



SERVIÇO PÚBLICO FEDERAL  
MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL  
SUPERINTENDÊNCIA DO DESENVOLVIMENTO DO NORDESTE

## **POLÍTICA INSTITUCIONAL Nº 1, DE 31 DE JULHO DE 2026**

### **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SUDENE (POSIN)**

Institui a Política de Segurança da Informação da Superintendência do Desenvolvimento do Nordeste (Sudene) e estabelece diretrizes para a governança, a proteção dos ativos de informação, a privacidade e a proteção de dados pessoais no âmbito da Autarquia.

O Superintendente da Superintendência do Desenvolvimento do Nordeste - SUDENE no uso das atribuições que lhe conferem os incisos IV, art. 19 do Anexo I ao Decreto nº 8.276, de 27 de junho de 2014.

#### **R E S O L V E:**

#### **CAPÍTULO I DAS DISPOSIÇÕES PRELIMINARES**

**Art. 1º** Fica instituída a Política de Segurança da Informação da Superintendência do Desenvolvimento do Nordeste (Sudene), denominada POSIN.

**Art. 2º** A POSIN estabelece princípios, diretrizes, responsabilidades e mecanismos destinados a orientar a governança, a privacidade, a proteção dos dados pessoais e a segurança da informação no âmbito da Sudene.

**Art. 3º** A presente Política constitui instrumento estruturante do Programa de Privacidade e Segurança da Informação (PPSI) da Sudene, contribuindo para a implementação gradual dos controles, das medidas e das diretrizes estabelecidos pelo Framework de Privacidade e Segurança da Informação da Administração Pública Federal.

**Art. 4º** São objetivos da POSIN:

- I. promover a proteção dos ativos de informação da Sudene;
- II. fortalecer a governança da segurança da informação;

- III. apoiar a proteção dos dados pessoais tratados pela instituição;
- IV. apoiar a implementação das medidas previstas no PPSI;
- V. promover a gestão dos riscos relacionados à segurança da informação, à privacidade e à proteção de dados pessoais;
- VI. contribuir para a continuidade dos serviços institucionais;
- VII. fomentar a cultura institucional de segurança da informação.

**Art. 5º** Esta Política aplica-se:

- I. aos servidores públicos;
- II. aos empregados públicos;
- III. aos ocupantes de cargos em comissão;
- IV. aos estagiários;
- V. aos terceirizados;
- VI. aos fornecedores;
- VII. aos prestadores de serviços;
- VIII. a qualquer pessoa física ou jurídica que utilize ou tenha acesso às informações ou aos ativos de informação da Sudene.

## **CAPÍTULO II DOS REFERENCIAIS NORMATIVOS**

**Art. 6º** A implementação desta Política observará:

- I. a Constituição Federal;
- II. a Lei nº 12.527, de 18 de novembro de 2011;
- III. a Lei nº 13.709, de 14 de agosto de 2018;
- IV. a Lei nº 14.129, de 29 de março de 2021;
- V. o Decreto nº 9.203, de 22 de novembro de 2017;
- VI. o Decreto nº 12.572, de 4 de agosto de 2025;
- VII. a Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025;
- VIII. a Instrução Normativa SGD/MGI nº 4, de 14 de janeiro de 2026;
- IX. os normativos expedidos pelo Gabinete de Segurança Institucional da Presidência da República;
- X. os normativos expedidos pela Autoridade Nacional de Proteção de Dados.

## **CAPÍTULO III DOS PRINCÍPIOS**

**Art. 7º** A segurança da informação na Sudene observará os seguintes princípios:

- I. gestão baseada em riscos;
- II. melhoria contínua;
- III. responsabilidade compartilhada;
- IV. transparência;
- V. proporcionalidade;

- VI. proteção desde a concepção;
- VII. proteção por padrão;
- VIII. prestação de contas;
- IX. alinhamento estratégico;
- X. continuidade dos serviços públicos.

#### **CAPÍTULO IV**

##### **DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO**

**Art. 8º** A governança da segurança da informação compreende o conjunto de estruturas, processos e mecanismos destinados a avaliar, direcionar e monitorar iniciativas relacionadas à segurança da informação, privacidade e proteção de dados pessoais.

**Art. 9º** Integram a Estrutura de Governança da Segurança da Informação da Sudene:

- I. a Alta Administração;
- II. o Comitê de Governança Digital (CGD);
- III. o Comitê Gestor de Segurança da Informação (CGSI);
- IV. a Coordenação-Geral de Tecnologia da Informação (CGTI);
- V. a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR);
- VI. o Encarregado pelo Tratamento de Dados Pessoais;
- VII. os gestores das unidades organizacionais.

**Art. 10** Compete à Alta Administração:

- I. promover o alinhamento institucional das ações relacionadas à segurança da informação;
- II. apoiar a implementação desta Política;
- III. acompanhar os riscos estratégicos relacionados à segurança da informação.

**Art. 11** Compete ao Comitê de Governança Digital:

- I. deliberar sobre matérias estratégicas relacionadas à segurança da informação;
- II. acompanhar a implementação do PPSI;
- III. apoiar a priorização institucional das iniciativas relacionadas ao tema.

**Art. 12** Compete ao Comitê Gestor de Segurança da Informação:

- I. assessorar tecnicamente o Comitê de Governança Digital;
- II. analisar propostas normativas;
- III. emitir pareceres técnicos;
- IV. acompanhar a implementação da POSIN.

