Programa de Integridade | Frimesa

POLÍTICA DE PROTEÇÃO DE DADOS

Índice

1. INTRODUÇÃO

- A FRIMESA COOPERATIVA CENTRAL tem o compromisso de proteger a privacidade dos dados pessoais de seus colaboradores, clientes, parceiros de negócios e outras pessoas identificáveis. São ações alinhadas à estratégia e à manutenção de uma cultura sustentável de integridade.

2. OBJETIVOS

- Esta Política tem por objetivo estabelecer e manter padrões elevados para coletar on ou off line, usar, divulgar, armazenar, proteger, acessar, transferir, compartilhar, eliminar ou processar dados pessoais;

- Garantir que, com a adoção dos mais elevados padrões de integridade, legalidade, eficiência, economicidade e transparência, além de disseminar a cultura da segurança das informações.

3. ABRANGÊNCIA

- As orientações estabelecidas nesta Política se aplicam e devem ser adotadas por todos os Conselheiros, Diretor Presidente Executivo, Colaboradores, Estagiários, Aprendizes e Terceiros;

- Em termos geográficos, a presente Política se aplica aos Colaboradores da Frimesa e Terceiros, localizados no Brasil e no exterior, independentemente da jurisdição/país em que venham a praticar qualquer ato em representação da Frimesa, sem qualquer distinção. Em todos os casos, o que deve ser seguido é sempre o padrão mais alto e restritivo.

4. DIRETRIZES

- A Gestão dos Dados conforme esta Política é de responsabilidade de todos os colaboradores, terceiros e filiadas, nos limites das atribuições de cada área envolvida;

- A Gestão se dará, conforme atribuições descritas no item "5. PAPÉIS E RESPONSABILIDADES" desta Política, a partir da execução de processos e monitoramentos descritos abaixo:

- Toda manipulação, aquisição ou experimentação de base de dados deverá passar pelo processo de avaliação, previsto no programa de Governança em Privacidade;

- Esta política deverá ser revista no mínimo a cada 02 (dois) anos ou se houver fato relevante a ser tratado para esta ação;

- Em qualquer observação ou constatação de não aderência a essa política, deverá ser informado imediatamente ao DPO;

- Observar ainda a LGPD, na seção II, do capítulo VII – Das Boas Práticas e da Governança (art. 50 e seguintes).

4.1. Do tratamento de dados pessoais

- Os dados pessoais somente poderão ser coletados e tratados de acordo com as bases legais definidas no artigo 7º, da Lei 13.709/18 – Lei Geral de Proteção de Dados – LGPD;

- As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

  a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
  b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
  c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
  d) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
  e) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
  f) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
  g) segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
  h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
  i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
  j) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

- O compartilhamento de dados pessoais somente poderá ser realizado com o consentimento do titular.

4.2. Da proteção de dados pessoais

- Deve-se controlar o acesso a dados pessoais, de acordo com o princípio do menor privilégio, ou seja, os colaboradores devem ter permissão de tratar apenas os dados que forem necessários a execução de suas funções.

4.3. Da proteção de dados sensíveis

- Deve-se evitar o tratamento de dados pessoais sensíveis, realizando o tratamento apenas quando for estritamente necessário ao negócio.

4.4. Dos direitos dos titulares de dados pessoais

- Deve ser garantido aos titulares de dados pessoais os direitos, constantes no artigo 18, da LGPD, sendo os seguintes:

  a) Confirmação da existência de tratamento;
  b) Acesso aos dados;
  c) Correção de dados incompletos, inexatos ou desatualizados;
  d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
  e) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
  f) Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
  g) Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
  h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
  i) Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

- O atendimento ao requerimento do titular de dados deve ser feito no prazo de 15 (quinze) dias, contados da data do requerimento, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade de tratamento;

- Caso tenha ocorrido o compartilhamento dos dados dos titulares, deverá ser informado aos agentes de tratamento que receberam os dados compartilhados, que atendam igualmente o pedido do titular dos dados pessoais.

4.5. Encarregado de Proteção de Dados (DPO)

- Nomeia-se como encarregado de proteção de dados da Frimesa Cooperativa Central, Darling Bosco, que será o canal de comunicação entre o titular dos dados pessoais ou a ANPD e a Frimesa Cooperativa Central;

- Foi criado o e-mail privacidade@frimesa.com.br, para o encarregado de proteção de dados e divulgado no website da Frimesa através da Política de Privacidade.

4.6. Do mapeamento e inventário dos dados pessoais e do Plano de Ação

- Trata-se de auditoria geral inicial para identificar todo o ciclo de vida dos dados pessoais, mediante as seguintes atividades:

  i. Mapear processos que contenham dados pessoais;
  ii. Mapear dados pessoais (quais dados, finalidades e bases legais);
  iii. Identificar os "donos" das atividades de tratamento;
  iv. Identificar as medidas de segurança existentes;
  v. Conhecer os riscos à proteção de dados;

- Após o preenchimento da planilha de mapeamento e inventário de dados pessoais, será elaborado o Plano de Ação, para definir medidas de adequação a LGPD;

- O mapeamento e inventário de dados pessoais deverá ser atualizado e revisto uma vez por ano, e, consequentemente, deve ser atualizado o Plano de Ação.

