PARANA
PREVIDÊNCIA

PROTOCOLO INTEGRADO DO ESTADO
Fls. 15
Mov. 6

# Resolução nº 147/ 2023

## Conselho Diretor

Dispõe sobre a Política
De Segurança da Informação.

O Conselho Diretor, no uso das atribuições que lhe confere o art. 29, do Estatuto da PARANAPREVIDÊNCIA, aprovado pelo Decreto Estadual nº 4.961, de 02 de julho de 2020, conforme deliberação contida na Ata da Vigésima Oitava Reunião, realizada em 19 de julho de 2023,

Resolve,

Aprovar a Política de Segurança da Informação, a qual visa estabelecer um conjunto de práticas, medidas e controles implementados para proteger os ativos de informação de uma organização contra ameaças e garantir a confidencialidade, integridade e disponibilidade desses ativos, conforme segue anexa e consta do protocolo n. 20.677.080-5.

Publique-se no Portal da Transparência da PARANAPREVIDÊNCIA.

Curitiba, 19 de julho de 2023.

Felipe José Vidigal dos Santos
Diretor-Presidente

PARANA
PREVIDÊNCIA

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

**JULHO/2023**

## 1. DEFINIÇÃO DE INFORMAÇÃO

Para os fins desta Política de Segurança da Informação, a informação pode ser definida como sendo dados processados ou não processados, documentos, registros, arquivos ou qualquer outra forma de mídia que contenha dados que tenham valor para a organização e precisem ser protegidos contra acesso não autorizado, modificação, divulgação ou destruição indevida.

A informação nesta Política de segurança da informação é considerada um ativo e pode incluir dados confidenciais, segredos comerciais, propriedade intelectual, informações pessoais identificáveis (PII), informações financeiras, estratégias de negócios, entre outros.

## 2. DEFINIÇÃO DE SEGURANÇA DA INFORMAÇÃO

Segurança da informação é um conjunto de práticas, medidas e controles implementados para proteger os ativos de informação de uma organização contra ameaças e garantir a confidencialidade, integridade e disponibilidade desses ativos.

## 3. OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O objetivo da Política de Segurança da Informação da PARANAPREVIDÊNCIA é proteger informações valiosas para a organização, mitigando riscos e garantindo a continuidade dos negócios, de forma a garantir disponibilidade, integridade, confidencialidade, legalidade e autenticidade da informação utilizada para atingimento dos objetivos organizacionais, sendo:

• **Disponibilidade**: garantia de que os ativos das as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

• **Integridade**: garantia de que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais;

• **Confidencialidade**: garantia de que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

• **Legalidade**: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos.

• **Autenticidade**: validação da autorização do usuário para acessar sistemas, informações etc. Isso ocorre por meio da solicitação de senhas, logins ou biometria.

## 4. EXECUÇÃO DA POLÍTICA

A presente Política será executada pelos seguintes meios:

- **Informativo:** Divulgação da Política, elaboração de manuais e normas tratando de assuntos pontuais relacionados, esclarecimento de dúvidas, orientações sobre boas práticas, notificação às pessoas sobre ações identificadas como desconformes em relação à Política, campanhas de conscientização e comunicação de ocorrências às autoridades competentes.

- **Delimitativo:** Discriminação dos direitos, deveres e limitações no uso dos recursos utilizados no manuseio das informações.

- **Prático:** Disponibilizar recursos com segurança, monitorar o uso, aplicar ações de correção e reportar as ocorrências às autoridades competentes.

## 5. ABRANGÊNCIA DA POLÍTICA

Esta Política aplica-se aos Conselheiros, Diretores, empregados, servidores cedidos, estagiários e prestadores de serviços da PARANAPREVIDÊNCIA e abrange diretrizes, procedimentos e práticas que visam proteger os ativos de informação da organização contra ameaças e riscos, dentro ou fora do seu ambiente. Ela abrange a proteção de dados confidenciais, dados pessoais, informações financeiras, sistemas de TI, infraestrutura de rede e outros ativos relevantes.

## 6. DIRETRIZES GERAIS

Todas as partes envolvidas nesta Política devem reconhecer e valorizar os ativos de informação utilizados pela PARANAPREVIDÊNCIA como bens de grande importância para a organização. Esses ativos são recursos críticos e indispensáveis para alcançar adequadamente os objetivos institucionais.

A segurança da informação é uma responsabilidade compartilhada por todos os funcionários e partes envolvidas. É fundamental que todos os colaboradores compreendam a relevância e responsabilidade da proteção dos ativos de informação e adotem práticas de segurança adequadas para garantir a integridade, confidencialidade e disponibilidade das informações.

Os abrangidos por esta Política têm permissão para utilizar as informações obtidas por meio dos recursos disponibilizados pela PARANAPREVIDÊNCIA exclusivamente para o cumprimento de suas funções dentro da instituição.

A PARANAPREVIDÊNCIA contará com uma área responsável pela Gestão da Segurança da Informação, que terá a responsabilidade de planejar, implementar e aprimorar continuamente os controles relacionados à segurança da informação, papel fundamental na proteção dos ativos de informação.

