Instituto de Previdência
do Servidor Municipal
de Diadema

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DEPARTAMENTO DE INFORMÁTICA

FEVEREIRO
2020

ÍNDICE

Capítulo I
CONCEITUAÇÃO

Art. 1º. Esta Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do Instituto de Previdência do Servidor Municipal de Diadema, também referido como IPRED, para a proteção dos ativos de informação e quanto à responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Autarquia, incluindo-se todos os colaboradores, internos ou externos, segurados e prestadores de serviço que tenham acesso às informações de propriedade do IPRED ou relativas a seus segurados.

Art. 2º. A segurança institucional compreende o conjunto de medidas adotadas para prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda do IPRED e de seus segurados, inclusive no que tange à sua imagem e reputação.

Art. 3º. Entende-se por usuário toda e qualquer pessoa natural ou jurídica, que tenha acesso às informações e/ou ativos, em qualquer meio ou suporte, inclusive os contratados, em regime estatutário, CLT ou temporário, e todos os prestadores de serviços, contratados por intermédio de pessoa jurídica ou não, bem como segurados ou terceiros que utilizem sistemas ou recursos do IPRED.

Capítulo II
OBJETIVOS DA PSI

Art. 4º. Constitui objetivo da PSI:

I - Estabelecer diretrizes que permitam aos usuários e fornecedores do IPRED seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e dos indivíduos;

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

III - Preservar as informações do IPRED quanto a:

a) Integridade: garantia de que a informação não sofra nenhuma modificação sem a devida autorização, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

b) Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas, compreendendo seu tráfego de forma sigilosa, conforme sua classificação; e

c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, respeitando as regras estabelecidas por esta PSI.

IV - Difundir mentalidade de Segurança Institucional, fazendo que todos que a ela tenham acesso compreendam as necessidades das medidas adotadas e incorporem o conceito de que cada indivíduo é responsável pela manutenção do nível de segurança adequado.

Capítulo III
DAS RESPONSABILIDADES ESPECÍFICAS

Art. 5º. As diretrizes aqui estabelecidas deverão ser seguidas por todos os usuários, que possuem como obrigação se manter atualizados em relação a esta PSI e aos procedimentos e normas a ela relacionados, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

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

Art. 6º. Os usuários deverão:

I – Atuar de forma ética e responsável, mantendo o adequado sigilo das informações do IPRED que não sejam classificadas como de acesso público;

II – Zelar pelos ativos de informação do IPRED, sejam eles físicos ou digitais, atuando de forma preventiva e proativa, visando antecipação aos diversos tipos de ameaças;

III – Seguir as diretrizes e recomendações da Diretoria Executiva quanto ao uso, divulgação e descarte de dados e informações, integrando as ações de planejamento e execução das atividades de segurança institucional.

Capítulo IV
DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 7º. Para garantir as regras mencionadas nesta PSI, o IPRED poderá:

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

II - Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação por escrito de superior hierárquico;

III - Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade; e

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

Capítulo V
CORREIO ELETRÔNICO

Art. 8º. O uso do correio eletrônico institucional do IPRED é para fins relacionados às atividades do usuário na Autarquia, sendo terminantemente proibido:

I - Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Autarquia;

II - Enviar mensagem por correio eletrônico usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

III - Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPRED vulneráveis a ações judiciais;

IV - Divulgar informações ou imagens de tela, sistemas, documentos e afins, sem a devida cautela quanto aos corretos procedimentos adotados para cada tipo de informação;

V - Apagar mensagens pertinentes de correio eletrônico quando o IPRED estiver sujeito a algum tipo de investigação.

Capítulo VI
INTERNET

Art. 9º. Exige-se dos usuários comportamento ético e profissional com o uso da internet disponibilizada pelo IPRED.

Art. 10. Os equipamentos, tecnologias e serviços para acesso à internet são recursos fornecidos pelo IPRED, que pode analisar e, se necessário, bloquear quaisquer arquivos, sites, correios eletrônicos, domínios ou aplicações, estejam eles em qualquer localização da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

§ 1º. Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a auditoria, tendo o IPRED, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela.