**Art. 13** Compete à Coordenação-Geral de Tecnologia da Informação:

- I. coordenar iniciativas relacionadas à implementação desta Política;
- II. apoiar tecnicamente as unidades organizacionais;

III. apoiar a implementação do PPSI;

IV. apoiar a gestão de riscos relacionados à segurança da informação.

**Art. 14** As unidades organizacionais são corresponsáveis pela proteção das informações sob sua guarda, uso, custódia ou tratamento.

**Art. 15** As unidades organizacionais colaborarão na produção e disponibilização das informações e evidências necessárias ao acompanhamento dos controles previstos pelo PPSI.

## **CAPÍTULO V DA GESTÃO DE RISCOS**

**Art. 16** A Sudene buscará implementar processo institucional voltado à identificação, análise, avaliação, tratamento e monitoramento dos riscos relacionados à segurança da informação, à privacidade e à proteção de dados pessoais.

**Art. 17** A implementação dos controles previstos nesta Política observará:

I. a gestão de riscos;

II. a disponibilidade orçamentária;

III. a capacidade operacional da instituição;

IV. o planejamento institucional;

V. os ciclos de implementação previstos no PPSI.

## **CAPÍTULO VI DA GESTÃO DOS ATIVOS DE INFORMAÇÃO**

**Art. 18** A Sudene promoverá iniciativas destinadas à identificação, catalogação e gestão dos ativos de informação necessários ao cumprimento de suas competências institucionais.

**Art. 19** A Sudene buscará identificar os responsáveis pelos ativos de informação de acordo com sua criticidade, relevância institucional e estrutura organizacional.

**Art. 20** Poderão ser considerados ativos críticos institucionais, entre outros:

I. sistemas corporativos voltados à gestão administrativa, de incentivos fiscais, de fundos institucionais e demais atividades finalísticas da Sudene.

II. serviços corporativos de identidade digital;

III. serviços corporativos de correio eletrônico;

IV. serviços corporativos de colaboração;

V. bases de dados corporativas.

## **CAPÍTULO VII DO CONTROLE DE ACESSO**

**Art. 21** A Sudene promoverá mecanismos de controle de acesso compatíveis com a criticidade dos ativos de informação e dos serviços institucionais.

**Art. 22** Os acessos deverão observar os princípios da necessidade de conhecimento e do menor privilégio.

**Art. 23** Os critérios e procedimentos relacionados ao controle de acesso poderão ser disciplinados em instrumentos complementares.

## **CAPÍTULO VIII DA PRIVACIDADE E DA PROTEÇÃO DE DADOS PESSOAIS**

**Art. 24** As atividades de tratamento de dados pessoais observarão a legislação vigente e as diretrizes institucionais aplicáveis.

**Art. 25** A Sudene buscará fortalecer continuamente as medidas administrativas e técnicas destinadas à proteção dos dados pessoais tratados em suas atividades.

## **CAPÍTULO IX DA GESTÃO DE INCIDENTES**

**Art. 26** A Sudene promoverá mecanismos destinados à prevenção, tratamento e resposta a incidentes relacionados à segurança da informação.

**Art. 27** A ETIR constitui a estrutura institucional de apoio técnico relacionada ao tratamento e resposta a incidentes cibernéticos.

## **CAPÍTULO X DA CONTINUIDADE E RESILIÊNCIA OPERACIONAL**

**Art. 28** A Sudene adotará medidas compatíveis com sua realidade organizacional, gestão de riscos e disponibilidade de recursos com o objetivo de fortalecer a continuidade dos serviços institucionais.

**Art. 29** Os procedimentos específicos relacionados à continuidade dos serviços, recuperação de informações e recuperação de desastres poderão ser disciplinados por instrumentos complementares.

## **CAPÍTULO XI DA CAPACITAÇÃO E CONSCIENTIZAÇÃO**

**Art. 30** A Sudene promoverá ações contínuas de capacitação e conscientização relacionadas:

- I. à segurança da informação;
- II. à privacidade;
- III. à proteção de dados pessoais;
- IV. ao uso adequado dos recursos institucionais;
- V. à gestão documental digital.

## **CAPÍTULO XII DOS INSTRUMENTOS COMPLEMENTARES**

**Art. 31** Complementam esta Política:

- I. o Programa de Governança em Segurança da Informação (PGSI);
- II. o Programa de Governança em Privacidade (PGP);
- III. a Política de Proteção de Dados Pessoais;
- IV. os processos relacionados à gestão de riscos;
- V. os processos relacionados à gestão de incidentes;

VI. o Plano de Trabalho do PPSI;

VII. os demais instrumentos normativos que venham a ser instituídos pela Sudene.

### **CAPÍTULO XIII DAS DISPOSIÇÕES FINAIS**

**Art. 32** A implementação desta Política ocorrerá de forma gradual, observados os ciclos de maturidade, o planejamento institucional e as diretrizes estabelecidas pelo PPSI.

**Art. 33** Esta Política deverá ser revisada periodicamente ou sempre que houver alteração normativa, tecnológica ou organizacional relevante.

**Art. 34** Os casos omissos serão submetidos à apreciação da instância de governança competente.

**Art. 35** Esta Política entra em vigor na data de sua publicação.

Documento assinado eletronicamente.