



**INSTITUTO DE PREVIDÊNCIA E ASSISTÊNCIA  
DOS SERVIDORES DO MUNICÍPIO DE LINHARES**

**Política de Segurança da  
Informação**

## ÍNDICE

<b>CAPÍTULO I - OBJETIVOS DA PSI.....</b>	<b>3</b>
<b>CAPÍTULO II - APLICAÇÕES DA PSI.....</b>	<b>3</b>
<b>CAPÍTULO III - DAS RESPONSABILIDADES ESPECÍFICAS.....</b>	<b>4</b>
<b>CAPÍTULO IV - DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE</b>	<b>4</b>
<b>CAPÍTULO V - CORREIO ELETRÔNICO .....</b>	<b>4</b>
<b>CAPÍTULO VI - INTERNET.....</b>	<b>5</b>
<b>CAPÍTULO VII - COMPUTADORES E OUTROS DISPOSITIVOS.....</b>	<b>6</b>
<b>CAPÍTULO VIII - IDENTIFICAÇÃO E CONTROLE DE ACESSO .....</b>	<b>7</b>
<b>CAPÍTULO IX – PROCEDIMENTOS DE CONTINGÊNCIA .....</b>	<b>7</b>

## **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 RPPS 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 RPPS 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 RPPS 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**

**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**

**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 RPPS.

§ 1º. Os colaboradores deverão:

I - manter sigilo das informações do RPPS;

II - zelar pelos ativos de informação do RPPS, sejam eles físicos (processos, documentos, etc) ou digitais (arquivos, sistemas, etc); e

III - seguir as diretrizes e recomendações do IPASLI 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 nesta PSI, o IPASLI 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.

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

**Art. 6º.** O uso do correio eletrônico do RPPS 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 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;

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 RPPS 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 IPASLI.

**Art. 8º.** Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade do IPASLI, 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 RPPS, 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. O uso de sites de notícias ou de serviços, por exemplo, 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 de negócio.

**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.** Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no RPPS e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Diretoria.

§ 1º. 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.

§ 2º. Os colaboradores não poderão em hipótese alguma utilizar os recursos do RPPS para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

**Art. 12.** É proibido o acesso, exposição, armazenamento, distribuição, edição, impressão ou gravação por meio de qualquer recurso, de materiais de cunho sexual.

**Art. 13.** Os colaboradores não poderão utilizar os recursos do RPPS para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

**Art. 14.** As regras expostas neste capítulo se aplicam no uso de computadores e outros dispositivos de propriedade do RPPS, bem como a dispositivos particulares dos usuários que estiverem conectados à internet do RPPS (cabeados ou sem fio).

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

**Art. 15.** Os computadores disponibilizados pelo IPASLI aos colaboradores, constituem instrumento de trabalho para execução das atividades de negócio do RPPS.

§ 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.

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

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

§ 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 cópias de segurança de:

- I - Sistemas informatizados;
- II – Bancos de dados utilizados pelos sistemas adotados no IPASLI; e
- III – Arquivos eletrônicos (documentos, planilhas, etc).

§ 1º. As rotinas de cópia de segurança serão estabelecidas por ato do Diretor Presidente, e deverão ser realizadas de forma automatizada, em horários pré-definidos.

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

§ 3º. O processo de realização de cópias de segurança deverá ser devidamente mapeado e manualizado.

§ 4º. Nas contratações que contemplam serviços de armazenamento de dados, a empresa contratada deverá apresentar ao RPPS seu plano de backup / cópias de segurança.



§5º. A área responsável pelos procedimentos de contingência é a área Administrativa e Financeira.

**IVAN SALVADOR FILHO**  
**DIRETOR PRESIDENTE - IPASLI**