§ 2º. Qualquer alteração dos parâmetros de segurança configurados, sem o devido credenciamento e a autorização para tal, deverá ser considerada inadequada e os riscos a ela relacionados serão informados ao usuário e ao respectivo superior hierárquico.

§ 3º. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, casos em que a Autarquia cooperará ativamente com as autoridades competentes.

Art. 11. Os colaboradores deverão cooperar ativamente para atender ao princípio da publicidade, principalmente quanto à transparência das informações de interesse público definidas legalmente, que deverão ser disponibilizadas na internet.

Art. 12. Os usuários com acesso à internet poderão fazer o *download* somente de programas e arquivos ligados diretamente às suas atividades no IPRED, devendo ser providenciado o que for necessário para regularizar a licença e o registro desses programas e a devida autorização.

§ 1º. O uso, a instalação, a cópia ou a distribuição, não autorizados, de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos.

§ 2º. Os usuários não poderão em hipótese alguma utilizar os recursos do IPRED para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Art. 13. É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou gravação por meio de qualquer recurso, de materiais de cunho sexual.

Art. 14. Os usuários não poderão utilizar os recursos do IPRED para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Art. 15. As regras expostas neste capítulo se aplicam no uso de computadores e outros dispositivos de propriedade do IPRED, bem como a dispositivos particulares dos usuários que estiverem conectados à internet ou rede do IPRED, seja ela cabeada ou sem fio.

Capítulo VII
COMPUTADORES E OUTROS DISPOSITIVO

Art. 16. Os computadores e demais dispositivos disponibilizados pelo IPRED aos colaboradores constituem instrumento de trabalho para execução das atividades de negócio desta Autarquia.

§ 1º. Cada usuário deve zelar para segurança e bom uso dos equipamentos, reportando à área competente qualquer incidente que tenha conhecimento.

§ 2º. É proibido empregar qualquer dispositivo destinado ao serviço público em tarefa particular.

§ 3º. Em caso de mau uso ou em desacordo com as instruções desta norma, o usuário poderá ser responsabilizado.

Capítulo VIII
IDENTIFICAÇÃO E CONTROLE DE ACESSO

Art. 17. Para o acesso aos recursos tecnológicos do IPRED será exigido, sempre que possível, identificação e senha exclusiva de cada usuário, permitindo assim o controle de acesso.

§ 1º. Não deve haver o compartilhamento de login individual entre os usuários, as ações realizadas com determinado login serão de responsabilidade do usuário nele cadastrado.

§ 2º. Caso o usuário não possua identificação única de acesso ao sistema, excepcionalmente poderá ser permitido que utilize o login de outro usuário, ficando este último responsável pelas ações daquele, devendo ser solicitada a criação de login individual o mais brevemente possível.

§ 3º. Recomenda-se como boa prática de segurança que, ao realizar o primeiro acesso ao ambiente de rede local, o usuário seja direcionado a trocar imediatamente a sua senha.

§ 4º. 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.

§ 5º. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login e senha.

Capítulo IX
PROCEDIMENTOS DE CONTINGÊNCIA

Art. 18. Para garantir a segurança da informação, deverão ser realizadas cópias de segurança dos sistemas e respectivos bancos de dados utilizados pelo IPRED.

§1º. As rotinas de cópia de segurança deverão, sempre que possível, ser realizadas de forma automatizada, em horários pré-definidos, devendo ainda ser realizadas verificações periódicas da sua execução e integridade.

§2º. O armazenamento das cópias de segurança deverá ser planejado de forma que impeça o seu acesso a pessoas não autorizadas.

§3º. O processo de realização de cópias de segurança deverá ser devidamente mapeado e manualizado.

Capítulo X
NORMATIZAÇÕES COMPLEMENTARES

Art. 19. Complementarmente a esta Política de Segurança da Informação serão elaborados os seguintes documentos:

I – Política de Transparência, incluindo procedimento para classificação da informação;

II – Tábua de temporalidade das informações em meio digital;

III – Plano de recuperação de desastres;

IV – Código de Ética no meio digital (Netiqueta).