Política de Segurança da Informação, de Documentos e de Proteção de dados pessoais do Instituto de Previdência do Município de João Pessoa

Prefeitura Municipal de João Pessoa (PMJP) - Instituto de Previdência do Município de João Pessoa (IPMJP). **Política de segurança de documentos, informações e de proteção de dados pessoais.** 2ª Edição revisada e ampliada. João Pessoa, 2022

FICHA TÉCNICA

Elaboração

Antônio Henrique Gomes dos Santos
Enéas Lyra de Albuquerque
Higor Delgado Leite Benício
Joseane Farias de Souza
Nicholas Frederico Freire Dias de Araújo
Weverton J. Moreira

Revisão

Joseane Farias de Souza
Antônio Henrique Gomes dos Santos

CONTROLE DE VERSÃO

2ª Edição revisada e ampliada
Última atualização: 13/05/2022

INFORMAÇÕES E CONTATO

Instituto de Previdência do Município de João Pessoa (IPMJP) | CNPJ: 40.955.403/0001-09
Rua Engenheiro Clodoaldo Gouveia, 166. Centro, João Pessoa – PB. CEP: 58013-370
Telefone e Whatsapp: (83) 3222-1005 | www.ipmjp.pb.gov.br

Encarregado pelo Tratamento de Dados Pessoais
Antônio Henrique Gomes dos Santos
https://www.ipmjp.pb.gov.br/site/ouvidoria

ESTRUTURA ORGANIZACIONAL

Superintendente:
Caroline Ferreira Agra
Superintendente Adjunto:
Rodrigo Ismael da Costa Macedo

Chefe da Divisão de Administração e Finanças:
Suzana Sitônio de Eça
Chefe da Divisão de Tecnologia da Informação:
Higor Delgado Leite Benício
Chefe da Divisão de Previdência:
Yuri Veiga Cavalcanti

Chefe da Assessoria de Gabinete do Superintendente:
Victor Assis de Oliveira Targino
Chefe da Assessoria Jurídica:
Carlos Eduardo dos Santos Farias
Chefe da Assessoria de Controle Interno:
Ernesto Fialho Pessoa
Chefe da Assessoria de Comunicação Social:
Francisco Emerson de Lucena Neto
Chefe da Assessoria de Secretaria Pessoal:
Jéssyca Patrícia Paiva Marques Brasileiro
Chefe da Ouvidoria:
Guilherme Carlos de Luna Coutinho
Chefe da Seção de Compras, Contratos e Patrimônio:
Isabella Duarte Gouvêa
Chefe da Seção de Contabilidade, Orçamento e Finanças:
Soraia Dias Monteiro
Chefe da Seção de Administração Geral:
Nathália Palmeira Silva Coutinho
Chefe da Seção Folha de Benefícios:
Karla Janaina Vergara de Sá
Chefe da Seção de Gestão de Tecnologia da Informação:
Eneas Lyra de Albuquerque
Chefe da Seção Desenvolvimento:
Thiago Henrique Sena de Souza
Chefe da Seção de Compensação Previdenciária:
Ana Paula Barreto Aquino
Chefe da Seção de benefícios:
Milena Medeiros de Alencar Feitosa Coutinho Torres
Chefe da Seção de Gestão de Pessoal:
Camila Pires de Sá Mariz Maia
Gerente Administrativo do Fundo Previdenciário:
João Carlos de Oliveira Leão

CONSELHO PREVIDENCIÁRIO

Biênio (2021 – 2023)

Superintendente do IPM/JP – como Membro nato, Presidente do Conselho:
Titular: Caroline Ferreira Agra
Suplente: Rodrigo Ismael da Costa Macedo

Servidor Ativo, indicado pelo Prefeito:
Titular: Rodrigo Hallan de Freitas Teixeira
Suplente: Camila Pires de Sá Mariz Maia

Servidor Inativo ou Pensionista, indicado pelo Prefeito:
Titular: Kelma Maria Pereira Dionísio
Suplente: José Augusto de Araújo Souza

Representante da Sociedade Civil:
Titular: Aldrovando Grisi Júnior
Suplente: Édipo Duarte Freire Júnior

Servidor Ativo, indicado por Associação de Classe:
Titular: Benilton Lúcio Lucena da Silva
Suplente: Valdegil Daniel de Assis

Servidor Inativo ou pensionista, indicado por Associação de Classe:
Titular: José Jansen
Suplente: Francisco Viana Garcia

Servidor Inativo ou Pensionista, indicado por Associação de Classe:
Titular: Luiz Carlos Fernandes de Souza
Suplente: Ednaldo José da Silva

Servidor Ativo indicado pelo Presidente da Câmara:
Titular: Marcone Bandeira Alves
Suplente: Rafael Barbosa Damasceno

CONSELHO FISCAL

Biênio (2021-2023)

Servidor Ativo, Aposentado ou Pensionista indicado pelo Prefeito
Titular: Irlen Braga dos Santos
Suplente: Eugênio Figueiredo de Albuquerque Júnior

Servidor Ativo, Aposentado ou Pensionista indicado pelo Prefeito:
Titular: Vladia Figueiredo Borborema de Sousa
Suplente: Luiz Henrique de Albuquerque Cavalcanti

Servidor Ativo, Aposentado ou Pensionista indicado pelo Prefeito:
Titular: Erico Heyller Medeiros de Alencar
Suplente: Joseane Farias de Souza

Servidor Ativo, Aposentado ou Pensionista indicado por Associação de Classe:
Titular: Thyago Luis Barreto Mendes Braga
Suplente: Alex Duarte Maia

Servidor Ativo, Aposentado ou Pensionista indicado por Associação de Classe:
Titular: Fábio Gomes da Silva
Suplente: Francisco Varela B. Júnior

DISPOSIÇÕES INICIAIS

A Política de Segurança de documentos, informações e proteção de dados pessoais pode ser definida como um conjunto de regras gerais que direcionam a segurança e privacidade da informação e são suportadas por normas e procedimentos que devem ser seguidas por toda a organização, orientando a segurança da informação, conforme o ramo de negócio, legislação e normas vigentes, possuindo caráter de documento jurídico.

