



Política Interna – Proteção de Dados

Requisitos a serem seguidos ao Processar Dados Pessoais
de acordo com as disposições da Lei 13.709 (Lei Geral de
Proteção de Dados)

1/11/2025

Área: Departamento Jurídico & Compliance

Autor: Ingrid Silva Mendes



CONTROLE DE APROVAÇÕES			
PAPEL	NOME	FUNÇÃO	ASSINATURA
RESPONSÁVEL	Ingrid S. Mendes	Compliance Officer	<u>Ingrid S. Mendes</u> Ingrid S. Mendes (12 de novembro de 2025 14:04:40 GMT-3)
REVISOR(A)	Sheila Cristina de Souza	DPO	<u>Sheila C. Souza</u> Sheila C. Souza (12 de novembro de 2025 14:16:05 GMT-3)
APROVADOR	Fabício Fatuch	CEO	<u>Fabicio Fatuch</u> Fabicio Fatuch (12 de novembro de 2025 19:40:31 GMT-3)
Cód. do documento	Versão	Controle de alterações	
5	V2	Atualização da primeira versão (criação) do documento.	

Validação Compliance	<u>ISM</u> ISM
Início de vigência	11/2025
Fim de vigência	11/2027

1. OBJETIVO

O objetivo desta Política de Proteção de Dados da CEABS é definir os principais requisitos a serem seguidos ao Processar Dados Pessoais tendo em conta as disposições da LGPD (LEI Nº 13.709 - Lei Geral de Proteção de Dados).

2. ABRANGÊNCIA

Esta política abrange o tratamento de dados pessoais em nome da CEABS de:

- Clientes corporativos e prospects;
- Beneficiários e clientes dos serviços fornecidos pela CEABS;
- Prestadores de serviço e terceiros que trabalham ou visitam a CEABS;
- Colaboradores da CEABS.

A responsabilidade pela implementação é de **todas as áreas** da CEABS.



2. PROCESSOS E ATIVIDADES

2.1. O processo de Controles internos

O detalhamento do processo de controles internos com seu passo a passo está no **Procedimento – Controles Internos**.

Neste documento é apresentada a metodologia e processo de identificação e avaliação dos riscos e controles da companhia, o acompanhamento e reporte destes riscos para tomada de decisão da alta direção.

Este processo está alinhado as práticas adotadas pelos acionistas para identificação, avaliação e reposta aos riscos corporativos.

2.2. Documentação interna – Manuais, Procedimentos e Memorandos

Os processos das áreas de negócio passam por alterações, que podem gerar novos riscos, e consequentemente exijam uma nova abordagem para a mitigação destes riscos. É fundamental que estes riscos sejam identificados, tratados e monitorados.

Além disto, é fundamental a documentação dos critérios e passos dos processos da empresa, para garantia de continuidade e uniformidade nas atividades.

Por isto, há processo estabelecido que através da documentação dos processos, visa a identificação, resposta e monitoramento dos riscos da empresa, bem como a definição e comunicação dos critérios que a empresa adota em seus processos.

A elaboração e definição destes documentos é realizada a partir do mapeamento da cadeia de valor da empresa, já citada neste documento

Para cada item da cadeia de valor, é avaliado a necessidade de documentações que cubram os processos.

A renovação dos documentos internos deve ocorrer de forma anual. O Departamento de Riscos e Compliance realiza a revisão dos documentos descritos, de modo que a validação dos riscos seja avaliada em mudanças de processos. Além disto o, também é sua função avaliar estes processos documentados, de modo a identificar deficiências que levam a materialização de riscos operacionais. Este é o principal insumo para a identificação de novos riscos.

3. DESCRIÇÃO DAS ATIVIDADES

É considerado na CEABS as seguintes definições com base na LGPD:

- a) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
- b) Dado pessoal sensível: 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;
- c) Dado anonimizado: dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- d) Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- e) Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;



- f) Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- g) Encarregado de dados pessoais (ou DPO): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
- h) ANPD: Agência Nacional de Proteção de Dados.

