DECRETO Nº 4.434
DE 09 DE NOVEMBRO DE 2021

"INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DA ADMINISTRAÇÃO DIRETA E INDIRETA NO MUNICÍPIO DE QUATÁ E DÁ OUTRAS PROVIDÊNCIAS

MARCELO DE SOUZA PÉCCHIO, Prefeito Municipal de Quatá, Estado de São Paulo, no uso de suas atribuições legais:

CONSIDERANDO a necessidade de estabelecer diretrizes e critérios para o acesso, uso, padronização e estruturação das informações e descrever normas de utilização dos dados;

CONSIDERANDO que a Política de Segurança da Informação visa a proteção e gestão da informação e direciona as condutas de todos os usuários e técnicos da entidade;

CONSIDERANDO os últimos apontamentos realizados pelo Tribunal de Contas, no sentido de que a Prefeitura não dispunha de uma Política de Segurança formalmente instituída e de cumprimento obrigatório;

DECRETA

Art. 1º - Fica instituída a Política de Segurança da Informação no âmbito da Administração Direta e Indireta no Município de Quatá, cujo texto foi elaborado pelo servidor público municipal, lotado no cargo de Analista de TI.

Art. 2º - Para efeito deste Decreto ficam estabelecidas as Diretrizes e Normas constantes no Anexo I.

Art. 3º - As diretrizes estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Art. 4º - A violação das normas descritas no art. 2° deste Decreto constitui infração disciplinar, previstas no artigo 204 e seguintes do Estatuto do Servidores Públicos Municipais – Lei Complementar Municipal nº. 2.567 de 15.06.2010.

Art. 3º - Este Decreto entra em vigor na data de sua publicação.

Prefeitura Municipal de Quatá, 09 de novembro de 2021.

MARCELO DE SOUZA PECCHIO
Prefeito Municipal

Publicado e registrado na Secretaria da Prefeitura Municipal de Quatá, na data supra.

FÁTIMA AP. CROSCATTO LOPES PEREIRA
Secretária Administrativa

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PREFEITURA MUNICIPAL DE QUATÁ

Histórico de Versões

Versão	Data
1.0.0	27/10/2021

Sumário

OBJETIVOS

Este documento tem por objetivo principal estabelecer diretrizes de Tecnologia da Informação (TI) para proteção legal da Prefeitura Municipal de Quatá, 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.

O documento é um guia que tem como objetivo a criação de um instrumento de referência para a implantação de um ambiente informacional mais seguro na Prefeitura Municipal de Quatá, facilitando desta forma os processos de gestão e controle.

A Segurança da Informação tende a se tornar um tema permanente na agenda de atividades da instituição, no qual questões estratégicas da área de TI são tratadas e discutidas de maneira a aprimorar os mecanismos de gestão governamental, visando a melhoria contínua da qualidade dos processos internos e serviços prestados ao cidadão.

O objetivo principal deste documento é servir como guia, promover e motivar a criação de uma cultura de Segurança da Informação. O documento deve servir como referência, na área de Segurança da Informação, para a Prefeitura Municipal de Quatá e suas secretarias, setores e departamentos. Estas dependências poderão desenvolver guias de melhores práticas, considerando o seu contexto de atuação e observando sempre o disposto na legislação vigente, bem como nos padrões de interoperabilidade. Como é uma Política relacionada com uma área tecnológica bem definida, Segurança da Informação, é importante que o mesmo seja revisto anualmente, com vista a sua atualização e adequação tecnológica e legal.

É importante salientar que, busca-se desenvolver um comportamento ético e profissional, para que todos possam utilizar da melhor forma as ferramentas de TI 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.

Preservar as informações do Prefeitura Municipal de Quatá 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.

SIGLAS E ABREVIATURAS

- **ABNT**. Associação Brasileira de Normas Técnicas.
- **LGPD**. Lei Geral de Proteção a Dados.
- **PSI**. Política de Segurança da Informação.
- **STI**. Setor de Tecnologia da Informação da Prefeitura Municipal de Quatá.
- **TI**. Tecnologia da Informação.

