POLÍTICA INSTITUCIONAL FRAME-PSI Nº 9656, DE 23 DE NOVEMBRO DE 2026

Política de Segurança da Informação

Dispõe sobre as diretrizes de segurança da informação adotadas pela Frame Tecnologia e Soluções Comerciais LTDA na proteção das informações próprias, de clientes e da Administração Pública, em todo o território nacional.

CÓDIGO	VERSÃO	EMISSÃO E VIGÊNCIA	CLASSIFICAÇÃO	ABRANGÊNCIA
FRAME-PSI-9656/2026	2.0	23/11/2026	Pública	Território nacional

ORGANIZAÇÃO

Razão Social: Frame Tecnologia e Soluções Comerciais LTDA | **CNPJ:** 43.357.981/0001-31 | **NIRE:** 41214045483
Sede: Rua Marechal Deodoro, 344, Conj. 151, Bloco Atalaia, Centro, Curitiba/PR, CEP 80010-010
Responsável pela Política: Alisson Sizenando Ferreira, sócio-administrador | **Contato:** frame@agencia.promo

CAPÍTULO I - DO OBJETO E DO ALCANCE

1.1. Esta Política estabelece as diretrizes de segurança da informação da FRAME TECNOLOGIA E SOLUÇÕES COMERCIAIS LTDA, doravante "FRAME", para a proteção das informações próprias e das informações de clientes, de titulares de dados pessoais e de órgãos e entidades da Administração Pública a que tenha acesso.

1.2. Aplica-se aos ativos de informação sob gestão da FRAME, entre eles sistemas, aplicações, bancos de dados, códigos-fonte, credenciais, equipamentos e documentos, e vincula sócios, administradores, colaboradores, prestadores de serviço e suboperadores, na medida das respectivas atribuições.

1.3. Esta Política complementa a Política de Privacidade e Proteção de Dados Pessoais, documento FRAME-PPD-8546/2026, e com ela deve ser lida em conjunto.

FIGURA 1 - FRENTES DE CONTROLE TRATADAS NESTA POLÍTICA



Ilustração de apoio à leitura, sem conteúdo normativo próprio. Prevalece o texto.

CAPÍTULO II - DAS REFERÊNCIAS

2.1. Esta Política considera os arts. 46 a 50 da Lei nº 13.709/2018 ("LGPD"), a Resolução CD/ANPD nº 15/2024, o art. 13 do Decreto nº 8.771/2016, a Lei nº 12.965/2014, o art. 198 da Lei nº 5.172/1966 e as normas de segurança da informação editadas pelo ente público contratante, quando aplicáveis.

2.2. As diretrizes inspiram-se em boas práticas de mercado, a exemplo das normas ABNT NBR ISO/IEC 27001, 27002 e 27701. A referência é orientativa e não importa declaração de certificação nem de conformidade integral a tais normas.

CAPÍTULO III - DOS PRINCÍPIOS

3.1. A segurança da informação na FRAME orienta-se pela preservação da confidencialidade, da integridade, da disponibilidade e da autenticidade das informações.

3.2. As medidas são definidas de modo proporcional à natureza das informações tratadas, aos riscos envolvidos, ao porte da FRAME e ao estado da técnica, e são consideradas desde a concepção dos produtos e dos serviços.

CAPÍTULO IV - DA GOVERNANÇA E DAS RESPONSABILIDADES

4.1. A administração da FRAME aprova esta Política, define prioridades de segurança e decide sobre o tratamento de riscos.

4.2. Cabe a cada pessoa com acesso a ativos de informação da FRAME utilizá-los apenas para as finalidades autorizadas, zelar pelas credenciais sob sua guarda e comunicar de imediato à administração qualquer suspeita de incidente.

4.3. O acesso a informações de clientes e da Administração Pública pressupõe compromisso de confidencialidade.

CAPÍTULO V - DA CLASSIFICAÇÃO DA INFORMAÇÃO

5.1. As informações são classificadas, para fins de tratamento, em:

a) Públicas: destinadas à divulgação irrestrita, como este documento;

b) Internas: de uso da FRAME, cuja divulgação não é autorizada, mas cujo vazamento não acarretaria dano relevante;

c) Restritas: dados pessoais, informações de clientes e da Administração Pública, informações protegidas por sigilo legal, credenciais, chaves criptográficas, certificados digitais e códigos-fonte.

