INSTITUTO DE PREVIDÊNCIA MUNICIPAL
DE ESPIGÃO DO OESTE

Política de Segurança da Informação do IPRAM

RESOLUÇÃO Nº010/IPRAM/2020

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA MUNICIPAL DE ESPIGÃO DO OESTE – IPRAM.

O PRESIDENTE INTERINO DO INSTITUTO DE PREVIÊNCIA MUNICIPAL DE ESPIGÃO DO OESTE, Senhor **VILSON RIBEIRO EMERICH**, no uso de suas atribuições legais, conforme disposto no artigo 69, da Lei nº 1.796/2014:

CONSIDERANDO os princípios da Legalidade, Impessoalidade, Moralidade, Publicidade e Eficiência à luz do artigo 37 da Constituição da República Federativa do Brasil;

CONSIDERANDO o Programa de Certificação Institucional e Modernização da Gestão dos Regimes Próprios de Previdência Social da União, dos Estados, do Distrito Federal e dos Municípios;

CONSIDERANDO o compromisso público e formal do IPRAM com os princípios éticos e morais, e com a segurança da informação entendida como "a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (vide ISO 27002);

CONSIDERANDO o expresso compromisso do IPRAM com a confidencialidade, integridade e disponibilidade de suas informações;

RESOLVE:

Art. 1º Instituir no âmbito do IPRAM a Política de Segurança da Informação conforme os termos do Anexo I, desta resolução, abrangendo todos os seus servidores, segurados, prestadores de serviço, Agentes Públicos, Conselheiros e membros do Comitê de Investimentos,

vinculados ao Instituto de Previdência Municipal dos Servidores Públicos do Município de Espigão do Oeste – RO, a fim de que se ateste sua compreensão e aceitação.

Art. 2º Após a implantação desta Política deverão ser realizados controles de melhoria contínua ou sempre que acontecer uma falha de segurança em especial de nível médio ou grave.

Art. 3º Deverá ser nomeado por portaria um servidor responsável pela Gestão da Política de Segurança da Informação no âmbito do IPRAM.

Art. 4º A presente política passa a vigorar a partir da data da publicação desta Resolução, devidamente aprovada pelo Conselho Fiscal do IPRAM, sendo válida por tempo indeterminado.

Espigão do Oeste, 10 de julho de 2020.

VILSON RIBEIRO EMERICH
Presidente do IPRAM
Port. nº 0580/GP/2020

ANEXO I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1 – INTRODUÇÃO

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005, “A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente”.

De acordo com a mesma norma; “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. A informação utilizada pelo IPRAM é um bem que tem valor. A informação deve ser protegida, cuidada e gerenciada adequadamente com o objetivo de garantir sua disponibilidade, integridade e confidencialidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

O desenvolvimento e a implantação da Política de Segurança da Informação - PSI é uma importante ferramenta para combater ameaças aos ativos do Instituto. Esta PSI é um conjunto de diretrizes e orientações de procedimentos que visam conscientizar e orientar os servidores, parceiros, colaboradores e fornecedores para o uso seguro dos ativos do Instituto.

2 - OBJETIVOS

A Política de Segurança da Informação – PSI tem como objetivos:

I. Registrar os princípios e as diretrizes de segurança, adotados pelo Instituto, a serem

observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos.

II. Definir o tratamento que deve ser dado às informações armazenadas, processadas ou transmitidas no ambiente convencional ou no ambiente tecnológico.

III. Preservar as informações do IPRAM quanto a:

a. Confidencialidade: propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

b. Integridade: propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital;

c. Disponibilidade: propriedade que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido.

3 - DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação do IPRAM que constituem os principais pilares da gestão de segurança da informação da autarquia, norteando a elaboração das normas e procedimentos.

3.1 Proteção da Informação

Define-se como necessária a proteção das informações da autarquia como fator primordial nas atividades profissionais de cada servidor, estagiário, aprendiz ou prestador de serviços do IPRAM, sendo que:

a. Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações do IPRAM e devem estar atentos a ameaças externas, bem como fraudes, furto de informações e acesso indevido a sistemas de informação sob responsabilidade do IPRAM;

b. As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;

c. Assuntos confidenciais não devem ser expostos publicamente;

d. Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos;

e. Todos os dados considerados como imprescindíveis aos objetivos do IPRAM devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos à testes periódicos de recuperação;

f. O acesso à dependências do IPRAM ou à ambientes sob controle do IPRAM deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação ali armazenada ou manipulada, garantindo a rastreabilidade e a efetividade do acesso autorizado;

g. São de propriedade do IPRAM todas as criações, códigos ou procedimentos desenvolvidos por qualquer servidor, estagiário, aprendiz ou prestador de serviço durante o curso de seu vínculo com o Instituto.