3.1 Princípios-chave que regem o tratamento de dados pessoais

Ao processar dados pessoais, os seguintes princípios serão sempre aplicados. Os dados pessoais devem ser:

- a) Processados de acordo com a lei, justa e transparente com relação ao titular dos dados;
- b) Coletada para um propósito específico, explícito e legítimo, e não devem ser processados para um fim incompatível daquele pelo qual foi coletado. O titular dos dados deve ser informado de forma clara e simples sobre a privacidade de seus dados.
- c) Adequados, relevantes e limitados para o que é necessário em relação ao propósito pelo quais é processado;
- d) Exatos, quando necessário, atualizados. Dados pessoais incorretos ou não precisos, devem ser deletados ou ajustados imediatamente.
- e) Armazenados de modo que a identificação do titular não dure mais que o necessário para o cumprimento da finalidade pelo qual o dado foi coletado. Após o cumprimento da finalidade, o dado pessoal pode ser armazenado somente em um formato que não permita a identificação do titular, desde que não exista conflito com outras leis aplicáveis.
- f) Processados de forma que garantam a segurança apropriada dos dados pessoais, usando medidas técnicas, administrativa e de segurança apropriadas

A CEABS deve poder demonstrar a qualquer momento a adoção e cumprimento dos princípios acima, através de políticas, procedimentos e processos e outras medidas, que podem incluir a registro das operações de tratamento, a execução da Avaliação de Impacto de tratamento de dados pessoais, e pela implementação de controles que verifiquem a implementação destes princípios.

3.2. Hipóteses para o tratamento de dados pessoais

Sempre que, no que diz respeito a um tratamento específico de Dados Pessoais, a CEABS deve respeitar as seguintes hipóteses de tratamento:

- a) com base no consentimento dado pelo Titular dos Dados para um ou mais propósitos específicos;
- b) necessários para a execução de: um contrato do qual o Titular dos Dados é parte ou atividades pré-contratuais;
- c) necessárias ao cumprimento de uma obrigação legal a que a Entidade Jurídica do Grupo esteja sujeita;



d) necessárias ao desempenho de uma tarefa realizada no interesse público ou no exercício de uma autoridade oficial;

e) Para o exercício regular do direito em processo judicial, administrativo ou arbitral.

3.3. Direitos dos titulares dos dados

Como regra geral e sujeito a certas circunstâncias definidas pela regulamentação aplicável, um titular dos Dados deve ser autorizado a exercer os seguintes direitos:

- a) Confirmação da existência de tratamento;
- b) Acesso aos dados pessoais;
- c) Correção de dados incompletos, inexatos ou desatualizados;
- d) Anonimização, bloqueio ou eliminação de dados (direito de ser esquecido) desnecessários ou excessivos.
- e) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
- f) Eliminação dos dados pessoais tratados com o consentimento do titular;
- 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.

3.4. Registros das atividades de tratamento de dados

O registro das atividades de tratamento de Dados Pessoais deve ser mantido pela CEABS e disponibilizado à Autoridade Nacional quando solicitado. Quanto a atuação como operadora, a CEABS deve possibilitar o registro dedicado de cada um dos controladores de dados.

3.5. Medidas técnicas, de segurança e organizacionais

Devem ser implementadas medidas técnicas, de segurança e organizacionais adequadas para garantir um nível adequado de segurança dos dados pessoais. Uma abordagem baseada em risco deve ser seguida ao identificar essas medidas. A abordagem baseada no risco deve considerar, entre outros, a probabilidade e severidade dos direitos e liberdades dos titulares dos Dados, bem como as tecnologias disponíveis e os custos de implementação relacionados.

Em toda nova operação de que envolva tratamento de dados pessoais, é necessária a avaliação sob a perspectiva de proteção de dados pessoais, de modo a garantir a implementação das medidas técnicas, de segurança e administrativas adequadas, de modo que estas medidas estejam incorporadas no desenho desta nova operação, e abranjam todo o ciclo de vida da operação (*privacy by Design*). Estas medidas devem por padrão (*privacy by default*) possuir controles que limitem somente os dados pessoais necessários acessados pelos envolvidos na atividade.

