MACRO PROCESSO	**POLÍTICAS DE GOVERNANÇA**
PROCESSO TÍTULO	**POLÍTICA DE PROTEÇÃO DE DADOS**
RESPONSÁVEL	**COMITÊ DE GOVERNANÇA, RISCOS E INTEGRIDADE**
CÓDIGO DE CONTROLE	**POLSUST005/002**
APROVAÇÃO	**CONSELHO DE ADMINISTRAÇÃO**
DATA	**04/12/2025**
VERSÃO	**2.0**

POLÍTICA GERAL DE PROTEÇÃO DE DADOS

1. INTRODUÇÃO

A Sustentalli confirma a importância da privacidade e da proteção de dados de todos/as os stakeholders (cooperados/as, clientes, parceiros, terceiros e demais envolvidos).
Em conformidade com a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), esta Política estabelece diretrizes básicas para o tratamento de dados, refletindo o compromisso da Cooperativa com a transparência, a responsabilidade e a segurança.
Este documento serve como base para a jornada de implementação da LGPD na Sustentalli, garantindo que o tratamento de dados ocorra dentro das capacidades atuais e do compromisso de evolução contínua da Cooperativa.

2. ESCOPO E APLICABILIDADE

Esta Política se aplica a todas as operações de tratamento de dados realizadas pela Sustentalli, abrangendo:

- Todos/as os/as cooperados/as;
- Terceiros e parceiros de negócios que, de alguma forma, tratem dados em nome da Cooperativa ou em conjunto com ela;
- Todas as áreas, comitês, órgãos de governança e projetos da Sustentalli que utilizem dados pessoais ou não.

A aplicação desta Política deve ser entendida e observada por todos/as que tenham acesso ou realizem o tratamento de dados sob responsabilidade da Sustentalli.
Os dados pessoais e/ou de empresas serão tratados exclusivamente para finalidades lícitas, específicas e previamente informadas aos/as titulares, tais como, exemplificativamente:

- Execução de contratos;
- Cumprimento de obrigações legais e regulatórias;
- Envio de comunicações institucionais;
- Melhoria de serviços e desenvolvimento de projetos personalizados;
- Promoção de iniciativas sociais e ambientais.

3. PRINCÍPIOS FUNDAMENTAIS DO TRATAMENTO DE DADOS

O tratamento de dados realizado pela Sustentalli é pautado nos princípios estabelecidos na LGPD, garantindo que todas as operações sejam justas, transparentes e limitadas ao necessário:

- **Finalidade:** O tratamento dos dados se restringe aos propósitos legítimos, específicos e explícitos listados no escopo desta política (como a execução de contratos, cumprimento de obrigações legais e desenvolvimento de projetos ESG), sem utilização posterior incompatível com as finalidades informadas.
- **Adequação:** A forma e a extensão do tratamento devem ser compatíveis com as finalidades informadas ao/à titular, no contexto da relação estabelecida com a Sustentalli.
- **Necessidade (Minimização de Dados):** A coleta e o uso dos dados serão limitados ao mínimo indispensável para o cumprimento da finalidade, evitando a coleta de dados excessivos ou desnecessários.
- **Livre Acesso:** É garantida aos/às titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados, bem como sobre a integralidade de seus dados.
- **Qualidade dos Dados:** A Sustentalli buscará garantir a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e com a finalidade do tratamento.
- **Transparência:** As informações sobre o tratamento de dados serão fornecidas de forma clara, precisa e facilmente acessível aos/as titulares, sempre que solicitado ou quando necessário.
- **Segurança:** Serão adotadas medidas técnicas e administrativas aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
- **Prevenção:** Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados, incluindo programas de treinamento, conscientização e controles de segurança.
- **Não Discriminação:** O tratamento de dados não será realizado para fins discriminatórios, ilícitos ou abusivos.
- **Responsabilização e Prestação de Contas (Accountability):** Demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados, bem como a eficácia dessas medidas.

4. CONCEITOS FUNDAMENTAIS (LGPD)

Para os fins desta Política, e em linha com a LGPD, consideram-se:

- **Dados Pessoais:** Informação relacionada a pessoa natural identificada ou identificável (ex.: nome, CPF, endereço, e-mail, telefone, dados de localização etc.).
- **Dados Pessoais Sensíveis:** Dados 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 vinculados a uma pessoa natural.

- **Titular:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Tratamento:** Toda operação realizada com dados, como as que se referem a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Controlador/a:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados. No contexto interno da Cooperativa, a Sustentalli é, em regra, a Controladora dos dados que trata para fins próprios.
- **Operador/a:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do/a Controlador/a.
- **Encarregado/a (*DPO – Data Protection Officer*):** Pessoa indicada pelo Controlador/a e/ou Operador/a para atuar como canal de comunicação entre o/a Controlador/a, os/as Titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).

5. GOVERNANÇA DE PRIVACIDADE, RISCOS E SUSTENTABILIDADE

5.1 Modelo de Governança

A Sustentalli adota um modelo de Governança de Privacidade alinhado:
- às melhores práticas internacionais (ISO 27701, NIST, IAPP);
- à legislação brasileira (LGPD – Lei nº 13.709/2018);
- aos princípios cooperativistas;
- aos *frameworks* de governança e sustentabilidade (IFRS S1 e S2, GRI, SASB, ABNT PR 2030).

Este modelo assegura que o tratamento de dados pessoais esteja integrado:
- à Governança Corporativa;
- aos pilares ESG (Ambiental, Social e Governança);
- à gestão de riscos;
- aos processos de continuidade de negócios da Cooperativa.

5.2 Estrutura de Governança

A governança de privacidade da Sustentalli é composta por:

a) Conselho de Administração (CA)

- Supervisionar o Programa de Privacidade e Proteção de Dados;
- Aprovar políticas, planos, indicadores e relatórios;
- Estabelecer diretrizes estratégicas de privacidade e segurança da informação;
- Avaliar impactos de riscos relevantes relacionados a dados e sua interface com a estratégia ESG.

b) DPO – Encarregado/a pelo Tratamento de Dados

Responsável por:

- Atender titulares e atuar como ponto focal junto à ANPD;
- Monitorar a conformidade da Cooperativa com a LGPD e esta Política;
- Assessorar o Conselho de Administração em temas de privacidade, risco e ESG;
- Supervisionar operadores/as internos e externos;
- Emitir relatórios periódicos de risco, incidentes e conformidade;
- Apoiar a elaboração e atualização do ROPA (Registro das Operações de Tratamento) e do Inventário de Dados.

c) Comitê de Gestão Administrativa e Financeira (CGAF)

Órgão de apoio técnico responsável por:

- Validar riscos relacionados a dados e segurança da informação;
- Avaliar contratações de terceiros que tratem dados;
- Aprovar planos de melhoria e planos de ação corretiva;
- Interagir com o DPO nas avaliações de impacto (DPIA/Relatórios de Impacto à Proteção de Dados, quando aplicável);
- Acompanhar indicadores de risco (KRIs) e conformidade (KPIs) de privacidade.

d) Cooperados/as e Colaboradores/as

Todos/as são responsáveis por:

- Cumprir esta Política e demais normas internas relacionadas à LGPD;
- Participar de treinamentos e ações de conscientização;
- Utilizar apenas sistemas autorizados para o tratamento de dados;
- Reportar, de forma imediata, incidentes ou fragilidades de segurança de que tenham conhecimento.

