



## RESOLUÇÃO Nº. 020/2023 CMP – CONSELHO MUNICIPAL DE PREVIDÊNCIA DE SENADOR CANEDO – GO

Aprova Política de  
Segurança de Informação do  
SENAPREV.

**O CONSELHO MUNICIPAL DE PREVIDÊNCIA DE SENADOR CANEDO**  
– **CMP**, Estado de Goiás, instituído por força das disposições da Lei Municipal nº. 767, de 23 de novembro de 2001, usando das atribuições que lhe confere por Lei e;

**CONSIDERANDO** ser necessária o estabelecimento de regras para segurança da informação dentro do SENAPREV;

**CONSIDERANDO** à necessidade difusão da prática de preceitos ligados à segurança da informação;

**CONSIDERANDO** à necessidade do contínuo cuidado com dados de terceiros sob guarda do SENAPREV;

**CONSIDERANDO** o teor da ata de reunião do mês de Julho do ano 2023 do Conselho de Previdência do SENAPREV ocorrida em 27/07/2023,

**RESOLVE:**

**APROVAR A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NOS SEGUINTE TERMOS:**

### 1. Introdução

Esta Política de Segurança da Informação estabelece o compromisso do Instituto de Previdência de Senador Canedo, o Regime Próprio de Previdência Social (RPPS) do Município, em proteger as informações sob sua guarda. A política ainda define os princípios básicos de segurança da informação, que são confidencialidade, integridade e disponibilidade, e



estabelece as diretrizes para a proteção e o uso adequado das informações pelos servidores e prestadores de serviço que têm acesso a elas.

## **2. Objetivos**

### **2.1 Proteção das informações**

O principal objetivo desta Política de Segurança da Informação é garantir a proteção das informações sensíveis e críticas do Instituto de Previdência de Senador Canedo contra acesso, divulgação, alteração ou destruição não autorizados.

### **2.2 Garantia da integridade das informações**

Outro objetivo fundamental é assegurar a integridade das informações, ou seja, garantir que elas sejam precisas, confiáveis e completas. Isso inclui a prevenção de qualquer modificação não autorizada nos dados e a manutenção da exatidão das informações armazenadas e processadas pelo RPPS.

### **2.3 Disponibilidade das informações**

Além disso, a política busca garantir a disponibilidade das informações para os usuários autorizados quando necessário. Isso envolve a implementação de medidas adequadas para evitar interrupções no acesso às informações e para garantir sua recuperação em caso de incidentes.

### **2.4 Conformidade regulatória**

Outro objetivo importante é assegurar a conformidade com as leis, regulamentos e normas aplicáveis à segurança da informação, garantindo que o RPPS esteja em conformidade com as obrigações legais e regulatórias relacionadas à proteção de dados e privacidade.

### **2.5 Conscientização e treinamento**

A promoção da conscientização e o treinamento contínuo dos servidores e prestadores de serviço são objetivos adicionais desta política. O

*Handwritten notes:*  
BPO/Divulg  
expus  
NP  
SD



objetivo é garantir que todos os envolvidos compreendam a importância da segurança da informação e estejam equipados com o conhecimento e as habilidades necessárias para implementar as medidas de segurança adequadas.

### 3. Princípios Básicos

#### 3.1 Confidencialidade

O princípio da confidencialidade visa proteger e garantir que determinadas informações só estejam disponíveis para pessoas autorizadas. Para cumprir esse princípio, o Instituto de Previdência de Senador Canedo e seus colaboradores devem:

- a) Com base em seu nível de sensibilidade das informações, definir o acesso apenas para aqueles que têm autorização;
- b) Implementar controles de acesso adequados, como autenticação, para garantir que apenas pessoas autorizadas possam acessar as informações;
- c) Garantir que as informações confidenciais não sejam divulgadas ou compartilhadas com terceiros não autorizados;

#### 3.2 Integridade

O princípio da integridade visa garantir a exatidão das informações e dos métodos de processamento. Para garantir a integridade das informações, o Instituto de Previdência de Senador Canedo e seus colaboradores devem:

- a) Implementar mecanismos de controle para evitar a modificação não autorizada ou não intencional das informações;
- b) Utilizar técnicas de validação de dados e mecanismos de verificação para garantir a precisão e a confiabilidade das informações;
- c) Manter registros de auditoria e logs para rastrear as alterações nas informações e identificar possíveis incidentes de segurança nos sistemas de gestão.

