



ESTADO DE ALAGOAS
REGIME PRÓPRIO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE JUNDIÁ
Rua Sebastião Lins de Melo, S/N, Centro - Jundiá - Alagoas
CNPJ: 21.868.680/0001-30 - Email: jundiaprev@hotmail.com

**Instituto Municipal de Previdência dos Servidores do Município de Jundiá –
JUNDIÁPREV**

RESOLUÇÃO Nº 01/2025

**DISPÕE SOBRE A POLÍTICA
DE SEGURANÇA DA
INFORMAÇÃO DO INSTITUTO
MUNICIPAL DE PREVIDÊNCIA
DOS SERVIDORES DO
MUNICÍPIO DE JUNDIÁ -
JUNDIÁPREV.**

O Presidente do Instituto Municipal de Previdência dos Servidores do Município de Jundiá – JUNDIÁPREV, no uso de suas atribuições legais e considerando a necessidade de adequação à Lei Geral de Proteção de Dados, resolve:

Art. 1º - Aprovar a Política de Segurança da Informação constante no Anexo I desta Resolução.

Art. 2º - Todos os colaboradores deverão, em um prazo de 45 dias, aderir a esta Política de Segurança da Informação.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Jundiá/AL, 19 de fevereiro de 2025.


Jeová Antônio da Silva
Diretor Presidente
Portaria nº 25/2023

JEOVA ANTONIO DA SILVA
Presidente
Portaria nº 025/2023

CNPJ: 21.868.680/0001-30 – Email: jundiaprev@hotmail.com

**Instituto Municipal de Previdência dos Servidores do Município de Jundiá –
JUNDIÁPREV**

Anexo I - Política de Segurança da Informação

CAPÍTULO I - DISPOSIÇÕES GERAIS

Art. 1º Esta Resolução estabelece a Política de Segurança da Informação do JUNDIÁPREV, visando garantir a proteção, confidencialidade, integridade e disponibilidade das informações tratadas pelo Instituto.

Art. 2º A Política de Segurança da Informação aplica-se a todos os membros da Diretoria Executiva, servidores, estagiários, membros dos órgãos colegiados, e aos colaboradores que tratam informações no âmbito do JUNDIÁPREV.

CAPÍTULO II - PRINCÍPIOS E DIRETRIZES

Art. 3º A Política de Segurança da Informação do JUNDIÁPREV está pautada nos seguintes princípios:

- I. Confidencialidade: Garantir que as informações sejam acessíveis apenas a pessoas autorizadas.
- II. Integridade: Preservar a exatidão e completude das informações e métodos de processamento.
- III. Disponibilidade: Assegurar que as informações estejam disponíveis para uso quando necessário.
- IV. Responsabilidade: Todos os agentes de tratamento de dados pessoais são responsáveis por garantir a proteção e a correta utilização das informações.

Art. 4º As diretrizes para a implementação da Política de Segurança da Informação são as seguintes:

- I. Classificação de informações: As informações do Instituto deverão ser classificadas conforme o nível de sensibilidade: pública, restrita ou confidencial.

II. Controle de acesso: O acesso às informações será restrito aos colaboradores devidamente autorizados pela Diretoria Executiva.

III. Treinamento e conscientização: Todos os colaboradores deverão receber treinamento básico sobre boas práticas de segurança da informação e proteção de dados pessoais, conforme os princípios da LGPD.

IV. Responsabilidade sobre incidentes: Qualquer incidente de segurança da informação deverá ser imediatamente comunicado ao Presidente, que coordenará as ações corretivas.

CAPÍTULO III - RESPONSABILIDADES

Art. 5º A Diretoria Executiva é responsável por:

I. Definir e aprovar normas e procedimentos complementares de segurança da informação;

II. Monitorar a conformidade da Política de Segurança da Informação;

III. Aprovar o acesso a informações classificadas como restritas ou confidenciais.

Art. 6º Os órgãos colegiados devem:

I. Assegurar que, no exercício de suas funções, os membros dos conselhos tratem as informações conforme esta política;

II. Zelar pelo sigilo e segurança das informações discutidas em suas reuniões.

Art. 7º - As medidas de segurança da informação adotadas deverão observar as seguintes ações mínimas:

I. Senhas fortes e individuais: Cada colaborador deverá utilizar senhas complexas para acessar sistemas e documentos eletrônicos, sendo estas trocadas periodicamente.

II. Backup de dados: Deverá ser realizado backup periódico das informações críticas, com cópias armazenadas em local seguro e, preferencialmente, fora do ambiente principal de trabalho.

III. Controle de acesso a documentos físicos: O acesso aos documentos físicos arquivados deverá ser restrito a pessoas autorizadas pela Diretoria Executiva, e todas as movimentações deverão ser registradas em um controle de entrada e saída.

IV. Descarte seguro de documentos: Documentos físicos que contenham informações sensíveis ou confidenciais deverão ser triturados ou outro método que impeça a recuperação dos dados.

V. Movimentação de documentos físicos: Sempre que necessário o transporte de documentos físicos contendo informações sensíveis, este deverá ser realizado de forma segura, utilizando envelopes ou pastas lacradas e identificadas.

VI. Antivírus e atualizações: O sistema de informática deverá contar com software antivírus atualizado regularmente, bem como a aplicação de atualizações de segurança nos sistemas operacionais e programas utilizados.

VII. Política de uso de dispositivos pessoais: O uso de dispositivos pessoais para acessar ou armazenar informações institucionais deve ser evitado. Caso seja necessário, deverá ser autorizado pela Diretoria Executiva e controlado com medidas adequadas de segurança.

VIII. Controle de mídias removíveis: O uso de pendrives, CDs, e outros dispositivos de armazenamento externo deverá ser minimizado e controlado, permitindo-se apenas quando estritamente necessário, com autorização prévia e garantindo que as mídias estejam limpas de vírus.

IX. Proteção física do arquivo: O arquivo de documentos físicos deverá ser armazenado em um local seguro, com controle de acesso físico, utilizando armários ou salas trancadas para evitar acesso não autorizado.

X. Manutenção de logs de acessos: Os sistemas eletrônicos do Instituto devem manter registros de acessos e alterações realizadas nos dados, permitindo o rastreamento e auditoria de eventuais incidentes.

XI. Treinamento contínuo: Todos os colaboradores deverão participar de treinamentos periódicos sobre boas práticas de segurança da informação e proteção de dados pessoais, de forma a reforçar a importância da segurança.

CAPÍTULO V - DISPOSIÇÕES FINAIS

Art. 8º Esta Política deverá ser revista sempre que houver mudanças significativas na legislação ou nos processos internos do Instituto.

Art. 9º Casos omissos ou situações não previstas nesta Política serão resolvidos pela Diretoria Executiva.

Art. 10º Esta Resolução entra em vigor na data de sua publicação.

Jundiá/AL, 19 de fevereiro de 2025.

Jeová Antônio da Silva
Diretor Presidente
Portaria nº 25/2023

JEOVÁ ANTÔNIO DA SILVA
Presidente
Portaria nº 2023