5.3 Princípios de Governança e ESG

A Sustentalli reconhece que a privacidade e a proteção de dados são pilares essenciais da Governança ESG (Environmental, Social and Governance), alinhados a IFRS S1, IFRS S2, GRI, SASB e ABNT PR 2030.

Assim, a Cooperativa se compromete a:

- Garantir tratamento ético e responsável dos dados;
- Respeitar direitos humanos e a não discriminação;
- Assegurar transparência na relação com todos/as os stakeholders;
- Prevenir riscos operacionais, jurídicos, reputacionais e socioambientais;
- Manter registros e evidências de conformidade (accountability);
- Integrar risco de privacidade à matriz de risco global da Sustentalli.

5.4 Relatórios, Indicadores e Accountability

O DPO apresentará ao Conselho de Administração um **relatório semestral** contendo, no mínimo:

- Indicadores de incidentes (KRIs) – número, classificação e severidade;

- Indicadores de conformidade (KPIs) – treinamentos, contratos com cláusulas LGPD, atualização de registros, prazos de atendimento a titulares;
- Avaliação da maturidade de privacidade da Cooperativa;
- Situação da cadeia de fornecedores e terceiros que tratam dados;
- Ações de melhoria contínua.

Em cumprimento ao Art. 6, X da LGPD, a Sustentalli manterá evidências formais de:

- Registros das operações de tratamento (ROPA – Art. 37);
- Políticas, fluxos e procedimentos relacionados à LGPD;
- Treinamentos e ações de conscientização;
- Gestão de incidentes de segurança (Art. 48)
- Gestão de terceiros e operadores (Art. 39).

6. BASES LEGAIS PARA O TRATAMENTO

A Sustentalli somente realizará o tratamento de dados quando amparada por uma das bases legais previstas na LGPD, tais como:

- **Consentimento:** Manifestação livre, informada e inequívoca do/a titular, concordando com o tratamento de seus dados para finalidades determinadas.
- **Cumprimento de Obrigação Legal ou Regulatória:** Tratamento necessário para cumprimento de determinações legais, regulatórias ou fiscais.
- **Execução de Contrato ou de Procedimentos Preliminares:** Tratamento necessário para executar um contrato do qual o/a titular é parte (por exemplo, ficha de matrícula de cooperado/a, prestação de serviços por parceiros) ou para procedimentos preliminares a pedido do/a titular.
- **Legítimo Interesse:** Tratamento realizado para atender aos interesses legítimos da Sustentalli ou de terceiros, desde que não viole os direitos e liberdades fundamentais do/a titular, observada a elaboração de avaliação de impacto/legítimo interesse quando aplicável.
- **Proteção do Crédito:** Tratamento para fins de avaliação de risco e prevenção de fraudes, quando cabível.

Outras hipóteses previstas na LGPD poderão ser utilizadas, sempre com a devida documentação e justificativa.

7. DECLARAÇÃO DE PAPÉIS E RESPONSABILIDADES NO TRATAMENTO DE DADOS

7.1 Definições Legais (Art. 5º, VI e VII da LGPD)

- **Controlador/a:** "Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais."
- **Operador/a:** "Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do/a controlador/a."

7.2 Sustentalli como Controladora

A Sustentalli atua como Controladora quando:

- Trata dados de cooperados/as;
- Trata dados de candidatos/as a vagas, projetos ou ingresso na Cooperativa;
- Trata dados de clientes para fins administrativos, de relacionamento e faturamento;
- Trata dados de fornecedores para fins de cadastro, avaliação e pagamento;
- Trata dados de *leads*, contatos comerciais e comunicação institucional;
- Gerencia plataformas internas, sistemas operacionais, ferramentas de CRM (*Customer Relationship Management*) e comunicação;
- Gere sistemas e bancos de dados da cooperativa em sua operação própria.

7.3 Sustentalli como Operadora

A Sustentalli poderá atuar como Operadora, mediante contrato ou análise para produção de uma proposta, em atividades como:

- Elaboração de diagnósticos ESG e de sustentabilidade que envolvam análise de dados dos clientes;
- Prestação de consultoria que envolva acesso a dados pessoais fornecidos pelo cliente;
- Produção de relatórios ou inventários de sustentabilidade contendo dados;
- Gestão de projetos em que haja acesso a dados de empregados/as, cooperados/as ou clientes de terceiros.

Nesses casos:

- O cliente será o Controlador;
- A Sustentalli obedecerá às instruções do Controlador, em conformidade com o Art. 39 da LGPD;
- As responsabilidades serão formalizadas em contrato e/ou DPA (*Data Processing Agreement*).

7.4 Cooperados/as como Operadores/as Internos

Os/As cooperados/as que manusearem dados em nome da Sustentalli atuarão como Operadores/as Internos, devendo:

- Cumprir integralmente esta Política e demais normas de privacidade da Cooperativa;
- Assinar Termo de Sigilo e Confidencialidade
- Cumprir o DPA interno (Acordo de Tratamento de Dados) quando aplicável;
- Utilizar somente sistemas, canais e dispositivos autorizados;
- Reportar incidentes ou usos indevidos de dados.

7.5 Operadores/as Externos

Terceiros que tratem dados por ordem da Sustentalli deverão:

- Assinar DPA (*Data Processing Agreement*) ou cláusulas contratuais específicas de proteção de dados;
- Demonstrar capacidade técnica e organizacional para proteção de dados;
- Comprovar controles de segurança adequados;
- Aceitar auditorias, avaliações e solicitações de evidências de conformidade;
- Atender às instruções da Sustentalli, na condição de Controladora.

