POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

São Paulo Consig LTDA.

Código: POL-PRIV-001
Versão: 2.0
Data de emissão: 02/09/2026
Classificação: Uso Interno
Periodicidade de revisão: Anual ou sempre que houver alteração relevante na legislação, nos processos, nos sistemas ou nas operações de tratamento de dados.

Sumário

1. OBJETIVO

Esta Política Interna de Privacidade e Proteção de Dados Pessoais estabelece as diretrizes, responsabilidades e procedimentos gerais adotados pela São Paulo Consig LTDA. para garantir o tratamento adequado, seguro, transparente e responsável de dados pessoais.

A Política tem como objetivos:

- estabelecer princípios e regras para o tratamento de dados pessoais;
- proteger os direitos e liberdades dos titulares;
- definir responsabilidades dos colaboradores e prestadores de serviços;
- estabelecer critérios para coleta, utilização, armazenamento, compartilhamento, retenção e eliminação de dados pessoais;
- reduzir riscos de acesso não autorizado, perda, alteração, destruição, divulgação ou utilização indevida de dados;
- estabelecer diretrizes para contratação e gestão de terceiros que tratem dados pessoais;
- estabelecer requisitos de segurança da informação aplicáveis à proteção de dados pessoais;
- promover a conformidade com a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD);
- estabelecer diretrizes para tratamento de incidentes envolvendo dados pessoais;
- promover a privacidade desde a concepção e durante todo o ciclo de vida dos sistemas e processos;
- estabelecer fundamentos para avaliação e gestão dos riscos relacionados à privacidade.

---

2. DIVULGAÇÃO E SCOPO

Este documento abrange todos os clientes, parceiros de negócio, fornecedores, prestadores de serviços, usuários e demais partes interessadas da SÃO PAULO CONSIG, estando disponível para consulta no site: https://spconsig.com.br/documentos/ e disponibilizado aos terceiros na formalização e na renovação contratual e, para os vínculos vigentes, com periodicidade mínima anual.

Esta Política aplica-se a:

- todos os colaboradores da São Paulo Consig;
- administradores e gestores;
- estagiários e aprendizes, quando aplicável;
- prestadores de serviços;
- terceiros que atuem em nome da empresa;
- fornecedores que tenham acesso ou participem do tratamento de dados pessoais;
- sistemas, aplicações, bancos de dados, servidores, dispositivos e demais recursos utilizados pela empresa;
- informações armazenadas em ambientes próprios ou de terceiros;
- operações de tratamento realizadas pela empresa, independentemente do meio utilizado.

A Política aplica-se tanto aos ambientes físicos quanto aos ambientes digitais.

---

3. FUNDAMENTAÇÃO LEGAL E NORMATIVA

Esta Política deverá ser interpretada em conjunto com a legislação e regulamentações aplicáveis, especialmente:

- Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD);
- regulamentações, resoluções e orientações publicadas pela Autoridade Nacional de Proteção de Dados (ANPD);
- legislação aplicável à atividade da empresa;
- contratos firmados com clientes, fornecedores e parceiros;
- políticas internas de segurança da informação;
- procedimentos internos relacionados a tecnologia, segurança e continuidade.

A legislação e as regulamentações aplicáveis deverão prevalecer em caso de conflito com esta Política.

---

4. DEFINIÇÕES

Para fins desta Política, aplicam-se as seguintes definições:

4.1 Dado pessoal
Informação relacionada a pessoa natural identificada ou identificável.

Exemplos:

- nome;
- CPF;
- endereço;
- telefone;
- e-mail;
- identificadores de usuário;
- informações cadastrais;
- registros de acesso;
- dados utilizados para identificação de pessoas.

4.2 Dado pessoal sensível
Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

4.3 Titular
Pessoa natural a quem se referem os dados pessoais tratados.

4.4 Tratamento
Toda operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

4.5 Controlador
Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

4.6 Operador
Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador e conforme suas instruções.

4.7 Encarregado — DPO
Pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, além de exercer as demais atribuições previstas na legislação e regulamentação aplicáveis.