4.7. Atualização constante do programa de privacidade – Manutenção da conformidade ao longo do tempo

- O programa de privacidade deve ser atualizado, para que a conformidade com a LGPD seja mantida ao longo do tempo;

- As seguintes atividades devem ser realizadas:

  a) Realizar integração com os novos colaboradores, mediante assinatura do (i) Termo de Confidencialidade e Proteção de Dados, (ii) política de tratamento de dados do colaborador e (iii) explicações sobre os principais aspectos sobre a LGPD;
  b) Realizar treinamentos e conscientização constantes;
  c) Atualizar o mapa de tratamento de dados, na forma do item 4.5;
  d) Monitorar as violações de dados pessoais:
  e) Vigilância constante do estado de sistemas em geral;
  f) Violação de segurança que leve à destruição acidental ou ilegal, perda, alteração, divulgação não autorizada ou acesso a dados pessoais, a Frimesa deverá prontamente avaliar o risco para

os direitos e liberdades das pessoas e, se apropriado, informar essa violação à autoridade competente;

g) Notificações à ANPD e aos titulares, em caso de incidente de segurança que haja violação de dados pessoais, na forma do item anterior;
h) Relatórios completos de cada violação.

4.8. Armazenamento e eliminação dos dados pessoais

- Deverá ser elaborada Política de Retenção de Dados Pessoais com Tabela de Temporalidade, para a gestão do armazenamento e eliminação dos dados pessoais.

4.9. Segurança da informação

- A Norma Interna nº 020 - Uso de Recursos de Informática e Segurança da Informação (NURI) disciplina o uso de recursos de Tecnologia da Informação/Informática e Segurança da Informação na Frimesa, zelando pela proteção de seu patrimônio, inclusive intelectual e também pelo patrimônio de seus parceiros, sejam eles fornecedores, clientes ou a sociedade. Esta Norma está disponível no Portal **eu.frimesa** e no sistema **SoftExpert.**

5. PAPÉIS E RESPONSABILIDADES

5.1. Colaboradores

- Proteger os dados pessoais contra acessos, modificação, destruição ou divulgação não autorizada;
- Cumprir as leis e normas que regulamentam a proteção de dados pessoais;
- Não discutir, citar ou compartilhar dados pessoais em ambientes públicos ou áreas expostas (transporte, restaurantes, encontros sociais, entre outros), incluindo comentários e opiniões em blogs, redes sociais, sites ou aplicativos;
- Não compartilhar dados pessoais e dados sensíveis sem a expressa autorização da Frimesa;
- Comunicar imediatamente à sua Liderança e ao Encarregados de Dados Pessoais, qualquer descumprimento ou violação desta política e/ou de normas e procedimentos relacionados.

5.2. Lideranças

- Comunicar imediatamente à sua Gerência e ao Encarregado de Dados qualquer descumprimento ou violação desta política e/ou de normas e procedimentos relacionados.

5.3. Gerentes

- Cabe aos Gerentes, supervisionar e fazer cumprir as diretrizes estabelecidas nesta Política e/ou de normas e procedimentos relacionados.

5.4. Área de Tecnologia da Informação

- Avaliar, sugerir e verificar controles de segurança que permitam a mitigação de riscos de vazamento de dados pessoais e/ou sensíveis armazenados física e/ou digitalmente;

- Acompanhar e validar controles de segurança de acesso a dados pessoais, tanto físico quanto digital.

5.5. Encarregado da proteção de dados

- Apoiar as áreas no entendimento da legislação de proteção de dados bem como sugerir mudanças nos processos que reforcem o compliance com a lei;

- Responder aos pedidos de informação e/ou solicitações sobre dados pessoais diretamente aos titulares, garantindo o direito dos titulares de dados na forma do item 4.5 desta Política;

- Representar a Frimesa em contato com a ANPD, quando necessário;

- Manter a atualização constante do programa de privacidade, na forma do item 4.6 desta Política;

- Auditar e acompanhar os termos de consentimento off line e os logs de consentimento on line coletados no site e nos aplicativos;

- Efetuar a gestão e guarda de trilha de auditoria para gestão dos logs de consentimento, coletados no site;

- Criar a atualizar sempre que necessário a tabela de temporalidade dos logs de consentimento e dos demais dados coletados e armazenados;

- Revisar a presente política no mínimo a cada 02 (dois) anos ou se houver fato relevante a ser tratado para esta ação;

- Validação e monitoramento das revisões contratuais/inclusão de cláusulas sobre proteção de dados pessoais nos contratos;

- Validação de Relatórios de Impacto a proteção de Dados Pessoas;

- Validação de outras avaliações em proteção de dados pessoais, como o Letimate Interest

Assessmente (LIA);

- Participação, desde as etapas inicias do projeto (desde a concepção) para que nele esteja embarcada privacidade (privacy by design);

- Coordenação/validação da Política de Privacidade (externa);

- Participação no Plano de Resposta à Incidentes, sempre que eles envolveram dados pessoais, inclusive quanto a providência de comunicações aos titulares e a Autoridade Nacional de Proteção de Dados.