7.6 Mapa de Papéis e Responsabilidades

A tabela abaixo exemplifica os papéis em diferentes atividades:

Atividade	Sustentalli	Cliente	Terceiro	Observação
Dados de cooperados/as	Controladora	—	Operadores/as internos/externos	Sistemas internos de RH/gestão
Diagnóstico ESG	Operadora	Controlador	—	Instruções do cliente
Relatórios de sustentabilidade	Operadora	Controlador	—	Dados podem incluir informações pessoais
Comunicação institucional Sustentalli	Controladora	—	Operador (agência/marketing)	Campanhas, newsletters, mídias sociais
Gestão financeira	Controladora	—	Sistema financeiro (ERP/banco)	Terceiros atuam como operadores
Sistema do site	Controladora	—	Desenvolvedor/Host	Terceiro atua como operador
CRM e gestão de *leads*	Controladora	—	Plataforma CRM	Terceiro atua como operador
Auditorias anuais	Controladora	—	Auditoria externa	Acesso controlado a dados pessoais, se houver

8. DIREITOS DOS TITULARES

A Sustentalli garante aos/às titulares o exercício pleno de seus direitos, conforme Art. 18 da LGPD. Os/As titulares poderão solicitar, a qualquer momento e mediante requisição:

- **Confirmação da existência de tratamento:** Saber se a Sustentalli trata ou não dados do/a titular.
- **Acesso aos dados:** Obter cópia dos dados que estão sendo tratados.
- **Correção de dados incompletos, inexatos ou desatualizados:** Solicitar a atualização ou retificação de seus dados cadastrais
- **Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD:** Desde que os dados se enquadrem nessas condições.
- **Portabilidade dos dados:** Solicitar a transferência dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, observadas normas da ANPD e segredos comerciais.

- **Eliminação dos dados tratados com consentimento:** Exceto nas hipóteses de retenção prevista em lei (por exemplo, cumprimento de obrigação legal ou regulatória).

- **Informação sobre o compartilhamento:** Conhecer as entidades públicas e privadas com as quais a Sustentalli realizou uso compartilhado de dados.

- **Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa:** Ser informado/a sobre os impactos de não autorizar o tratamento de seus dados, quando a base legal usada for o consentimento.

- **Revogação do consentimento:** Retirar o consentimento concedido a qualquer momento, sem que isso afete a legalidade do tratamento realizado antes da revogação.

- **Oposição ao tratamento:** Opor-se a tratamento realizado com fundamento em bases legais distintas do consentimento, em caso de descumprimento à LGPD.

9. PROCEDIMENTO DE ATENDIMENTO AOS DIREITOS DO TITULAR (SOP LGPD)

Para garantir atendimento seguro, padronizado e auditável aos/às titulares, a Sustentalli adota o seguinte procedimento:

9.1 Canais de Solicitação

As solicitações de titulares deverão ser feitas por:
- E-mail oficial de privacidade: lgpd@sustentalli.com.br (e/ou outro canal oficial definido pela Cooperativa);
- Formulário específico no site da Sustentalli, quando disponível;
- Outros canais oficiais que venham a ser formalmente comunicados.

9.2 Prazos de Atendimento (referência LGPD)

- Confirmação da existência de tratamento: até 15 dias;
- Acesso aos dados: até 15 dias;
- Correção/atualização: até 15 dias;
- Eliminação/bloqueio: até 30 dias;
- Portabilidade: entre 30 e 60 dias, conforme complexidade;
- Revogação de consentimento: imediata, sempre que tecnicamente possível.

9.3 Etapas do Processo
1. Recebimento da solicitação pelo canal oficial;
2. Validação da identidade do/a titular (Art. 18, parágrafo único), com comprovação razoável de autenticidade;
3. Classificação da solicitação por tipo de direito;
4. Análise técnica pelo DPO e, se necessário, pelas áreas envolvidas;
5. Consulta a terceiros (operadores, parceiros), quando aplicável;
6. Decisão e elaboração de resposta formal ao/a titular;
7. Envio da resposta dentro dos prazos previstos;
8. Registro em livro eletrônico de solicitações, para fins de auditoria e accountability.

9.4 Recusa Justificada (Art. 18, §4º)

O atendimento ao pedido do/a titular poderá ser negado, de forma justificada, quando:

- Houver risco de violar segredos comerciais ou industriais;
- Comprometer investigações, auditorias ou processos judiciais/administrativos em curso;
- Existir obrigação legal ou regulatória de retenção de dados;
- A informação solicitada não puder ser fornecida sem exposição de dados de terceiros.

Em qualquer hipótese, o/a titular receberá resposta formal, com explicação clara sobre os motivos da recusa parcial ou total.

9.5 Evidências de Conformidade

Toda solicitação será registrada com:

- Número do caso;
- Data, hora e canal de recebimento;
- Titular/identificação verificada;
- Tipo de pedido;
- Decisão tomada e justificativas;
- Evidências e documentos enviados ao/a titular;
- Data de encerramento do atendimento.

10. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

10.1 Objetivo

Estabelecer diretrizes de segurança da informação para proteger dados pessoais e corporativos, em alinhamento com a LGPD e com a estratégia de riscos da Sustentalli.

10.2 Princípios

- **Confidencialidade –** acesso à informação somente por pessoas autorizadas;
- **Integridade –** garantia de exatidão, consistência e fidedignidade das informações;
- **Disponibilidade –** acesso às informações quando necessário para as atividades autorizadas;
- **Autenticidade –** garantia de que a informação foi produzida por quem declara tê-la produzido;
- **Minimização de Dados** – limitação do tratamento ao estritamente necessário.

10.3 Controles Mínimos

A Sustentalli adotará medidas de segurança, técnicas e administrativas, como:

- Políticas de senha forte e renovação periódica (ex.: a cada 90 dias);
- Acesso restrito por perfil e necessidade de conhecimento (“need-to-know”);
- Bloqueio de contas inativas ou suspeitas de uso indevido;
- Uso de antivírus, firewall e, quando cabível, criptografia;
- VPN (*Virtual Private Network*) para acesso remoto a sistemas internos;
- Proibição de envio de dados sensíveis por aplicativos não corporativos (ex.: WhatsApp pessoal, e-mail pessoal);
- Armazenamento de dados apenas em plataformas autorizadas pela Cooperativa; Registro e rastreabilidade de acessos a dados pessoais, sempre que tecnicamente possível.

10.4 Dispositivos Pessoais (BYOD)

O uso de dispositivos pessoais para tratamento de dados da Sustentalli somente será permitido se:

- Dispositivo estiver criptografado, quando tecnicamente viável;
- Houver senha, biometria ou outro mecanismo de autenticação forte;
- O dispositivo estiver cadastrado ou autorizado internamente;
- O/A cooperado/a e/ou o/a colaborador/a assuma a responsabilidade de cumprir a PSI e permitir, quando necessário, ações de segurança (ex.: limpeza remota de dados corporativos).

10.5 Treinamento e Conscientização

- Será implementado programa contínuo de conscientização e treinamento para cooperados/as e colaboradores/as, abrangendo LGPD, segurança da informação e boas práticas;
- O treinamento será, no mínimo, anual e obrigatório, podendo haver ações adicionais em caso de incidentes ou mudanças relevantes na política.

