POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PSI

1 - OBJETIVOS DA PSI

Este documento tem como objetivo estabelecer a Política de Segurança da Informação do TATUIPREV, definindo as diretrizes relacionadas à segurança da informação.

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do TATUIPREV para a proteção dos ativos de informação e a responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Autarquia e por todos os servidores e prestadores de serviço que tenham acesso às informações de propriedade do TATUIPREV.

1.1 - Constitui objetivo da PSI

Estabelecer diretrizes que permitam aos colaboradores e fornecedores do TATUIPREV seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e do indivíduo;

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento;

1.2 - Preservação das informações do TATUIPREV

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

A segurança da informação deve abranger três aspectos básicos, destacados a seguir:

- **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; e

- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2 - APLICAÇÕES DA PSI

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.

Parágrafo único. É obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

3 - DAS RESPONSABILIDADES ESPECÍFICAS

Entende-se por colaborador toda e qualquer pessoa física, contratada no regime estatutário, CLT ou temporário, e os prestadores de serviço, contratados por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do TATUIPREV.

Os colaboradores deverão:

I - Manter sigilo das informações do RPPS;

II - Zelar pelos ativos de informação do RPPS, sejam eles físicos (processos, documentos etc.) ou digitais (arquivos, sistemas etc.); e

III - Seguir as diretrizes e recomendações da Diretoria Executiva quanto ao uso, divulgação e descarte de dados e informações.

Será de inteira responsabilidade de cada servidores, todo prejuízo ou dano que vier a sofrer ou causar ao TATUIPREV e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

4 – DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Os documentos integrantes da estrutura devem ser divulgados a todos os servidores, segurados, estagiários e prestadores de serviços do TATUIPREV quando de sua admissão, bem como, através dos meios oficiais de divulgação interna da Instituição e, também, publicadas no seu site oficial, de maneira que seu conteúdo possa ser consultado a qualquer momento.

Os documentos integrantes da estrutura normativa, relacionados às diretrizes estabelecidas por esta Política de Segurança da Informação, deverão ser revistos periodicamente.

5 – PROTEÇÃO DA INFORMAÇÃO

Define-se como necessária a proteção das informações da Instituição ou sob sua custódia como fator primordial nas atividades profissionais de cada servidor, segurado, estagiário ou prestador de serviços TATUIPREV.

Os servidores deverão:

- Assumir uma postura proativa no que diz respeito à proteção das informações do TATUIPREV e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido a sistemas de informação sob responsabilidade da Autarquia;
- Assuntos confidenciais não devem ser expostos publicamente;
- Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
- Somente softwares homologados podem ser utilizados no ambiente computacional do TATUIPREV;
- Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos.

6 – USO DO AMBIENTE WEB (INTERNET)

A internet disponibilizada pela instituição aos seus servidores, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades. Como é do interesse do TATUIPREV que seus

servidores 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.

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.

Os servidores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no TATUIPREV e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Diretoria Executiva. 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 T.I.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios do TATUIPREV;
- Que promovam discussão pública sobre os negócios da Autarquia, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”;
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

Não é permitido instalar programas provenientes da Internet nos microcomputadores do TATUIPREV, sem a expressa autorização da Diretoria

Executiva, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os servidores devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

7 – USO DO CORREIO ELETRÔNICO

O objetivo desta norma é informar aos servidores do TATUIPREV quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo. O uso do correio eletrônico 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 o TATUIPREV e não cause impacto no tráfego da rede.

O correio eletrônico fornecido pelo TATUIPREV é um instrumento de comunicação interna e externa da Autarquia. As mensagens devem ser escritas em linguagem profissional e não devem comprometer a imagem da Instituição, não podendo ser contrárias aos princípios éticos.

É termicamente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização e
- Possam prejudicar a imagem de outras empresas

Para incluir um novo usuário no correio eletrônico, a respectiva a Diretoria Executiva do Instituto deverá fazer um pedido formal à equipe de informática, que providenciará a inclusão do mesmo.

Todo arquivo em mídia proveniente de entidade externa ao TATUIPREV deve ser verificado por programa antivírus. Todo arquivo recebido/obtido através do ambiente Internet deve ser verificado por programa antivírus.

