Política de Segurança da Informação, de Documentos e de Proteção de Dados Pessoais do Instituto de Previdência do Município de João Pessoa

© Instituto de Previdência do Município de João Pessoa. TODOS OS DIREITOS RESERVADOS.

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 de dados pessoais. 3º Edição revisada e ampliada.** João Pessoa. 2026.

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
Dahise Emanuelly Santos

Revisão
Joseane Farias de Souza
Higor Delgado Leite Benício
Dahise Emanuelly Santos
Greicy Pessoa Rodrigues Crispim
José Antônio Gonçalves Cabral

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Renato Gomes de Lacerda Alves, renatoalves@ipmjp.pb.gov.br
(83) 3222-1005 | https://www.ipmjp.pb.gov.br/site/ouvidoria/lgpd/4

CONTROLE DE VERSÃO

4ª Edição revisada e ampliada Última atualização: 17/07/2026

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 | https://www.ipmjp.pb.gov.br .

ESTRUTURA ORGANIZACIONAL

PREFEITURA MUNICIPAL DE JOÃO PESSOA

Prefeito
Leopoldo Araújo Bezerra Cavalcanti

INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE JOÃO PESSOA

Superintendente:
Caroline Ferreira Agra

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:
Leonardo Neiva de Gouvea Ribeiro
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:
Camila Pires de Sá Mariz Maia
Chefe da Seção Folha de Benefícios:
Daniela Araújo Agostinho Fortes
Chefe da Seção de Gestão de Tecnologia da Informação:
Eneas Lyra de Albuquerque
Chefe da Seção Desenvolvimento:
Henrique de Paiva Araujo Pontes
Chefe da Seção de Compensação Previdenciária:
Ana Paula Barreto Aquino Victor de Vasconcelos
Chefe da Seção de Benefícios:
Angélica da Costa Ferreira
Chefe da Seção de Gestão de Pessoal:
Karla Janaina Vergara de Sá
Gerente Administrativo do Fundo Previdenciário:
Ayrton Ciraulo Neto

CONSELHO PREVIDENCIÁRIO

Biênio (2025 – 2026)

Superintendente do IPM/JP – como Membro nato, Presidente do Conselho:
Titular: Caroline Ferreira Agra

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

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

Servidor ativo da Câmara Municipal, indicado pelo presidente daquela casa legislativa:
Titular: Rafael Barbosa Damasceno
Suplente: Germana Lins Lopes

Servidor Ativo, indicado por Associação de Classe:
Titular: Valdegil Daniel de Assis
Suplente: Raquel do Nascimento Sabino

Servidor Inativo ou pensionista, indicado por Associação de Classe:
Titular: Francisco de Assis Araújo Neto
Suplente: Giucélia Araújo de Figueiredo

Servidor Inativo ou Pensionista, indicado por Associação de Classe:
Titular: Aristovora de Sousa Santos
Suplente: Odon Vilar

Representante da sociedade civil, indicado pelo prefeito:
Titular: Jessyca Patrícia Paiva Marques Brasileiro
Suplente: Diego Fernandes Hermínio

CONSELHO FISCAL

Biênio (2025-2026)

Servidor Ativo, Aposentado ou Pensionista indicado pelo Prefeito
Titular: Antônio Henrique Gomes dos Santos
Suplente: Karina Leal Ernesto de Amorim

Servidor Ativo, Aposentado ou Pensionista indicado pelo Prefeito:
Titular: Joseane Farias de Souza
Suplente: Daniela Araújo Agostinho Fortes

Servidor Ativo, Aposentado ou Pensionista indicado pelo Prefeito:
Titular: Milena Medeiros de Alencar Feitosa
Suplente: Érico Heyller Medeiros de Alencar

Servidor Ativo, Aposentado ou Pensionista indicado por Associação de Classe:
Titular: Alex Maia Duarte Filho
Suplente: Yan Cavalcanti Aragão

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

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, incluindo as ferramentas, sistemas e algoritmos de Inteligência Artificial (IA), 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.

Inteligência Artificial (IA): é a tecnologia que permite que sistemas computacionais realizem tarefas que normalmente exigiriam inteligência humana, como aprender, analisar informações, reconhecer padrões, tomar decisões e gerar conteúdos, de forma automatizada e com base em dados.

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.