4.8 Incidente de segurança
Evento adverso, confirmado ou suspeito, que possa comprometer a confidencialidade, integridade ou disponibilidade de informações, especialmente quando envolver dados pessoais.

4.9 ROPA
Registro das Operações de Tratamento de Dados Pessoais — documento que registra os principais tratamentos realizados pela organização.

4.10 RIPD
Relatório de Impacto à Proteção de Dados Pessoais — documentação destinada a descrever tratamentos que possam gerar riscos aos direitos e liberdades dos titulares, bem como as medidas de mitigação adotadas.

4.11 Terceiro
Pessoa ou organização externa à São Paulo Consig que participe direta ou indiretamente de determinada atividade ou tratamento.

4.12 Suboperador
Terceiro contratado por um operador para realizar atividades de tratamento de dados pessoais relacionadas ao serviço prestado ao controlador.

---

5. PRINCÍPIOS DE PRIVACIDADE
A São Paulo Consig deverá observar os princípios aplicáveis à proteção de dados pessoais, incluindo:

- finalidade;
- adequação;
- necessidade;
- livre acesso;
- qualidade dos dados;
- transparência;
- segurança;
- prevenção;
- não discriminação;
- responsabilização e prestação de contas.

5.1 Como tratamos os dados pessoais

Os dados pessoais são tratados apenas quando houver finalidade legítima, base legal aplicável e necessidade para a execução de nossas atividades. O tratamento poderá ocorrer para finalidades como:

- Prestação de serviços e suporte aos clientes;
- Cumprimento de contratos e acordos estabelecidos;
- Atendimento a obrigações legais, fiscais e regulatórias;
- Gestão de relacionamento comercial e administrativo;
- Proteção da segurança da informação, privacidade e prevenção a fraudes;
- Exercício regular de direitos em processos judiciais, administrativos ou arbitrais;
- Melhoria contínua de nossos serviços, produtos e soluções tecnológicas.

Nas operações relacionadas às soluções de tecnologia, tais como a plataforma

CONSIGSIMPLES, a organização atua majoritariamente na condição de Operadora de Dados Pessoais, realizando o tratamento das informações cadastrais, de salários e margens de servidores públicos sob contrato e em estrita conformidade com as instruções lícitas fornecidas pelas organizações e entes públicos contratantes, que figuram como Controladores desses dados.

---

6. GOVERNANÇA DE PRIVACIDADE

A São Paulo Consig deverá manter estrutura mínima de governança destinada à proteção de dados pessoais.

Essa estrutura deverá contemplar, conforme aplicável:

- definição de responsabilidades;
- políticas e procedimentos;
- registro das operações de tratamento;
- gestão de riscos;
- gestão de terceiros;
- gestão de incidentes;
- atendimento aos direitos dos titulares;
- treinamento e conscientização;
- controles de segurança;
- revisão periódica dos processos.

A Diretoria deverá fornecer suporte para a implementação e manutenção das medidas necessárias à proteção de dados pessoais.

---

7. RESPONSABILIDADES DA DIRETORIA

Compete à Diretoria:

- aprovar esta Política;
- disponibilizar recursos necessários para sua implementação;
- apoiar a adoção de medidas técnicas e administrativas;
- definir responsabilidades relacionadas à privacidade;
- avaliar riscos relevantes relacionados à proteção de dados;
- apoiar ações corretivas quando identificadas não conformidades;
- promover cultura organizacional de proteção de dados.

---

8. RESPONSABILIDADES DO ENCARREGADO DE DADOS — DPO

Quando aplicável, o Encarregado deverá:

- atuar como canal de comunicação com titulares;
- atuar como canal de comunicação com a ANPD;
- orientar colaboradores e contratados sobre práticas de proteção de dados;
- acompanhar a implementação desta Política;
- apoiar a elaboração e atualização do ROPA;
- apoiar avaliações de riscos de privacidade;
- acompanhar incidentes envolvendo dados pessoais;
- apoiar a elaboração de RIPDs quando aplicável;
- acompanhar solicitações relacionadas aos direitos dos titulares;
- recomendar melhorias nos processos de privacidade;
- manter registros das atividades relacionadas à governança de privacidade.

O Encarregado deverá possuir autonomia compatível com suas atribuições e acesso às informações necessárias para desempenhar sua função.