Para fins da elaboração deste documento, foram consideradas as normas ABNT NBR ISO/IEC 27001:2013 – Segurança da Informação e ABNT NBR ISO/IEC 27002:2013 – Código de Prática para controles de segurança da informação, a Lei nº 8.159/1991 – Política Nacional de Arquivos Públicos e Privados, a Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI) e a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

OBJETIVO

Estabelecer os procedimentos para utilização correta dos ativos de tecnologia da informação, de documentos arquivísticos e dados pessoais tratados no âmbito do Instituto de Previdência do Município de João Pessoa (IPMJP), com o objetivo de evitar incidentes que possam inutilizar, extinguir ou alterar as informações e recursos utilizados no instituto, bem como promover a conscientização para com a segurança da informação e prover meios que contribuam para a manutenção dos princípios da confidencialidade, integridade, disponibilidade e autenticidade.

ABRANGÊNCIA

Esta norma abrange todos os recursos e ambientes computacionais, bem como os documentos, informações e dados produzidos e/ou recebidos e custodiados pelo IPMJP, devendo ser observada por todos os servidores e prestadores de serviços responsáveis pelo tratamento das informações, nos termos da LGPD, da LAI e da Política nacional de arquivos públicos e privados.

PRINCIPAIS DEFINIÇÕES

Para fins desta Política de Segurança de documentos, informações e proteção de dados pessoais, considera-se:

Segurança: É a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Informação: Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

Documento: Unidade de registro de informações, qualquer que seja o suporte ou formato;

Documento arquivístico: Documento produzido e/ou recebido por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos.

Dado pessoal: dado relacionado à pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político; dado referente à saúde, ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Agentes de tratamento: São o Controlador e o Operador.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Encarregado: pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados pessoais (ANPD). Também denominado *Data Protection Officer* (DPO).

Disponibilidade: Qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

Autenticidade: Qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

Integridade: Qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

Credencial de acesso: O conjunto de usuário e senha, que permite acesso a determinado sistema ou ambiente;

Ativo: Todos os itens da organização onde informações/documentos são criadas, processadas, armazenadas, transmitidas ou eliminadas;

Proxy: *Software* de controle de acesso à rede, que pode produzir relatórios sobre os acessos;

Backup: Cópia de dados de um dispositivo de armazenamento para outro dispositivo para que possam ser restaurados em caso da perda dos dados originais;

Firewall: Dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança;

Spam: É o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

Log: Os *logs* são registros de atividades gerados por programas de computador. No caso de *logs* relativos aos incidentes de segurança, eles normalmente são gerados por *firewalls* ou por sistemas de detecção de intrusão.

Outras definições importantes podem ser consultadas nas fontes de base legal desta Política: ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013, Lei nº 8.159/1991 (Lei de Arquivos), Lei nº 12.527/2011 (LAI) e Lei nº 13.709/2018 (LGPD).

PARTE I

POLÍTICA DE SEGURANÇA DOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

DO USO DE HARDWARE, SOFTWARE E INTERNET

I – Uso da Internet e do portal do IPMJP

O acesso à internet deve ser feito seguindo as diretrizes compostas nesta Política de Segurança, levando em conta os princípios da segurança da informação, quais sejam confidencialidade, integridade, disponibilidade e autenticidade.

O acesso à internet é monitorado através de *Proxy* - *software* de monitoramento que registra as informações de acesso, como sites visitados, horários de visita, quantidade de visitas, arquivos baixados, usuário que acessou e etc.

O usuário não deve compartilhar sua credencial de acesso ao computador e à internet para que terceiros acessem a internet de sua máquina, caso contrário será responsabilizado pelo acesso indevido.

É vedado o acesso a sites que estejam fora do interesse do instituto, como sites de bate papo, redes sociais, sites com conteúdo ofensivo, racista ou pornográfico e comércio eletrônico.

É vedado o acesso a sites de estrutura duvidosa que ofereçam risco à segurança da informação ou que possuam ferramentas que visem burlar os mecanismos de segurança do Instituto ou ocultar as credenciais de acesso à internet, como navegadores anônimos e *proxy* anônimo.

A critério da administração, sites com conteúdo não pertinente ao trabalho, terão o acesso bloqueado.

O servidor que fizer mau uso da internet terá o acesso bloqueado.

O portal do IPMJP armazena dados como cookies para habilitar suas funcionalidades, incluindo análises e personalização.

Os tipos de cookies recolhidos pelo portal são: cookies essenciais, cookies de sessão, cookies persistentes, identificação do usuário e segurança.

Todas as informações relativas aos cookies podem ser conferidas no TERMO DE PRIVACIDADE (https://www.ipmjp.pb.gov.br/site/privacidade).

II – Uso da Rede sem fio

A utilização da rede sem fio de internet (Wi-Fi) deve ser feita somente por dispositivos autorizados e configurados pela equipe de suporte, do mesmo modo que os roteadores sem fio. A utilização das redes sem fio deve ser realizada seguindo as regras dispostas nesta Política de Segurança da Informação.

Em caso de descumprimento desta Política ou má utilização do recurso, a Divisão de Tecnologia da Informação (DIV-TIN), por meio do Setor de Suporte (SET-SPT), poderá tomar providências como a suspensão do recurso ou bloqueio da máquina ou usuário na rede sem fio.

