Este exame deve acontecer antes que o arquivo seja executado ou aberto por outro programa, como por exemplo, por um processador de texto e também, antes e depois que o material tenha sido descompactado.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) não poderão ser realizados por usuários.

Materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à Internet não poderão efetuar upload (subida) de qualquer software licenciado à Câmara Municipal ou de dados de sua propriedade aos seus parceiros, colaboradores e munícipes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da Câmara para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (P2P) (Kazaa, eMule, BitTorrent, µTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos, mediante autorização da Diretoria Geral. Porém, os serviços de comunicação instantânea (MSN, WhatsApp, Telegram e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o diretor ou vereador requisite formalmente ao Departamento de TI.

Não é permitido acesso a sites de *proxy*.

É expressamente proibido utiliza-se de qualquer meio para conectar à "*Deep* WEB" na rede da Câmara Municipal.

Caso necessário, haverá bloqueios de acesso a domínios que comprometam o uso de banda e ofereçam riscos à segurança da rede, sempre com autorização da Diretoria Geral.

O acesso remoto é permitido apenas aos prestadores de serviço da Câmara Municipal para manutenção, atualização ou instalação de sistemas ou recursos tecnológicos e será supervisionada por um servidor do Departamento de TI. Também é permitida o acesso remoto a determinados computadores para casos de identificação de problemas em sistemas utilizados na Câmara Municipal ou treinamento de servidores.

O Departamento de TI recomenda adoção de algumas práticas que visam garantir segurança ao utilizar a Internet:

- ✓ Utilizar criptografia sempre que enviar e receber dados com informações sensíveis;
- ✓ Certificar a procedência do sítio e a utilização de conexões seguras (criptografadas) ao realizar transações via *Web*;
- ✓ Verificar se o certificado do sítio ao qual se deseja acessar está integro e corresponde realmente aquele sítio, observando ainda, se o mesmo está dentro do prazo de validade;
- ✓ Certificar que o endereço apresentado no navegador corresponde ao sítio 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 outro endereço destino.
- ✓ Nunca acessar um site ou tentar instalar um programa a pedido de uma pessoa externa durante uma ligação telefônica ou através de qualquer meio de chat online.

Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Câmara Municipal e/ou terceiros.

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na Câmara Municipal, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir *login* de uso compartilhado por mais de um colaborador, a responsabilidade perante a Câmara e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do diretor/vereador de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de TI responde pela criação, atualização e desativação da identidade lógica dos colaboradores na instituição.

Devem ser distintamente identificados os visitantes, estagiários, funcionários temporários, funcionários regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar a sua senha após 24h da criação conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, que atenda os seguintes requisitos:

- Ter pelo menos 08 (oito) caracteres de comprimento;
- Não conter partes significativas do nome da conta do usuário ou o nome todo;
- Conter caracteres de três das quatro categorias a seguir:
    - Caracteres maiúsculos (A-Z);
    - Caracteres minúsculos (a-z);
    - 10 (dez) dígitos básicos (0-9);
    - Caracteres não alfabéticos (por exemplo, “!”, “$”, “#”, “%”, “=”).

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de tamanho variável, que atenda os seguintes requisitos:

- Ter pelo menos 10 (dez) caracteres de comprimento;
- Não Conter partes significativas do nome da conta do usuário ou o nome todo;
- Conter caracteres das quatro categorias a seguir:
    - Caracteres maiúsculos (A-Z);
    - Caracteres minúsculos (a-z);
    - 10 (dez) dígitos básicos (0-9);
    - Caracteres não alfabéticos (por exemplo, “!”, “$”, “#”, “%”, “=").

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, Notepad, etc.), compreensíveis por linguagem humana (não criptografados); é aconselhado que as senhas não sejam baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da instituição, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 6 (seis) meses, não podendo ser repetidas as 05 (cinco) últimas senhas. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Se o usuário informar a senha errada por 10 (dez) vezes consecutivas (com interstício inferior a 30 minutos), terá seu login bloqueado automaticamente. O desbloqueio deverá ser solicitado, pessoalmente ou por escrito, ao Departamento de TI.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário deixar de ser servidor (efetivo ou comissionado) da Câmara Municipal ou solicitar exoneração, o Departamento de Pessoal deverá imediatamente comunicar tal fato ao Departamento de TI, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente ao Departamento de TI para cadastrar uma nova.

As solicitações para novas identificações de usuários e alterações de privilégios devem ser feitas por escrito (ofício) e aprovadas pela chefia imediata do usuário antes que o Departamento de TI realize tal solicitação.

Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da Câmara Municipal, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas diretorias responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico do Departamento de TI da Câmara Municipal, ou de quem este determinar. As diretorias que necessitarem fazer testes deverão solicitá-los previamente ao Departamento de TI, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Não mover equipamentos dos locais onde foram instalados, exceto sob autorização do superior imediato, mesmo para os notebooks.

Notificar imediatamente ao Departamento de TI as ocorrências com o computador quer seja invasão, dano ou roubo.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Departamento de TI.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário, mediante autorização do Departamento de TI, juntamente com a Diretoria Geral.

Arquivos pessoais e/ou não pertinentes ao negócio da Câmara Municipal (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário. Essa regra vale também aos sistemas de armazenamentos locais (discos rígidos dos computadores, unidades externas de armazenamento, NAS, etc) pertencentes à instituição.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede (NAS, por exemplo). Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da Câmara Municipal e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização do Departamento de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os colaboradores devem informar ao Departamento de TI qualquer identificação de dispositivo estranho conectado ao seu computador;

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico do Departamento de TI da Câmara Municipal ou por terceiros devidamente contratados para o serviço.

- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;

- O colaborador deverá manter a configuração do equipamento disponibilizado pela Câmara Municipal, seguindo os devidos controles de segurança exigidos nesta PSI e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;

- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados ("Tela Limpa");

- Todos os recursos tecnológicos adquiridos pela Câmara Municipal devem ter imediatamente suas senhas padrões (default) alteradas;

- Somente implantar serviços de WWW, e-mail e FTP em seus computadores quando for necessário, comunicando o Departamento de TI e ficando responsável pelas medidas de segurança e atualizações destes sistemas;

- Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Câmara Municipal:

    - Colocar objetos sobre o equipamento de maneira que prejudique o sistema de ventilação do computador;

    - Manipular líquidos ou substâncias que possam danificar o equipamento quando os estiver operando, assim como não fumar;

    - Acessar, modificar, remover ou copiar arquivos que pertençam a outro usuário sem a permissão expressa do mesmo;

    - Tentar ou obter acesso não autorizado a outro computador, servidor ou rede, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidade nos sistemas de TI;

    - Burlar quaisquer sistemas de segurança;

    - Acessar informações confidenciais sem explícita autorização do proprietário;

    - Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (***sniffers***). Esse procedimento só será permitido ao Departamento de TI, quando o objetivo for garantir o cumprimento das regras mencionadas nesta PSI;

    - Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

    - Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional;

- Conectar computadores pessoais na rede da Câmara Municipal, exceto quando autorizado, por escrito, pela Diretoria Geral, juntamente com o Departamento de TI.

- Utilizar-se de mecanismo para burlar o sistema de segurança da informação da Câmara Municipal (Firewall e Proxy).

No desligamento de um usuário, seus arquivos armazenados em computadores ou em qualquer servidor de rede da Câmara Municipal, devem ser imediatamente revisados pela chefia imediata para determinar quem se tornará curador das informações relacionadas, assim como nos casos devidos, identificando o método mais adequado para eliminação destas, levando-se em conta as orientações sobre a eliminação de informações classificadas contidas na legislação vigente.

Como sugestão, os usuários deverão realizar cópia de segurança (Backup) dos arquivos pessoais armazenados no computador que utiliza na Câmara.

Os dispositivos de backup e/ou gravação de origem externa devem ser submetidos ao exame de um software antivírus antes de conectá-los aos computadores da Câmara Municipal, bem como nos servidores de rede.

Os sistemas computacionais utilizados para os processos do poder legislativo são acessados apenas no ambiente interno da Câmara Municipal, isto é, não é possível acessar externamente. Isto é feito para acrescentar uma segurança maior ao sistema, garantindo que não tenha acesso de terceiros aos sistemas computacionais e evite algum tipo de invasão, pois um computador, que não está na Câmara Municipal é cabível de possuir vírus ou outros tipos de ameaças. O acesso externo é liberado exclusivamente para os casos de autorização do Diretor Geral, na qual deve ser documentado em ofício. Caso fique constatado alguma invasão no sistema e a causa seja por esta liberação, a responsabilidade será do autorizador.

Dispositivos Móveis

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pelo Departamento de TI, como: notebook, smartphone e tablets.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os usuários que utilizem tais equipamentos.