11. MEDIDAS DE SEGURANÇA E REGISTRO DE DADOS

A Sustentalli está no início da jornada para implementar uma política robusta de proteção de dados. Reforça-se o compromisso em evoluir continuamente, em alinhamento com a LGPD, para garantir a privacidade e segurança de todos os dados pessoais tratados.

11.1 Medidas de Segurança

- **Controles de Acesso:** Acesso aos dados restrito apenas aos/às cooperados/as, colaboradores/as e parceiros estritamente necessários ao desempenho de suas funções.
- **Treinamento:** Programa contínuo de capacitação sobre segurança e privacidade, como descrito nesta Política.
- **Tecnologia:** Compromisso de implantar e evoluir soluções tecnológicas de segurança (criptografia, *firewalls*, antivírus, *backups*, etc.), de forma progressiva, em conformidade com o planejamento estratégico e a maturidade da jornada LGPD da Sustentalli.

11.2 Registro das Operações de Tratamento (ROPA – Art. 37)

A Sustentalli estruturará progressivamente e manterá o Registro das Operações de Tratamento de Dados Pessoais (ROPA), contendo, no mínimo:

- Finalidade do tratamento;
- Base legal utilizada;
- Categorias de titulares e de dados;
- Compartilhamentos e transferências;
- Responsáveis internos;
- Medidas de segurança aplicadas;
- Prazos de retenção;
- Riscos identificados e medidas de mitigação.

Esse registro será elemento central para garantir o princípio da responsabilização e prestação de contas.

12. COMPARTILHAMENTO E TRANSFERÊNCIA INTERNACIONAL DE DADOS

12.1 Compartilhamento de Dados

O compartilhamento de dados pessoais com terceiros (Operadores/as ou outros/as Controladores/as) será realizado apenas:

- Para cumprimento de obrigações legais ou regulatórias (ex.: órgãos reguladores, Receita Federal);
- Para execução de serviços essenciais (ex.: processamento de transações, serviços de tecnologia, hospedagem de dados, auditoria), sempre sob rígidos contratos que estabeleçam as obrigações de proteção de dados;
- Mediante consentimento do/a titular, quando essa for a base legal aplicável;
- Em outras hipóteses previstas na LGPD, com *due diligence* prévia de terceiros.

12.2 Transferência Internacional de Dados

A Sustentalli evitará, sempre que possível, a transferência de dados pessoais para países ou organismos internacionais que não proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD.

Quando a transferência internacional for necessária, ela ocorrerá apenas mediante:

- Verificação de que o país ou organismo garante nível de proteção adequado nos termos da ANPD;
- Adoção de cláusulas contratuais específicas, normas corporativas globais ou outros mecanismos admitidos em lei;
- Atendimento às exigências da LGPD e de orientações da ANPD.

13. PROCESSO DE *DUE DILIGENCE* EM TERCEIROS (LGPD + ESG)

13.1 Fundamentação

A Sustentalli adotará processo obrigatório de avaliação *("due diligence")* de terceiros que tratem dados em seu nome, com base em:

- **Art. 39 da LGPD –** operador deve seguir instruções do/a controlador/a;
- **Art. 46 da LGPD –** segurança da informação e proteção contra acessos não autorizados;
- **Art. 50 da LGPD –** boas práticas e governança;
- **Diretrizes de ESG –** governança exige avaliação prévia de riscos de terceiros.

13.2 Itens Avaliados

No processo de *due diligence*, serão avaliados, entre outros:

- Capacidade técnica e organizacional para tratamento de dados;
- Controles de segurança da informação;
- Existência de política de privacidade e proteção de dados;
- Histórico de incidentes relevantes de segurança;
- Local de tratamento e armazenamento (incluindo eventual transferência internacional).

13.3 Requisitos para Contratação

Como condição para contratação de terceiros que tratem dados em nome da Sustentalli, será exigido:

- Assinatura de DPA (*Data Processing Agreement*) ou cláusulas específicas de proteção de dados;
- Assinatura de Termo de Confidencialidade;
- Aceitação de auditorias ou avaliações pela Sustentalli, quando justificadas;
- Compromisso de não realizar transferências ilícitas de dados para outros países ou suboperadores sem autorização e sem garantia de proteção adequada.

14. POLÍTICA DE RETENÇÃO, ARQUIVAMENTO E DESCARTE DE DADOS

Com base nos Arts. 15 e 16 da LGPD, os dados devem ser eliminados quando deixarem de ser necessários para as finalidades para as quais foram coletados, ou quando não houver outra base legal que justifique sua manutenção.

14.1 Princípios

- **Retenção mínima necessária –** manter dados apenas pelo tempo estritamente necessário;
- **Eliminação segura –** adoção de técnicas que impeçam a recuperação indevida dos dados;
- **Arquivamento obrigatório –** manutenção dos dados quando houver obrigação legal, regulatória, fiscal, contábil ou necessidade de defesa em processos;
- **Transparência ao/à titular –** informações claras sobre prazos e critérios de retenção, sempre que solicitado.

14.2 Prazos de Retenção (exemplos)

Os prazos abaixo são referenciais e poderão ser detalhados em documento complementar e ajustados conforme legislação específica:

- **Dados de cooperados/as:**
  Prazo: 5 anos após desligamento, salvo obrigações legais específicas que exijam prazo maior;
  Base legal: obrigações legais e regulatórias, defesa em processos.

- **Dados de fornecedores:**
  Prazo: 5 anos após término da relação;
  Base legal: Código Civil, obrigações fiscais e contratuais.

- **Dados de *leads:***
  Prazo: 1 ano após último contato efetivo ou até revogação do consentimento;
  Base legal: consentimento e legítimo interesse (quando aplicável).

- **Dados de projetos**
  Prazo: enquanto durar o contrato e, após, pelo prazo necessário à defesa em processos e cumprimento de obrigações legais;
  Base legal: execução contratual e obrigações legais.

- **Dados sensíveis:**
  Prazo: mínimo necessário à finalidade específica;
  Base legal: hipóteses do Art. 11 da LGPD.

14.3 Métodos de Eliminação

A eliminação ou descarte de dados poderá ocorrer por:
- Destruição criptográfica;
- Sobrescrita segura dos registros;
- Anonimização irreversível, quando for necessário manter informações para fins estatísticos ou históricos, sem identificação de titulares.

14.4 Prova de Descarte

Sempre que houver eliminação relevante de dados, será emitido e arquivado pelo/a DPO um Certificado Interno de Descarte, contendo:
- Data;
- Tipo de dado;
- Sistema ou local;
- Método de descarte;
- Responsáveis envolvidos.