III – Uso da Rede Cabeada

A utilização da rede cabeada de internet deve ser feita somente por dispositivos autorizados e configurados pelo SET-SPT. Estes dispositivos receberão um endereço IP e serão configurados com o *Proxy* para que funcionem de acordo com a Política de Segurança da Informação.

IV – Controle de Acesso e Uso dos arquivos da rede

Todos os arquivos deverão ser salvos na rede, nas pastas dos respectivos setores, os quais passarão por *backups* periódicos. Os arquivos de interesse do Instituto salvos no disco do computador pessoal de trabalho não terão garantia de recuperação em caso de pane. Diante disto, recomenda-se o uso da rede como principal meio de criação, uso, compartilhamento e armazenamento de documentos institucionais.

A rede só será acessada mediante identificação do usuário por meio da credencial de acesso. As pastas liberadas para o acesso são definidas de acordo com o critério de uso e nível organizacional da função/atividade do usuário.

V – Uso do e-mail corporativo

O e-mail deve ser utilizado apenas para os interesses do instituto, não devendo ser utilizado para fins particulares, envio de *spans*, propaganda, conteúdo impróprio, difamatório, calunioso ou que prejudique a imagem do instituto e de seus colaboradores;

O usuário deve utilizar senha com a complexidade descrita nesta Política de Segurança e não está autorizado a fornecer sua senha para terceiros sob qualquer hipótese;

O acesso ao e-mail deverá ser realizado somente através da página de *webmail* do Instituto (https://mail.ipmjp.pb.gov.br), não devendo ser acessado por outros meios;

A senha deverá ser alterada a cada 180 dias de acordo com a definição do controlador de domínio;

O usuário não deverá abrir e-mails de origem duvidosa ou que julgar não pertinentes ao trabalho do instituto, incluindo anexos. Diante de qualquer dúvida deverá entrar em contato com o setor de suporte e mover a mensagem suspeita para a caixa de *spam*.

VI – Uso dos computadores

O acesso aos computadores, sistemas e arquivos da rede do Instituto será fornecido através de credenciais de acesso de uso pessoal. A credencial de acesso será composta por login e senha (individual);

A senha deverá ser composta de, no mínimo, 8 caracteres, incluindo letras maiúsculas e minúsculas, números e caracteres especiais.

A senha de acesso aos computadores deve ser alterada a cada 180 dias, de acordo com a definição do controlador de domínio.

Todo computador deve possuir sistema antivírus instalado, ativo e atualizado que será fornecido, instalado e monitorado pelo SET-SPT;

Não devem ser instalados *software* não homologados pela DIV-TIN, *software* pirata, *software* de acesso remoto, *software* para fins que não são do interesse do instituto ou não relacionados com a função do usuário;

Somente ao SET-SPT está autorizado à instalação de *software* de qualquer tipo, devendo o servidor solicitar o serviço previamente;

Não devem ser baixados e/ou executados arquivos desconhecidos ou fora do interesse do instituto, que possuam as extensões: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, ou qualquer outra extensão que represente um risco à segurança;

Os computadores poderão ser monitorados e auditados pela equipe de suporte a qualquer tempo, para fim de verificação de conformidade dessa Política de Segurança.

Os computadores possuem os seguintes itens padronizados: papel de parede, impressoras, ícones e unidades de rede mapeadas, de acordo com cada setor. Essas configurações são definidas através do controlador de domínio.

O computador deve ser bloqueado quando o usuário se ausentar do seu setor, mesmo que por breve período de tempo. Se o usuário tiver que se ausentar por tempo indeterminado deve desligar o computador;

Não será fornecida credencial de acesso do tipo Administrador.

VII – Usuário e Senha

A senha de acesso de um novo usuário de qualquer sistema deve ser requisitada pelo superior imediato do setor, através de e-mail ou memorando, descrevendo o nome do usuário, os sistemas que serão utilizados e o tipo de acesso a ser fornecido ao usuário.

A senha de acesso aos sistemas e computadores é de uso pessoal e não deve ser compartilhada.

Após 3 tentativas seguidas de acesso com senha inválida, a senha é bloqueada e o usuário deverá entrar em contato com a equipe de suporte para desbloqueio da senha.

As senhas terão validade de 180 dias, após esse período deverão ser alteradas para uma nova senha.

DA AUDITORIA E REGISTRO DE *LOGS* DE ACESSO

VIII – Credenciais de acesso

Todos os acessos dos usuários aos recursos do instituto, incluindo acesso aos sistemas, criação, exclusão e alteração de arquivos, horário de *logon* na máquina, utilização de impressora e outros sistemas, são registrados em *logs* automáticos.

IX – Arquivos pessoais

Não é permitido a guarda de arquivos pessoais na rede do Instituto, o que inclui arquivos de músicas, imagens, vídeos e outros arquivos em geral que não possuam ligação funcional com o Instituto.

X – Descarte de dados e informações

Os dados e informações do instituto que estejam armazenados em mídias como cd, dvd, disquete, disco rígido, fita de dados ou outro meio digital e os dados registrados em papel, formulários, deverão ser descartados de maneira a preservar a confidencialidade das informações, obedecendo o estabelecido em Tabela de Temporalidade e Destinação de Documentos, para o caso de documentos arquivísticos físicos, digitais ou híbridos.

XI – Uso dos dispositivos pessoais (celular, tablet, notebook)

É permitido o uso de dispositivos pessoais desde que estejam de acordo com essa Política de Segurança da Informação, após serem avaliados pelo SET-SPT.