5.2. A informação recebida de órgão ou de entidade pública conserva a classificação e o grau de sigilo atribuídos pelo ente de origem, nos termos da Lei nº 12.527/2011 e da legislação local.

5.3. Na dúvida, a informação é tratada como Restrita.

FIGURA 2 - CLASSIFICAÇÃO DA INFORMAÇÃO

PÚBLICA	Destinada à divulgação irrestrita, como este documento.
INTERNA	De uso da FRAME, sem divulgação autorizada.
RESTRITA	Dados pessoais, informações de clientes e da Administração Pública, informações sob sigilo legal, credenciais, chaves, certificados e códigos-fonte. Na dúvida, a informação é tratada como Restrita.

Ilustração de apoio à leitura, sem conteúdo normativo próprio. Prevalece o texto.

CAPÍTULO VI - DO CONTROLE DE ACESSO E DAS CREDENCIAIS

6.1. O acesso a sistemas e a informações segue os critérios da necessidade de conhecer e do privilégio mínimo.

6.2. As credenciais são pessoais ou atribuídas a serviço identificado, e seu compartilhamento fora dos meios autorizados é vedado.

6.3. A FRAME adota autenticação em múltiplos fatores nos sistemas e nos serviços que a disponibilizam, com prioridade para os ambientes de administração e para os que guardam informações Restritas.

6.4. Senhas, chaves de interface de programação, certificados digitais e demais segredos são guardados em repositório de credenciais de acesso restrito. É vedada a sua gravação em código-fonte, em repositório de código ou em canal de comunicação não protegido.

6.5. Os acessos são revistos e revogados quando cessa a necessidade que os justificou, em especial ao término de vínculo contratual ou de projeto.

6.6. Credenciais cedidas por cliente ou por ente público são utilizadas somente para o objeto contratado e devolvidas ou inutilizadas ao seu término.

CAPÍTULO VII - DA PROTEÇÃO DE REDES, DE COMUNICAÇÕES E DE INFRAESTRUTURA

7.1. O tráfego entre usuários e aplicações operadas pela FRAME é protegido por criptografia em trânsito.

7.2. A administração remota de servidores ocorre por canais cifrados e autenticados, preferencialmente por rede privada.

7.3. A exposição de serviços à internet limita-se ao necessário. Arquivos de configuração, cópias de bancos de dados, registros de eventos e repositórios de código não ficam acessíveis ao público.

7.4. Em ambiente de produção, as mensagens de erro detalhadas e a listagem de diretórios permanecem desabilitadas.

7.5. A FRAME emprega, quando aplicável ao serviço, mecanismos de proteção de borda, a exemplo de firewall de aplicação e de mitigação de tráfego malicioso.

7.6. A infraestrutura pode ser contratada de provedores especializados de computação em nuvem e de hospedagem, selecionados com consideração às garantias de segurança que oferecem.

CAPÍTULO VIII - DO DESENVOLVIMENTO SEGURO E DA GESTÃO DE MUDANÇAS

8.1. Os códigos-fonte são mantidos em repositórios privados, com controle de versão e histórico de alterações.

8.2. Nos projetos dotados de esteira automatizada de integração e de entrega, as alterações em produção passam por essa esteira, com registro e possibilidade de reversão.

8.3. Os ambientes de desenvolvimento e de teste são segregados do ambiente de produção, na medida do tecnicamente viável.

8.4. Os testes utilizam dados fictícios ou anonimizados, sempre que tecnicamente viável. O uso de dados reais em teste, quando indispensável, observa as mesmas salvaguardas do ambiente de produção.

8.5. As alterações estruturais em bancos de dados são precedidas de cópia de segurança e de plano de reversão.

8.6. A FRAME acompanha a atualização de componentes e de dependências de software e trata, segundo a criticidade, as vulnerabilidades de que tenha conhecimento.