A Coordenadoria de TI terá como responsabilidade e atribuição, a implementação de medidas de segurança do ambiente computacional, monitoramento e detecção de incidentes, gerenciamento de identidades de acesso e avaliação de riscos e conformidade.

Os dados pessoais manuseados pelos abrangidos por esta Política devem ser tratados em estrita observância à Lei Geral de Proteção de Dados Pessoais, respeitando-se o direito à privacidade das pessoas naturais.

Todas as ações relacionadas à segurança da informação levarão em conta as disposições da Lei de Acesso à Informação, para que se observem os Princípios da Transparência.

Esta Política está consonante às disposições contidas no Código de Ética da Instituição, relacionadas à Segurança da Informação e Proteção de Dados Pessoais, e às previstas na Política de Privacidade de Dados Pessoais.

## 7. TRATAMENTO DA INFORMAÇÃO

### 7.1. Classificação e Guarda da Informação.

A organização da informação gerada nos processos de trabalho de todas as áreas da Instituição é de responsabilidade do gestor de cada unidade de trabalho.

Cabe ao gestor de cada unidade de trabalho cercar-se de todos os cuidados visando a segurança da informação utilizada nos processos de trabalho de sua unidade.

Compete também ao gestor de cada unidade de trabalho zelar para que a guarda e a integridade das informações sejam garantidas, bem como, determinar a eliminação daquelas que já não são mais utilizadas, recorrendo à área de informática quando se tratarem de informações armazenadas em meio computacional.

As informações sigilosas da organização são classificadas de acordo com seu grau de sigilo como: **“ultrassecretas”; “secretas”;** ou **“reservadas”**, em

conformidade com as disposições contidas na Lei Federal 12.527/2011 e Decreto PR 10.285/2014. Os prazos máximos da classificação de sigilo são os estabelecidos na legislação citada.

Outras informações, não sigilosas, podem ser classificadas como **"restritas"** com prazo de classificação de até cem anos.

A relação das informações classificadas como sigilosas ou restritas será publicada no espaço da transparência institucional, acessível por meio do site da PARANAPREVIDÊNCIA.

A classificação nos graus de sigilo secreto e reservado é de competência do Diretor-Presidente, podendo haver delegação para a classificação no grau "reservado".

Ao Conselho Diretor cabe a ratificação das classificações das informações, independentemente do grau de classificação.

As informações não classificadas como restritas ou sigilosas, são consideradas públicas podendo ser acessadas por meio do site da PARANAPREVIDÊNCIA ou Portal da Transparência Institucional.

As informações manuseadas pelos agentes da PARANAPREVIDÊNCIA não devem ser armazenadas ou de alguma forma manuseadas em ambiente digital ou físico não previsto em legislação aplicável ou autorizado pela organização. Igualmente, não devem ser utilizados equipamentos, acessórios, programas, sistemas ou outros recursos obtidos externamente sem as devidas licenças dos respectivos proprietários e sem a autorização da Coordenadoria de Tecnologia da Informação.

A organização adotará providências para que as informações detidas individualmente por empregados sejam compartilhadas de forma a disseminar o conhecimento e evitar a perda da informação.

### 7.2. Acesso a Informações Contendo Dados Pessoais e Dados Pessoais Sensíveis

Os Dados Pessoais, independente da sua classificação, dos quais a PARANAPREVIDÊNCIA detenha a posse em quaisquer meios, suportes ou formatos, processados ou não, têm seus acessos restritos aos titulares dos Dados Pessoais e aos agentes internos vinculados à PARANAPREVIDÊNCIA, no exercício das suas atribuições institucionais.

As exceções ao disposto no parágrafo anterior são as previstas na Lei Geral de Proteção de Dados Pessoais e os acessos disponibilizados serão feitos mediante o atendimento de todos os requisitos contidos na referida Lei e em normas internas, além do preenchimento obrigatório de Termo de Recebimento, Ciência, Compromisso e Responsabilidade de Dados Pessoais.

Todos os empregados da PARANAPREVIDÊNCIA assinarão Termo de Compromisso de Confidencialidade de Dados Pessoais, com vistas à conscientização sobre o manuseio de dados pessoais.

A organização contará com um Encarregado pelo Tratamento de Dados Pessoais visando facilitar o processo de orientação, aculturamento e implementação da Lei Geral de Proteção de Dados Pessoais.

### 7.3. Recursos Computacionais

Os Recursos Computacionais adquiridos e disponibilizados pela Coordenadoria de Tecnologia da Informação deverão ser sempre originais, oficiais e licenciados, não sendo admitidas versões “pirata”.

A Coordenadoria de TI deve estabelecer diretrizes para manutenção regular de sistemas e software, incluindo a aplicação de patches de segurança, a atualização de versões de software e a utilização de soluções de segurança atualizadas.

