

RESOLUÇÃO N° 004/2020

“Dispõe sobre a Política de Gestão e Segurança da Informação do Instituto de Gestão Previdenciária do Município de Petrolina – IGEPREV, e dá outras providências.”

O Diretor-Presidente do Instituto de Gestão Previdenciária do Município de Petrolina - IGEPREV, no uso das atribuições conferidas pela Lei, e

CONSIDERANDO que foi instituído a Unidade Setorial de Controle Interno - USCI do Poder Executivo Municipal, através da Lei Municipal de N° 2206/09 de Junho de 2009;

CONSIDERANDO o que dispõe as Leis Federais n° 9.717/1998 e n° 10.887/2004, que redefiniram o marco institucional dos RPPS, estabelecendo regras gerais de organização e funcionamento que proporcionaram significativos avanços na sua gestão e a segregação e preservação dos recursos a eles vinculados;

CONSIDERANDO que a gestão do instituto deve pautar suas ações a fim de garantir, com sustentabilidade, a concessão e manutenção dos benefícios previdenciários aos seus segurados e dependentes;

CONSIDERANDO os preceitos normativos contidos nos artigos 40, 149, § 1º e 249 da Constituição Federal de 1988;

CONSIDERANDO que é atribuição do Ministério da Previdência Social (atualmente Secretaria de Previdência - SPREV do Ministério da Economia - ME orientar, supervisionar e acompanhar o funcionamento dos RPPS e estabelecer os parâmetros e diretrizes gerais para sua organização e funcionamento, nos termos do art. 9º, I e II da Lei n° 9.717/1998, com o objetivo de auxiliar os entes federativos na melhoria da gestão do RPPS, por meio do aprimoramento do controle dos ativos e passivos previdenciários e de uma maior transparência no relacionamento destes com os segurados e a sociedade;

CONSIDERANDO que no exercício desta missão a Secretaria de Previdência - SPREV do Ministério da Economia - ME, por força da Lei n° 13.341/2016, editou a Portaria MPS n° 185/2015, que instituiu 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 - Pró-Gestão RPPS;

CONSIDERANDO que o inciso I, do art. 6º, da Portaria MPS n° 185/2015, aprovou o Manual do Pró-Gestão RPPS;

RESOLVE:

Art. 1º Fica estabelecida a Política de Segurança da Informação, no Instituto de Gestão Previdenciária do Município de Petrolina “IGEPREV”, aplicável a todos os servidores públicos, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento do IGEPREV, ou acesso as informações pertencentes ao Instituto de Gestão Previdenciária.

Art. 2º É dever de todos os Servidores do IGEPREV considerar a informação como sendo um bem da entidade, um dos recursos críticos para a realização das atividades, que possui grande valor para o IGEPREV e deve sempre ser tratada profissionalmente.

Art. 3º Constitui Missão do Núcleo de TI do IGEPREV:

I - Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

II - Objetivo da Política de Segurança da Informação do IGEPREV:

III - Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização das atividades do IGEPREV.

Art. 4º Todo e qualquer servidor que utilize o sistema informatizado do IGEPREV tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática atrelados ao cumprimento da finalidade pública cumprida pelo Instituto.

Parágrafo Único. Todo Diretor/Gerente deve orientar seus subordinados a não propagarem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não 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.

Art. 5º Configura violação a política de segurança informacional do Instituto de Gestão Previdenciária do Município de Petrolina os atos que:

I - Exponha o IGEPREV a uma perda monetária potencial ou efetiva por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento;

II - Envolver a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos governamentais;

III - Envolve o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer Lei, regulamento ou qualquer outro dispositivo governamental.

Art. 6º As informações inerentes ao Instituto de Gestão Previdenciária do Município de Petrolina – IGEPREV será classificada da seguinte forma:

I - Informação Pública, sendo toda aquela que é permitido o acesso por servidores da entidade, usuários, fornecedores, prestadores de serviços e público em geral.