15. INCIDENTES DE SEGURANÇA E PLANO DE RESPOSTA

A Sustentalli está comprometida com a adoção e aprimoramento contínuo de rigorosas medidas de segurança. Contudo, reconhece que nenhum sistema é totalmente imune a falhas ou incidentes.

15.1 Definição de Incidente de Segurança

Considera-se Incidente de Segurança qualquer evento que resulte em tratamento de dados em desconformidade com a LGPD, como:

- Destruição, perda, alteração, acesso ou comunicação de dados pessoais de forma não autorizada ou ilícita;
- Vazamento intencional ou acidental;
- Ataques externos (ex.: *ransomware, phishing* bem-sucedido);
- Uso indevido interno ou compartilhamento não autorizado.

15.2 Tipos de Incidentes Abrangidos

Entre outros, estão abrangidos:
- Vazamento de dados;
- Acesso não autorizado;
- Perda, destruição ou alteração acidental;
- Uso indevido interno;
- *Phishing* bem-sucedido;
- *Ransomware*;
- Compartilhamento incorreto ou envio para destinatário/a errado/a;
- Transferência inadequada para país/terceiro não autorizado.

15.3 Time de Resposta a Incidentes (TRI)

O Time de Resposta a Incidentes (TRI) será composto por:
- **Líder:** DPO – Encarregado/a de Dados;

- **Apoio:** Comitê de Gestão Administrativa e Financeira;
- **Especialistas:** representantes de Segurança da Informação, Jurídico, Comunicação e demais áreas impactadas.

15.4 Fluxo de Resposta – 8 Etapas

1. **Detecção**
- Recebimento de alerta por cooperado/a, sistema ou terceiro;
- Registro inicial do incidente.

2. **Contenção imediata**
- Bloqueio de acessos;
- Desconexão de máquinas ou contas comprometidas;
- Isolamento de sistemas afetados.

3. **Análise técnica**
- Confirmação da ocorrência do incidente;
- Identificação do tipo de dado afetado;
- Quantidade de titulares envolvidos;
- Determinação da causa raiz.

4. **Classificação de severidade**
- Baixo risco;
- Médio risco;
- Alto risco (potencial risco ou dano relevante – obriga notificação à ANPD e aos titulares).

5. **Ação corretiva**
- Aplicação de correções (patches, restauração de backup, mudança de senha, revogação de acessos etc.);
- Mitigação de danos e prevenção de reincidência.

6. **Comunicação interna**
- Comunicação ao Conselho de Administração;
- Comunicação às áreas e comitês afetados.

7. **Comunicação obrigatória (Art. 48 da LGPD):** Quando houver risco ou dano relevante, a Sustentalli se compromete a:
- Notificar a ANPD, no prazo mais curto possível, contendo:
  - Descrição da natureza dos dados pessoais afetados;
  - Indicação dos titulares envolvidos;
  - Indicação das medidas técnicas e de segurança utilizadas;
  - Descrição dos riscos relacionados ao incidente;
  - Medidas adotadas ou a serem adotadas para reverter ou mitigar os efeitos.
- Comunicar os/as titulares afetados/as, em linguagem clara e acessível, descrevendo:
  - Natureza dos dados pessoais afetados;
  - Informações de contato do/a Encarregado/a (DPO);
  - Medidas adotadas pela Sustentalli;
  - Recomendações de medidas que o/a titular pode adotar para mitigar eventuais danos.

8. **Registro e melhoria contínua**
- Elaboração de relatório pós-incidente;
- Atualização da matriz de risco;
- Ajustes em políticas, processos e controles;
- Treinamentos específicos, se necessário.

15.5 Prazos Recomendados

- **Classificação preliminar do incidente:** até 24 horas após detecção;
- **Notificação à ANPD (quando aplicável):** até 72 horas após classificação, sempre buscando o menor prazo possível;
- **Comunicação aos/às titulares (quando aplicável):** preferencialmente até 72 horas, alinhada à comunicação com a ANPD.

16. INDICADORES DE PRIVACIDADE E RISCO

Para apoiar a governança, a Sustentalli adotará indicadores (KPIs e KRIs) de privacidade e proteção de dados.

16.1 KPIs (Indicadores de Conformidade)

Exemplos:
- % de cooperados/as e colaboradores/as treinados/as em LGPD;
- % de solicitações de titulares atendidas dentro do prazo;
- % de contratos com cláusulas específicas de LGPD;
- Atualização periódica do ROPA;
- Atualização da matriz de risco de privacidade.

16.2 KRIs (Indicadores de Risco)

Exemplos:
- Número total de incidentes de segurança envolvendo dados;
- Severidade média dos incidentes;
- Vulnerabilidades detectadas e não tratadas em prazo adequado;
- Casos de uso indevido de dados;
- Atrasos ou falhas na eliminação de dados após o prazo de retenção.

16.3 Relatórios ao Conselho de Administração

- **Periodicidade:** semestral (no mínimo);
- **Conteúdo:** consolidação de KPIs, KRIs, incidentes relevantes, ações de melhoria, auditorias de terceiros e ajustes de governança.

17. INVENTÁRIO DE DADOS PESSOAIS E REGISTRO DAS OPERAÇÕES DE TRATAMENTO (ROPA) – MODELOS

17.1 Inventário de Dados Pessoais – Modelo

O inventário deverá conter, no mínimo, os seguintes campos:
- Atividade/processo de negócio;
- Finalidade do tratamento;
- Titular (categoria: cooperado/a, colaborador/a, fornecedor, cliente, *lead*, etc.);

- Tipo de dado (comum ou sensível, categorias específicas);
- Base legal;
- Local de armazenamento (sistemas, repositórios físicos, nuvem);
- Riscos associados;
- Medidas de segurança aplicadas;
- Encarregado/a da área responsável;
- Terceiros envolvidos (operadores/as, controladores conjuntos);
- Prazo de retenção;
- Data da última revisão.

17.2 ROPA – Registro das Operações de Tratamento

Em conformidade com o Art. 37 da LGPD, o ROPA será um documento estruturado, alinhado ao inventário de dados, que detalhará:

- Nome e contatos do/a Controlador/a e do/a DPO;
- Finalidades de cada operação de tratamento;
- Descrição das categorias de titulares e dados envolvidos;
- Categorias de destinatários a quem os dados foram ou serão divulgados;
- Transferências internacionais, quando existentes;
- Prazos de retenção previstos;
- Descrição geral das medidas técnicas e organizacionais de segurança;
- Referência a avaliações de impacto (quando aplicáveis).