XII – Uso de Impressoras

A quantidade de impressões é registrada em *Log* e poderá ser auditada quanto ao usuário que imprimiu, a quantidade de páginas e o nome do arquivo impresso. O uso das impressoras deve ser feito para os interesses do Instituto e utilizadas com consciência ecológica.

DO PROCEDIMENTO DE BACKUP E DE CONTINGÊNCIA

XIII – Procedimento de backup dos arquivos e bancos de dados

O backup é realizado diariamente, sendo este incremental e realizado de maneira automatizada por meio de *script.*

O backup dos Bancos de Dados é realizado diariamente, sendo este completo e automatizado.

O backup do sistema Gerenciador Eletrônico de Documentos (GED) é realizado diariamente, sendo este incremental e automatizado, dividido em 2 tarefas: arquivos e banco de dados.

O backup do sistema 1DOC-PMJP é realizado através da Amazon Web Services, o maior datacenter do mundo, que possui backup automático, segue rigorosos protocolos de segurança com camada de criptografia de dados, seguindo a legislação vigente do país (lei 12.965/14).

XIV – Armazenamento dos backups

Os backups são armazenados em discos rígidos, espelhados em RAID 1 e armazenados mensalmente em mídias Blu-ray rotulados com a data.

XV – Teste de recuperação

Os testes de recuperação de *backups* são realizados a cada 30 dias.

XVI – Procedimento de contingência

Em caso de indisponibilidade dos sistemas ou da internet, o Instituto, por meio da DIV-TIN, utilizará o servidor de contingência, bem como *nobreak*, *switch* e internet redundante.

Esses procedimentos de contingência serão utilizados somente para os setores e sistemas considerados críticos para o Instituto, ou seja, cuja indisponibilidade lhe cause impacto à reputação ou à saúde financeira.

DO CONTROLE DE ACESSO À INFRAESTRUTURA

XVII – Acesso ao Datacenter

O acesso ao d*atacenter* é restrito aos funcionários da DIV-TIN. O acesso por terceiros deverá ser expressamente autorizado e sempre acompanhado de um servidor da Divisão.

O *datacenter* é monitorado por câmeras de segurança.

A porta de acesso ao *datacenter* deve permanecer fechada, mesmo quando houver servidores autorizados em suas dependências.

XVIII – Bloqueio do acesso aos servidores desligados

O Setor Gestão de Pessoal (SET-GPE) deve informar quando houver o desligamento de servidores ao SET-SPT ou à DIV-TIN para que as credenciais de acesso aos sistemas, computadores, e-mail e ambiente de rede sejam bloqueadas.

XIX – Registro de Chamados Internos

Diante de qualquer incidente ou pedido de suporte deverá ser registrado o pedido ou demanda no sistema *helpdesk* do instituto, de modo detalhado, acessando o sistema com suas credenciais de acesso.

Em caso de indisponibilidade do sistema *helpdesk, a demanda* deverá ser enviada por e-mail (suporte@ipmjp.pb.gov.br) ou através do sistema 1DOC-PMJP.

PARTE II

POLÍTICA DE SEGURANÇA DE DOCUMENTOS, INFORMAÇÕES E ARQUIVO

DOS PROCEDIMENTOS DE PROTOCOLO

XX – Recebimento e Expedição de documentos

Todas as correspondências oficiais ou particulares são recepcionadas no Setor de Protocolo.

Ao receber a documentação, o servidor verifica, primeiramente, se o destinatário é o Instituto de Previdência (correspondência oficial) ou um servidor em atividade no Instituto (correspondência particular). Em caso negativo, o setor procede a devolução da correspondência.

No caso de correspondência particular, deve ser mantida lacrada e encaminhada para o destinatário, que deverá assinar o seu recebimento.

No caso de correspondência oficial, deve ser observado se possui indicativo de grau de sigilo. Em caso positivo, deve ser mantida lacrada e encaminhada diretamente ao destinatário, que deverá assinar o seu recebimento.

No caso de correspondência oficial e ostensiva, ou seja, sem restrição de acesso, deve ter seu invólucro aberto para fins de conhecimento do seu conteúdo e autuação de processo administrativo, quando necessário. Esse processo administrativo deve ser tramitado para o setor correspondente, o qual deverá assinar o seu recebimento.

Quanto à expedição dos documentos, todos os processos ou correspondências físicas que saem do Instituto, tramitam, necessariamente, pelo Setor de Protocolo.

XXI – Carimbos e Paginação para processos físicos, digitais e/ou híbridos

As folhas dos processos devem ser numeradas em ordem crescente, sem rasuras, devendo ser utilizado carimbo próprio do IPMJP para inserção do número da página.

O carimbo deve ser inserido no canto superior direito da página. A primeira folha (capa) não é numerada, portanto, a partir da segunda folha do processo, a numeração se inicia com o número 02 e a rubrica do responsável pela numeração. Se houver informação no verso da página, deve ser aposto no canto superior esquerdo o carimbo, com a

numeração da frente da página seguida da letra “v”. Exemplo: 02-v.

Para documentos com o verso em branco, deve ser inserido no meio da página o carimbo “EM BRANCO”, evitando a inserção de informações de forma indevida.

A autuação, ou seja, a formação do processo deve ser no Setor de Protocolo. As folhas seguintes que forem sendo anexadas ao processo devem ser numeradas e rubricadas pelo setor responsável pela respectiva anexação do(s) documentos(s).

Ao receber um processo, o setor deve verificar se o mesmo se encontra numerado até a sua última folha, e caso não esteja, solicitar ao setor que está tramitando o processo, que faça a numeração de forma correta.

É vedada a inserção de letras na numeração do processo, como por exemplo: 02, 02-A.