II - Informação Interna, assim considerada toda informação gerada pelo fluxo administrativo executado pelos agentes internos no desempenho das finalidades da entidade e aquelas geradas pelas relações jurídicas formadas oficialmente pelo instituto;

III - Informação Confidencial, considerada aquela cujo teor representa informações sensíveis sobre o instituto e que sua divulgação injustificada pode gerar risco à administração e ao interesse público;

IV - Informação Restrita, assim considerada toda informação cujo acesso é permitido somente aos servidores da entidade explicitamente indicado pelo nome ou por área a que pertence.

Art. 7º É de responsabilidade do Diretor/ Gerente de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) geradas por sua área de acordo com a classificação abaixo:

I – Dados Pessoais dos Segurados do IGEPREV.

a) Os dados pessoais dos servidores serão coletados na medida estritamente necessária para resolução da demanda administrativa provocada.

b) Todos os Dados Pessoais de Servidores serão considerados dados confidenciais

c) Dados Pessoais de Servidores sob a responsabilidade do IGEPREV não serão usados para fins diferentes daqueles para os quais foram coletados.

d) Dados Pessoais de Servidores não serão transferidos para terceiros, exceto quando devidamente justificado ou em cumprimento as obrigações inerentes a entidade, devendo o agente receptor guardar os mesmos cuidados de sigilo, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos servidores do IGEPREV.

Art. 8º Fica proibido o uso de programas ilegais ou não licenciados no âmbito do IGEPREV.

Parágrafo único. O setor de TI deverá realizar verificações periódicas nos dados e/ou computadores dos servidores, visando garantir a utilização lícita e escoreita dos recursos de informática do Instituto.

Art. 9º Quando da necessidade de cadastramento de um novo servidor para utilização da "rede", sistemas ou equipamentos de informática do IGEPREV, o setor de origem

do novo servidor deverá comunicar esta necessidade ao setor de TI, por meio de comando interno ou e-mail, informando a que tipo de rotinas e programas o novo servidor terá direito de acesso e quais serão restritos.

§1º. O TI fará o cadastramento e informará ao novo servidor qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 180 (cento e oitenta) dias.

§2º. As senhas ser definidas com um mínimo de 8 (oito) caracteres alfanuméricos.

Art. 10º É de obrigação dos servidores rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

Art. 11º Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do TI e deverão ser feitas diariamente.

§1º. Ao final de cada mês, também deverá ser feita uma cópia de segurança com os dados de fechamento do mês do Sistema Integrado. Esta cópia será feita imediatamente após a comunicação formal da Contabilidade, por meio de memorando, que o referido mês foi encerrado.

§2º. Bimestralmente, a TI enviará 1 (uma) cópia extra da fita do "backup" de fechamento do referido mês, para ser arquivada na Contabilidade.

Art. 12º O gerenciamento dos bancos de dados é responsabilidade exclusiva do TI, assim como a manutenção, alteração e atualização de equipamentos e programas, que o fará diretamente ou através de terceirizadas contratadas.

§1º. O terceiro eventualmente contratado será totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.

§2º. O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções.

§3º. Acessos desnecessários ou com poder excessivo deverão ser imediatamente inabilitados.

§4º. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Art. 13º O setor de Recursos Humanos do IGEPREV deverá informar ao setor de TI, toda e qualquer movimentação de servidores quanto a admissão/exoneração/demissão, para que os mesmos possam ser cadastrados ou excluídos no sistema do IGEPREV, incluindo o fornecimento de sua senha ("password") e registro do seu nome como servidor usuário no sistema (login).

Art. 14º Cabe ao setor solicitante da contratação/nomeação a comunicação ao Núcleo de TI sobre as rotinas a que o novo servidor terá direito de acesso. No caso de

servidores comissionados, deverá também ser informado a atividade que o mesmo realizará no IGEPREV, para que na data de seu desligamento/exoneração/demissão possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

Art. 15º Nos casos de exoneração/demissão, o setor de Recursos Humanos do IGEPREV deverá comunicar imediatamente ao Núcleo de TI o desligamento do servidor ou prestador de serviços, devendo ser tomadas todas as medidas necessárias para eliminar suas chaves de acesso.