DEFINIÇÕES

- **Ativo**. Ativos físicos e lógicos dentro do escopo de TI.
- **Ativo físico.** Dentro do escopo de TI, todos equipamentos que apresentam um valor, como por exemplo: computadores, notebooks, impressoras, monitores, roteadores, equipamentos de acesso sem fio, *switches* etc.
- **Ativo lógico.** Sistemas, redes, dados estruturados (banco de dados), dados não estruturados (e-mails, planilhas, documentos de texto etc).
- **Estação de trabalho.** Conjunto de equipamentos e seus sistemas operacionais utilizados pelos colaboradores para acesso à Internet, ao sistema de arquivos ou aos demais sistemas institucionais. Tipicamente compreendem: computador e monitor, notebook, tablet ou smartphone.
- **Colaborador**. Servidores, empregados, contratados por tempo determinado, estagiários e prestadores de serviços que exercem atividades no âmbito da Prefeitura Municipal de Quatá.
- **Credencial de acesso.** Conjunto de login e senha capazes de identificar um usuário.
- **Gestor de unidade.** Secretário ou chefe de setor.
- **Internet.** Rede mundial de computadores, compreende todas as redes externas que podem ser acessadas publicamente.
- **Plataforma de Suporte Técnico de Informática.** Plataforma pela qual podem ser solicitados ao STI: reparos de ativos, instalações e ações referentes às credenciais de acesso.
- **Pastas compartilhadas.** Pastas que estão armazenadas nos servidores de arquivos e são compartilhadas entre diferentes estações de trabalho sejam elas do mesmo setor ou não.
- **Pastas de Setor**. Pastas compartilhadas com acesso permitido às estações de trabalho de um setor.
- **Pastas de Secretaria**. Pastas compartilhas com acesso permitido às estações de trabalho da mesma secretaria ou de setores correlatos
- **Pasta Pública**. Pastas compartilhadas com acesso permitido a todas as estações de trabalho da instituição.
- **Ponto de Acesso sem Fio**. Equipamento que é ou desempenha função de acesso sem fio à rede local.
- **Rede cabeada.** Sistema que interliga equipamentos utilizando cabos de par trançado ou fibras ópticas.

- **Rede local.** Conjunto de recursos compartilhados através dos servidores de rede, switches e estações de trabalho nos quais circulam as informações corporativas da Prefeitura Municipal de Quatá.
- **Rede sem fio.** Sistema que interliga equipamentos com transmissão através de ondas eletromagnéticas.
- **Usuário externo.** Indivíduo que não faz parte do quadro de colaboradores da Prefeitura Municipal de Quatá.

1. INTRODUÇÃO

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

1.1. Público-alvo

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

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Sistemas sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações

1.2. Evolução e atualização do documento

A PSI será atualizada anualmente. Poderão acontecer atualizações antes desse período no documento principal ou nos seus anexos quando o Setor de Tecnologia da Informação (STI) e a Secretaria de Administraçao e Finanças julgarem necessário.

2. FUNDAMENTOS E CONCEITOS DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Para a implementação de controles de segurança faz-se necessária a criação de um processo de gestão da segurança da informação. Este processo deve considerar o incentivo à definição de políticas de segurança, cujos escopos devem abarcar o gerenciamento de riscos baseado em analise quantitativa e qualitativa, como analises de custo benefício e programas de conscientização.

A gestão da segurança da informação inicia-se com a definição de políticas, procedimentos, guias e padrões. As políticas podem ser consideradas como o mais alto nível de documentação da segurança da informação, enquanto nos níveis mais baixos podemos encontrar os padrões, procedimentos e guias. Isto não quer dizer que as políticas sejam mais importantes que os guias, procedimentos e padrões.