3.2 Classificação da Informação

Define-se como necessária a classificação de toda a informação de propriedade do IPRAM, de maneira proporcional ao seu valor para a autarquia, para possibilitar o controle adequado da mesma, devendo ser utilizados os seguintes níveis de classificação:

a. Confidencial: É uma informação crítica para o IPRAM. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais ao IPRAM. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por servidores, beneficiados ou segurados vinculados e/ou fornecedores.

b. Pública: É uma informação do IPRAM com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

c. Interna: É uma informação do IPRAM cujo acesso por parte de indivíduos externos à autarquia deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à Imagem do Instituto, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os servidores e prestadores de serviços do IPRAM.

d. Informação Restrita: É toda informação que pode ser acessada somente por usuários do Instituto explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos à organização e/ou comprometer a estratégia da organização.

3.3 Privacidade da Informação

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e que são manipuladas ou armazenadas nos meios às quais o IPRAM detém total controle administrativo, físico, lógico e legal.

As diretivas abaixo refletem os valores institucionais do IPRAM e reafirmam o seu

compromisso com a melhoria contínua desse processo:

a. As informações são coletadas de forma ética e legal, com o conhecimento do segurado, para propósitos específicos e devidamente informados;

b. As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;

c. As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;

d. As informações somente são fornecidas a terceiros, mediante autorização prévia da Diretoria-Executiva ou para o atendimento de exigência legal ou regulamentar;

e. As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

4 – REGRAS GERAIS DE UTILIZAÇÃO DOS RECURSOS DE TI

Computadores e demais recursos da Autarquia devem ser utilizados exclusivamente para os serviços do IPRAM. Quanto ao uso dos recursos tecnológicos observar-se-á:

4.1 Acesso a Internet

a. O acesso à internet pela rede do IPRAM se caracteriza como uma ferramenta de trabalho para os agentes públicos do IPRAM, sendo seu uso destinado às funções relativas as atribuições de cada agente público;

b. Será permitido o uso do acesso à internet disponibilizado pelo IPRAM para o uso com fins particulares pelos servidores e terceiros nas seguintes condições, cumulativamente:

- Seja utilizado para acesso a sites cujo conteúdo proporcione desenvolvimento pessoal aos agentes públicos;
- O tempo de acesso e conteúdo acessado não interfiram no cumprimento das funções do agente público;
- O acesso não interfira no bom funcionamento da rede e dos sistemas do Instituto;
- Não seja contabilizado para justificar a necessidade de aumento da capacidade de acesso;
- Todas as conexões feitas e conteúdos transmitidos estão sujeitos à monitoração e auditoria, mesmo que para uso particular e de conteúdo privado;

- O acesso não coloque em risco a segurança da rede e dos sistemas do IPRAM;
- O acesso poderá ser bloqueado a qualquer momento devido a critérios técnicos ou requerimento de qualquer um dos membros da Diretoria Executiva do IPRAM, sem que o IPRAM seja responsabilizado por qualquer perda ou dano decorrente do bloqueio do acesso;
- O IPRAM não será responsabilizado por qualquer perda ou dano decorrente de alguma falha na segurança durante o acesso (exemplo: usuário ter sua senha de banco capturada por um malware que eventualmente esteja sendo executado no terminal de acesso utilizado).

d. No caso de terceiros, para acesso à rede de internet sem fio, os mesmos deverão utilizar a rede "VISITANTES".