Se o processo for numerado de forma incorreta, pode ser posto um X na numeração anterior, colocando a numeração correta logo abaixo.

Os processos devem ser paginados utilizando caneta esferográfica, sendo vedado o uso de lápis grafite, o qual pode ser facilmente apagado e/ou adulterado.

Os processos digitais são numerados automaticamente pelo sistema 1Doc.

XXII – Tramitação de documentos

O procedimento de tramitação, ou seja, de movimentação do processo deve ser feito pelo Sistema de Gerenciamento Eletrônico de Documentos (GED), quando o processo for físico, e no 1Doc, com o processo sendo digital.

No GED, ao tramitar os documentos, deve ser impressa a folha de tramitação de processos, a qual deve ser assinada pelo receptor dos documentos.

As folhas de tramitação de processos devem ser arquivadas pelo setor de origem da tramitação para fins informacionais e de prova dos atos realizados.

Em caso de erro na tramitação no GED, solicitar ao Protocolo que seja realizado o cancelamento da última ação.

Em caso de necessidade de cancelamento de processo, deverá o setor informar em despacho anexado ao processo os motivos pelo qual se deseja proceder o cancelamento.

O processo cancelado deve ser arquivado no Setor de Protocolo.

Quando o processo for digital, toda sua tramitação ocorrerá dentro do 1Doc, se atentando ao último despacho proferido, para assim, encaminhar ao setor responsável.

XXIII – Apensação de processos físicos, digitais e/ou híbridos

Para proceder a apensação de um ou mais processos a outro processo, deverá o

interessado informar essa ação no despacho e inserir o Termo de Anexação de Processos. Em caso de necessidade de apensação durante a marcha processual, solicitar o termo de apensação ao Setor de Arquivo. Cabe observar que a solicitação ou realização da apensação deve se dar por via expressa em folha de despacho anexada ao processo.

Por fim, realizada a apensação deve ser inserido na capa do processo principal a seguinte informação: "*O processo nº xxxxx/xxxx está apenso a este processo nº xxxxx/xxxx conforme Termo de Apensação de Processo constante na fl. nº xx".*

Importante mencionar que quando o processo principal for tramitado via GED, deve ser tramitado também o(s) processo(s) apensos.

A paginação do processo deve seguir a do processo principal, sendo necessário, sempre que houver a apensação, proceder a repaginação dos processos.

DA CONSERVAÇÃO E PRESERVAÇÃO DOS DOCUMENTOS

XXIV – Conservação e Preservação de documentos

Alguns procedimentos devem ser observados com vistas a manter a integridade física dos documentos, dentre os quais:

Não ingerir alimentos perto dos documentos, sobretudo alimentos líquidos, a exemplo de café, sucos e água;

Não usar grampos demasiadamente;

Priorizar o uso de clipes e grampos plásticos;

Usar o furador na margem de papel A4, evitando que as folhas fiquem tortas, amassadas e/ou rasgadas.

Acondicionar o documento em material adequado (pastas suspensas, pasta A-Z, caixa polionda, envelopes de papel ph neutro e etc);

Armazenar os documentos acondicionados em armários e estantes próprias;

Evitar a exposição das caixas ao sol;

Não armazenar os documentos em local sem ventilação, sem invólucro e sem armários e/ou estantes.

XXV – Higienização de documentos

A higienização é a retirada, por meio de técnicas apropriadas, de poeira e outros resíduos do documento. Esse procedimento é obrigatório para os documentos que serão submetidos ao processo de digitalização.

Para a retirada de sujidades, é indicado utilizar a trincha. Para a retirada de grampos, utilizar o extrator de grampos. As margens em branco dos documentos impressos em formatos maiores que o convencional podem ser retiradas com o uso de material apropriado.

DA TRANSFERÊNCIA DE DOCUMENTOS

XXVI – Procedimentos para a transferência de documentos para o SET-ARQ

Os processos são transferidos para o SET-ARQ sempre ao final de sua finalidade administrativa para arquivamento na pasta do servidor a que se refere (nos casos de processos de benefícios), ou nas caixas-arquivo dos respectivos setores (no caso de processos administrativos).

A depender da capacidade de armazenamento do SET-ARQ, os documentos administrativos podem ser transferidos anualmente, ao final do exercício, ou ao final da gestão municipal, vinculada à necessidade de uso do documento.

Não podem ser enviados ao SET-ARQ documentos que não sejam produzidos e/ou recebidos em função das atividades do Instituto, bem como cópias, revistas, jornais, rascunhos e outros que não possuam relação direta ou indireta com o IPMJP.

Antes da transferência, os documentos devem passar por rigorosa avaliação separando os documentos oficiais de outros que não possuam essa característica, conforme citado anteriormente.

Todos os documentos – que não constituem processo – devem ser listados em LibreOffice Writer ou Calc e os conjuntos devem ser enviados para o SET-ARQ juntamente com essa listagem.

Os processos só são recebidos pelo SET-ARQ mediante tramitação via sistema de Gerenciamento Eletrônico de Documentos (GED) ou via 1DOC.

Todos os processos, findo sua tramitação, devem, necessariamente, serem encaminhados para a Digitalização (GED) e posterior arquivamento no SET-ARQ. Só serão recebidos processos previamente digitalizados e tramitados via sistema ou processos digitais tramitados em sistema autêntico e seguro.

XXVII – Transferência de documentos do SET-ARQ para o Arquivo Central da Prefeitura Municipal de João Pessoa (PMJP)

Quando há a necessidade de transferência dos documentos do SET-ARQ para o Arquivo

Central da PMJP, a mesma é comunicada ao chefe da Divisão de Previdência e decidida em reunião conjunta com o chefe do SET-ARQ e do Arquivo Central da PMJP, bem como o presidente da CPAD do Instituto e da Prefeitura (se houver).