3. DIRETRIZES GERAIS

3.1. Uso aceitável dos recursos de TI

O uso correto e responsável dos recursos de TI deve ser aplicado a todos os colaboradores da instituição, inclusive aos externos, servidores e prestadores de serviço, que utilizam esses recursos e a infraestrutura disponível. Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelo usuário, no âmbito da infraestrutura de TI, ficando os transgressores sujeitos à Lei Penal, Civil e Administrativa, na medida da conduta, dolosa ou culposa, que praticarem.

Os sistemas de TI deverão ser utilizados sem violação dos direitos de propriedade intelectual de qualquer pessoa ou empresa, como marcas e patentes, nome comercial, segredo empresarial, domínio na Internet, desenho industrial ou qualquer outro material, que não tenha autorização expressa do autor ou proprietário dos direitos, relativos à obra artística, científica ou literária. As informações pertencentes à instituição devem ser utilizadas apenas para os propósitos definidos na sua missão institucional.

3.2. Uso seguro dos recursos de TI

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:

1. Fazer regularmente cópias de segurança de seus dados;
2. Manter registro das cópias de segurança;
3. Guardar as cópias de segurança em local seguro e distinto daquele onde se encontra a informação original;
4. Utilizar senhas que contenham, pelo menos, oito caracteres, compostos de letras, 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;
5. Alterar periodicamente suas senhas;
6. Utilizar criptografia sempre que enviar ou receber dados com informações sensíveis;
7. Certificar a procedência do site e a utilização de conexões seguras (criptografadas) ao realizar transações via web;

8. 8. Verificar se o certificado do site ao qual se deseja acessar, esta integro e corresponde realmente aquele sítio, observando ainda, se o mesmo está dentro do prazo de validade;

9. Certificar que o endereço apresentado no navegador corresponde ao site que realmente se quer acessar, antes de realizar qualquer ação ou transação;

10. Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;

11. Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus;

12. Não utilizar o formato executável em arquivos compactados, pois estes tipos são propícios à propagação de vírus.

3.3. Atividades permitidas

1. Utilizar programas de computador licenciados para uso pela instituição, de acordo com as disposições específicas previstas em contrato. A instalação de programas e sistemas homologados é atribuição do STI.;

2. Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente àquelas referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade;

3. Fazer cópia de documentos e ou programas de computador a fim de salvaguardá-los, respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos no âmbito da Administração Pública Municipal, exigindo-se autorização para aqueles protegidos pelos direitos autorais, inclusive músicas, textos, documentos digitalizados e qualquer conteúdo encontrado em revistas, livros ou quaisquer outras fontes protegidas por direitos aurorais

3.4. Atividades não permitidas

1. Introduzir códigos maliciosos nos sistemas de TI;

2. Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;

3. Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;

4. Tentar interferir desautorizadamente em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;

5. Alterar registro de evento dos sistemas de TI;

6. Modificar cabeçalho de qualquer protocolo de comunicação de dados;

7. Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;

8. Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização do setor competente;

9. Violar medida de segurança ou de autenticação, sem autorização do setor competente;

10. Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;

11. Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente;

12. Armazenamento ou uso de jogos em computador ou sistema informacional;

13. Uso de recurso informacional da entidade pública para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza;

14. Uso de aplicativos não homologados nos recursos informacionais da insituição.

4. DIRETRIZES ESPECÍFICAS

4.1. Acesso à Internet

4.1.1. O acesso à Internet nas dependências da Prefeitura Municipal de Quatá será restrito e liberado somente mediante a utilização de credencial de acesso.

4.1.2. O acesso à Internet nas dependências da Prefeitura Municipal de Quatá contará com filtros de acesso e monitoramento por meio do registro de logs vinculados à credencial de cada colaborador.

4.1.3. Sites e serviços com conteúdos pornográficos, racistas, com apologia ao terrorismo, disseminação de ódio e com violação de direitos autorais serão bloqueados.

4.1.4. Sites e serviços com conteúdo não necessário ao desempenho das funções dos colaboradores—por exemplo, redes sociais e serviços de *streaming* de vídeo—serão bloqueados.