5.6. Comitê Gestor de Proteção de Dados

- Implementação de um plano de ação que prevê a conformidade da instituição com a lei, incluindo um conjunto de ações envolvendo processos, políticas, controles de segurança, adequações jurídicas e adequações de sistemas de informação.

5.7. Diretor Presidente Executivo

- Promover e apoiar o processo de atendimento às diretrizes aprovadas e garantir que estejam alinhadas as leis, às boas práticas de gestão, inclusive ao planejamento estratégico da Frimesa;

- Deliberar sobre os procedimentos que sejam encaminhados pelo Encarregado no caso de ocorrências.

6. DESCUMPRIMENTO DESTA POLÍTICA

- Para orientações adicionais, consultar o Comitê Gestor de Proteção de Dados (CGPD) ou Diretor Presidente Executivo.

- O descumprimento desta Política, bem como o descumprimento da Legislação Aplicável e demais Políticas da Frimesa, tal como os Fundamentos Corporativos, pode estar sujeito a procedimentos disciplinares internos avaliados pelo Diretor Presidente Executivo, sem prejuízo de eventuais medidas legais aplicáveis.

- Casos omissos ou exceções a essa Política deverão ser comunicados e deliberados pelo Diretor Presidente Executivo, conforme o caso. Além disso, buscando manter os padrões éticos da Cooperativa e monitorar as relações comerciais com Terceiros, bem como auxiliar na prevenção e detecção de todas as formas de Corrupção, a Frimesa apoia e encoraja as Pessoas a denunciarem quaisquer práticas que possam representar violação ou potencial violação a essa Política, ao Sistema de Integridade, ou que estejam em desacordo com as legislações nacionais e estrangeiras aplicáveis.

- As denúncias devem ser feitas ao Canal de Denúncias: https://www.canalconfidencial.com.br/frimesa/ ou pelo 0800 645 5040.

- Não será permitida nem tolerada qualquer retaliação contra um colaborador que, de boa-fé, relate uma preocupação sobre conduta ilegal ou em não conformidade às diretrizes estabelecidas no Código de Ética e Conduta.

7. DISPOSIÇÕES FINAIS

- Esta Política entra em vigor a partir da data de sua assinatura, podendo ser alterado a qualquer tempo e critério;

- Esta Política deverá ser publicada no SoftExpert.

8. NORMAS EXTERNAS RELACIONADOS E OUTRAS REFERÊNCIAS

Lei nº 12.965/2014 - Marco Civil da Internet;
Lei nº 13.709/2018 - LGPD – Lei Geral de Proteção de Dados;
ISO 27001 e 27002 – SGSI – Sistema de Gestão da Segurança da Informação;
ISO 27701 – SGPI – Sistema de Gestão da Privacidade da Informação;
Política de Segurança da Informação – NURI (Norma nº 020);
Guia Orientativo Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) - por agentes de tratamento no contexto eleitoral – ANPD.

	Elaboração	Aprovação
Revisão nº 000001 em 20/02/2023	Assessoria de Governança, Riscos e Integridade	Diretor Presidente Executivo

9. GLOSSÁRIO / DEFINIÇÕES

- A proteção de dados pessoais deve ser realizada de acordo com a Lei Nº 13.709, de 14 de agosto de 2018, disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm, que apresenta os seguintes conceitos:

a) Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
b) Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
c) Encarregado ou DPO – Data Protection Officer – encarregado, indicado pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
d) Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de

dados pessoais em nome do controlador;

e) Dados pessoais caracterizam-se por qualquer dado que permita a identificação do titular dos dados pessoais (pessoa física), exemplos: Nome, CPF, Endereço, Dados de consumo, Dados de localização, Perfil comportamental, etc.

f) Dados pessoais sensíveis é dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato 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.

g) Dados pessoais de Crianças e de Adolescentes deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

h) Tratamento de dados pessoais é a coleta, acesso, utilização, processamento, arquivamento, armazenamento, avaliação, controle, modificação, reprodução, transmissão, distribuição, compartilhamento, transferência ou eliminação de dados pessoais;

i) Uso compartilhado de dados: Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

j) Das infrações cometidas às normas previstas nesta Lei, ficam os infratores sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

k) advertência, com indicação de prazo para adoção de medidas corretivas;

l) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

    i. multa diária, observado o limite total a que se refere o inciso II;
    ii. publicização da infração após devidamente apurada e confirmada a sua ocorrência;
    iii. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
    iv. eliminação dos dados pessoais a que se refere a infração;

m) ANPD – Autoridade Nacional de Proteção de Dados: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;

n) Programa de Governança em Privacidade: programa que demonstre o comprometimento da empresa em adotar processos e políticas que assegurem o cumprimento das normas e boas práticas em relação a proteção de dados pessoais.