18. ENCARREGADO/A PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

Embora a nomeação de Encarregado/a não seja obrigatória em todos os casos, por boa prática de governança e para facilitar a comunicação entre a Sustentalli, os/as titulares e a ANPD, foi nomeado:

- **Nome do DPO:** Paulo Josef Gouvea da Gama
- **Comitê Responsável:** Comitê de Gestão Administrativa e Financeira
- **E-mails para Contato:**
  admfin@sustentalli.com.br
  lgpd@sustentalli.com.br

19. PROCEDIMENTOS OPERACIONAIS, DOCUMENTOS COMPLEMENTARES

Esta Política é complementada por documentos internos que detalham procedimentos e modelos, que foram desenvolvidos ou serão desenvolvidos no decorrer do crescimento da Sustentalli:

- Procedimentos Operacionais Padrão (POP) relacionados à LGPD;
- Modelos de Inventário de Dados e ROPA;
- Modelos de DPA (*Data Processing Agreement*) e Termos de Confidencialidade;
- Matriz de Riscos de Privacidade;
- Plano de Resposta a Incidentes (detalhado);
- Política de Segurança da Informação (documento-mãe, quando aplicável);
- Manuais de boas práticas para cooperados/as e parceiros;
- Outras políticas de governança, risco, crise e ESG, em especial aquelas atualizadas em função dos pareceres jurídicos e da evolução do Estatuto Social da Cooperativa.

20. ANEXOS

Anexo 1: Mapa de Papéis e Responsabilidades no Tratamento de Dados
Anexo 2: Modelo de Inventário LGPD
Anexo 3: Modelo de ROPA
Anexo 4: POP – Atendimento aos Direitos dos Titulares
Anexo 5: POP – Due Diligence em Terceiros (LGPD + ESG)
Anexo 6: Resposta Incidentes RACI + Fluxo
Anexo 7: Tabela Consolidada de Retenção, Arquivamento e Descarte
Anexo 8: Certificado Interno de Descarte de Dados
Anexo 9: Integração com Gestão de Risco, Crise, Comunicação e ESG
Anexo 10: Matriz de Risco de Privacidade

21. DISPOSIÇÕES FINAIS

Esta Política de Proteção de Dados:

- Constitui o compromisso formal da Sustentalli com a observância das normas relativas à proteção de dados;
- Serve como guia para todas as operações de tratamento de dados pessoais realizadas pela Cooperativa;
- Reconhece que algumas medidas serão implementadas de imediato e outras de forma progressiva, ao longo da jornada de conformidade;
- Será revisada periodicamente, especialmente em caso de alterações legislativas, orientações da ANPD, mudanças relevantes na estrutura da Cooperativa ou nas suas atividades.

A versão atual entra em vigor na data de sua aprovação pelo Conselho de Administração e permanecerá válida até revisão ou revogação formal.

APROVAÇÕES

MIRIAM LUTTGEN RIBEIRO RODRIGUES
Presidente do Conselho de Administração
eliana@camejo.com.br

ELIANA ROSA CAMEJO
1ª Vice-Presidente do Conselho de Administração

MARIA HELENICE DE ALMEIDA CARNEIRO
2ª Vice-Presidente do Conselho de Administração

ANEXO 1
MAPA DE PAPÉIS E RESPONSABILIDADES NO TRATAMENTO DE DADOS

1.1. Tabela Resumo – Controlador / Operador / Terceiros

Atividade / Processo	Sustentalli	Cliente	Terceiros / Sistemas	5. Observações
Gestão de cooperados/as	**Controladora**	—	Operadores internos/ERP /RH	Dados cadastrais, financeiros e históricos de participação
Gestão de candidatos/as (processos seletivos)	**Controladora**	—	Plataforma de recrutamento (se houver)	Avisos de privacidade em formulários
Gestão de colaboradores/as CLT / prestadores/as	**Controladora**	—	Sistema contábil/folha, banca etc.	Compartilhamento limitado ao necessário
Diagnósticos ESG	**Operadora**	**Controlador**	—	Cliente define escopo e finalidades
Relatórios de sustentabilidade	**Operadora**	**Controlador**	—	Atenção a dados sensíveis de colaboradores/as de clientes
Projetos ESG com dados de colaboradores de clientes	**Operadora**	**Controlador**	—	Instruções formais do cliente
Comunicação institucional Sustentalli (*newsletter*)	**Controladora**	—	Agência/ Plataforma de e-mail marketing	Terceiro como Operador
CRM e gestão de leads	**Controladora**	—	Plataforma CRM	Base de *leads*, consentimento/ legítimo interesse
Gestão financeira (contas a pagar/receber)	**Controladora**	—	Bancos, ERP financeiro	Dados compartilhados estritamente necessários
Sistema do site (formulários, cookies)	**Controladora**	—	Desenvolvedor, hospedagem, analytics	Política de Cookies e Aviso de Privacidade
Auditorias anuais	**Controladora**	—	Auditoria externa	Acesso limitado, contrato com cláusula LGPD
Eventos e ações de relacionamento	**Controladora**	—	Produtora de eventos, fornecedores	Cadastro de participantes

*ERP (*Enterprise Resource Planning*)

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br

1.2. Papéis Internos

- **CA:** Supervisiona o Programa de Privacidade, aprova políticas e indicadores.
- **DPO:** Coordena privacidade, atende titulares, interage com ANPD, lidera incidentes.
- **CGAF:** Apoia risco, *due diligence*, orçamento de segurança, acompanhamento de indicadores.
- **Cooperados/as:** Atuam como Operadores internos quando tratam dados em nome da Cooperativa.
- **Demais comitês:** integram risco LGPD nas suas pautas (ESG, Governança, Comunicação

ANEXO 2
MODELO DE INVENTÁRIO DE DADOS PESSOAIS

2.1. Campos Obrigatórios

Campo	Descrição
ID do Processo	Código interno do processo (ex.: PRC-01, PRC-02)
Nome do Processo / Atividade	Ex.: "Gestão de Cooperados", "Diagnóstico ESG Cliente X"
Área Responsável	Comitê, Gestão, célula ou responsável principal
Finalidade do Tratamento	Objetivo principal (ex.: cadastro, faturamento, diagnóstico ESG, comunicação comercial)
Categorias de Titulares	Cooperados/as, colaboradores/as, fornecedores, clientes, *leads*, participantes de eventos etc.
Categorias de Dados	Dados cadastrais, financeiros, profissionais, sensíveis etc.
Dados Sensíveis?	Sim/Não — especificar quais, se houver
Base Legal	Consentimento, execução de contrato, obrigação legal, legítimo interesse, etc.
Origem dos Dados	Fornecidos pelo/a titular, obtidos de terceiros, gerados internamente
Canal de Coleta	Formulário online, contrato, e-mail, planilha, sistema etc.
Local de Armazenamento	Sistema, nuvem, servidor local, arquivo físico, e-mail etc.
Acesso Interno	Quem acessa (funções/cargos, e não nomes de pessoas)
Compartilhamento Externo	Bancos, plataformas, parceiros, clientes, autoridades etc.
Transferência Internacional?	Sim/Não — se sim, indicar país e base jurídica
Riscos Principais	Ex.: vazamento, acesso não autorizado, perda de dados, uso indevido
Medidas de Segurança	Técnicas e administrativas (controle de acesso, criptografia, treinamento etc.)
Prazo de Retenção	Quantidade de anos, evento gatilho (ex.: término do contrato + 5 anos)
Critério de Eliminação	Eliminação, anonimização, arquivamento legal
Encarregado/a -Responsável Interno	Área e responsável pelo processo
Data da Última Revisão	Data da última atualização do inventário para esse processo