Os documentos são descritos na Lista de Transferência Temporária de Documentos e é lavrado o Termo de Transferência Temporária de Documentos, assinado entre as partes.

Esses documentos devem ser mantidos íntegros e autênticos para comprovação do ato de transferência, bem como para solicitação do retorno dos documentos transferidos para a unidade geradora.

Os documentos transferidos para o Arquivo Central da Prefeitura Municipal de João Pessoa permanecem com acesso restrito aos servidores autorizados do Instituto de Previdência.

DO ARQUIVAMENTO DE DOCUMENTOS

XXVIII – Acondicionamento e Armazenamento de documentos no SET-ARQ

Os documentos serão acondicionados em caixas poliondas ou pasta suspensa, a depender da série documental. O armazenamento também depende da série documental, podendo ser em armários, arquivo deslizante ou estante de aço.

DA ELIMINAÇÃO DE DOCUMENTOS PÚBLICOS

XXIX – Procedimentos para eliminação de documentos

Documentos públicos só podem ser eliminados mediante constituição da Comissão Permanente de Avaliação de Documentos (CPAD), responsável pela avaliação de documentos e elaboração do Plano de Classificação e a Tabela de Temporalidade e Destinação de Documentos (TTDD), os quais deverão ser remetidos para apreciação e aprovação pela Instituição Arquivística Pública Municipal, nos moldes da Lei nº 8.159/1991, bem como seguir rigorosamente os procedimentos elencados na Resolução nº 40/2014, alterada pela Resolução nº 44/2020 do Conselho Nacional de Arquivos (CONARQ): elaboração da Listagem de Eliminação de Documentos, Edital de Ciência de Eliminação de Documentos e Termo de Eliminação de Documentos.

O Plano de Classificação e a TTDD devem considerar os documentos físicos, digitais e híbridos. Documentos considerados permanentes, devem ser recolhidos para o Arquivo Público Municipal ou, em sua ausência, preservados permanentemente pela Instituição Custodiadora.

Em consonância com art. 16 da LGPD, é importante ressaltar que no caso de cumprimento de obrigação legal, como ocorre com a administração pública na maior parte dos casos, é autorizada a conservação do dado pessoal. Isso significa que, da mesma forma que o titular dos dados não precisa consentir o tratamento dos dados pessoais pela administração pública em casos determinados, também não é possível ao titular do dado solicitar a eliminação.

DO ACESSO AOS DOCUMENTOS

XXX – Acesso aos documentos do SET-ARQ por usuários internos

Usuários internos são todos os servidores – efetivos, comissionados e prestadores de serviços - que exercem funções e atividades no IPMJP.

O acesso aos processos e pastas funcionais arquivados no SET-ARQ é fornecido, prioritariamente, via GED ou 1DOC, aos servidores autorizados, de acordo com as funções e atividades que exercem. Em casos extraordinários em que a informação digitalizada estiver ilegível, o usuário interno pode solicitar vistas aos documentos no Arquivo, com antecedência mínima de 24 horas. Nos casos em que o processo ou pasta funcional estiverem indisponíveis, deve o usuário solicitar por e-mail ou memorando que o documento seja digitalizado e inserido no GED, por onde será franqueado o acesso. Esse procedimento deve ser solicitado com antecedência mínima de 48 horas, salvo em casos de urgência.

XXXI – Acesso aos documentos do SET-ARQ por usuários externos

Usuários externos são todos aqueles que integram o processo ou pasta funcional como titular, interessado, curador ou procurador.

Para ter acesso a esses documentos, o titular, interessado, curador ou procurador deve solicitar vistas aos autos ou cópia integral/parcial do processo ou pasta funcional em que é parte. A solicitação é feita no Setor de Atendimento (SET-ATE) que encaminhará para o Protocolo para autuação e tramitação inicial. O processo será findo com a entrega das cópias ao requerente e assinatura do mesmo em declaração de recebimento que será anexada ao processo. Em caso de processo digital tramitado no 1DOC, o titular poderá acessar a íntegra do processo diretamente no sistema.

Nos moldes da Lei de Acesso à Informação, os usuários externos que tenham relação ou não com o IPMJP, poderão solicitar informações de interesse público ou particular, observadas as hipóteses descritas na referida lei, pelo canal de ouvidoria do IPMJP

(http://www.ipmjp.pb.gov.br/site/ouvidoria), pelo Sistema de Informações ao Cidadão (SIC) ou pelo Portal de Transparência do Município de João Pessoa (https://transparencia.joaopessoa.pb.gov.br/#/).

PARTE III

POLÍTICA DE SEGURANÇA DE DADOS PESSOAIS

DO CONTROLADOR E DO OPERADOR DE DADOS PESSOAIS

XXXII – Identificação do Controlador de dados pessoais

Para fins de conformidade com a LGPD, o Controlador, no que se refere ao escopo dessa Política, é o Instituto de Previdência do Município de João Pessoa (IPMJP), órgão da administração indireta da Prefeitura Municipal de João Pessoa. Autarquia responsável por gerir o Regime Próprio de Previdência dos Servidores efetivos do município de João Pessoa.

XXXIII – Identificação do Operador de dados pessoais

No exercício de sua finalidade pública, o IPMJP possui prerrogativa, também, de operador de dados pessoais

DO ENCARREGADO DE PROTEÇÃO DE DADOS (DATA PROTECTION OFFICER – DPO)

XXXIV – Da indicação do Encarregado de dados pessoais (DPO)

Nos moldes da LGPD, o DPO deve ser indicado pelo Controlador dos dados pessoais, o qual deverá ocorrer por ato administrativo. A identidade e informações de contato do DPO deverão constar no site do IPMJP.