4.1.5. Sites e serviços bloqueados poderão ser liberados a colaboradores mediante solicitação devidamente justificado ao STI pelo gestor da unidade.

4.1.6. Os gestores das unidades, gestores de contratos, supervisores de estágio e o Setor Pessoal deverão sempre informar imediatamente ao STI o desligamento de algum colaborador, seja qual for o motivo, para que seja realizado o bloqueio de acesso.

4.1.7. Sempre que ausentar-se da estação de trabalho, o colaborador deve remover sua credencial de acesso, desautenticando-se.

4.1.8. 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.

4.1.9. É vedado compartilhar credeciais de acesso com outros colaboradores ou usuários externos à instituição.

4.2. Acesso à rede local

4.2.1. Somente estação de trabalho e equipamentos devidamente registrados e configuraoas pelo STI terão acesso à rede local.

4.2.2. O colaborador dever solicitar por meio de plataforma de suporte técnico o mapeamento de recursos de rede com a liberação do acesso à rede local.

4.2.3. É permitido ao colaborador o acesso remoto à rede local. O acesso deverá ser solicitado de forma expressa ao STI e será realizado mediante a utilização de VPN e de credencial de acesso.

4.3. Utilização da rede sem fio

4.3.1. A utilização da rede sem fio acontecerá mediante a utilização de senha.

4.3.2. 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 STI. Os pontos de acesso da rede sem fio só podem ser instalados, registrados e configurados pelo STI.

4.3.3. É vedado compartilhar senhas de acesso à rede sem fio com usuários externos à instituição.

4.4. Utilização de Estações de Trabalho

4.4.1. É responsabilidade do colaborador zelar pelo bom uso e conservação de sua estação de trabalho.

4.4.2. É responsabilidade do colaborador realizar solicitações de reparo e manutenção da estação de trabalho na plataforma de Suporte Técnico de Informática.

4.4.3. É vedado permitir o acesso físico ou remoto de usuário não autorizado à estação de trabalho.

4.4.4. É vedado armazenar arquivos com conteúdos pessoais, pornográficos, com violação direitos autorais, com incitação de violência e ódio ou com qualquer outro tipo de conteúdo incompatível com as funções desempenhadas pelo colaborador.

4.4.5. O colaborador é o único responsável pelos arquivos localmente armazenados em sua estação de trabalho.

4.4.6. É responsabilidade do colaborador realizar cópias de segurança dos arquivos localmente armazenados na sua estação de trabalho. O STI só se responsabiliza por arquivos armazenados nos servidores.

4.4.7. Arquivos cuja perda acarreta prejuízo à instituição devem ser sempre que possível armazenados nos servidores.

4.4.8. Toda estação de rabalho deve possuir credencial de acesso para não permitir o acesso não autorizado.

4.4.9. Sempre que ausentar-se da estação de trabalho, o colaborador deve remover suas credenciais de acesso, desautenticando-se.

4.4.10. Sempre que realizar a impressão de documento com informação confidencial, este documento deve ser retirado da impressora de forma mais rápida possível.

4.5. Utilização do Sistema de Arquivos

4.5.1. O sistema de arquivos compreende o conjunto de pastas compartilhadas que são armazenados nos servidores e mapeadas nas estações de trabalho.

4.5.2. As pastas compartilhadas são organizadas em três tipos: a) pastas de setor: acesso compartilhado somente entre as estações de trabalho do mesmo setor; b) pastas de secretaria: acesso compartilhado somente entre a estações de trabalho da mesma secretaria ou de setores correlatos; e c) pasta pública: acesso compartilhado entre todas as estações de trabalho da instituição.

4.5.3. É responsabilidade do colaborador manter dados sigilosos armazenados apenas nas pastas de setor.

4.5.4. O colaborador sempre deverá optar, nesta ordem, pela pasta de setor e pela pasta de secretaria em detrimento à pasta pública.

