



**IPMO - Instituto de Previdência  
dos Servidores Públicos do  
Município de Ourinhos**

**RESOLUÇÃO Nº 02, DE 06 DE JUNHO DE 2022**

*Aprova a **Política de Segurança da Informação** do Regime Próprio de Previdência Social - RPPS do Município de Ourinhos.*

**O PRESIDENTE DO CONSELHO DE ADMINISTRAÇÃO DO IPMO**, usando das atribuições que lhe são conferidas por lei, e

**CONSIDERANDO** que a informação é um ativo essencial da organização e precisa ser protegida quanto a eventuais ameaças, preservando e minimizando os riscos para a continuidade dos serviços prestados pelo RPPS;

**CONSIDERANDO**, ainda, que a adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante do RPPS, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;

**CONSIDERANDO**, mais, o disposto no Manual do Pró-Gestão;

**CONSIDERANDO**, por fim, a deliberação do Conselho de Administração na reunião extraordinária realizada em 06 de maio de 2022.

**RESOLVE:**

Rua Cambará nº. 1351 - CEP: 19905-000 - Ourinhos/SP  
Telefone / Fax: (14) 3603 1900  
e-mail: ipmo@ipmo.ourinhos.sp.gov.br

Página 1 de 11

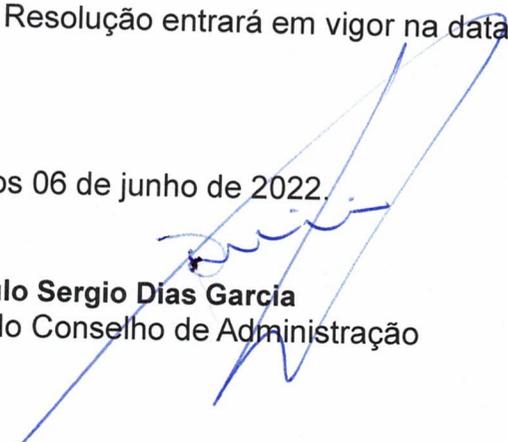


**IPMO - Instituto de Previdência  
dos Servidores Públicos do  
Município de Ourinhos**

**Art. 1º** Fica instituída a **Política de Segurança da Informação** do Regime Próprio de Previdência Social - RPPS do Município de Ourinhos, na forma do Anexo Único desta Resolução.

**Art. 2º** Esta Resolução entrará em vigor na data de sua publicação.

Ourinhos, aos 06 de junho de 2022.

  
**Paulo Sergio Dias Garcia**  
Presidente do Conselho de Administração

2

  
**João Marcelo Martelozo**

  
**Danilo Leopoldino**

  
**Antônio Francisco Robles**

  
**Marcio Alessandre Messias de Souza**

  
**Rubens Gonçalves dos Santos**

  
**Fernando Gonçalves Marconi dos Santos**



**IPMO - Instituto de Previdência  
dos Servidores Públicos do  
Município de Ourinhos**

**ÍNDICE**

CAPÍTULO I - OBJETIVOS DA PSI .....	4
CAPÍTULO II - APLICAÇÕES DA PSI .....	4
CAPÍTULO III - DAS RESPONSABILIDADES ESPECÍFICAS .....	5
CAPÍTULO IV - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE .....	6
CAPÍTULO V - CORREIO ELETRÔNICO .....	6
CAPÍTULO VI - INTERNET .....	7
CAPÍTULO VII - COMPUTADORES E OUTROS DISPOSITIVOS .....	9
CAPÍTULO VIII - IDENTIFICAÇÃO E CONTROLE DE ACESSO .....	10
CAPÍTULO IX - PROCEDIMENTOS DE CONTINGÊNCIA .....	10

*Manu*  
*JR*  
*fm*



## IPMO - Instituto de Previdência dos Servidores Públicos do Município de Ourinhos

### CAPÍTULO I OBJETIVOS DA PSI

**Art. 1º** A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do IPMO para a proteção dos ativos de informação e a responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da Autarquia e por todos os colaboradores e prestadores de serviço que tenham acesso às informações de propriedade do RPPS.

**Art. 2º** Constitui objetivo da PSI:

- I - estabelecer diretrizes que permitam aos colaboradores e fornecedores do IPMO seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e do indivíduo;
- II - nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento; e
- III - preservar as informações do IPMO quanto à:
  - a) integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
  - b) confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas; e
  - c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

### CAPÍTULO II APLICAÇÕES DA PSI

Rua Cambará nº. 1351 - CEP: 19905-000 - Ourinhos/SP  
Telefone / Fax: (14) 3603 1900  
e-mail: ipmo@ipmo.ourinhos.sp.gov.br

Página 4 de 11

*Marcio*  
*D.R.*  
*ipm*



**Art. 3º** As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

**Parágrafo único.** É obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

### **CAPÍTULO III DAS RESPONSABILIDADES ESPECÍFICAS**

5

**Art. 4º** Entende-se por colaborador toda e qualquer pessoa física, contratada no regime estatutário, CLT ou temporário, e os prestadores de serviço, contratados por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora do IPMO.

**§ 1º** Os colaboradores deverão:

- I - manter sigilo das informações do IPMO;
- II - zelar pelos ativos de informação do IPMO, sejam eles físicos (processos, documentos e outros) ou digitais (arquivos, sistemas e outros); e
- III - seguir as diretrizes e recomendações da Superintendência quanto ao uso, divulgação e descarte de dados e informações.