Apesar de não especificar o profissional que deverá ocupar essa função, o Controlador deve levar em consideração que o DPO precisa possuir conhecimentos essenciais às suas atribuições, unindo preferencialmente, as áreas de gestão da privacidade e proteção de dados pessoais, conhecimento da legislação pertinente, da gestão de riscos, da governança de dados e acesso à informação no setor público.

Além disso, para evitar o conflito de interesses, o DPO não pode ser servidor das Unidades da Divisão de Tecnologia da Informação ou Gestor de sistemas do IPMJP.

DO TRATAMENTO DE DADOS PESSOAIS E DISPENSA DE CONSENTIMENTO

XXXV – Tratamento de dados pessoais pelo Poder Público e dispensa de consentimento

É facultado à Administração Pública o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do capítulo IV da LGPD.

Sempre que a Administração Pública realizar o tratamento de dados pessoais no exercício de suas competências legais vinculadas a políticas públicas e entrega de serviços públicos, não precisará colher o consentimento do titular, porém, necessariamente, estará obrigada a informar a finalidade e a forma como o dado será tratado.

Os aspectos de finalidade e tratamento dos dados estão explícitos nessa Política de Segurança de documentos, informações e proteção de dados pessoais, a qual se constitui enquanto documento de acesso público.

O consentimento de que trata a LGPD também é dispensado no caso de exercício regular de direitos em processo judicial, administrativo ou arbitral (este último, nos moldes da Lei nº 9.307/1996), o que inclui o exercício do contraditório, ampla defesa e devido processo legal. Isso quer dizer que a proteção de dados pessoais não compromete o direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário, ou seja, não cabe oposição ao tratamento de dados pessoais no contexto dos processos judiciais, administrativos e arbitrais.

O tratamento deve contemplar o conceito de privacidade desde a concepção (*privacy by design*), sendo concebida segurança integral no ciclo de vida dos dados pessoais.

A eliminação de dados pessoais no contexto dos órgãos públicos deve observar o disposto no item XXIX desta política, que trata dos procedimentos para eliminação de documentos públicos.

DA FINALIDADE DE TRATAMENTO

XXXV – Tratamento de dados pelo IPMJP

No uso de suas atribuições, todos os dados, documentos e informações tratados pelo IPMJP vinculam-se exclusivamente à finalidade pública, destinados a subsidiar a

prestação do serviço público para o qual o IPMJP foi criado.

DOS DIREITOS DOS TITULARES DOS DADOS

XXXVI – Direitos dos titulares de dados explícitos na LGPD

Conforme expresso na LGPD, o titular dos dados pessoais possuem o direito a obter do Controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

Confirmação da existência de tratamento;

Acesso aos dados;

Correção de dados incompletos, inexatos ou desatualizados;

Anonimização, bloqueio ou eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;

Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD, observados os segredos comercial e industrial;

Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;

Informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;

Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

Revogação do consentimento, nos termos do §5º do art. 8º da LGPD.

DA EXECUÇÃO DOS DIREITOS DOS TITULARES

XXXVII – Meios de execução do direito de petição ao IPMJP

Nos moldes da Lei de Acesso à Informação, os cidadãos podem efetivar seu direito de acesso pelo canal de ouvidoria do IPMJP (http://www.ipmjp.pb.gov.br/site/ouvidoria), pelo Sistema de Informações ao Cidadão (SIC), ou pelo Portal de Transparência do Município de João Pessoa (https://transparencia.joaopessoa.pb.gov.br/#/).

Quanto aos titulares de dados pessoais, a LGPD estabelece que esse poderá solicitar do órgão esclarecimentos acerca da finalidade e forma de tratamento dos dados, os quais estão especificados no teor desta Política de Segurança de documentos, informações e proteção de dados pessoais, a qual constará no portal do IPMJP para consulta, além da

possibilidade de solicitar informações por meio do 1DOC, através do setor “IPM-DPO - Departamento de Proteção de Dados”.

DO COMPARTILHAMENTO DE DADOS PESSOAIS

XXXVIII – Em razão do exercício do fim público e das suas atividades legais, o IPMJP necessita compartilhar dados com outras entidades da prefeitura e entidades externas, a fim de melhorar o serviço prestado ao cidadão e aos beneficiários deste Instituto.

XXXIX - Todos os documentos e dados devem ser compartilhados via 1DOC, e-mail e/ou sistemas institucionais, ficando vedado o compartilhamento desses documentos via aplicativos de mensagens instantâneas, exceto ao se tratar de canais de comunicação oficiais deste Instituto.

DISPOSIÇÕES FINAIS

DAS RESPONSABILIDADES

XL – É de responsabilidade do Instituto de Previdência do Município de João Pessoa, enquanto agente de tratamento de dados, nos termos da LGPD:

Formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regimento de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados;

Manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse;

Indicar o Encarregado pelo tratamento de dados pessoais;

Comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

Elaborar relatório de impacto à proteção de dados pessoais, quando solicitado pela ANPD;

Realizar, na qualidade de Operador, o tratamento dos dados segundo as instruções fornecidas pelo Controlador, que verificará a observância das próprias instruções e das

normas sobre a matéria;

Reparar dano patrimonial, moral, individual ou coletivo, que eventualmente tenha causado em razão do exercício de atividade de tratamento de dados pessoais, em que houver violação da LGPD.

XLI – É de responsabilidade do Encarregado (ou *Data Protection Officer* – DPO) do IPMJP:

Atuar como canal de comunicação entre o Controlador, os titulares dos dados e ANPD;

Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

Receber comunicações da ANPD e adotar providências;

Orientar os servidores e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

Executar as demais atribuições determinadas pelo Controlador ou estabelecidas em normas complementares.

XLII – É de responsabilidade do Setor de Suporte (SET-SPT) e do Setor de Arquivo (SET-ARQ):

Acompanhar a execução desta Política de Segurança de documentos, informações e proteção de dados pessoais;

Manter registro das operações de tratamento realizadas;

Preservar o acesso restrito aos relatórios e planilhas desenvolvidas para controle das informações sob sua custódia;

Prestar orientações quanto aos procedimentos descritos neste documento aos servidores dos demais setores do IPMJP;

Manter e atualizar essa política periodicamente;

XLIII – É de responsabilidade da Assessoria de Controle Interno (ASS-CIN):

Acompanhar a execução desta Política de Segurança de documentos, informações e proteção de dados pessoais no Instituto, zelando pelo seu cumprimento junto aos servidores do Instituto.

XLIV – É de responsabilidade dos servidores:

Manter-se atualizado dos procedimentos de segurança adotados no IPMJP;

Cumprir o descrito nesta Política de Segurança de documentos, informações e proteção de dados pessoais;

Consultar esse documento e/ou buscar orientação junto ao DPO, ao SET-SPT e/ou SET-ARQ quando necessário à execução dos dispositivos desta Política;

Manter registro das operações de tratamento realizadas no exercícios das suas atividades;

Contribuir para a melhoria e eficiência desta Política no âmbito do IPMJP.

XLV – É de responsabilidade dos Gestores e Diretores:

Aprovar esta Política de Segurança de documentos, informações e proteção de dados pessoais e apoiar a sua implementação.

DO CUMPRIMENTO

É dever de todos os servidores o cumprimento dos dispositivos constantes nesta Política de Segurança de documentos, informações e proteção de dados pessoais.

Diante do descumprimento desta política em geral, o usuário poderá, a qualquer tempo, ser auditado por meio de procedimento internos de interesse do Controlador, do Encarregado (DPO), do SET-SPT, SET-ARQ e/ou ASS-CIN estando sujeito a receber em consequência, a aplicação de ações disciplinares cabíveis quando se fizerem necessárias, inclusive no compete às sanções por violação aos direitos tutelados pelas leis que versam sobre as matérias descritas nesta Política.

_____

CAROLINE FERREIRA AGRA

Superintendente do Instituto de Previdência do Município de João Pessoa

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991**. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em:<http://www.planalto.gov.br/ccivil_03/leis/l8159.htm>. Acesso em:

_____. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em:

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em:

CONARQ, Conselho Nacional de Arquivos. **Resolução nº 40, de 09 de dezembro de 2014**. Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Disponível em: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-40-de-9-de-dezembro-de-2014-alterada>. Acesso em: 17/04/2021.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (Brasil). **Proteção de Dados Pessoais no Setor Público** (Curso online), Brasília, 2020.

_____. **Introdução à Lei Brasileira de Proteção de Dados Pessoais** (Curso online), Brasília, 2020.

HINTZBERGEN, K; HANS BAARS, S. **Fundamentos de segurança da informação**: com base na ISSO 27001 e na ISSO 27002. Tradução Alan de Sá. Rio de Janeiro: BRASPORT, 2018.

JOÃO PESSOA. **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD)**. Comitê Intersecretarial de Análise da Aplicação da Lei Geral de Proteção de Dados em João Pessoa, 2020.

_____. **Relatório Definitivo das Proposições para Implementação da Lei Geral de Proteção de Dados no âmbito do Município de João Pessoa**. Comitê Intersecretarial de Análise da Aplicação da Lei Geral de Proteção de Dados em João Pessoa, 2020.

PREFEITURA MUNICIPAL DE JOÃO PESSOA

Prefeito
Cícero Lucena Filho

INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE JOÃO PESSOA

Superintendente
Caroline Ferreira Agra

Superintendente Adjunto
Rodrigo Ismael da Costa Macedo

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Antônio Henrique Gomes dos Santos
antoniohenrique@ipmjp.pb.gov.br
(83) 3222-1005

FICHA TÉCNICA

Elaboração
Antônio Henrique Gomes dos Santos
Enéas Lyra de Albuquerque
Higor Delgado Leite Benício
Joseane Farias de Souza
Nicholas Frederico Freire Dias de Araújo
Weverton J. Moreira

Revisão
Joseane Farias de Souza
Antônio Henrique Gomes dos Santos

Layout e Diagramação
Joseane Farias de Souza

ANEXO I

TERMO DE RESPONSABILIDADE

POLÍTICA DE SEGURANÇA DE DOCUMENTOS, INFORMAÇÕES E PROTEÇÃO DE DADOS PESSOAIS DO INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE JOÃO PESSOA (Edição revisada e ampliada, 2022)

Eu, ...

Titular do cargo ..... Lotado no setor .....

Matrícula nº. ..... e CPF nº. ..... Pelo presente termo, declaro que li e entendi o conteúdo da presente norma e me comprometo a cumprir suas recomendações e determinações. Declaro ainda que estou ciente da minha responsabilidade pelo uso indevido dos meios de informática pertencentes a esta entidade, dos documentos, informações e dados pessoais em que obtive acesso no exercício das minhas funções e atividades, bem como qualquer desvio ou prejuízo causado por ato ou omissão de minha parte por desobediência às normas de segurança da informação descritas na Política de Segurança de documentos, informações e proteção de dados pessoais.

João Pessoa, .../...../2022

.....

(Assinatura)