A Câmara Municipal, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na instituição, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo usuário deverá realizar periodicamente cópia de segurança (backup) dos dados do dispositivo móvel em sua posse. Deverá, também, manter estes backups separados do dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade da Câmara Municipal e aos seus usuários deverá seguir o mesmo fluxo de suporte fornecido pela instituição.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico do Departamento de TI.

O usuário deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico do Departamento de TI.

A reprodução não autorizada do software instalado nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Câmara Municipal, notificar imediatamente seu diretor ou vereador e ao Departamento de TI. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O usuário deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a instituição.

Não será permitido o uso de equipamentos portáteis particulares na rede da Câmara Municipal (rede cabeada e sem fio). Para esse fim, deverá ser utilizada a rede sem fio "SJRioPreto". Só será permitido conectar esses equipamentos na rede da Câmara Municipal mediante análise e aprovação da Diretoria Geral, em conjunto com o Departamento de TI.

Fica expressamente proibido o uso de dispositivos de redes (*switches*, *Access Point*, Roteadores etc.) particulares nas dependências da Câmara Municipal.

O Departamento de TI não se responsabiliza por prestar manutenção ou instalar software em computadores, notebooks e celulares (*smartphones*) que não sejam os da instituição.

O Departamento de TI tem o direito de, periodicamente, auditar os notebooks utilizados na instituição, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo executados na instituição.

É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, no caso de equipamentos particulares liberados para utilizar a rede da Câmara Municipal.

Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, bem como a captura de informações confidenciais, como por exemplo: senhas de usuários.

Fica proibida a apropriação de arquivos que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam a instituição não podem ser carregados nos notebooks ou dispositivos de armazenamento móvel (ex.: pendrive), sem autorização da área responsável pelos dados.

Sala dos Servidores de Rede

Somente os colaboradores com autorização poderão entrar na Sala de Servidores. Essa autorização será emitida pelo Departamento de TI, juntamente com a Diretoria Geral.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

Deverão existir duas cópias de chaves da porta da Sala dos Servidores. Uma das cópias ficará de posse do coordenador responsável pelo Departamento de TI, a outra, de posse da Diretoria Geral.

A Sala dos Servidores deverá ser mantida limpa e organizada. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da Manutenção Predial.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

Deve-se sempre manter o ar condicionado, pelo menos um, ligado durante todo o dia para manter os servidores refrigerados e seguros contra superaquecimento.

A entrada ou retirada de quaisquer equipamentos da Sala de Servidores somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Departamento de TI.

Pasta Compartilhada

A pasta de rede compartilhada é liberada para troca de arquivos entre os membros do grupo, como comissões, gabinetes de vereadores e departamentos da Câmara Municipal. Ela é criada em um computador de um dos membros do grupo e é acessada apenas se esta estiver ligada. A Câmara Municipal não se responsabiliza pela segurança e disponibilidade dos arquivos da pasta compartilhada, portanto a cópia de segurança (backup) é de total responsabilidade do grupo a quem pertence.

Backup

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup poderão realizar pesquisas para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da Câmara Municipal, exigem uma regra de retenção especial, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou *restore* é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Todo processo de restauração de backup deverá ser solicitado por ofício direcionado à Diretoria Geral e Departamento de TI. Só os responsáveis pela informação poderão solicitar sua restauração.

O tempo de restauração varia de acordo com o tamanho da informação.

Rede sem-fio "SJRioPreto"

Todo acesso à rede sem-fio "SJRioPreto" é liberado, onde o usuário realiza o cadastro na rede através de formulário online ao acessar o link "Registre-se".

O Departamento de TI não se responsabiliza ao acesso a essa rede. O controle desta rede é feito pela EMPRO, que disponibiliza esse serviço gratuitamente para a população.

Das Infrações e Penalidades

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis, podendo incorrer em processo administrativo disciplinar, assegurado o contraditório e a ampla defesa.

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à Câmara Municipal de São José do Rio Preto e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Das Disposições Finais

Caso seja identificado algum descumprimento das regras expostas, a Comissão Gestora de Proteção de Dados irá entrar em contato com o Departamento de TI para bloquear temporariamente o acesso do usuário infrator e comunicará os motivos ao profissional e ao gestor da área.

Esta PSI estará disponível no site da Câmara Municipal de São José do Rio Preto (www.riopreto.sp.leg.br) ou realizar um pedido a um membro da Comissão Gestora de Proteção de Dados, que enviará o arquivo PDF por e-mail ou outra forma digital.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Câmara Municipal. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.