CAPÍTULO IX - DAS CÓPIAS DE SEGURANÇA E DA CONTINUIDADE

9.1. A FRAME mantém cópias de segurança periódicas das informações e dos sistemas críticos sob sua gestão, com acesso restrito e, preferencialmente, em local distinto do ambiente principal.

9.2. A periodicidade, a retenção e os objetivos de recuperação de cada serviço são os definidos no Instrumento Específico firmado com o cliente ou, na falta deste, os compatíveis com a criticidade do serviço.

CAPÍTULO X - DOS REGISTROS E DO MONITORAMENTO

10.1. As aplicações e os sistemas operados pela FRAME geram registros de acesso e de eventos relevantes, conservados pelos prazos legais e pelos necessários à apuração de incidentes.

10.2. Os registros têm acesso restrito e são utilizados para fins de segurança, de auditoria, de cumprimento de obrigação legal e de exercício regular de direitos.

CAPÍTULO XI - DOS TERCEIROS E DOS SUBOPERADORES

11.1. O acesso de prestadores de serviço e de suboperadores a informações Restritas limita-se ao necessário e sujeita-se a dever de confidencialidade e de proteção de dados.

11.2. Nas contratações com a Administração Pública, a subcontratação observa as condições e as autorizações previstas no Instrumento Específico.

CAPÍTULO XII - DA GESTÃO DE INCIDENTES

12.1. Considera-se incidente de segurança o evento adverso confirmado que comprometa a confidencialidade, a integridade, a disponibilidade ou a autenticidade de informações.

12.2. O tratamento de incidentes compreende a identificação, a contenção, a avaliação de causa e de impacto, a comunicação, a correção e o registro.

12.3. O incidente que envolva dados pessoais é comunicado na forma do Capítulo XI da Política de Privacidade e Proteção de Dados Pessoais: à ANPD e aos titulares, quando a FRAME for controladora e houver risco ou dano relevante; ao controlador, quando a FRAME for operadora.

12.4. O incidente que envolva informação de ente público é comunicado ao órgão ou à entidade contratante, na forma e no prazo do Instrumento Específico.

12.5. A FRAME mantém registro dos incidentes de que tenha conhecimento, na forma da regulamentação.

FIGURA 3 - ETAPAS DO TRATAMENTO DE INCIDENTES



Ilustração de apoio à leitura, sem conteúdo normativo próprio. Prevalece o texto.

CAPÍTULO XIII - DAS PESSOAS, DOS EQUIPAMENTOS E DO DESCARTE

13.1. As pessoas com acesso a informações Restritas são orientadas quanto a esta Política e quanto às regras de proteção de dados pessoais.

13.2. Os equipamentos utilizados no trabalho devem contar com controle de acesso e com bloqueio de sessão.

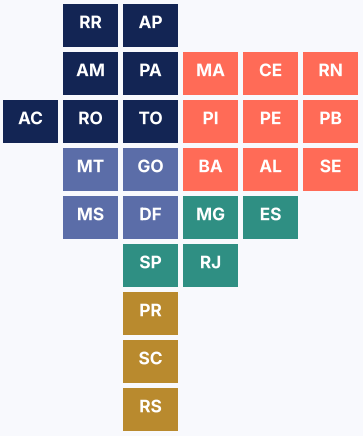
13.3. O descarte de informações e de mídias é feito de modo a impedir a sua recuperação, observados os prazos de guarda aplicáveis.

CAPÍTULO XIV - DA ABRANGÊNCIA TERRITORIAL

14.1. Esta Política aplica-se às atividades da FRAME em todo o território nacional e alcança as relações mantidas com a União, com os Estados do Acre, de Alagoas, do Amapá, do Amazonas, da Bahia, do Ceará, do Espírito Santo, de Goiás, do Maranhão, de Mato Grosso, de Mato Grosso do Sul, de Minas Gerais, do Pará, da Paraíba, do Paraná, de Pernambuco, do Piauí, do Rio de Janeiro, do Rio Grande do Norte, do Rio Grande do Sul, de Rondônia, de Roraima, de Santa Catarina, de São Paulo, de Sergipe e do Tocantins, com o Distrito Federal e com todos os Municípios, incluídas as respectivas administrações indiretas.