4.2 E-mail Institucional

a. Será disponibilizado para cada setor um e-mail institucional;

b. O e-mail institucional é uma ferramenta disponibilizada pelo Instituto aos seus agentes públicos, e é considerado como um ativo do Instituto, não podendo, portanto, ser utilizado para fins particulares;

c. Todo e-mail enviado deve conter a identificação do agente público, e seu cargo ou função, que o está enviando (assinatura do e-mail);

d. Toda informação relevante ao serviço que for enviada ou recebida por e-mail não devem ser apagados da caixa-postal;

e. As caixas postais e as conexões para recebimento e envio de e-mails poderão ter seu conteúdo monitorado pelo servidor responsável pela Política de Segurança da Informação do Instituto, a qualquer momento, sem aviso prévio, independente de autorização superior, para fins de detecção de uso indevido, invasão ou malwares.

4.3 Uso dos equipamentos de informática

a. Os equipamentos de informática do Instituto são ferramentas destinadas ao exercício das atividades exclusivamente dos agentes públicos do IPRAM, não podendo portanto, serem utilizadas por terceiros, salvo prestadores de serviços de T.I quando solicitado o serviço;

b. Em caso de uso pelos agentes públicos para fins particulares, é liberado desde que, o uso não gere prejuízos significativos ao Instituto, tanto quanto ao desgaste dos equipamentos quanto ao consumo de materiais de consumo;

c. A responsabilidade pelas ações durante o uso é da pessoa do agente público.

4.4 Controle de Acesso Lógico

a. Cada usuário terá uma identificação única em cada sistema a ser utilizado para execução de suas atividades.

b. A senha para acesso aos sistemas é pessoal, sigilosa e de responsabilidade do usuário, que, em hipótese alguma poderá divulga-la e/ou compartilhá-la.

c. O usuário será responsável pelo uso correto de suas senhas e *tokens de acesso* individuais perante a autarquia e a legislação (cível e criminal).

4.5 Cópia de Segurança dos Arquivos

a. É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos servidores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do IPRAM, caso contrário, o IPRAM disponibilizará um servidor, onde cada usuário deverá manter estas informações que serão incluídas na rotina de backup.

5 - PAPÉIS E RESPONSABILIDADES

I - Cabe aos servidores e demais colaboradores e prestadores de serviços do IPRAM cumprir com as seguintes obrigações:

a. Zelar continuamente pela proteção das informações da autarquia contra acesso, modificação, destruição ou divulgação não autorizada;

b. Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades estatutárias do IPRAM;

c. Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;

d. Garantir a continuidade do processamento das informações críticas para o funcionamento do IPRAM;

e. Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;

f. Atender às leis que regulamentam as atividades do Instituto;

g. Selecionar de maneira coerente os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;

h. Comunicar imediatamente ao servidor designado como responsável pela Segurança da Informação qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação.

II – Compete ao Presidente:

a. Conscientizar, orientar e divulgar aos servidores, parceiros, colaboradores e fornecedores o uso seguro dos ativos do Instituto, nos termos constantes da Política de Segurança da Informação – PSI;

b. Orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, nem deixar relatórios nas impressoras e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

III - Compete ao servidor designado como responsável pela Gestão da Segurança da Informação:

a. Propor projetos de ajustes, aprimoramentos e modificações na estrutura normativa da Política de Segurança da Informação – PSI à Diretoria-Executiva;

b. Prover as informações de Gestão de Segurança da Informação solicitadas pela Diretoria Executiva;

c. Requisitar informações das demais áreas do IPRAM, com o intuito de verificar o cumprimento da política, das normas e procedimentos de segurança da informação;

d. Receber, documentar e analisar casos de violação da política e das normas e procedimentos de segurança da informação;

e. Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades com a política, as normas ou os procedimentos de segurança da informação;

f. Notificar à Diretoria-Executiva quanto a casos de violação da política e das normas e procedimentos de segurança da informação;

g. Receber sugestões dos usuários para implantação de normas e procedimentos de segurança da informação;

h. Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os servidores e prestadores de serviços;

i. Promover ações de conscientização sobre Segurança da Informação para os servidores e

prestadores de serviços;

IV - Compete à Controladoria e Procuradoria Jurídica do IPRAM:

a. Informar ao responsável pela Política de Segurança da Informação sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação;

b. Incluir na análise e elaboração de contratos, sempre que necessárias, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do IPRAM;

c. Avaliar, quando solicitado, a política, as normas e procedimentos de segurança da informação.

5 – SANÇÕES

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à Política de Segurança da Informação do IPRAM são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.

VILSON RIBEIRO EMERICH
Presidente do IPRAM
Port. nº 0580/GP/2020