A identidade e os canais de contato do Encarregado deverão ser divulgados internamente e, quando aplicável, externamente.

---

9. RESPONSABILIDADES DOS COLABORADORES

Todos os colaboradores são responsáveis por:

- cumprir esta Política;
- proteger as informações às quais tenham acesso;
- utilizar dados pessoais somente para atividades autorizadas;
- não compartilhar credenciais;
- utilizar senhas individuais;
- comunicar incidentes ou suspeitas de incidentes;
- não copiar ou transferir dados pessoais sem autorização;
- respeitar as regras de acesso aos sistemas;
- participar dos treinamentos disponibilizados pela empresa;
- manter sigilo sobre informações pessoais e corporativas;
- utilizar equipamentos e sistemas corporativos de maneira adequada.

O descumprimento desta Política poderá resultar em medidas administrativas e disciplinares cabíveis.

---

10. COLETA DE DADOS PESSOAIS

A coleta de dados pessoais deverá ser limitada às informações necessárias para o cumprimento de finalidade legítima e previamente definida.

Antes da coleta, sempre que aplicável, deverão ser avaliados:

- finalidade;
- necessidade;
- base legal;
- categoria dos dados;
- titular dos dados;
- forma de armazenamento;

- período de retenção;
- possibilidade de compartilhamento;
- riscos à privacidade.

A coleta excessiva de dados deverá ser evitada.

---

11. BASE LEGAL

Todo tratamento de dados pessoais deverá possuir fundamento jurídico adequado, conforme as hipóteses previstas na LGPD.

A definição da base legal deverá considerar a finalidade específica do tratamento e as circunstâncias da operação.

As bases legais deverão ser registradas no inventário/ROPA quando aplicável.

O consentimento, quando utilizado, deverá ser obtido de maneira livre, informada e inequívoca e estar relacionado a finalidade determinada.

O consentimento não deverá ser utilizado quando outra base legal for mais adequada à operação.

---

12. TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

O tratamento de dados pessoais sensíveis deverá observar requisitos adicionais previstos na LGPD.

A empresa deverá:

- limitar o acesso;
- utilizar somente quando necessário;
- adotar medidas adicionais de segurança;
- evitar compartilhamentos desnecessários;
- documentar a finalidade e fundamento jurídico;
- avaliar riscos quando apropriado.

Dados biométricos, informações de saúde ou outros dados sensíveis deverão receber tratamento compatível com seu nível de criticidade.

---

13. CONTROLE DE ACESSO

O acesso a dados pessoais deverá obedecer ao princípio do **menor privilégio**.

Cada usuário deverá possuir credenciais individuais e intransferíveis.

Deverão ser adotados, conforme aplicável:

- autenticação individual;
- controle de permissões;
- segregação de funções;
- revisão periódica dos acessos;
- remoção imediata de acessos de usuários desligados;
- alteração de privilégios quando houver mudança de função;
- proteção das credenciais;
- registro de atividades relevantes.

É proibido compartilhar senhas ou utilizar credenciais de terceiros.

---

14. SEGURANÇA DA INFORMAÇÃO

A São Paulo Consig deverá adotar medidas técnicas e administrativas para proteger dados pessoais contra:

- acessos não autorizados;
- perda;
- destruição;
- alteração;
- divulgação;
- vazamento;
- indisponibilidade;
- tratamento inadequado ou ilícito.

As medidas deverão ser proporcionais aos riscos, à natureza dos dados e à criticidade dos sistemas.

Entre as medidas poderão estar:

- firewall;

- antivírus/EDR;
- controle de acesso;
- autenticação;
- criptografia, quando aplicável;
- backups;
- monitoramento;
- registros de logs;
- atualizações de segurança;
- gestão de vulnerabilidades;
- segregação de ambientes;
- proteção física dos equipamentos;
- controles de rede.

---

15. ARMAZENAMENTO DE DADOS

Os dados pessoais deverão ser armazenados somente em ambientes autorizados.

A empresa deverá manter controle sobre:

- onde os dados são armazenados;
- quem possui acesso;
- período de retenção;
- mecanismos de proteção;
- fornecedores envolvidos;
- localização da infraestrutura, quando relevante.