**§ 2º** Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao RPPS e/ou a terceiros, em decorrência da



não obediência às diretrizes e normas aqui referidas.

#### **CAPÍTULO IV DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE**

**Art. 5º** Para garantir as regras mencionadas neste documento, o IPMO poderá:

I - implantar sistemas de monitoramento nas estações 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;

II - tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação do superior hierárquico;

III - realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade; e

IV - instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

6

#### **CAPÍTULO V CORREIO ELETRÔNICO**

**Art. 6º** O uso do correio eletrônico do IPMO é para fins corporativos e relacionados às atividades do colaborador usuário da Autarquia, sendo terminantemente proibido:

I - enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Autarquia;

II - enviar mensagem por correio eletrônico usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

III - enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o RPPS vulneráveis a ações civis ou criminais;



- IV - divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- V - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas; e
- VI - apagar mensagens pertinentes de correio eletrônico quando o IPMO estiver sujeito a algum tipo de investigação.

#### **CAPÍTULO VI INTERNET**

**Art. 7º** Exige-se dos colaboradores comportamento ético e profissional com o uso da internet disponibilizada pelo IPMO.

7

**Art. 8º** Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do IPMO, 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.

**§ 1º** Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria, tendo o IPMO, em total conformidade legal, o direito de monitorar e registrar todos os acessos a ela.

**§ 2º** Qualquer alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador



e ao respectivo superior hierárquico.

§ 3º O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a Autarquia cooperará ativamente com as autoridades competentes.

§ 4º A ausência de bloqueio de sites e serviços na internet pelos mecanismos de proteção estabelecidos pelo IPMO não valida seu acesso, devendo ser observadas as restrições estabelecidas pela PSI, pelas regras do Estatuto do Servidor e outras regras aplicáveis ao exercício do cargo ou prestação de serviços.

8

**Art. 9º** Somente os colaboradores que estão devidamente autorizados a falar em nome do RPPS para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

**Art. 10.** Apenas os colaboradores autorizados pela Autarquia poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

**Art. 11.** É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou gravação por meio de qualquer recurso, de materiais de cunho sexual.

**Art. 12.** Os colaboradores não poderão utilizar os recursos do IPMO para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.



**Art. 13.** As regras aqui definidas se aplicam no uso de computadores e outros dispositivos de propriedade do IPMO, bem como a dispositivos particulares dos usuários que estiverem conectados à internet do Instituto (cabeados ou sem fio).

#### **CAPÍTULO VII COMPUTADORES E OUTROS DISPOSITIVOS**

**Art. 14.** Os computadores disponibilizados pelo IPMO aos colaboradores, constituem instrumento de trabalho para execução das atividades de negócio do Instituto.

§ 1º Cada colaborador deve zelar para segurança e bom uso dos equipamentos, reportando à área competente qualquer incidente que tenha conhecimento.

§ 2º Em caso de mau uso, ou uso em desacordo com as instruções desta norma, o colaborador poderá ser responsabilizado.

§ 3º Os computadores deverão ser providos de aplicativos contra vírus e outras pragas virtuais que possam comprometer a segurança ou a integridade dos dados.

**Art. 15.** A rede de computadores do IPMO deverá ser protegida com:

I - Solução de segurança tipo *firewall*, que implemente regras e instruções para garantir que somente a recepção ou envio de dados autorizados sejam trafegados pela rede; e

II - Sistema de proteção para o acesso à internet (*proxy*), que implemente



regras e instruções que impeçam o acesso a sites e recursos da internet que possam prejudicar a integridade ou a segurança da rede e dos dados armazenados.

### **CAPÍTULO VIII IDENTIFICAÇÃO E CONTROLE DE ACESSO**

**Art. 16.** Para o acesso aos recursos tecnológicos do IPMO será exigido, sempre que possível, identificação e senha exclusiva de cada colaborador, permitindo assim o controle de acesso.

10

§ 1º É proibido o compartilhamento de login entre os colaboradores.

§ 2º Recomenda-se como boa prática de segurança que, ao realizar o primeiro acesso ao ambiente de rede local, o usuário seja direcionado a trocar imediatamente a sua senha.

§ 3º 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.

§ 4º Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

### **CAPÍTULO IX PROCEDIMENTOS DE CONTINGÊNCIA**

**Art. 17.** Para garantir a segurança da informação, deverão ser realizadas

*[Handwritten signatures and initials]*



cópias de segurança de:

- I - sistemas informatizados;
- II - bancos de dados utilizados pelos sistemas adotados no IPMO; e
- III - arquivos (documentos, planilhas etc.).

§ 1º As rotinas de cópia de segurança deverão, sempre que possível, ser realizadas de forma automatizada, em horários pré-definidos, devendo ainda ser realizadas verificações periódicas da sua execução e integridade.

§ 2º O armazenamento das cópias de segurança deverá ser planejado de forma que impeça o acesso a pessoas não autorizadas.

#### **CAPÍTULO X DISPOSIÇÕES FINAIS**

11

**Art. 18.** Na rede de computadores do IPMO, não é permitida instalação de programas sem aquisição da devida licença de uso.

**Art. 19.** Havendo descumprimento da presente Política de Segurança da Informação, poderão ser aplicadas as penalidades previstas no Estatuto dos Funcionários Públicos, no caso de servidor, ou no contrato de prestação de serviços, no caso de contratado.

**Art. 20.** Os casos omissos deverão ser submetidos pela Diretoria Presidente e pelo Conselho de Administração.