#### 3.3 Disponibilidade

*BR/Canedo*  
*após*  
*M. P.*



O princípio da disponibilidade visa garantir que os usuários autorizados e os interessados tenham acesso às informações quando necessário. Para garantir a disponibilidade das informações, o Instituto de Previdência de Senador Canedo e seus colaboradores devem:

- a) Implementar medidas adequadas de redundância e tolerância a falhas para evitar interrupções no acesso às informações;
- b) Realizar backups regularmente e testar a capacidade de recuperação dos dados;
- c) Estabelecer procedimentos de resposta a incidentes para mitigar os impactos de eventos adversos na disponibilidade das informações.

#### **4. Responsabilidades**

##### **4.1 Diretoria Executiva**

A Diretoria Executiva do Instituto de Previdência de Senador Canedo é responsável por:

- a) Estabelecer e revisar regularmente as políticas, normas e procedimentos de segurança da informação;
- b) Promover uma cultura de segurança da informação e garantir a alocação adequada de recursos para sua implementação;
- c) Definir papéis e responsabilidades claras para a segurança da informação.

##### **4.2 Responsável pela Segurança da Informação**

O Gestor do Instituto de Previdência será o responsável pela segurança da informação, devendo:

- a) Desenvolver, implementar e manter as políticas, normas e procedimentos de segurança da informação;
- b) Monitorar a conformidade com as políticas de segurança da informação e realizar auditorias regulares;
- c) Identificar e avaliar riscos de segurança da informação e propor medidas para mitigá-los;

*BRUNO* *expans* *[assinatura]*



- d) Manter-se atualizado sobre as melhores práticas de segurança da informação e as ameaças emergentes;
- e) Promover a conscientização e o treinamento em segurança da informação.

#### **4.3 Servidores e Prestadores de Serviço**

Os servidores e prestadores de serviço do Instituto de Previdência de Senador Canedo são responsáveis por:

- a) Cumprir as políticas, normas e procedimentos de segurança da informação;
- b) Proteger as informações confidenciais e sensíveis contra acesso não autorizado;
- c) Utilizar as informações apenas para fins autorizados e dentro dos limites definidos em suas atribuições;
- d) Relatar quaisquer incidentes ou violações de segurança da informação ao responsável pela segurança da informação;
- e) Participar de treinamentos regulares de segurança da informação e estar atualizado sobre as melhores práticas.

#### **5. Conscientização e Treinamento**

O Instituto de Previdência de Senador Canedo promoverá a conscientização sobre a segurança da informação por meio de treinamentos regulares e campanhas de sensibilização. Os treinamentos visam garantir que todos os colaboradores compreendam as políticas e os procedimentos de segurança da informação, bem como as melhores práticas para proteger as informações do RPPS.

#### **6. Revisão e Atualização**

Esta Política de Segurança da Informação será revisada periodicamente para garantir sua eficácia contínua e será atualizada conforme necessário para refletir as mudanças nas ameaças, nas regulamentações e nos requisitos do RPPS.

*Handwritten signature*

*Handwritten signature*



## 7. Controles de Acesso

Cabe ao Responsável pela Segurança da Informação:

- Implementar autenticação forte para acessos aos sistemas, como o uso de senhas complexas, autenticação de dois fatores e tokens de segurança.
- Definir níveis de acesso apropriados para diferentes funções e responsabilidades.
- Monitorar e revisar regularmente as permissões de acesso para garantir que estejam alinhadas com as necessidades atuais.

