
# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

IPREV PBA

2019

**APROVAÇÃO**

Anna Paula Cardoso Ribeiro Araújo – Diretora Presidente

Bruna Greice da Silva Assing - Diretora Administrativa e Financeira

Carlos Renato Simões Avelar - Diretor Secretário e de Seguridade

Raquel Duarte Nunes Oliveira - Conselheira Fiscal

Cláudia Regina Pinto – Conselheira Fiscal

Marlúcia Rodrigues Teixeira - Conselheira Fiscal

Ailton Alves da Rocha – Conselheiro Fiscal

## INTRODUÇÃO

A Política de Segurança da Informação é o documento que orienta e estabelece as diretrizes de informação do Instituto de Previdência dos Servidores Públicos Municipais de Paraopeba – IPREV PBA, para sua proteção, prezando pela responsabilidade de todos os usuários e observando a publicidade como preceito geral e o sigilo como exceção.

## OBJETIVOS

1 - Estabelecer diretrizes que permitam aos servidores, membros e fornecedores do IPREV PBA seguirem padrões de comportamento relacionados à segurança da informação, adequados às necessidades operacionais e de proteção legal da autarquia e do indivíduo.

2- Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

3 - Preservar as informações do Instituto quanto à:

a) Integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino.
b) Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados.
c) autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
d) primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

## APLICAÇÕES

As diretrizes estabelecidas deverão ser seguidas por todos os servidores, bem como os prestadores de serviço e membros do Instituto, e se aplicam à informação em qualquer meio ou suporte, dando ciência a cada servidor de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, conforme previsto nas leis brasileiras, obrigando-o a manter-se atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

## PRINCÍPIOS

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pelo IPREV PBA pertence à referida instituição.

As exceções devem ser explícitas e formalizadas em contrato entre as partes. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos servidores para a realização das atividades profissionais.

## REQUISITOS

Para a uniformidade da informação, a Política de Segurança de Informação deverá ser comunicada a todos os servidores da AUTARQUIA a fim de que a política seja cumprida dentro e fora da instituição.

Tanto a Política de Segurança de Informação quanto às normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada ou ainda quando seja editado ato do executivo que altere as normas já publicadas, como o Decreto Municipal 013/2018, que regulamenta na administração direta e indireta do Município de Paraopeba, o acesso à informação.

Qualquer ato ou fato que afete a segurança da informação deverá ser comunicado imediatamente ao gestor.

O IPREV PBA exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus servidores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis, tendo ampla liberdade para aplicar a legislação federal e o Estatuto do Servidor Público Municipal, quando da violação das regras internas de informação.

## DAS RESPONSABILIDADES ESPECÍFICAS DOS SERVIDORES E FORNECEDORES EM GERAL

Conforme previsão no Estatuto dos Servidores Públicos do Município de Paraopeba, servidor público é a pessoa legalmente investida em cargo público, de provimento efetivo ou em comissão, em função gratificada ou em função pública.

Fornecedor, segundo do Código de Defesa do Consumidor, é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes

despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.

Será de inteira responsabilidade cada servidor ou fornecedor todo prejuízo ou dano que vier a causar ao IPREV PBA e/ou a terceiros, em decorrência da não obediência às diretrizes e normas referidas.

## DOS GESTORES DE PESSOAS E/OU PROCESSOS

a) Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os servidores sob a sua gestão.
b) Atribuir aos servidores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança de Informação.
c) Exigir dos servidores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do IPREV PBA.
d) Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

## DOS PRESTADORES DE SERVIÇOS DE SOFTWARES

a) Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
b) Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança de Informações.
c) Os administradores e operadores dos sistemas de computador, podem, pelas características de seus privilégios como usuários, acessar arquivos e dados de outros usuários.
d) Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

e) Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o IPREV PVA.

f) Quando ocorrer movimentação interna dos ativos de tecnologia de informação, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

g) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

h) Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (*logins*) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (*logins*) de terceiros serão de responsabilidade do gestor da área contratante.

i) Garantir, da forma mais rápida possível, o bloqueio de acesso de usuários por motivo de exoneração de servidor, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar as informações do Instituto.

j) Promover a conscientização dos servidores em relação à relevância da segurança da informação para as atividades precípuas ao IPREV PBA.

k) Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

## DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política de Segurança de Informação, o IPREV PBA poderá:

- implantar sistemas de monitoramento nos locais de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação dos seus membros;

- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

## CORREIO ELETRÔNICO

O objetivo desta norma é informar aos servidores do IPREV PBA quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do IPREV PBA é para fins corporativos e relacionados às atividades do servidor dentro da instituição, sendo proibido o uso do correio eletrônico para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o IPREV PBA vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário dessa informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando o IPREV PBA estiver sujeito a algum tipo de investigação.
- produzir, transmitir ou divulgar mensagem que:

1. contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do IPREV PBA;
2. contenha ameaças eletrônicas;
3. contenha arquivos com código executável ou qualquer outra extensão que represente um risco à segurança;
4. vise obter acesso não autorizado a outro computador, servidor ou rede;

5. vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

6. vise burlar qualquer sistema de segurança;

7. vise vigiar secretamente ou assediar outro usuário;

8. vise acessar informações confidenciais sem explícita autorização do proprietário;

9. vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

10. inclua imagens criptografadas ou de qualquer forma mascaradas;

11. tenha conteúdo considerado impróprio, obsceno ou ilegal;

12. seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

13. contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

14. tenha fins políticos locais ou do país (propaganda política);

15. inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

## INTERNET

Todas as regras atuais do IPREVPBA visam basicamente o desenvolvimento de um comportamento eminentemente ético (Código de Ética do IPREV PBA) e profissional do uso da internet. Embora a conexão direta e permanente da rede da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria (CONTROLE INTERNO). Portanto, o IPREV PBA, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet,

estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O IPREV PBA, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos administrativo, civil e criminal.

O uso de sites de notícias ou de serviços, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos, e seja site de caráter informativo, orientativo.

Apenas os servidores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à Lei de Acesso à Informação, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais federais e municipais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, ou qualquer outra tecnologia correlata que venha surgir na internet.

Os servidores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades no IPREV PBA e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Os servidores não poderão em hipótese alguma utilizar os recursos do IPREV PBA para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Servidores com acesso à internet não poderão efetuar upload de qualquer software licenciado ao IPREV PBA ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os servidores não poderão utilizar os recursos do IPREV PBA para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.Não é permitido acesso a sites de proxy.

## IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o IPREV PBA e/ou terceiros.

Todos os dispositivos de identificação utilizados no IPREV PBA, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma única pessoa física.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir *login* de uso compartilhado por mais de um colaborador, a responsabilidade perante o IPREV PBA e a legislação será dos usuários que dele se utilizarem.

Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

## COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos servidores são de propriedade do IPREV PBA, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um servidor do Presidente do Instituto ou de alguém que ele determinar.

Documentos imprescindíveis para as atividades dos servidores da instituição deverão ser salvos em drives de rede.

**No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:**

- Os servidores devem informar qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por profissional competente contratado para o serviço.
- O servidor deverá manter a configuração do equipamento, seguindo os devidos controles de segurança
- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pelo IPREV PBA devem ter imediatamente suas senhas padrões (default) alteradas.

**É proibido o uso de computadores no IPREV para:**

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário,
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

## DISPOSITIVOS MÓVEIS

O IPREV PBA deseja facilitar a mobilidade e o fluxo de informação entre seus servidores. Por isso, permite que eles usem equipamentos portáteis.

O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no IPREV PBA, mesmo depois de terminado o vínculo contratual mantido com a instituição. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição ou de propriedade do próprio servidor, constituirá uso indevido do equipamento e infração legal aos direitos autorais da fabricante.

## BACKUP

Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

## DAS DISPOSIÇÕES FINAIS

A segurança, bem como a ética devem ser entendidas como parte fundamental da cultura interna de transparência, de acessibilidade, de controle social da administração pública, em especial, do IPREV PBA, ou seja, qualquer incidente de segurança, ou de desacordo a esta política de segurança, subtende-se como alguém agindo contra o Código de Ética.

FONTE

LEI FEDERAL Nº 12.527/2011

DECRETO MUNICIPAL Nº 013/2018 (PREFEITURA MUNICIPAL DE PARAOPEBA/MG)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ADAPTADA) ACESSO EM *HTTPS://PAULIPREV.SP.GOV.BR/WP-CONTENT/UPLOADS/2019/04/POL%C3%ADTICA-DE-SEGURAN%C3%A7A-DE-INFORMA%C3%A7%C3%A3O-1.PDF*