14.2. Requisitos de segurança próprios de cada ente, previstos em norma local ou no Instrumento Específico, somam-se a esta Política na relação correspondente.

FIGURA 4 - ABRANGÊNCIA TERRITORIAL



26 Estados, o Distrito Federal e os respectivos Municípios

Norte	7 unidades da Federação
Nordeste	9 unidades da Federação
Centro-Oeste	4 unidades da Federação
Sudeste	4 unidades da Federação
Sul	3 unidades da Federação

Âmbito federal: União, autarquias, fundações, empresas públicas e sociedades de economia mista.

Ilustração de apoio à leitura, sem conteúdo normativo próprio. Prevalece o texto.

CAPÍTULO XV - DAS DISPOSIÇÕES GERAIS

15.1. Natureza. Esta Política é ato unilateral de governança e de caráter informativo. Não constitui proposta, oferta ou promessa de contratar, para os fins do art. 427 do Código Civil, nem garantia de resultado, de nível de serviço ou de inviolabilidade, confissão, reconhecimento de responsabilidade, novação ou renúncia a direito, a prerrogativa ou a meio de defesa. Interpreta-se estritamente, nos termos do art. 114 do Código Civil.

15.2. Obrigações de meio. As medidas aqui descritas são obrigações de meio. Nenhum sistema é imune a falhas, e a ocorrência de incidente não faz presumir o descumprimento desta Política, nos termos dos arts. 43 e 44 da LGPD.

15.3. Prevalência. Em caso de divergência, prevalecem, nesta ordem, a legislação aplicável, o Instrumento Específico e as instruções lícitas e documentadas do contratante. Níveis de serviço, prazos e penalidades são exclusivamente os previstos no Instrumento Específico.

15.4. Responsabilidade. Eventual responsabilidade da FRAME é apurada caso a caso, em procedimento regular, nos limites da legislação e do Instrumento Específico, preservadas as excludentes do art. 43 da LGPD e as hipóteses do art. 393 do Código Civil.

15.5. Autonomia patrimonial. As diretrizes desta Política são assumidas exclusivamente pela pessoa jurídica. A assinatura do representante legal é aposta nessa qualidade e não importa obrigação pessoal, fiança, aval ou garantia de qualquer natureza, nos termos dos arts. 49-A e 1.052 do Código Civil.

15.6. Reserva de detalhamento. Procedimentos, configurações e parâmetros técnicos de segurança constituem informação Restrita e não integram este documento. O seu fornecimento a contratante ou a órgão de controle ocorre mediante dever de sigilo, na forma do Instrumento Específico.

15.7. Atualização. A FRAME pode alterar, substituir ou revogar esta Política a qualquer tempo, com efeitos prospectivos. Vigora a versão mais recente.

15.8. Foro. Fica indicado o foro da Comarca de Curitiba, Estado do Paraná, ressalvadas as hipóteses de competência absoluta e o foro definido em Instrumento Específico firmado com a Administração Pública.

15.9. Assinatura. Este documento é assinado eletronicamente com certificado digital ICP-Brasil, nos termos do art. 10, § 1º, da Medida Provisória nº 2.200-2/2001 e do art. 4º, III, da Lei nº 14.063/2020.

Curitiba, 23 de novembro de 2026.

Frame Tecnologia e Soluções Comerciais LTDA
CNPJ: 43.357.981/0001-31
Alisson Sizenando Ferreira, Sócio-Administrador e Representante Legal

Assinado digitalmente por FRAME TECNOLOGIA E SOLUCOES COMERCIAIS LTDA, CNPJ 43.357.981/0001-31
Certificado ICP-Brasil e-CNPJ A1, AC SAFEWEB RFB v5
Data: 23/11/2026 17:14 (UTC-3)
Documento FRAME-PSI-9656/2026 | Hash SHA-256 do documento: 155ec744198e7e13
Verifique a autenticidade em validar.iti.gov.br