A utilização de dispositivos pessoais, serviços de armazenamento particulares ou sistemas não autorizados para armazenar dados corporativos ou pessoais deverá ser proibida ou previamente autorizada.

---

16. BACKUP E RECUPERAÇÃO

Dados e sistemas críticos deverão possuir mecanismos de backup compatíveis com sua importância.

Os backups deverão, quando aplicável:

- possuir controle de acesso;
- ser protegidos contra alteração ou exclusão indevida;
- possuir retenção definida;
- ser armazenados em ambiente apropriado;
- ser periodicamente verificados;
- ser testados quanto à possibilidade de restauração.

A empresa deverá manter procedimentos para recuperação dos sistemas críticos.

---

17. RETENÇÃO E ELIMINAÇÃO

Os dados pessoais não deverão ser mantidos por período superior ao necessário para a finalidade do tratamento, salvo quando houver fundamento legal ou regulatório que justifique sua conservação.

A empresa deverá estabelecer critérios de retenção considerando:

- finalidade;
- obrigações legais;
- obrigações contratuais;
- necessidade operacional;
- riscos;
- solicitações de titulares;
- requisitos regulatórios.

Quando os dados não forem mais necessários e não houver obrigação de retenção, deverão ser eliminados, anonimizados ou submetidos a outra medida adequada.

---

18. COMPARTILHAMENTO DE DADOS

O compartilhamento de dados pessoais deverá ocorrer somente quando:

- houver finalidade legítima;
- existir base legal adequada;
- for necessário;

- o destinatário estiver autorizado;
- houver medidas de segurança apropriadas;
- forem observadas obrigações contratuais e legais.

Compartilhamentos deverão ser registrados no ROPA quando aplicável.

---

19. TERCEIROS, OPERADORES E SUBOPERADORES

Antes da contratação de terceiros que possam tratar dados pessoais, deverão ser avaliados, conforme o risco:

- necessidade de acesso aos dados;
- finalidade do tratamento;
- medidas de segurança;
- reputação e capacidade do fornecedor;
- localização dos dados;
- subcontratados;
- transferência internacional;
- requisitos contratuais;
- incidentes anteriores, quando disponíveis.

Contratos com terceiros que tratem dados pessoais deverão conter, quando aplicável:

- finalidade do tratamento;
- obrigações de confidencialidade;
- requisitos de segurança;
- limitações de uso;
- regras de compartilhamento;
- regras para suboperadores;
- comunicação de incidentes;
- devolução ou eliminação dos dados;
- responsabilidades das partes;
- requisitos relativos à proteção de dados.

20. INFRAESTRUTURA TERCEIRIZADA

Quando a empresa utilizar infraestrutura de terceiros para armazenamento ou processamento de dados pessoais, deverá avaliar:

- localização dos ambientes;
- controles de segurança;
- disponibilidade;
- backup;
- recuperação;
- controle de acesso;
- certificações relevantes;
- subcontratados;
- transferência internacional de dados;
- obrigações contratuais.

A utilização de infraestrutura terceirizada não elimina as responsabilidades da empresa relacionadas ao adequado tratamento dos dados pessoais.

21. TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados pessoais deverá ser previamente avaliada.

Quando dados pessoais forem armazenados, processados ou disponibilizados em infraestrutura localizada fora do Brasil, deverão ser analisados:

- país de destino;
- finalidade da transferência;
- categorias de dados;
- fornecedor envolvido;
- existência de operador ou suboperador;
- mecanismo jurídico aplicável;
- medidas de segurança;
- cláusulas contratuais;

- requisitos estabelecidos pela LGPD e regulamentação da ANPD.

A empresa deverá manter documentação suficiente para demonstrar a regularidade da transferência internacional.

---

22. PRIVACIDADE DESDE A CONCEPÇÃO — PRIVACY BY DESIGN

A privacidade deverá ser considerada desde o planejamento de novos sistemas, produtos, serviços, processos e alterações relevantes.

