



**PORTARIA nº 486, de 19 de dezembro de 2017.**

**Institui e disciplina a Política de Segurança da Informação do Instituto de Previdência Social dos Servidores Públicos Municipais de Santos**

**RUI SÉRGIO GOMES DE ROSIS JÚNIOR**, Presidente do Instituto de Previdência Social dos Servidores Públicos Municipais de Santos - IPREVSANTOS, usando das atribuições que lhe são conferidas pela Lei Complementar nº 592, de 28 de dezembro de 2006 e considerando o disposto no art. 28 do citado diploma legal, resolve:

Art. 1º - Aprovar a Política de Segurança da Informação - PSI, constituída por um conjunto de conceitos, objetivos, princípios, diretrizes, responsabilidades e vedações, disciplinados nos termos dessa Portaria.

## **CAPÍTULO I**

### **DOS PRINCIPAIS CONCEITOS**

Art. 2º - Para efeitos desta política, entende-se:

I – Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa;

II – Segurança da Informação: proteção contra o uso ou acesso não autorizado à informação;



---

III - Princípios da Tecnologia da Informação: são valores e responsabilidades adotadas por uma organização. Convicções que orientam e impõem limites à tomada de decisão em relação a informações, à comunicação dentro e fora da organização, bem como a sua administração;

IV - Governança Digital: é a utilização, pelo setor público, de recursos de Tecnologia da Informação com o objetivo de melhorar a informação e a prestação de serviços por meio digital, aprimorando os níveis de responsabilidade, transparência e efetividade do governo.

## CAPÍTULO II

### DOS OBJETIVOS E PRINCÍPIOS

Art. 3º - A Política de Segurança de Informação tem por objetivos:

I - contribuir para o cumprimento da missão do Instituto e a melhoria contínua dos resultados institucionais em prol da sociedade;

II - prover mecanismos de transparência e gestão das informações;

IV - estabelecer diretrizes a serem seguidas na gestão das informações;

V - definir papéis e responsabilidades.

Art. 4º - As práticas de governança e de gestão da PSI, bem como o uso dos recursos de Tecnologia da Informação, deverão obedecer as seguintes premissas, conhecidas pela sigla “**CIDA**”:

I - **Confidencialidade**: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

II - **Integridade**: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;



## INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES PÚBLICOS MUNICIPAIS DE SANTOS

**III - Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las;

**IV - Autenticidade:** propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria.

Parágrafo único - Além dos princípios elencados no *caput*, deverão ser considerados os princípios fundamentais que regem a Administração Pública Municipal e as boas práticas preconizadas por normas e modelos de referência relativos ao tema.

### **CAPÍTULO III**

#### **DAS DIRETRIZES E RESPONSABILIDADES**

Art. 5º - As regras da "PSI" aqui estabelecidas, assim como aquelas constantes na legislação vigente são de observância obrigatória por todos os colaboradores, sejam funcionários, estagiários ou prestadores de serviços que de alguma forma tenham acesso a quaisquer dados de propriedade deste Instituto. Sua observância é de extrema importância para o adequado monitoramento do ambiente de Tecnologia da Informação, evitando a inadequada exposição de dados e a vulnerabilidade do sistema, a infestação dos programas com códigos maliciosos, utilização de softwares desatualizados, bem como eventuais instalações de softwares suspeitos.

Art. 6º - É de responsabilidade dos responsáveis pela área de Segurança da Informação publicar e promover as versões da PSI, bem como conscientizar os colaboradores em relação à relevância da Segurança da Informação para a o bom funcionamento do Instituto.

Art. 7º - A configuração de todos os equipamentos, ferramentas e sistemas



INSTITUTO DE PREVIDÊNCIA SOCIAL DOS  
SERVIDORES PÚBLICOS MUNICIPAIS DE SANTOS

---

para que fiquem de acordo com as normas estabelecidas pela Política de Segurança da Informação – PSI, é de total responsabilidade do Instituto.

Art. 8º - Cada usuário deverá possuir sua própria senha com os devidos privilégios, composta, preferencialmente, por oito dígitos com ao menos um caractere maiúsculo e um especial. Devendo ser destacado que caso a senha seja compartilhada, a responsabilidade por eventuais alterações, inclusões ou qualquer outra atividade efetivada com a mesma será do detentor original da senha.

Art. 9º - A senha do administrador do sistema só deverá ser solicitada quando estritamente necessária, como no caso, por exemplo, de downloads, manutenção, atualização ou instalação de programas essenciais à elaboração de tarefas. Os privilégios de administrador só serão aceitos e cedidos após análise e validação da causa.

Art. 10 - O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções.

Art. 11 - Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Art. 12 - A padronização deverá ser utilizada com o fim de garantir integridade, melhor acessibilidade e facilidade em todos os processos envolvendo Tecnologia da Informação.



INSTITUTO DE PREVIDÊNCIA SOCIAL DOS  
SERVIDORES PÚBLICOS MUNICIPAIS DE SANTOS

---

Art. 13 – É obrigatória a “salva” regular e programada de arquivos, independente do tamanho.