## 8. Política de Senhas:

O Responsável pela Segurança da Informação deverá:

- Exigir o uso de senhas fortes e regularmente atualizadas.
- Implementar a política de troca de senhas regularmente.
- Orientar os usuários a não utilizar senhas compartilhadas.

## 9. Proteção de Dados Pessoais:

O Responsável pela Segurança da Informação deverá garantir o cumprimento das leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados).

## 10. Backup e Recuperação de Dados:

Com relação aos Backups e a recuperação de dados, o Instituto de Previdência deverá:

- Realizar backups regulares de todos os dados importantes.
- Armazenar backups em locais seguros, preferencialmente fora das instalações do Instituto.
- Testar regularmente a restauração de dados a partir dos backups para garantir que o processo seja eficaz.

*Handwritten signature and initials in blue ink.*



## 11. Segurança Física

No que atine à segurança física de dados o Instituto de Previdência deverá:

- Controlar o acesso físico a áreas restritas do Instituto, como a sala de atendimento do RPPS, por meio de fechaduras ou outras medidas de segurança apropriadas.
- Garantir a devida proteção de documentos físicos, como armários trancados para arquivamento seguro.
- Não deixar documentos com dados pessoais dos segurados disponibilizados, com livre acesso na repartição do Instituto.

## 12. Conscientização e Treinamento

O Instituto deverá:

- Realizar treinamentos regulares para conscientizar os funcionários sobre boas práticas de segurança da informação.
- Fornecer orientações sobre o manuseio seguro de documentos físicos, como evitar deixá-los desacompanhados em áreas de acesso público.
- Estabelecer procedimentos claros para relatar incidentes de segurança e fornecer canais de comunicação adequados para isso.

## 13. Proteção de Documentos Físicos:

Sobre a proteção dos Documentos Físicos, o Instituto deverá:

- Armazenar documentos físicos confidenciais em armários trancados ou cofres com acesso restrito.
- Implementar um sistema de controle de registros para acompanhar a movimentação dos documentos, incluindo registros de retirada e devolução.
- Estabelecer procedimentos para a destruição segura de documentos físicos, incluindo o uso de trituradores ou serviços especializados de destruição.

## 14. Aplicação



Esta Política de Segurança da Informação é aplicável a todos os servidores e prestadores de serviço do Instituto de Previdência de Senador Canedo que têm acesso as informações do RPPS. O não cumprimento desta política pode resultar em medidas disciplinares, conforme estabelecido nas políticas internas do RPPS.

Esta Política de Segurança da Informação entra em vigor a partir da data de sua aprovação pela Diretoria Executiva do Instituto de Previdência de Senador Canedo.

**CONSELHO MUNICIPAL DE PREVIDÊNCIA**, aos 27 dias do mês de julho de 2023.

**BERONICIA PEREIRA DE OLIVEIRA**  
Representante do Poder Executivo  
Membro Titular

**VALCIR MARTA BATISTA**  
Representante do Poder Executivo  
Membro Suplente

**CLÁUDIA DUTRA JORGE**  
Representante do Poder Executivo  
Membro Titular

**ÂNGELA ROSA NUNES SILVA**  
Representante do Poder Executivo  
Membro Suplente

**ROBSON HENRIQUE DE OLIVEIRA**  
Representante do Poder Legislativo  
Membro Titular

**CLEIDE PAULA RIBEIRO ARAÚJO**  
Representante do Poder Legislativo  
Membro Suplente

**WILSON CARLOS DA SILVA**  
Representante dos Segurados Ativos  
Membro Titular

**ANDREIA EUZI DE PAULA SOUZA**  
Representante dos Segurados Ativos  
Membro Suplente

**ELÉCIO INOCÊNCIO TELES**  
Representante dos Segurados Inativos  
Membro Titular

**NADIR SIQUEIRA BATISTA**  
Representante dos Segurados Inativos  
Membro Suplente