Art. 16º Cabe ao setor de Recursos Humanos do IGEPREV dar conhecimento e obter as devidas assinaturas de concordância dos novos servidores contratados, comissionados ou nomeados em relação à Política de Segurança da Informação do IGEPREV.

Art. 17º Nenhum servidor, efetivo ou comissionado, poderá ser contratado/nomeado, sem ter expressamente concordado com esta política, devendo o expressar em Termo de Ciência escrito.

Art. 18º Quando um servidor for comissionado ou transferido de função/atribuição, o setor Recursos Humanos do IGEPREV procederá a comunicação do fato ao Núcleo de TI, para que sejam feitas as adequações necessárias.

Art. 19º É responsabilidade dos próprios servidores 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 trabalhos do IGEPREV.

Parágrafo único. As informações consideradas de essencial importância para o regular funcionamento do Instituto deverá ser armazenadas em pasta específica compartilhada entre setores, cabendo ao Núcleo de TI sua manutenção e atualização diária.

Art. 20º É de propriedade do IGEPREV todos os "designs", criações ou procedimentos desenvolvidos por qualquer servidor durante o desempenho de suas funções para o IGEPREV.

Art. 21º O acesso a rede mundial de computadores (INTERNET) será disponibilizado exclusivamente para a realização dos trabalhos pelos servidores do Instituto, ficando proibido o acesso e uso para fins estranhos às funções exercidas ou para realização de atividades afins.

Art. 22º O uso da Internet será monitorado pelo Núcleo de TI, inclusive através de "logs" (arquivos gerados no servidor) que informam qual servidor está conectado, o tempo que usou a Internet e qual página acessou.

Art. 23º A definição dos servidores que terão permissão para uso (navegação) da Internet é atribuição da Direção Executiva do IGEPREV, com base em recomendação do Supervisor de TI.

Art. 24º Não é permitido instalar programas provenientes da Internet nos microcomputadores do IGEPREV, sem expressa anuência do Núcleo de TI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

Art. 25º Os servidores devem evitar ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Art. 26º Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

I - De estações de rádio;

II - De conteúdos pornográficos ou relacionados a sexo;

III - Que defendam atividades ilegais;

IV - Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

V - Que promovam a participação em salas de discussão de assuntos não relacionados das atividades do IGEPREV;

VI - Que promovam discussão pública sobre as atividades do IGEPREV, a menos que autorizado pela Diretoria Executiva;

VII - Que possibilitem a distribuição de informações de nível “Confidencial”.

VIII - Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

Art. 27º O correio eletrônico fornecido pelo IGEPREV é um instrumento de comunicação interna e externa para a realização das atividades do IGEPREV.

Parágrafo Único. As mensagens remetidas devem ser escritas em linguagem profissional, não devem comprometer a imagem do IGEPREV, não podem ser contrárias à legislação vigente e nem aos princípios éticos do IGEPREV.

Art. 28º O uso do correio eletrônico é pessoal e o servidor titular é responsável por toda mensagem enviada pelo seu endereço.

Art. 29º É terminantemente proibido o envio de mensagens que:

I - Contenham declarações difamatórias e linguagem ofensiva;

II - Possam trazer prejuízos a outras pessoas;

III - Sejam hostis e inúteis;

IV - Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;

V - Possam prejudicar a imagem da entidade;

VI - Possam prejudicar a imagem de outras entidades ou empresas;

VII - Sejam incoerentes com as políticas do IGEPREV.

§1º. Para incluir um novo servidor no correio eletrônico, o setor de Recursos Humanos do IGEPREV, deverá fazer um pedido formal ao Núcleo de TI, que providenciará sua inclusão.

§2º. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.

§3º. Em caso de congestionamento no Sistema de correio eletrônico o Núcleo de TI fará auditorias no servidor de correio e/ou nas estações de trabalho dos servidores, visando identificar o motivo que o ocasionou.

§4º. O Núcleo de TI poderá, visando evitar a entrada de vírus no IGEPREV, bloquear o recebimento de e-mails provenientes de sites gratuitos.

Art. 30º O Núcleo de TI é responsável pela aplicação da Política do IGEPREV em relação a definição de compra e substituição de "software" e "hardware".

Parágrafo único. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo Núcleo de TI.

Art. 31º Os servidores que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade do IGEPREV, devem estar cientes de que:

I - Os recursos de tecnologia da informação, disponibilizados para os servidores, têm como objetivo a realização de atividades profissionais.

II - A proteção do recurso computacional de uso individual é de responsabilidade do próprio servidor.

III - É de responsabilidade de cada servidor assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação armazenada.

IV - O servidor não deve alterar a configuração do equipamento recebido.

Art. 32º Ao portar o equipamento fora das dependências do Instituto o servidor deverá:

I - Manter o equipamento sempre consigo, sendo vedado a sua transferência para terceiros por qualquer título;

II - Manter a atenção e o guardar em segurança quando utilizado em hall de hotéis, aeroportos, aviões, táxi etc.;

III - Quando transportar o equipamento em automóvel o armazenar em segurança e de modo sigiloso;

IV - Em caso de furto, deverá ser procedido imediato registro de ocorrência perante a autoridade policial competente, devendo ser o fato comunicado imediatamente ao Núcleo de TI;

Art. 32º Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso dos servidores aos sistemas e informações do IGEPREV, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

Art. 33º O Núcleo de TI fará auditorias periódicas sobre o acesso dos servidores às informações, verificando:

I – A compatibilidade dos acessos realizados pelos Servidores com a política estabelecida nesta norma;

II – A compatibilidade hierárquica de acesso a informações entre o servidor e o setor que ocupa;

III – Quem acessou determinada rotina e informação;

IV - Quem autorizou o servidor a ter permissão de acesso à determinada rotina ou informação;

V - Que informação ou rotina determinadas servidor acessou;

VI - Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

Art. 34º O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos do IGEPREV, assim como, o uso de eventuais ramais virtuais instalados nos computadores constituirá responsabilidade do Núcleo de TI, que ficará vinculada as políticas e diretrizes estipuladas pela Diretoria Executiva do IGEPREV.

Parágrafo único. Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência qual custo foi gerado por cada ramal.

Art. 35º Todo arquivo em mídia proveniente de entidade externa o IGEPREV deverá ser verificado por programa antivírus.

Art. 36º Todo arquivo recebido / obtido através do ambiente Internet deverá ser verificado por programa antivírus.

Art. 37º Todas as estações de trabalho devem ter um antivírus instalado.

§1º. A atualização do antivírus será automática, agendada pelo Núcleo de TI, via rede.

§2º. O servidor não pode, independente do motivo, desabilitar o programa antivírus instalado nas estações de trabalho.

Art. 38º O não cumprimento desta Política de Segurança da Informação implicará em falta e poderá sujeitar o infrator as seguintes sanções:

- I - Advertência formal;
- II – Suspensão;
- III - exoneração/rescisão do contrato de trabalho.

Parágrafo único. A aplicação das sanções elencadas não obstará a tomada das demais medidas legais cabíveis.

Petrolina/PE, 17 de dezembro de 2020.

Willames Barbosa Costa
Diretor-Presidente
IGEPREV



VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: 4EB8-02B7-3A21-3272

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

- ✓ WÍLLAMES BARBOSA COSTA (CPF 265.728.691-72) em 28/12/2020 15:13:19 (GMT-03:00)
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

<https://petrolina.1doc.com.br/verificacao/4EB8-02B7-3A21-3272>