As aquisições de quaisquer recursos de informática, com vistas ao manuseio de informações, deverão ser executadas em conformidade com a legislação em vigência, inclusive no que se refere a pré-avaliação por parte do **Conselho Estadual de Tecnologia da Informação e Comunicação do Paraná – CETIC-PR**, criado pela Lei Estadual nº 17.480 de 10/01/2013 e regulamentado pelo Decreto Estadual nº 6.063 de 31/01/2017, Conselho este que possui caráter consultivo, normativo e deliberativo e tem como finalidade regulamentar, promover a implantação, gerenciar e acompanhar ações relativas à utilização da TIC no âmbito do Sistema Estadual de Informações de Governo – Paraná.

A PARANAPREVIDÊNCIA contará, mediante a celebração de contrato de prestação de serviços, com os serviços da Companhia de Tecnologia da Informação e Comunicação do Paraná – Celepar, ou outra prestadora de serviços, para fins de armazenamento de informações digitais, manutenção e desenvolvimento de soluções de sistemas para fins da execução dos seus processos de trabalho.

A(s) prestadora(s) de serviços, mediante previsão em contrato, deverão tomar todas as providências e se responsabilizar pela segurança da informação manuseada.

São recursos de TI qualquer equipamento, objeto ou método capaz de reter ou transmitir informação, como exemplo:

- Computadores Desktop, notebook;
- Periféricos: teclado, mouse, impressora, câmeras, gravadores de áudio, etc.;
- Dispositivos de armazenamento e suas mídias;
- Equipamentos de rede, servidores;
- Equipamentos de telecomunicação pessoal: telefone, smartphone, rádio;
- Programas de computador e sistemas;
- Impressos e anotações;
- Os procedimentos adotados para a aquisição da informação;
- Serviços de telecomunicações como telefonia e internet;
- A própria informação.

Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo único a realização de atividades profissionais relacionadas à PARANAPREVIDÊNCIA.

A proteção do recurso de TI de uso individual é de responsabilidade do próprio usuário.

É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade das informações contidas nele.

As comunicações devem ser escritas em linguagem profissional, não devem comprometer a imagem da Instituição, não podem ser contrárias à legislação vigente e nem aos princípios contidos no Código de Ética e Conduta da PARANAPREVIDÊNCIA.

### 7.4. Tratamento, Disponibilização e Utilização dos Recursos Computacionais

Os recursos de Tecnologia da Informação, disponibilizados para os usuários, têm como objetivo único a realização de atividades profissionais relacionadas à PARANAPREVIDÊNCIA.

É de responsabilidade de cada usuário a proteção do recurso de TI de uso individual, devendo o mesmo assegurar a integridade do equipamento, a confidencialidade e disponibilidade das informações contidas nele.

Serão elaboradas, pela Coordenadoria de Tecnologia da Informação, normas internas com vistas a regulamentar o controle de acessos físicos e lógicos, a realização de cópias de segurança e Banco de Dados, a utilização de Internet

Corporativa e de correio eletrônico, computadores e outros recursos tecnológicos, bem como, a liberação de acessos ao sistema tramitador e-protocolo, as permissões e senhas de acesso e outras voltadas ao ambiente computacional, que se façam necessárias para a execução desta Política de Segurança da Informação.

### 7.5. Monitoramento e controle da utilização dos Recursos Computacionais

A Coordenadoria de Tecnologia da Informação exercerá o monitoramento e o controle sobre todo o ambiente computacional da PARANAPREVIDÊNCIA e produzirá relatórios de acesso aos recursos computacionais. Em constatando a necessidade, tomará providências para garantir a segurança da informação, tais como: bloquear transmissão de dados de aplicativos; bloquear usuários com padrão de utilização prejudicial a algum recurso; desinstalar aplicativos não autorizados por meio remoto ou local; bloquear ou desativar qualquer dispositivo ou equipamento que prejudique a integridade das informações; promover ações de conscientização sobre segurança da informação e elaborar relatório contendo parecer técnico sobre incidentes no ambiente computacional.

### 7.6. Plano de Contingência para situação de Incidente de Segurança da Informação no ambiente computacional

O Plano de Contingência visa planejar preventivamente as iniciativas a serem adotadas quando de cenários que apresentem risco à continuidade dos serviços essenciais da Instituição.

A PARANAPREVIDÊNCIA deve constituir seu Plano de Contingência, prevendo todos os protocolos de ações para os casos de concretizações de riscos de segurança.

### 7.7. Violações da Política de Segurança da Informação e disposições finais

Implicam em violação desta Política de segurança da informação, qualquer ato que:

a) Envolva a revelação de dados confidenciais/sigilosos;
b) Exponha dados ainda não tratados ou divergentes;
c) Faça uso não autorizado de dados da organização;

d) Exponha a Instituição a possíveis prejuízos de qualquer natureza por meio da exposição de informações;

e) Exponha a Instituição a quaisquer perdas por motivo de mau uso ou guarda indevida de recursos de tecnologia da informação;

f) Envolva o uso de dados para propósitos ilícitos, que venham a violar qualquer lei, regulamento ou outro dispositivo normativo externo ou interno.

Ao tomar ciência desta Política, todos os colaboradores da PARANAPREVIDÊNCIA concordam em não divulgar nenhuma informação institucional a que tiverem acesso, seja por meios lícitos ou não, bem como, garantir a guarda das informações que lhes forem confiadas.