Sempre que aplicável, deverão ser avaliados:

- quais dados serão tratados;
- finalidade;
- necessidade;
- base legal;
- período de retenção;
- compartilhamentos;
- riscos;
- controles de acesso;
- segurança;
- possibilidade de anonimização ou minimização;
- direitos dos titulares.

Projetos que apresentem risco elevado poderão demandar avaliação específica de impacto à proteção de dados.

---

23. REGISTRO DAS OPERAÇÕES DE TRATAMENTO — ROPA

A empresa deverá manter registro das operações relevantes de tratamento de dados pessoais.

O ROPA deverá conter, conforme aplicável:

- processo;
- finalidade;
- categoria de dados;

- categoria de titulares;
- base legal;
- origem dos dados;
- sistemas utilizados;
- armazenamento;
- compartilhamentos;
- operadores;
- suboperadores;
- transferências internacionais;
- retenção;
- medidas de segurança;
- responsáveis.

O ROPA deverá ser revisado quando houver alterações relevantes nos processos.

---

24. AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS

Quando determinado tratamento puder apresentar riscos relevantes aos direitos e liberdades dos titulares, a empresa deverá avaliar a necessidade de elaboração de RIPD.

A avaliação deverá considerar:

- natureza do tratamento;
- volume de dados;
- sensibilidade;
- quantidade de titulares;
- tecnologia utilizada;
- finalidade;
- compartilhamentos;
- transferência internacional;
- riscos;
- medidas de mitigação.

O RIPD deverá ser atualizado quando houver alteração relevante no tratamento ou nos riscos.

---

25. TESTE DE BALANCEAMENTO — LEGÍTIMO INTERESSE

Quando o tratamento estiver fundamentado em legítimo interesse, a empresa deverá avaliar, quando aplicável:

- existência de interesse legítimo;
- necessidade do tratamento;
- expectativa razoável do titular;
- impacto sobre os direitos dos titulares;
- medidas de mitigação;
- possibilidade de utilização de alternativa menos invasiva.

O resultado da avaliação deverá ser documentado quando aplicável.

---

26. DIREITOS DOS TITULARES

A empresa deverá disponibilizar meios adequados para recebimento e tratamento de solicitações relacionadas aos direitos dos titulares previstos na LGPD.

Entre os direitos estão, conforme aplicável:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção;
- anonimização;
- bloqueio;
- eliminação;
- portabilidade, observadas as regulamentações aplicáveis;
- informação sobre compartilhamento;
- informação sobre possibilidade de não fornecer consentimento;
- revogação do consentimento;
- oposição ao tratamento nas hipóteses previstas em lei;

- revisão de decisões automatizadas, quando aplicável.

As solicitações deverão ser registradas e tratadas dentro dos prazos legais e regulamentares aplicáveis.

---

27. INCIDENTES DE SEGURANÇA

Todos os colaboradores deverão comunicar imediatamente qualquer suspeita ou confirmação de incidente envolvendo dados pessoais.

São exemplos:

- vazamento;
- envio de informação para destinatário incorreto;
- acesso indevido;
- roubo ou perda de equipamento;
- comprometimento de credenciais;
- malware;
- ransomware;
- indisponibilidade provocada por incidente;
- alteração não autorizada;
- exposição pública de dados;
- acesso indevido a banco de dados.

A empresa deverá manter procedimento específico para:

1. identificação;
2. registro;
3. classificação;
4. contenção;
5. investigação;
6. avaliação de impacto;
7. mitigação;
8. comunicação;
9. recuperação;

10. documentação;
11. melhoria preventiva.

Quando aplicável, deverão ser observadas as regras da ANPD relativas à comunicação de incidentes de segurança envolvendo dados pessoais. A ANPD possui regulamentação específica sobre comunicação de incidentes.

---

28. COMUNICAÇÃO DE INCIDENTES

A comunicação de incidente deverá ser avaliada considerando:

- natureza dos dados afetados;
- quantidade de titulares;
- potencial impacto;
- risco ou dano relevante;
- natureza do incidente;
- medidas adotadas;
- obrigações contratuais;
- obrigações legais e regulatórias.

Quando aplicável, a empresa deverá comunicar o incidente à ANPD e aos titulares dentro dos prazos estabelecidos pela regulamentação vigente.