Art. 14 - As regras atuais de “PSI” estabelecidas pelo IPREVSANTOS tem o objetivo de estimular o desenvolvimento de um comportamento ético e profissional do uso da internet.

Art. 15 - 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.

Art. 16 - O uso da internet será liberado para todo e qualquer colaborador do instituto, devendo, a mesma, ser usada com cautela de forma a não atrapalhar a saúde administrativa e financeira do Instituto, assim como o a qualidade dos serviços prestados.

Art. 17 - Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao IPREVSANTOS ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Art. 18 - É proibida a propagação de qualquer tipo de malware, tais como worm, virus, trojan, ransomware, keylogger, etc., pela rede do instituto. O “click” em links desconhecidos, suspeitos ou sem o devido parâmetro de segurança são propícios à atividade maliciosa.

Art. 19 - O uso de correios eletrônicos é permitido tanto para uso de trabalho



---

quanto pessoal, sendo este último permitido desde que não entre em conflito com o ordenamento do IPREVSANTOS, ou cause qualquer tipo de prejuízo ou constrangimento a este órgão.

Art. 20 - Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o Instituto, nem devem ser conectados às redes do Instituto.

#### **CAPÍTULO IV**

#### **DAS VEDAÇÕES**

Art. 21 - O cumprimento das regras estabelecidas pela “PSI” são obrigatórias e sua não observância, além de afetar diretamente o Instituto, acarretará penalidades ao seu infrator.

Art. 22 - São consideradas violações, além daquelas previstas na legislação própria, as seguintes condutas:

- I - Uso ilegal de software;
- II - Introdução (intencional ou não) de malwares;
- III - Tentativas de acesso não autorizado a dados e sistemas;
- IV - Compartilhamento de informações sensíveis do negócio;
- V - Divulgação de informações de clientes e das operações contratadas;
- VI – Instalação de software sem a devida homologação;
- VII – Atualização de software sem o devido acompanhamento.

Art. 23 - São proibidas as seguintes atividades com relação ao uso de e-mails:

- I - Envio de informações privadas do Instituto;
- II - Envio de e-mail usando o nome de outro usuário;



---

III - Envio de spam;

IV - Falsificação de qualquer tipo de informação;

V - Envio de executáveis maliciosos;

VI - Envio de conteúdo pornográfico, ilegal ou obsceno;

VII - Envio de mensagem com o caráter ofensivo, desrespeitoso, degradante, infame, ameaçador entre outros;

VIII - Envio de softwares pirateados, sem a devida licença.

Art. 24 - A alteração de qualquer parâmetro ou regra presente na Política de Segurança da Informação sem a devida autorização será considerada ilegal.

Art. 25 - O uso de qualquer recurso para atividades ilícitas poderá acarretar em ações administrativas e penalidades de acordo com os processos civil e criminal. Assim, site de conteúdos impróprios, de cunho sexual e/ou ilícitos não serão permitidos.

Art. 26 - Ressalte-se que é vedada a captura de tela e divulgação de qualquer informação do instituto para aqueles que não possuem a devida autorização para tal ato. O desvio de conduta pode gerar medidas administrativas e penalidades de acordo com o ordenamento jurídico civil e criminal.

## **CAPÍTULO V**

### **DISPOSIÇÕES FINAIS**

Art. 27 - A salva de arquivos deve ser feita regular e periodicamente por todos os colaboradores do Instituto e em diversos tipos de dispositivos de armazenamento, cabendo ao órgão garantir a obtenção de espaço suficiente para os respectivos arquivos.



INSTITUTO DE PREVIDÊNCIA SOCIAL DOS  
SERVIDORES PÚBLICOS MUNICIPAIS DE SANTOS

---

Art. 28 - Dispositivos móveis ou mídias digitais devem ser conectados com cautela aos computadores, uma vez que podem conter arquivos maliciosos ou as mais variadas espécies de vírus.

Art. 29 - O usuário deverá conhecer a origem dos arquivos digitais utilizados. Caso ocorra download de algum arquivo, de forma repentina, independente da extensão, o mesmo não deverá ser executado.

Art. 30 - Arquivos em geral, mesmo aqueles deletados, ocupam espaço em disco, por essa razão deverão ser evitadas a criação de cópias desnecessárias ou pessoais em ambiente de trabalho, uma vez que podem comprometer o desempenho do computador, resultando, portanto, em inadequado desempenho do serviço.

Art. 31 – A presente Política de Segurança da Informação deve ser observada e respeitada como parte fundamental da cultura interna do IPREVSANTOS e, por tal razão, qualquer incidente que caracterize infringência às suas normas será ato contra as normas e políticas da Instituição.

Art. 32 – Esta Portaria entra em vigor na data da publicação.

Atenciosamente,

**RUI SÉRGIO GOMES DE ROSIS JR**  
**Presidente**