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br

ANEXO 3
MODELO DE ROPA – REGISTRO DAS OPERAÇÕES DE TRATAMENTO (ART. 37 LGPD)

3.1. Campos do ROPA

Campo	Descrição
Identificação do Controlador	Sustentalli – nome empresarial, CNPJ, endereço, contatos
DPO/Encarregado/a	Nome, e-mail, telefone
Número/ID da Operação de Tratamento	Código interno (ex.: ROP-01, ROP-02)
Processo/Atividade	Nome do processo (ex.: "Cadastro de Cooperados/as")
Finalidade(es) do Tratamento	Objetivo específico da operação
Descrição da Operação	O que é feito com os dados (coleta, armazenamento, análise, compartilhamento etc.)
Categorias de Titulares	Cooperados/as, colaboradores/as, fornecedores, clientes, *leads* etc.
Categorias de Dados	Cadastrais, financeiros, sensíveis etc.
Categorias de Destinatários	Terceiros, operadores/as, autoridades, clientes
Transferências Internacionais	País(es), base legal, mecanismo de transferência
Prazo de Retenção	Conforme política de retenção
Descrição Geral das Medidas de Segurança	Controles técnicos e organizacionais relevantes
Base(s) Legal(is)	Artigos e incisos aplicáveis da LGPD
Relacionamento com Avaliação de Impacto (DPIA)	"Existe/Não existe" – se sim, indicar referência
Data de Criação / Última Atualização	Datas

3.2. Exemplo Resumido

ID	Processo	Finalidade	Titulares	Base Legal	Destinatários	Retenç
ROP1	Cadastro de Cooperados/as	Adesão à cooperativa, gestão de contas	Cooperados/as	Execução de contrato, obrigação legal	Bancos, contador, sistemas ERP	Término 5 anos

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br

ANEXO 4
POP – ATENDIMENTO AOS DIREITOS DOS TITULARES

4.1. Objetivo
Estabelecer o fluxo padronizado para receber, analisar e responder solicitações dos titulares de dados.

4.2. Escopo
Aplica-se a todos os pedidos de titulares com base no Art. 18 da LGPD.

4.3. Fluxo – Passo a Passo

- **Recebimento**
  -Canais: lgpd@sustentalli.com.br, formulário do site ou outro canal oficial.
  -Responsável: DPO ou equipe designada.

- **Registro Inicial**
  -Gerar número de caso (ex.: LGPD-2025-0001).
  -Registrar data, canal, nome do titular (quando identificado).

- **Validação de Identidade**
  -Solicitar comprovação razoável (documento oficial ou validação por dados já existentes).
  -Em caso de representante legal, solicitar procuração ou documento equivalente.

- **Classificação da Solicitação**
  - Tipo de direito: acesso, confirmação, correção, eliminação, portabilidade, revogação, oposição
  - Classificar prioridade se houver risco evidente ao titular.

- **Análise Técnica**
  -DPO consulta inventário/ROPA para localizar bases de dados envolvidas.
  -Solicita informações às áreas responsáveis (CGAF, RH, comunicação, projetos etc.).

- **Verificação de Possibilidade e Limitações**
  - Avaliar se há obrigação legal de retenção ou risco a segredos comerciais, investigações etc.
  -Se for caso de negativa parcial ou total, registrar fundamentação.

- **Resposta ao Titular**
  -Enviar resposta clara, dentro do prazo legal.
  - Em caso de atendimento positivo, explicar o que será feito (ex.: correção, eliminação).
  - Em caso de recusa, indicar razões legais/regulatórias.

- **Execução da Ação Interna**
  - Realizar correção, anonimização, bloqueio, eliminação etc.
  - Registrar quem executou, em qual sistema e quando.

- **Registro Final e Arquivamento**
  - Atualizar livro eletrônico de solicitações com: decisão, evidências, datas.
  - Arquivar comunicações com o titular.

4.4. Prazos Internos

- Confirmar recebimento: até 3 dias úteis.

Responder no mérito: dentro dos prazos definidos na Política (15/30/60 dias conforme o caso).

ANEXO 5
POP – DUE DILIGENCE EM TERCEIROS (LGPD + ESG)

5.1. Objetivo

Avaliar riscos de privacidade e segurança antes da contratação de terceiros que tratem dados em nome da Sustentalli.

5.2. Etapas

1. **Identificação do Terceiro**

- Tipo: fornecedor de tecnologia, consultoria, agência, desenvolvedor, auditor etc.
- Descrição dos serviços e possíveis dados envolvidos.

2. **Questionário de Due Diligence -** Checklist mínimo:

- Possui política de privacidade escrita e implementada?
- Possui política de segurança da informação?
- Adota controles de acesso, criptografia, backups?
- Processa dados em nuvem? Se sim, qual provedor e em que países?
- Já sofreu incidente relevante de segurança de dados? Como tratou?
- Tem DPO ou responsável por privacidade designado?
- Está sujeito a outras legislações de proteção de dados (ex.: GDPR)?

3. **Classificação de Risco**

- Avaliar risco Baixo / Médio / Alto, considerando:
  - Volume de dados;
  - Presença de dados sensíveis;
  - Transferência internacional;
  - Histórico de conformidade.

4. **Decisão de Contratação**

- Se risco aceitável: prosseguir com contrato.
- Se risco alto: considerar controles adicionais, mitigação contratual ou não contratação.

5. **Cláusulas Contratuais Mínimas (DPA)**

- Obrigações do/a Operador/a;
- Proibição de uso dos dados para fins próprios;
- Proibição de subcontratação sem autorização;
- Notificação obrigatória em caso de incidente;
- Cooperação em pedidos de titulares;
- Regras de devolução/eliminação de dados ao término do contrato.