Clientes e parceiros deverão ser comunicados conforme as obrigações contratuais e legais aplicáveis.

---

29. REGISTRO E EVIDÊNCIAS

A empresa deverá manter registros adequados para demonstrar a adoção das medidas de proteção de dados.

Podem constituir evidências:

- políticas;
- procedimentos;
- registros de treinamento;
- registros de acesso;
- logs;

- evidências de backup;
- testes de restauração;
- contratos;
- avaliações de fornecedores;
- ROPA;
- RIPD;
- avaliações de risco;
- registros de incidentes;
- atas de reuniões;
- relatórios de auditoria;
- registros de solicitações de titulares.

---

30. TREINAMENTO E CONSCIENTIZAÇÃO

A empresa deverá promover ações de conscientização sobre privacidade e proteção de dados.

Os treinamentos poderão abordar:

- LGPD;
- proteção de dados;
- segurança da informação;
- phishing;
- senhas;
- uso adequado de sistemas;
- compartilhamento de informações;
- incidentes;
- direitos dos titulares;
- responsabilidades dos colaboradores.

Treinamentos deverão ser registrados sempre que possível.

---

31. AUDITORIA E MONITORAMENTO

A empresa poderá realizar avaliações periódicas de conformidade com esta Política.

As avaliações poderão ser:

- internas;
- realizadas por terceiros;
- específicas para determinado processo;
- relacionadas a fornecedores;
- relacionadas à segurança;
- relacionadas à privacidade.

Não conformidades deverão ser registradas e tratadas de acordo com sua criticidade.

---

32. GESTÃO DE RISCOS

A empresa deverá avaliar riscos relacionados ao tratamento de dados pessoais considerando:

- confidencialidade;
- integridade;
- disponibilidade;
- possibilidade de acesso indevido;
- perda;
- vazamento;
- uso incompatível com a finalidade;
- riscos aos titulares.

Os riscos identificados deverão ser tratados por meio de medidas proporcionais.

---

33. CONTINUIDADE DO NEGÓCIO

Processos e sistemas considerados críticos deverão possuir mecanismos de continuidade e recuperação compatíveis com sua importância.

A empresa deverá buscar manter:

- backups;

- procedimentos de restauração;
- infraestrutura adequada;
- fornecedores críticos identificados;
- contatos de emergência;
- procedimentos de recuperação;
- definição de prioridades;
- avaliação de impacto;
- RTO e RPO, quando aplicável;
- testes de recuperação.

Planos de continuidade e recuperação deverão ser revisados periodicamente.

---

34. USO DE SISTEMAS E SERVIÇOS DE TERCEIROS

É proibido utilizar serviços externos não autorizados para armazenamento, processamento ou compartilhamento de dados corporativos ou pessoais.

Antes da utilização de uma nova solução que envolva dados pessoais, deverá ser avaliado:

- finalidade;
- necessidade;
- fornecedor;
- segurança;
- localização dos dados;
- compartilhamento;
- retenção;
- transferência internacional;
- contrato;
- riscos.

---

35. INTELIGÊNCIA ARTIFICIAL

A utilização de ferramentas de Inteligência Artificial que envolvam dados pessoais deverá ser previamente avaliada.

É proibido inserir dados pessoais, informações confidenciais ou informações de clientes em ferramentas de Inteligência Artificial não autorizadas pela empresa.

Quando uma solução de IA for utilizada em processos corporativos, deverão ser avaliados:

- finalidade;
- fornecedor;
- dados enviados;
- armazenamento;
- utilização dos dados para treinamento;
- localização do processamento;
- transferência internacional;
- segurança;
- riscos;
- possibilidade de decisões automatizadas.

---

36. CONFIDENCIALIDADE

Todos os colaboradores e terceiros autorizados deverão manter sigilo sobre os dados pessoais e informações corporativas às quais tenham acesso.

As obrigações de confidencialidade deverão permanecer aplicáveis mesmo após o encerramento do vínculo profissional ou contratual, quando previsto em lei ou contrato.