VIII – Uso de Ferramentas de Inteligência Artificial (IA)

É vedado inserir em plataformas de Inteligência Artificial públicas (ChatGPT, ChatPDF, Gemini) ou de terceiros, informações sigilosas, dados financeiros ou previdenciários custodiados pelo IPMJP.

As informações geradas por ferramentas de Inteligência Artificial deverão ser revisadas e validadas pelo servidor humano responsável antes de produzir efeitos administrativos ou jurídicos, não podendo ser consideradas como fonte única de informação.

O instituto poderá restringir ou bloquear a utilização de ferramentas de Inteligência Artificial em seus ambientes tecnológicos, bem como o acesso a serviços que apresentem riscos à segurança da informação ou ao tratamento adequado dos dados.

DA AUDITORIA E REGISTRO DE *LOGS* DE ACESSO

IX – 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.

X – 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.

XI – 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.

XII – 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.

XIII – 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

XIV – 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).

XV – Armazenamento dos backups

Os backups são armazenados em servidores específicos para esse propósito, permitindo a rápida recuperação dos sistemas e arquivos.

XVI – Teste de recuperação

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

XVII – 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

XVIII – 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.

XIX – 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.

XX – 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

DO GERENCIAMENTO DO ACERVO LEGADO

XXI – Recebimento de documentos físicos no Arquivo

Processos físicos devem ser tramitados para o Arquivo via Sistema de Gerenciamento Eletrônico de Documentos (GED).

Em caso de documentos físicos de cunho administrativos que não estejam autuados em processos, mas acondicionados em caixas-arquivo, deverá o remetente analisar os documentos, descrevê-los em uma lista específica fornecida pelo Setor de Arquivo, assim como deverá preencher o espelho e colar na caixa-arquivo correspondente.

Pastas Funcionais físicas devem ser devidamente identificadas e enviadas para o Setor de Arquivo nos casos em que o servidor se aposenta ou vem à óbito, nestes casos, deverá a Secretaria ou órgão de origem correspondente enviar uma lista contendo as informações sobre as pastas que estão sendo enviadas. O responsável pelo Setor de Arquivo dará vistas e atestará o recebimento das pastas funcionais.

Não serão recebidos processos físicos sem tramitação prévia.

Não serão recebidos documentos ou volumes de documentos sem organização e descrição prévia.

Não serão recebidas pastas funcionais sem constatação devida em lista enviada pela Secretaria ou órgão de origem do servidor.

XXII – 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.

XXIII – 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.

DA CONSERVAÇÃO E PRESERVAÇÃO DOS DOCUMENTOS FÍSICOS

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.

XXVI - Digitalização de documentos

A digitalização dos processos deverá ser realizada, prioritariamente, no Setor de Arquivo, mas havendo necessidade e previsibilidade, poderá ser apoiada por empresas terceirizadas e acompanhada pelo responsável do Setor de Arquivo.

A digitalização deverá ser mapeada e manualizada.

Os procedimentos adotados na digitalização deverão considerar o ordenamento jurídico brasileiro, assim como as recomendações do Conselho Nacional de Arquivos (CONARQ).

DA TRANSFERÊNCIA DE DOCUMENTOS

XXVII – 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).

Todos os documentos tramitados no 1DOC deverão ser encaminhados para o Setor de Arquivo, que realizará a transferência do processo final com verificação de autenticidade para o GED.

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

Não poderão 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 serão 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.

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

Quando houver a necessidade de transferência dos documentos do SET-ARQ para o Arquivo Central da PMJP, a mesma deverá ser 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 pelo Instituto de Previdência.

DO ARQUIVAMENTO DE DOCUMENTOS

XXVII – 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

XXVIII - Procedimentos para eliminação de documentos

Documentos públicos só poderão ser eliminados mediante constituição da Comissão Permanente de Avaliação de Documentos (CPAD), responsável pela avaliação de documentos e elaboração do Plano de Classificação de Documentos (e a Tabela de Temporalidade e Destinação de Documentos (TTD), 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, com alterações dadas pela Resolução nº 44/2020 do Conselho Nacional de Arquivos (CONARQ), a saber: elaboração da Listagem de Eliminação de Documentos, Edital de Ciência de Eliminação

de Documentos e Termo de Eliminação de Documentos.

O PCD e a TTD devem considerar os documentos físicos, digitais e híbridos. Documentos considerados permanentes, devem ser recolhidos para o Arquivo Público Municipal ou, em sua ausência, preservados 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

XXVIII - 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 será 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 esteja ilegível, o usuário interno poderá 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 via 1DOC 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.

XXVIII - Acesso aos documentos do SET-ARQ por usuário 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 via 1DOC, cujo acesso também será franqueado neste Sistema. 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

XXVIII – 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), pessoa jurídica de direito público da administração indireta do Município de João Pessoa, de natureza autárquica, responsável por gerir o Regime Próprio de Previdência dos Servidores efetivos do município de João Pessoa.

XXIX – 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)

XXX – 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, em observância à LGPD e à Resolução CD/ANPD nº 18, de 16 de julho de 2024 (Regulamento sobre a atuação do Encarregado)".

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.

O Encarregado não poderá ocupar posição que enseje conflito de interesses, o qual se presume sempre que houver acúmulo da função com atribuição dotada de competência decisória sobre o tratamento de dados pessoais. Em decorrência, é vedada a indicação de servidor lotado na Divisão de Tecnologia da Informação ou de gestor de sistemas do IPMJP

para a função de Encarregado.

Ao Encarregado serão assegurados autonomia técnica no exercício de suas atribuições, acesso às informações necessárias e recursos adequados ao desempenho de suas funções, com comunicação direta às instâncias superiores do IPMJP.

Por fim, em caso de ausência, impedimento ou vacância deve ser designado, por ato formal, Encarregado substituto.

DO TRATAMENTO DE DADOS PESSOAIS E DISPENSA DE CONSENTIMENTO

XXXI – 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, observando-se, contudo, eventuais restrições decorrentes da cláusula de reserva de jurisdição, casos em que o compartilhamento dependerá de decisão judicial.

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.

Considerando que o IPMJP trata dados pessoais sensíveis – notadamente dados de saúde (perícias e concessão de benefícios por incapacidade), dados biométricos (prova de vida) e dados de filiação sindical (consignações) –, hipótese em que o tratamento deve observar as bases específicas do art. 11, II, da LGPD, em especial o cumprimento de obrigação legal ou

regulatória (alínea “a”), o tratamento compartilhado necessário à execução de políticas públicas (alínea “b”) e o exercício regular de direitos (alínea “d”), assegurada sempre a estrita necessidade e finalidade.

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 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 possui 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.

PARTE IV

GOVERNANÇA DE IA

Essa Política estabelece as diretrizes de segurança aplicáveis ao uso, desenvolvimento, aquisição e implementação de Sistemas de Inteligência Artificial (Sistemas de IA) no âmbito do instituto, visando garantir a proteção de dados, a conformidade legal e a mitigação de riscos tecnológicos.

O uso, o desenvolvimento, a aquisição, a contratação, a disponibilização e a implementação de Sistemas de Inteligência Artificial no âmbito do Instituto deverão observar os princípios da transparência, explicabilidade, segurança digital, supervisão humana e proteção de dados.

Esses princípios deverão ser aplicados de forma proporcional à finalidade, ao contexto de utilização, à natureza dos dados tratados e aos riscos que o Sistema de IA possa representar para o Instituto, para os titulares de dados, para os usuários dos serviços públicos e para a sociedade.

A aplicação dos princípios deverá considerar todo o ciclo de vida do Sistema de IA, incluindo seu planejamento, desenvolvimento, aquisição, implantação, operação, monitoramento, atualização e descontinuação.

I - Transparência
II - Explicabilidade
III - Segurança Digital
IV - Supervisão Humana
V - Proteção dos dados

I - Transparência: A transparência consiste na disponibilização de informações claras, adequadas, acessíveis e compatíveis com o contexto de utilização dos Sistemas de Inteligência Artificial.

O Instituto deverá adotar medidas para que os usuários, gestores, servidores, titulares de

dados e demais partes interessadas possam identificar, conforme aplicável:

I – Quando estiverem interagindo diretamente com um Sistema de IA;
II – A finalidade para a qual o Sistema de IA é utilizado;
III – Os tipos e as fontes de dados empregados;
IV – As limitações conhecidas do sistema;
V – Os riscos relevantes associados à sua utilização;
VI – A forma como os resultados produzidos pelo sistema serão utilizados;
VII – A existência de supervisão humana;
VIII – Os responsáveis pela operação, pelo monitoramento e pela tomada de decisão;
IX – Os canais disponíveis para esclarecimentos, questionamentos, contestação ou comunicação de incidentes.

O nível de transparência deverá ser proporcional aos riscos e aos possíveis impactos do Sistema de IA, respeitados os limites relativos à segurança da informação, à propriedade intelectual, ao sigilo legal e à proteção de dados pessoais.

II - Explicabilidade: A explicabilidade consiste na capacidade de apresentar informações compreensíveis sobre o funcionamento, os fatores relevantes, os critérios utilizados e as limitações dos resultados produzidos por um Sistema de Inteligência Artificial.

Os Sistemas de IA utilizados pelo Instituto deverão possibilitar, na medida tecnicamente viável e de acordo com os riscos envolvidos, a compreensão dos elementos relevantes que contribuíram para suas decisões, recomendações, classificações, predições ou conteúdos gerados.

A explicação deverá ser adequada ao conhecimento e às necessidades de cada parte interessada, podendo apresentar diferentes níveis de detalhamento para usuários, gestores, equipes técnicas, órgãos de controle e titulares de dados.

Para os Sistemas de IA capazes de produzir efeitos jurídicos, administrativos, financeiros, previdenciários ou outros impactos relevantes sobre direitos e interesses, deverão ser mantidos registros suficientes para permitir:

I – A identificação dos dados e critérios relevantes utilizados;
II – A compreensão das principais razões que fundamentaram o resultado;
III – A identificação das limitações e do nível de confiança do sistema, quando disponível;
IV – A reprodução ou reavaliação do processo realizado;

V – A revisão do resultado por pessoa competente;
VI – A contestação pelo interessado, quando aplicável.

Não deverão ser utilizadas, como fundamento exclusivo para decisões de alto impacto, soluções de IA cuja operação seja incompatível com o nível de explicabilidade, rastreabilidade e responsabilização exigido para o processo.

III - Segurança Digital: A segurança digital consiste na adoção de medidas técnicas, administrativas e organizacionais destinadas a preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade, a resiliência e a rastreabilidade dos Sistemas de Inteligência Artificial e dos dados por eles tratados.

Os riscos de segurança deverão ser identificados, avaliados, tratados e monitorados durante todo o ciclo de vida do Sistema de IA, considerando, entre outros:

I – Acessos não autorizados;
II – Vazamento ou exposição indevida de informações;
III – Perda, alteração, destruição ou indisponibilidade de dados;
IV – Manipulação indevida de dados de entrada, treinamento ou saída;
V – Ataques adversariais e exploração de vulnerabilidades;
VI – Geração de conteúdo incorreto, malicioso ou incompatível com a finalidade institucional;
VII – Dependência de fornecedores ou serviços externos;
VIII – Uso indevido de credenciais, integrações ou interfaces de programação;
IX – Alterações não autorizadas em modelos, parâmetros ou configurações;
X – Indisponibilidade, descontinuidade ou perda de controle sobre o Sistema de IA.

Sempre que possível deverão ser adotados controles compatíveis com os riscos identificados, incluindo, conforme aplicável:

I – Controle de acesso baseado em perfis e responsabilidades;
II – Autenticação adequada;

III – Criptografia de dados;
IV – Registro e monitoramento de atividades;
V – Gestão de vulnerabilidades e atualizações;
VI – Segregação de ambientes;
VII – Cópias de segurança e planos de continuidade;
VIII – Testes de segurança, robustez e desempenho;

IX – Gestão de incidentes;
X – avaliação periódica dos fornecedores e serviços contratados.

Somente poderão ser utilizados Sistemas de IA previamente avaliados e autorizados pelo Instituto, sendo vedado o uso de ferramentas não autorizadas para o tratamento de informações classificadas, sigilosas, estratégicas, pessoais ou pessoais sensíveis.

Os incidentes relacionados a Sistemas de IA deverão ser registrados, comunicados, investigados e tratados conforme os procedimentos institucionais de segurança da informação, proteção de dados e continuidade dos serviços.

IV - Supervisão Humana: A supervisão humana consiste na manutenção de responsabilidade, autoridade e controle humano adequado sobre o desenvolvimento, a implantação, a operação e os resultados produzidos pelos Sistemas de Inteligência Artificial.

A utilização de um Sistema de IA não transfere ao sistema, ao algoritmo ou ao fornecedor a responsabilidade pelas decisões administrativas ou institucionais adotadas.

Deverão ser definidos formalmente os agentes responsáveis por:

I – Autorizar o uso do Sistema de IA;
II – Acompanhar seu funcionamento;
III – Analisar seus resultados;
IV – Verificar a ocorrência de erros, vieses ou resultados inadequados;
V – Intervir em sua operação;
VI – Suspender ou interromper sua utilização;
VII – Revisar ou invalidar decisões e recomendações produzidas.

O grau de supervisão humana deverá ser proporcional ao risco e ao impacto do Sistema de IA. Quanto maior a possibilidade de afetar direitos, benefícios, obrigações, acesso a serviços públicos ou interesses dos cidadãos, maior deverá ser a capacidade de intervenção, revisão e responsabilização humana.

As pessoas responsáveis pela supervisão deverão possuir competência, capacitação, autoridade, informações e recursos suficientes para compreender as limitações do sistema e exercer julgamento independente.

As decisões de alto impacto não deverão ser tomadas exclusivamente com fundamento em resultados produzidos por Sistemas de IA sem que exista mecanismo adequado de revisão

humana, especialmente quando houver possibilidade de prejuízo aos direitos ou interesses dos indivíduos.

V - Proteção de dados: A proteção de dados consiste na garantia de que os dados utilizados pelos Sistemas de Inteligência Artificial sejam tratados de forma lícita, adequada, segura, responsável e compatível com as finalidades institucionais.

O tratamento de dados em Sistemas de IA deverá observar os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

Antes da utilização de dados em um Sistema de IA, o Instituto deverá identificar e documentar:

I – A finalidade do tratamento;
II – A necessidade e a proporcionalidade da utilização dos dados;
III – A base legal aplicável;
IV – As categorias de dados utilizadas;

V – A origem e a qualidade dos dados;
VI – Os agentes de tratamento envolvidos;
VII – Os prazos de retenção e os critérios de descarte;
VIII – Os possíveis compartilhamentos ou transferências;
IX – Os riscos aos titulares;
X – As medidas adotadas para proteção dos dados.

A coleta e a utilização de dados deverão limitar-se ao mínimo necessário para a realização das finalidades legítimas e previamente definidas, sendo vedado o uso posterior incompatível com essas finalidades.

Sempre que possível e adequado, deverão ser adotadas técnicas de proteção de dados, tais como:

Anonimização: remoção ou transformação de informações que permitam identificar diretamente ou indiretamente uma pessoa.

Pseudonimização: substituição de identificadores por códigos ou referências, mantendo os dados necessários à reidentificação protegidos e separados.

Mascaramento: ocultação total ou parcial de informações sensíveis, limitando sua visualização ao estritamente necessário.

Agregação: consolidação de dados individuais em informações agrupadas, reduzindo a possibilidade de identificação dos titulares.

Minimização: coleta, uso, armazenamento e compartilhamento apenas dos dados necessários para a finalidade definida.

A aplicação dessas técnicas deverá considerar a finalidade do tratamento, a sensibilidade dos dados, os riscos envolvidos e os requisitos legais e regulatórios aplicáveis.

A utilização de dados pessoais sensíveis, dados de crianças e adolescentes ou outras categorias de dados de maior risco dependerá de avaliação específica, autorização institucional e adoção de controles reforçados.

É vedada a inserção, o envio ou o compartilhamento de dados pessoais, documentos internos, informações sigilosas ou bases de dados institucionais em ferramentas públicas ou não autorizadas de Inteligência Artificial.

A contratação de fornecedores de Sistemas de IA deverá prever requisitos relacionados à proteção dos dados, incluindo:

I – Finalidade e limites do tratamento;
II – Armazenamento e localização dos dados;
III – Compartilhamento com terceiros;
IV – Utilização dos dados para treinamento ou aperfeiçoamento de modelos;
V – Medidas de segurança;
VI – Comunicação de incidentes;
VII – Eliminação ou devolução dos dados ao término da contratação;
VIII – Direito de auditoria e fiscalização;
IX – Responsabilidades do fornecedor.

Os dados utilizados para treinamento, teste, validação e operação dos Sistemas de IA deverão ser avaliados quanto à sua qualidade, pertinência, representatividade, atualização, integridade e possibilidade de gerar discriminação ou resultados inadequados.

Quando o tratamento puder representar alto risco aos titulares, deverá ser realizada avaliação de impacto antes da implantação ou da alteração relevante do Sistema de IA.

DAS RESPONSABILIDADES

Compete aos Servidores e prestadores: Utilizar apenas ferramentas de IA formalmente autorizadas pela Divisão de Tecnologia da Informação deste instituto, reportando qualquer suspeita de comportamento anômalo ou vazamento de dados gerado por esses sistemas;

Compete à equipe de TI: Supervisionar e orientar os servidores do instituto a forma adequada para utilização das plataformas de Inteligência Artificial disponíveis publicamente, de forma a preservar os dados sensíveis dos servidores e do instituto.

A observância dos princípios previstos nesta Política deverá ser comprovada por meio de documentação, definição de responsabilidades, avaliações de riscos e impactos, controles técnicos e administrativos, monitoramento de desempenho, auditorias, tratamento de não conformidades e ações de melhoria contínua.

DISPOSIÇÕES GERAIS

Os Sistemas de IA deverão ser reavaliados periodicamente e sempre que ocorrer:

I – alteração relevante em sua finalidade;
II – mudança significativa no modelo, nos dados ou na infraestrutura;
III – identificação de novos riscos ou impactos;
IV – ocorrência de incidente;
V – alteração legal ou regulatória aplicável;
VI – mudança de fornecedor; ou
VII – evidência de desempenho inadequado, discriminação, erro sistemático ou violação de direitos.

A identificação de riscos inaceitáveis, falhas relevantes ou desconformidade com esta Política poderá determinar a limitação, suspensão ou descontinuação do Sistema de IA.

PARTE V

POLÍTICA DE ATAQUES CIBERNÉTICOS

Esta política busca estabelecer diretrizes para prevenção, detecção, resposta e recuperação diante de ataques cibernéticos, garantindo a confidencialidade, integridade e disponibilidade das informações, bem como a continuidade dos serviços prestados pela organização. Aplicando-se a todos os servidores, prestadores de serviço, terceiros e demais usuários que utilizem recursos tecnológicos da organização, incluindo computadores, servidores, dispositivos móveis, equipamentos de rede e sistemas corporativos.

A organização adota uma estratégia de defesa em profundidade (Defense in Depth), utilizando múltiplas camadas de segurança para reduzir riscos e minimizar impactos decorrentes de ameaças cibernéticas.

Todas as medidas de proteção devem ser implementadas considerando os princípios do menor privilégio, necessidade de acesso e gestão de riscos.

I. Controles de Segurança

Firewall

Todo o tráfego entre a rede corporativa e a Internet é obrigatoriamente direcionado ao firewall do instituto, implementado por meio da plataforma pfSense.

O firewall atua como o principal mecanismo de proteção da infraestrutura de rede, sendo responsável por:

- controlar o tráfego de entrada e saída da rede corporativa;
- permitir apenas conexões previamente autorizadas;
- bloquear acessos não autorizados;
- aplicar políticas de segurança definidas pela organização;
- registrar eventos e tentativas de conexão para fins de monitoramento e auditoria.

Nenhum equipamento poderá estabelecer comunicação direta com a Internet sem passar pelos controles implementados no firewall.

Filtro De Ameaças

Como camada adicional de proteção, o firewall utiliza o pfBlockerNG, responsável pela implementação de mecanismos de filtragem baseados em inteligência de ameaças.

Entre os controles aplicados destacam-se:

- bloqueio de endereços IP classificados como maliciosos por bases de inteligência reconhecidas;
- bloqueio de redes utilizadas para atividades maliciosas, como ataques automatizados, botnets, scanners e tentativas de exploração de vulnerabilidades;

- bloqueio geográfico (GeoIP), restringindo conexões provenientes de países ou regiões que não possuam necessidade operacio nal de comunicação com a organização;
- bloqueio de domínios associados a campanhas de phishing, malware, ransomware e outras ameaças conhecidas;
- atualização periódica das listas de bloqueio utilizadas pelo sistema.

Os critérios de bloqueio são definidos e revisados pelo Setor de Tecnologia da Informação, considerando as necessidades operacionais da organização e a redução da superfície de ataque.

Monitoramento e Registro de Eventos
O firewall mantém registros das conexões estabelecidas, bloqueios realizados e demais eventos relevantes de segurança.

Esses registros poderão ser utilizados para:

- Identificação de tentativas de invasão;
- Investigação de incidentes de segurança;
- Apoio às auditorias internas e externas;
- Análise de comportamento da rede;
- Aprimoramento contínuo das políticas de segurança.

II. Controle de acesso

O acesso aos recursos tecnológicos da organização é gerenciado por meio do Active Directory (AD), responsável pela autenticação dos usuários, aplicação de políticas de segurança e gerenciamento centralizado das permissões de acesso aos recursos computacionais.

A concessão, alteração e revogação de acessos deverão seguir processo formal de solicitação e aprovação, respeitando as atribuições e necessidades de cada função exercida pelo colaborador.

São adotadas as seguintes diretrizes:

- Cada colaborador deverá possuir uma conta de usuário individual e intransferível, sendo vedado o compartilhamento de credenciais.
- As permissões de acesso serão concedidas conforme o princípio do menor privilégio, permitindo apenas os acessos necessários ao desempenho das atividades profissionais.
- Sempre que possível, as permissões serão atribuídas por meio de grupos de segurança do Active Directory, evitando a concessão direta de permissões individuais e facilitando o gerenciamento dos acessos.
- Alterações de cargo, setor ou função deverão resultar na revisão das permissões concedidas ao colaborador, garantindo que permaneçam compatíveis com suas atribuições.
- O desligamento de colaboradores ou prestadores de serviço deverá resultar na revogação imediata dos acessos aos sistemas corporativos, conforme procedimento estabelecido pela organização.
- Contas de usuários inativas, temporárias ou de terceiros deverão ser revisadas periodicamente e desabilitadas ou removidas quando não houver mais necessidade de utilização.
- Contas com privilégios administrativos deverão ser concedidas apenas quando

houver necessidade operacional devidamente justificada e autorizada, sendo utilizadas exclusivamente para atividades administrativas.

- Sempre que tecnicamente possível, atividades administrativas deverão ser realizadas utilizando contas administrativas dedicadas, distintas das contas utilizadas para as atividades rotineiras do usuário.
- Políticas de senha, bloqueio de contas, tempo de sessão e demais requisitos de autenticação serão aplicados de forma centralizada por meio das Políticas de Grupo (Group Policy Objects – GPO), garantindo a padronização dos controles de segurança.
- O Setor de Tecnologia da Informação realizará revisões periódicas das permissões de acesso, grupos de segurança e contas privilegiadas, a fim de identificar acessos indevidos, inconsistências ou permissões incompatíveis com as funções desempenhadas.

Todas as atividades de autenticação e gerenciamento de contas poderão ser registradas em logs para fins de auditoria, rastreabilidade e investigação de incidentes de segurança.

Acesso remoto

O acesso remoto à rede é permitido exclusivamente por meio da Rede Privada Virtual (VPN) disponibilizada e gerenciada pelo instituto. É vedada a utilização de qualquer outro método de acesso remoto aos recursos internos da empresa.

A concessão de acesso à VPN é restrita a colaboradores cuja atividade profissional justifique a necessidade de acesso remoto. A autorização deverá ser solicitada pelo chefe do setor ao Setor de Suporte de TI (SET-SPT), que será responsável pela análise da solicitação, concessão das permissões necessárias e instalação/configuração do software de VPN no equipamento autorizado.

Quando o acesso for realizado por meio de equipamento pessoal, a instalação e configuração da VPN deverão ser executadas exclusivamente pelo Setor de Suporte de TI (SET-SPT), garantindo que o dispositivo atenda aos requisitos mínimos de segurança estabelecidos pela organização.

O usuário é responsável por utilizar a VPN exclusivamente para fins profissionais, manter suas credenciais em sigilo e comunicar imediatamente ao Setor de Suporte de TI qualquer suspeita de comprometimento da conta ou do dispositivo utilizado para o acesso remoto.

III. Recuperação de Incidentes

A organização manterá procedimentos de Recuperação de Desastres (Disaster Recovery – DR) com o objetivo de restabelecer a infraestrutura tecnológica e os serviços críticos em caso de falhas de hardware, indisponibilidade de servidores, corrupção de dados ou outros eventos que comprometam a continuidade das operações.