Todas as estações de trabalho devem ter um software de antivírus corporativo instalado, para maior proteção na realização de transações bancárias e a proteção dos dados e informações compartilhadas. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

8 – CÓPIA DE SEGURANÇA DE ARQUIVOS INDIVIDUAIS.

A importância dos backups nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

A cópia de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos, pastas e outros arquivos ou documentos, desenvolvidos pelos servidores, em suas estações de trabalho, serão feitas de forma automática desde que sejam salvas na área de trabalho do computador, todos os documentos relacionados ao processo devem ser armazenados nesta área, uma cópia de cada arquivo e pasta será enviada (“upload”) de forma automática para nuvem em tempo real.

São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos servidores, que não sejam parte integrante dos serviços do TATUIPREV, seja ele interno ou para colaboradores. Alguns exemplos são: rascunhos ou lembretes, memórias de cálculo, mensagens, diagramas ou instruções técnicas etc. A cópia de segurança destes arquivos é de responsabilidade dos próprios servidores.

O TATUIPREV para manter a integridade e disponibilidade da informação e dos recursos de processamento de informação deverá realizar pesquisas frequentes 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.

9 – COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade do TATUIPREV, 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 pelo departamento de T.I.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico departamento de T.I do TATUIPREV. Os servidores que necessitarem fazer testes deverão solicitá-los previamente ao Departamento de T.I, ficando responsáveis tecnicamente pelas ações realizadas.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do TATUIPREV.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares.
- Interromper um serviço 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.

9.1 – DISPOSITIVOS MÓVEIS

O TATUIPREV deseja facilitar a mobilidade e o fluxo de informação entre seus servidores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Diretoria Executiva, como: notebooks, smartphones e pendrives.

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

O TATUIPREV, 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.

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

O servidor 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 Tecnologia da Informação.

É permitido o uso de rede banda larga de locais conhecidos pelo servidor como: sua casa, hotéis, empresas etc.

O servidor 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 ao TATUIPREV e/ou a terceiros.

9.2 – IMPRESSORAS

Uso das Impressoras seguem as regras que devem ser observadas por todos os servidores quando da utilização deste equipamento:

- Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;
- Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;
- Impressões coloridas apenas devem ser feitas apenas em caráter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir.

10 – PAPÉIS E RESPONSABILIDADES

Cabe ao Diretor-Presidente:

- Aprovar a política e as normas de segurança da informação e suas revisões;
- Tomar decisões referentes aos casos de descumprimento da política e das normas de segurança da informação, mediante a apresentação de propostas da equipe de Informática.

Cabe aos Diretores:

- Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;
- Assegurar que suas equipes possuam acesso e entendimento desta Política, bem como, das normas e dos procedimentos de Segurança da Informação;
- Sugerir ao Diretor-Presidente, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;
- Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo Diretor-Presidente;
- Comunicar imediatamente ao Diretor-Presidente eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

Servidores, estagiários, e prestadores de serviços.

- Cabe aos servidores, estagiários e prestadores de serviços do Instituto de Previdência Própria do Município de Tatuí - TATUIPREV cumprir com as seguintes obrigações:
- Zelar continuamente pela proteção das informações da Instituição ou de seus segurados contra acesso, modificação, destruição ou divulgação não autorizada;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Comunicar imediatamente à Diretoria Executiva da Autarquia e à equipe de Informática qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

Compete à equipe de Informática:

- Sugerir procedimentos ao Diretor-Presidente e aos Diretores para proteger os ativos de informação nos termos do estabelecido nesta Política de Segurança da Informação;
- Auxiliar, no que for necessário, o Diretor-Presidente e Diretores da Autarquia na realização de quaisquer ações necessárias visando um controle efetivo do acesso à informação e para que os responsáveis pela Autarquia possam estabelecer, documentar e fiscalizar o cumprimento do estabelecido nesta Política de segurança da informação, bem como, realizar a definição da classificação das informações sob a responsabilidade da Instituição.
- Ajudar na reavaliação periódica das autorizações dos usuários que acessam as informações sob da responsabilidade da Autarquia, propondo o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;

- Auxiliar, no que for possível, em caso de eventual necessidade de investigação dos incidentes de segurança relacionados às informações sob a responsabilidade da Autarquia.

_____

Rosan Paes Camargo Filho

Diretor Presidente