O Procedimento – Verificação de Privacy by Design detalha o processo de avaliação do desenho de novas operações de tratamento de dados pessoais.

3.6. Transferência Internacional de dados

Devem ser tomadas as medidas de proteção adequadas para transferências de dados fora do Brasil. O Procedimento - Transferência Internacional de dados detalha os critérios e medidas para a transferência internacional de dados.



3.7. Relação com Operadores

Sempre que a CEABS realizar a contratação de um operador para o tratamento de dados pessoais, deve ser garantido que o Operador possua implementadas medidas técnicas, de segurança e organizacionais apropriadas para garantir o compliance com os princípios dos dados pessoais (item 3.1 deste documento).

3.8. CEABS como Controladora/Operadora

Sempre que a CEABS atuar como Controladora ou Operadora de dados pessoais, devem:

- Processar os dados pessoais de acordo com os princípios estabelecidos no item 3.1 deste documento e de acordo com as leis de proteção de dados aplicáveis;
- Garantir que os indivíduos autorizados a processar os dados pessoais tenham se comprometido com a confidencialidade ou estejam sob obrigação adequada de confidencialidade;

Processar os dados pessoais somente de acordo com as instruções do Controlador de dados, a menos que seja exigido de outra forma pela Autoridade Nacional;

- Manter um registro de todas as atividades de tratamento;
- Implementar medidas técnicas e organizacionais apropriadas para proteger o tratamento de dados pessoais;
- Nomear um responsável pela Proteção de Dados, denominado encarregado ou DPO;
- No caso de transferência de Dados Pessoais fora do Brasil, aplicar as medidas de proteção conforme o Procedimento - Transferência Internacional;
- Assinar um contrato ou outro ato legal que determine a relação com o Controlador ou com o Operador;
- Abster-se de nomear outro Operador sem a prévia autorização específica do Controlador. Caso se tenha recebido uma autorização geral por escrito para envolver outros Operadores, esta alteração no tratamento deve ser tempestivamente informada ao Controlador de dados.
- Sempre que forem contratados outros operadores para executar as atividades de tratamento específicas em nome do Controlador de Dados, deve ser assinado um contrato com este Operador para impor a ele as mesmas obrigações de proteção de dados.
- Auxiliar o Controlador de Dados no cumprimento de suas obrigações com respeito à resposta de solicitações relacionadas aos direitos de Titulares;
- Fornecer notificação imediata ao Controlador de Dados em relação a qualquer violação de dados pessoais ou incidente que Dados Pessoais sendo processados em nome do Controlador de Dados;
- Após o término da prestação de serviços, excluir as cópias existentes dos dados pessoais, a pedido do Controlador, a menos que a legislação exija a conservação dos dados pessoais; e
- Disponibilizar ao Controlador de dados todas as informações necessárias para demonstrar estar em compliance com suas obrigações legais e permitir e cooperar com auditorias, incluindo inspeções, conduzidas pelo Controlador de Dados ou outro auditor nomeado pelo Controlador de Dados.

3.9 Violações de dados pessoais

As violações de dados pessoais devem seguir o estabelecido no Procedimento – Gestão de violações de dados Pessoais, que obedece ao tratamento de violações de dados pessoais, incluindo a tomada de medidas adequadas, o que pode incluir a comunicação com os titulares dos dados e com a Autoridade Nacional.



3.10 Encarregado de dados pessoais (DPO)

O encarregado é a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

O encarregado dentro da CEABS tem como atividades:

- a) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- b) Receber comunicações da Autoridade Nacional e adotar providências;
- c) Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- d) Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A identidade e informações de contato do encarregado devem ser divulgadas publicamente.

O e-mail de contato do DPO da CEABS é dpo@ceabs.com.br.

3.11 Comitê de Proteção de dados

Está estabelecido comitê multidisciplinar que trata de decisões e assuntos relacionados a Proteção de dados. A estrutura, periodicidade e diretrizes deste comitê está descrita no Regimento – Comitê de Proteção de Dados. Qualquer exceção a esta política deve ser submetida à alçada de aprovações (revisor e aprovador) que deve escalar a situação, internamente, caso aplicável.