---

37. DESCARTE SEGURO

Documentos físicos e digitais contendo dados pessoais deverão ser descartados de maneira que impeça sua recuperação ou acesso indevido, quando não houver obrigação de retenção.

Exemplos:

- destruição segura de documentos físicos;

- eliminação segura de arquivos;
- revogação de acessos;
- exclusão de contas;
- descarte seguro de dispositivos.

---

38. SEGURANÇA FÍSICA

O acesso às áreas onde estejam localizados equipamentos ou documentos contendo dados pessoais deverá ser controlado.

Quando aplicável, deverão existir:

- controle de acesso;
- restrição a áreas técnicas;
- proteção de equipamentos;
- controle de visitantes;
- procedimentos para descarte;
- medidas contra furto, perda ou acesso não autorizado.

Quando a infraestrutura estiver sob responsabilidade de fornecedor especializado, deverão ser avaliadas as medidas de segurança e garantias oferecidas pelo fornecedor.

---

39. FORNECEDORES CRÍTICOS

A empresa deverá manter identificação dos fornecedores que possam representar risco relevante para a continuidade ou proteção de dados.

Entre os critérios de criticidade poderão estar:

- acesso a dados pessoais;
- acesso a sistemas críticos;
- hospedagem;
- armazenamento;
- backup;
- conectividade;
- segurança;

- processamento;
- dependência operacional.

Fornecedores críticos deverão ser avaliados periodicamente conforme o risco.

---

40. NÃO CONFORMIDADES

O descumprimento desta Política deverá ser avaliado pela área responsável e poderá resultar em:

- orientação;
- treinamento;
- correção do processo;
- restrição ou revogação de acesso;
- medidas administrativas;
- medidas disciplinares;
- medidas contratuais;
- medidas legais, quando aplicáveis.

---

41. EXCEÇÕES

Exceções a esta Política deverão:

- possuir justificativa;
- ser documentadas;
- possuir prazo definido;
- ser aprovadas pelo responsável competente;
- possuir avaliação de risco quando aplicável.

Exceções não poderão comprometer direitos dos titulares ou contrariar obrigações legais.

---

42. REVISÃO DA POLÍTICA

Esta Política deverá ser revisada:

- pelo menos uma vez ao ano;

- quando houver alteração relevante na legislação;
- quando houver alteração relevante nas regulamentações da ANPD;
- após incidentes relevantes;
- após alterações significativas nos sistemas;
- após mudanças relevantes nos processos de tratamento;
- quando identificadas deficiências relevantes.

Toda revisão deverá ser registrada com número da versão e data.

---

43. APROVAÇÃO E VIGÊNCIA

Esta Política entra em vigor após sua aprovação pela Diretoria da São Paulo Consig LTDA.

A versão vigente deverá ser disponibilizada aos colaboradores e partes relevantes.

Os colaboradores deverão declarar ciência da Política quando solicitado.

---

44. DOCUMENTOS RELACIONADOS

Esta Política deverá ser complementada, conforme aplicável, pelos seguintes documentos:

1. Política de Segurança da Informação;
2. Política de Controle de Acesso;
3. Política de Senhas;
4. Procedimento de Gestão de Incidentes;
5. Plano de Continuidade de Negócios;
6. Plano de Recuperação de Desastres;
7. Registro de Operações de Tratamento — ROPA;
8. Relatórios de Impacto à Proteção de Dados — RIPD;
9. Procedimento de Atendimento aos Titulares;
10. Procedimento de Gestão de Terceiros;
11. Procedimento de Gestão de Vulnerabilidades;
12. Política de Backup;

13. Política de Retenção e Descarte;
14. Termos de Confidencialidade;
15. Procedimento de Privacy by Design;
16. Procedimento de Transferência Internacional de Dados;
17. Plano de Resposta a Incidentes.

---

45. CONTROLE DE VERSÕES

Versão	Data	Descrição	Responsável
2.0	02/09/2026	Emissão inicial	Gestor de TI / Diretoria

APROVAÇÃO

Responsável pela elaboração:
Johnatan Alves — Gestor de TI

Responsável pela aprovação: Huerta Ferreira de Melo Neto

Cargo: Diretor Executivo

Data de aprovação:
02/09/2026

Assinatura:
