IPM JP

INSTITUTO DE PREVIDÊNCIA D
MUNICÍPIO DE JOÃO PESSOA

CARTILHA INFORMATIVA

SEGURANÇA DA INFORMAÇÃO

JOÃO PESSOA
cidade em crescimento

APRESENTAÇÃO

Esta Cartilha foi elaborada para orientar os servidores, prestadores de serviços e colaboradores do Instituto de Previdência do Município de João Pessoa (IPMJP) sobre o uso seguro dos recursos tecnológicos, a proteção dos dados pessoais dos beneficiários e a preservação do acervo documental da instituição.

A necessidade deste material decorre da constante modernização dos sistemas institucionais e da importância de assegurar a conformidade com as diretrizes de segurança e a Lei Geral de Proteção de Dados (LGPD).

Por meio desta cartilha, escrita em linguagem simples e direta , buscamos fornecer orientações práticas baseadas na Política de Segurança de documentos, informações e proteção de dados pessoais do IPMJP (4ª edição revisada e ampliada).

IPM JP
INSTITUTO DE PREVIDÊNCIA D
MUNICÍPIO DE JOÃO PESSOA

PREFEITURA JOÃO PESSOA cidade em crescimento

Nesta cartilha você vai encontrar informações essenciais sobre:

01 Por que a Segurança da Informação é Importante e Quem Deve Seguir?

02 Gestão Prática de Credenciais e Senhas Pessoais

03 Uso Seguro do Computador, Programas e Internet

04 Proteção de Documentos, Impressões e Descarte Seguro

05 E-mails Institucionais, Phishing e Ferramentas de Mensagem

06 Cuidados ao Usar Inteligência Artificial (IA) Pública

07 Lei Geral de Proteção de Dados (LGPD) e Acesso Remoto

08 Notificação de Incidentes, Deveres Principais e Checklist Diário

IPM JP
INSTITUTO DE PREVIDÊNCIA D
MUNICÍPIO DE JOÃO PESSOA

PREFEITURA JOÃO PESSOA cidade em crescimento

01

Por que a Segurança da Informação é Importante e Quem Deve Seguir?

A Segurança da Informação garante que os sistemas, documentos e dados sob responsabilidade do IPMJP fiquem protegidos contra acessos não autorizados, perdas, alterações indevidas ou vazamentos.
A política institucional fundamenta-se em quatro princípios básicos:

- **Confidencialidade:** Garantir que a informação seja acessada apenas por quem tem autorização.
- **Integridade:** Manter a exatidão e a perfeição dos dados sem alterações indevidas.
- **Disponibilidade:** Garantir que os dados e sistemas estejam acessíveis sempre que necessário.
- **Autenticidade:** Confirmar que a informação ou o usuário é realmente quem diz ser.

Quem deve seguir estas regras?
As normas aplicam-se a todos os servidores públicos, prestadores de serviços, estagiários e colaboradores que utilizem os computadores, a rede, a internet, os sistemas ou que tratem dados pessoais do IPMJP.

02

Gestão Prática de Credenciais e Senhas Pessoais

As suas credenciais de acesso (login e senha) funcionam como sua assinatura digital e são estritamente pessoais e intransferíveis.

- **Nunca compartilhe seu login e senha:** Em hipótese alguma repasse suas credenciais para colegas ou terceiros.
- **Requisitos da senha forte:** A senha deve conter, no mínimo, 8 caracteres, combinando letras maiúsculas, letras minúsculas, números e caracteres especiais.
- **Periodicidade de alteração:** As senhas dos computadores e sistemas devem ser trocadas a cada 180 dias.
- **Bloqueio automático:** Após 3 tentativas seguidas de senha incorreta, o usuário será bloqueado e o suporte técnico deverá ser acionado.

Regra de Ouro: Qualquer ação realizada com o seu usuário ficará vinculada e registrada no seu nome.

03

Uso Seguro do Computador, Programas e Internet

O uso correto dos equipamentos evita contaminações por vírus e perda de dados institucionais.

- **Bloqueio de tela:** Sempre que se ausentar da sua mesa, mesmo por poucos minutos, pressione as teclas de atalho (Windows + L) para bloquear o computador.
- **Desligamento:** Ao final do expediente ou em ausências prolongadas, desligue a máquina.
- **Instalação de programas:** É proibida a instalação de softwares por conta própria, piratas ou não homologados. Somente o Setor de Suporte de TI (SET-SPT) tem permissão para instalar programas.
- **Proteção Antivírus:** O antivírus institucional deve permanecer permanentemente ativo, atualizado e não pode ser desativado pelo usuário.

04

Proteção de Documentos, Impressões e Descarte Seguro

Documentos físicos e digitais do IPMJP contêm informações sensíveis de aposentados e pensionistas.

- **Armazenamento digital:** Guarde os arquivos de trabalho nas pastas institucionais de rede indicadas pela TI, evitando salvar dados em diretórios locais que não possuem backup.
- **Mesa Limpa:** Não deixe documentos impressos contendo dados pessoais sobre as mesas após o término das atividades diárias ou durante longas ausências.
- **Impressão consciente:** Imprima apenas o estritamente necessário e recolha o material da impressora imediatamente após o envio.
- **Descarte seguro:** Papéis com informações institucionais ou dados pessoais devem ser descartados utilizando fragmentadoras de papel ou em recipientes específicos para descarte confidencial.

05

E-mails Institucionais, Phishing e Ferramentas de Mensagem

O e-mail institucional é uma ferramenta oficial de trabalho e exige cautela constante.

- **Atenção aos e-mails falsos (Phishing):** Desconfie de mensagens que solicitem a confirmação de senhas, contenham promessas suspeitas, apresentem erros gramaticais ou venham de remetentes desconhecidos.
- **Links e anexos:** Não clique em links nem abra anexos de e-mails cuja procedência você não possa confirmar com segurança.
- **Envio de dados:** Nunca compartilhe dados institucionais sigilosos ou cadastrais por aplicativos de mensagens instantâneas (como WhatsApp) não autorizados pela gestão.

Cuidados ao Usar Inteligência Artificial (IA) Pública

O uso de ferramentas tecnológicas inovadoras traz ganho de produtividade, mas requer atenção à proteção do acervo institucional.

- **Proibição de dados sigilosos e pessoais:** É rigorosamente proibido inserir dados pessoais de aposentados, pensionistas, processos internos sigilosos ou documentos confidenciais do IPMJP em plataformas públicas de Inteligência Artificial.
- **Transparência:** Utilize ferramentas de IA como suporte ao trabalho somente com autorização e em estrita observância à LGPD.

07

Lei Geral de Proteção de Dados (LGPD) e Acesso Remoto

A proteção dos dados pessoais de aposentados e pensionistas é um compromisso legal e ético do IPMJP.

- **Tratamento adequado:** Acesse e manipule apenas os dados pessoais indispensáveis ao desempenho de suas atribuições profissionais.
- **Sigilo das informações:** É proibido expor, repassar ou utilizar dados de beneficiários para fins particulares ou não autorizados.
- **Acesso Remoto:** Quando autorizado o trabalho em regime remoto/home office, utilize exclusivamente os meios seguros e canais VPN disponibilizados e homologados pela TI do IPMJP.

Notificação de Incidentes, Deveres Principais e Checklist Diário

O que fazer em caso de incidentes?

Caso note qualquer comportamento estranho no computador, perda de equipamento, vazamento de senha ou suspeita de invasão, avise imediatamente ao setor de Suporte de TI ou ao DPO.

Checklist Diário do Servidor

Antes de encerrar seu dia de trabalho, certifique-se:

- Não revelar a ninguém sua senha pessoal.
- Bloquear o computador sempre que me se afastar.
- Não instaar nenhum aplicativo sem autorização prévia da TI.
- Salvar os arquivos nas pastas de rede indicadas.
- Não clicou em links suspeitos no e-mail.
- Não inserir informações sigilosas ou dados de beneficiários em IAs.
- Guardar documentos impressos sensíveis longe de vista.

08

CONTATOS IMPORTANTES

- **Setor de Suporte de TI:** * E-mail: suporte@ipmjp.pb.gov.br
  - Telefone: (83) 3222-1005
- **Encarregado pelo Tratamento de Dados Pessoais (DPO):**
  DPO: Renato Gomes de Lacerda Alves
  - E-mail: renatoalves@ipmjp.pb.gov.br
  - Telefone: (83) 3222-1005
- **Canais Institucionais Adicionais:** * Canal de Ouvidoria e setor IPM-DPO - Departamento de Proteção de Dados no sistema 1DOC.

08

FICHA TÉCNICA E NORMATIVA

- **Base Normativa:** Política de Segurança de Documentos, Informações e Proteção de Dados Pessoais do IPMJP (4ª edição revisada e ampliada, atualizada em 17/07/2026).
- **Elaboração e Publicação:** Instituto de Previdência do Município de João Pessoa (IPMJP).

SEGURANÇA DA INFORMAÇÃO É RESPONSABILIDADE DE TODOS.

IPMJP
INSTITUTO DE PREVIDÊNCIA D
MUNICÍPIO DE JOÃO PESSOA

PREFEITURA JOÃO PESSOA cidade em crescimento

PREFEITURA MUNICIPAL DE JOÃO PESSOA
Léo Bezerra
PREFEITO

INSTITUTO DE PREVIDÊNCIA DO MUNICÍPIO DE JOÃO PESSOA
Caroline Ferreira Agra
SUPERINTENDENTE