6. **Monitoramento Contínuo**

- Revisão periódica de fornecedores críticos;
- Verificação de incidentes e não conformidades;
- Reavaliação a cada renovação de contrato

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br

ANEXO 6
PLANO DETALHADO DE RESPOSTA A INCIDENTES (RACI + FLUXO)

6.1. Matriz RACI Resumida

Atividade	DPO	CA	CGAF	TI/ Segurança	Jurídico	Comuni -cação
Detecção e registro	R	I	I	R	I	I
Contenção inicial	A/R	I	C	R	I	I
Análise técnica	A	I	C	R	C	I
Classificação de severidade	A	C	C	C	C	I
Decisão de notificar ANPD	A	C	I	C	C	I
Notificação ANPD	R	I	I	C	C	I
Comunicação aos titulares	A	I	I	C	C	R
Ações corretivas técnicas	C	I	I	R	I	I
Relatório pós-incidente	R	C	C	C	C	I
Atualização de políticas e treinamentos	R	C	C	C	C	C

(R = Responsible, A = Accountable, C = Consulted, I = Informed)

6.2 Fluxo Resumido em 8 Etapas

(já descrito na política - aqui você pode colocar em formato de organograma depois)

1. Detecção e Registro
2. Contenção Imediata
3. Análise Técnica
4. Classificação de Severidade
5. Ação Corretiva
6. Comunicação Interna
7. Comunicação à ANPD e Titulares (quando aplicável)
8. Relatório Pós-Incidente e Melhoria Contínua

ANEXO 7

TABELA CONSOLIDADA DE RETENÇÃO, ARQUIVAMENTO E DESCARTE

Tipo de Dado / Processo	Titulares	Prazo de Retenção	Base Legal Principal	Responsável Interno	Observações
Cadastro de Cooperados/as	Cooperados/as	Término da relação + 5 anos	Execução de contrato, obrigação legal	CGAF / RH	Podem existir prazos maiores para fins fiscais
Documentos societários	Cooperados/as	Conforme legislação cooperativista (longa)	Obrigações legais	CA / Jurídico	Estatuto, atas, livros
Dados de Folha de Pagamento CLT	Colaboradores /as CLT	5 a 10 anos (conforme legislação trabalhista)	Obrigação trabalhista e previdenciária	CGAF / Contabilidade	Ver CLT, INSS, FGTS
Cadastro de Fornecedores	Fornecedores	5 anos após término do contrato	Código Civil, obrigações fiscais	CGAF / Compras	
Dados de Clientes	Clientes	Contrato + 5 anos	Execução de contrato, defesa em processos	CGAF / Projetos	
Dados de Projetos ESG	Clientes	Enquanto durar o contrato + prazo legal	Execução de contrato	Comitê de Projetos/ESG	Alguns relatórios podem ser anonimizados
Leads Comerciais	Leads	1 ano após último contato útil	Consentimento/Legítimo Interesse	Comunicação / Comercial	Eliminar ou renovar consentimento após o prazo
Dados de Eventos	Participantes	1 a 2 anos após o evento	Consentimento/Legítimo Interesse	Comunicação	Fotos/imagem, observar direito de imagem
Dados Sensíveis	Vários	Mínimo necessário	Art. 11 LGPD	Responsável do processo	Avaliar caso a caso
Registros de Incidentes de Segurança	Titulares diversos	Pelo menos 5 anos após encerramento	Legítimo interesse, defesa em processos	DPO / CGAF	Evidências para prestação de contas
Registros de Solicitações LGPD	Titulares diversos	5 anos	Obrigações legais, defesa em processos	DPO	Livro eletrônico de solicitações

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br

ANEXO 8
CERTIFICADO INTERNO DE DESCARTE DE DADOS

1. Identificação

- ID do Certificado: CID-/
- Data do Descarte: //____
- Área Responsável: _____
- Responsável Técnico: _____

2. Escopo do Descarte

- Sistema/Repositório: _____
- Tipo de Dados Eliminados: _____
- Categoria de Titulares: _____
- Volume aproximado de registros: _____

3. Fundamento do Descarte

- Motivo:
  ( ) Término de prazo de retenção
  ( ) Solicitação do titular atendida
  ( ) Encerramento de contrato/projeto
  ( ) Outro: _____

- Base Legal de Retenção antes do Descarte: _____

4. Método de Eliminação

( ) Exclusão lógica com sobrescrita segura
( ) Anonimização irreversível
( ) Destruição física (para mídia física)
( ) Outro: _____

5. Declaração

Declaro que o descarte foi realizado em conformidade com a Política de Retenção, Arquivamento e Descarte de Dados da Sustentalli e com a LGPD.

Local e data: _____

Assinatura do Responsável Técnico: _____

Assinatura do DPO: _____

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br

ANEXO 9
INTEGRAÇÃO COM GESTÃO DE RISCO, CRISE, COMUNICAÇÃO E ESG

9.1. Risco

- Incidentes LGPD entram formalmente na **Matriz de Risco Corporativo**.
- Riscos de privacidade são reportados ao CA junto com outros riscos estratégicos.

9.2. Crise

- Incidentes graves de dados (alto risco) ativam o **Plano de Gerenciamento de Crise** da Sustentalli.
- O DPO atua em conjunto com a área de Comunicação e com o CA na gestão da narrativa pública.

9.3. Comunicação

- Mensagens a titulares afetados seguem padrão definido com o DPO e Jurídico.
- Notas públicas (se necessárias) serão aprovadas pelo CA, considerando transparência e mitigação de dano reputacional.

9.4. ESG

- Privacidade e proteção de dados são reportadas nos pilares de Governança e Social em relatórios ESG.
- Indicadores LGPD podem ser incluídos em relatórios de sustentabilidade, demonstrando maturidade de governança de dados.

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br

ANEXO 10

MATRIZ DE RISCO DE PRIVACIDADE (MODELO)

	Descrição do Risco	Causa Principal	Impacto Potencial	Prob. (Baixa/ Média/Alta)	Impacto (B/M/A)	Nível (Ex.: P x I)	Controles Existentes	Ações de Melhoria Planejadas	Responsável
1	Vazamento de dados de cooperados/as por e-mail pessoal	Envio de planilhas para e-mails pessoais	Multa, dano reputacional, ação civil	M	A	Alta	PSI proíbe envio, treinamento básico	Reforçar bloqueios técnicos e campanhas	DPO/TI
2	Acesso indevido a dados de *leads*	Permissões excessivas no CRM	Uso indevido, spam, reputação	M	M	Média	Perfis de acesso configurados	Revisão de perfis e logs	Comercial/ TI
3	Incidente em fornecedor de tecnologia	Falha de segurança em nuvem	Vazamento de dados de clientes	B	A	Média/Alta	Contratos com cláusulas LGPD, due diligence	Auditoria anual, plano de continuidade	CGAF/DPO

CENTRO INDUSTRIAL E EMPRESARIAL ALPHAVILLE
Alameda Rio Negro, 503, conj. 2005
Alphaville - BARUERI/SP CEP 06454000
+55 11 99121-9145 | +55 5198158-7771
contato@sustentalli.com.br