Os ambientes virtualizados deverão possuir rotinas automatizadas de backup, armazenadas em infraestrutura de contingência com redundância, de forma a garantir a disponibilidade dos dados e possibilitar sua restauração em caso de incidentes.

Na ocorrência de falhas, o Setor de Tecnologia da Informação deverá:

- Avaliar a causa da indisponibilidade e o impacto sobre os serviços corporativos;
- Priorizar a recuperação da infraestrutura por meio da substituição de

componentes defeituosos ou correção da falha identificada, sempre que tecnicamente viável;
- Realizar a restauração das máquinas virtuais a partir do backup íntegro mais recente quando a recuperação direta não for possível;
- Validar a integridade do sistema operacional, das aplicações, dos bancos de dados, dos serviços e da conectividade de rede antes da liberação do ambiente para uso;
- Registrar todas as ocorrências, incluindo a causa do incidente, as ações executadas, o backup utilizado, o tempo de recuperação e as medidas adotadas para prevenir recorrências.

Os procedimentos operacionais de recuperação serão executados utilizando a infraestrutura de virtualização adotada pela organização, contemplando mecanismos de restauração em ambiente de contingência e armazenamento redundante dos backups.

As rotinas de backup e recuperação deverão ser revisadas periodicamente e submetidas a testes, com o objetivo de verificar a efetividade dos procedimentos, assegurar a integridade dos dados armazenados e reduzir o tempo de indisponibilidade dos serviços em situações de desastre.

Os procedimentos detalhados para recuperação da infraestrutura encontram-se descritos no POP de Recuperação de Desastres, documento complementar a esta política.

IV. Responsabilidades

Compete ao Setor de Tecnologia da Informação:

- Administrar a infraestrutura de tecnologia da informação da organização, garantindo sua disponibilidade, integridade e segurança.
- Gerenciar o ambiente do Active Directory, incluindo a criação, alteração, bloqueio e remoção de contas de usuários e grupos de segurança.
- Conceder, alterar e revogar permissões de acesso mediante solicitação formal e autorização do gestor responsável.
- Administrar o firewall corporativo, a VPN e os demais mecanismos de proteção da rede.
- Manter atualizados os sistemas operacionais, aplicações, equipamentos de rede e demais ativos tecnológicos.
- Monitorar os eventos de segurança e analisar registros (logs) para identificação de incidentes ou atividades suspeitas.
- Executar as rotinas de backup e os procedimentos de recuperação de desastres previstos pela organização.
- Realizar revisões periódicas das permissões de acesso e das configurações de segurança da infraestrutura.
- Implementar medidas preventivas e corretivas para redução dos riscos de segurança da informação.
- Prestar suporte aos usuários quanto à utilização segura dos recursos tecnológicos e promover ações de conscientização sobre segurança da informação.

Compete aos servidores e colaboradores da organização:

- Utilizar os recursos tecnológicos exclusivamente para o desempenho de suas atividades profissionais.
- Manter em sigilo suas credenciais de acesso, sendo proibido o compartilhamento de senhas ou contas de usuário.

- Cumprir as diretrizes estabelecidas nesta Política de Segurança da Informação e nos demais normativos relacionados.
- Zelar pela integridade dos equipamentos e informações sob sua responsabilidade.
- Não instalar softwares, equipamentos ou serviços sem autorização do Setor de Tecnologia da Informação.
- Utilizar exclusivamente os meios de acesso remoto autorizados pela organização.
- Comunicar imediatamente ao Setor de Tecnologia da Informação qualquer suspeita de incidente de segurança, tentativa de fraude, perda de equipamento ou comportamento anormal dos sistemas.
- Cooperar com as ações de segurança da informação e com os processos de auditoria quando solicitado.

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.

REFERÊNCIAS BIBLIOGRÁFICAS

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:<https://www.planalto.gov.br/ccivil_03/leis/l8159.htm>

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: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://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: CONARQ, Conselho Nacional de Arquivos.

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.

Associação Brasileira de Normas Técnicas - ABNT, NBR ISO/IEC 42001:2024: Tecnologia da informação - Inteligência artificial - Sistema de gestão. Rio de Janeiro: ABNT, 2024.

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, 2026)

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, .../……/……..

.....

(Assinatura)