4.5.5. A pasta pública só deve ser usada quando for necessário compartilhar um arquivo com um setor de uma outra secretaria. Quando for necessário realizar um compartilhamento, o colaborador deve colocar uma cópia do arquivo na pasta pública e manter a versão original na sua pasta de setor.

4.5.6. O STI realizará periodicamente a limpeza da pasta pública a fim de garantir o sigilo de informações e a economicidade de recursos computacionais.

4.5.7. Pastas compartilhadas devem possuir cópias de segurança. O STI é responsável por criar cópias de segurança e executar rotinas de backups nas pastas compartilhadas.

4.5.8. É vedado realizar qualquer tentativa de acesso não autorizado às pastas compartilhadas.

4.6. Utilização de Correio Eletrônico

4.6.1. É vedado a utilização de serviços de e-mail que não sejam o oficial (@quata.sp.gov.br), como por exemplo: GMail e Hotmail.

4.6.2. A comunicação corporativa interna, a comunicação com cidadãos e a comunicação com outras instituições deverá ser realizada com e-mail oficial.

4.6.3. É vedado o envio de *spams*, correntes e quaisquer outros assuntos que não sejam de interesse institucional.

4.6.4. O uso do e-mail é estritamente corporativo, sendo vedado utilizar em redes sociais, *e-commerce*, serviços de *streaming* e outros.

4.6.5. É vedado compartilhar credenciais de acesso do e-mail a usuário não autorizado.

4.7. Utilização de Sistemas e Aplicações Corporativas

4.7.1. Deve ser vedado aos usuários que fazem uso de sistemas de informação o acesso não autorizado a qualquer outro sistema que não possua permissão de uso, assim como a danificação, a alteração a interrupção da operação de qualquer sistema do ambiente de TI. Da mesma maneira deve ser vedado aos usuários a obtenção indevida de senhas de acesso,chaves criptográficas ou qualquer outro mecanismo de controle de acesso que possa possibilitar o acesso não autorizado a recursos informacionais;

4.7.2. A classificação ou reclassificação da informação deve seguir as orientações da legislação vigente, assim como aquelas regras definidas pelo Decreto Nº 4553 ou sua

atualização;

4.7.3. São vedados aos usuários o acesso, modificação, a remoção ou a cópia de arquivos que pertençam a outro usuário sem a permissão expressa do mesmo;

4.7.4. A instituição deve se reservar o direito de revogar os privilégios de usuário de qualquer sistema e a qualquer momento. Não sendo permitidas condutas que interfiram com a operação normal e adequada dos sistemas de informação e que adversamente afetem a capacidade de outras pessoas utilizarem esses sistemas de informação, bem como condutas que sejam prejudiciais e ofensivas;

4.7.5. É vedada aos usuários a execução de testes ou tentativas de comprometimento de controles interno, este tipo de prática somente pode ser permitida a usuários técnicos, em situações nas quais esteja ocorrendo monitoramento e análise de riscos, com a autorização da unidade competente;

4.7.6. Deve ser exigido a assinatura de termo de confidencialidade antes que seja fornecido o acesso aos sistemas governamentais relacionados com a cadeia de privilégios dousuário.

4.7.7. Quando do desligamento do usuário, seus arquivos armazenados em estação de trabalho ou em qualquer servidor de rede e, também, seus documentos em papel devem ser imediatamente revisados pela chefia imediata para determinar quem tornar-se-á curador das informações relacionadas, assim como nos casos devidos, identificar o método mais adequado para a eliminação das mesmas, levando-se em conta as orientações sobre a eliminação de informações classificadas contidas na legislação vigente.

4.7.8. Todas as atividades dos usuários que podem afetar os sistemas de informação devem ser possíveis de reconstituição a partir dos logs de maneira a evitar ou dissuadir o comportamento incorreto. Estes procedimentos devem contar inclusive commecanismos de responsabilização claros e amplamente divulgados nos meios de comunicação internos.

4.7.9. É vedada a utilização de software da Internet ou de qualquer outro sistema externo não configurado ou instaldo pelo STI. Esta proibição é necessária porque tal software pode conter vírus, worms, cavalos de tróia e outros softwares maliciosos que podem comprometer o ambiente de TI.

4.7.10. Deve ser vedada a utilização de dispositivos de armazenamento de origem externa, nas estações de trabalho ou nos servidores de rede antes de serem submetidos a um sotware antivírus.

4.7.11. Colaboradores e usuários externos devem evitar fumar, comer ou beber próximo aos equipamentos de TI a fim de evitar danos.

4.8. Utilização e Manipulação de Informações

4.8.1. A palavra "usuário" será utilizada para designar todos utilizadores do ambiente de TI, independente do cargo ocupado;

4.8.2. Instruções claras e bem divulgadas sobre normas existentes sobre a manipulação de informações;

4.8.3. Todos os usuários têm que observar as exigências para manipulação da informação, baseadas no tipo de informação considerada e que será definida pelo seu proprietário (ou responsável) seguindo as orientações encontradas no documento de Política de Segurança de cada órgão ou instituição.

4.8.4. A divulgação de informações CONFIDENCIAL ou RESTRITA, para qualquer pessoa (usuário ou não do ambiente de TI do órgão ou instituição), é proibida, a menos que este acesso tenha sido previamente autorizado pelo proprietário da informação. Todas as pessoas que não forem usuários diretos do órgão ou instituição devem assinar um termo de confidencialidade antes de terem acesso a esses tipos de informação. Os curadores dessas informações devem verificar a existência deste termo, devidamente assinado, antes de divulgá-las para pessoas que não pertençam ao quadro funcional do órgão ou instituição. O acesso a este tipo de informação deve ser sempre devidamente registrado.

4.8.5. A reprodução da informação CONFIDENCIAL e/ou RESTRITA, incluindo a impressão de cópias adicionais, não é permitida a menos que seja explicitamente autorizada or seu proprietário. Da mesma forma, trechos, resumos, traduções ou qualquer material derivado de informações sensíveis ou resguardadas por direitos autorais, não poderão ser feitos a menos que o proprietário da informação tenha aprovado previamente.

4.8.6. O transporte físico das informações CONFIDENCIAIS e/ou RESTRITAS requer a

observação no disposto em legislação relacionada.

4.8.7. Quando as informações são CONFIDENCIAIS e/ou RESTRITAS não forem mais necessárias e quando exigências legais ou regulatórias para sua retenção não se aplicarem mais, elas deverão ser destruídas de acordo com os métodos aprovados. É proibida a eliminação em latas de lixo ou em depósitos de papel que serão encaminhados para reciclagem. A informação sensível em forma de papel deve ser eliminada com o uso de picotador de papel. A informação sensível armazenada em disquetes, fitas magnéticas ou outras mídias magnéticas computacionais deve ser destruída via refornatação ou apagando-se a informação caso a mídia seja reutilizada por outros sistemas do órgão ou instituição pública. A simples "remoção" de uma informação sensível armazenada em uma mídia magnética não é suficiente porque a informação pode ser definitivamente destruída com cortadores ou colocada em um recipiente especialmente destinado a armazenagem de informação sensível que será destruída.

4.8.8. A manipulação das informações deverá atender à legislação vigente e, em especial, à regulamentação local da LGPD.

TERMO DE CIÊNCIA

Política de Segurança da Informação

Eu,_____,
Portador do documento de identidade nº _____, expedido pela _____, CPF nº _____, órgão de origem _____, lotado n(a) Secretaria de _____, declaro que tenho ciência de Política de Segurança da Informação e comprometo-me a seguir suas diretrizes.

Comprometo-me ainda a manter sigilo de processos, informações, documentos e materiais não públicos que eu venha a ter acesso ou conhecimento em razão das atividades profissionais. Tenho ciência que o descuprimento de normas poderá levar

_____

(Assinatura)