



Política de Compliance de Proteção de Dados

Código - Cadeia de Valor

7.4 Compliance

Data de Publicação

20/10/2022

CONTROLE DE APROVAÇÕES				
RESPONSÁVEIS	NOME	FUNÇÃO	ASSINATURA	DATA
ELABORADOR	Milena Danielski	Analista de Auditoria e Compliance	DocuSigned by: Milena Danielski D22DC0F73943438...	20/10/2022 11:16:29 BR
REVISOR/APROVADOR	Helga Inssa	Diretora de Tecnologia e Governança	DocuSigned by: Helga Inssa 8EEF994AE5AD437...	20/10/2022 13:09:49 BR
APROVADOR	Delcio Custodio	CEO	DocuSigned by: Delcio Custodio F7B3F2E318B2413...	24/10/2022 11:12:57 BR
APROVADOR	Rodrigo Rosa	Diretor Adm & Financeiro	DocuSigned by: Rodrigo da Rosa C1EE68B5CCD4D8...	20/10/2022 13:46:01 BR
APROVADOR	Vanessa Meneses	Diretora de Operações	DocuSigned by: Vanessa Meneses DBC2A15463A1481...	20/10/2022 13:10:33 BR
APROVADOR	Leandro Roncatto	Diretor de Estratégia e Performance	DocuSigned by: Leandro Roncatto 879D1923611B48D...	24/10/2022 09:58:31 BR
APROVADOR	Cláudio Vilar	Diretor Comercial	DocuSigned by: Cláudio Vilar Jr AE994495283749B...	24/10/2022 05:55:08 PD
Código do documento	Versão	Controle de alterações		
7.4	V1	V1: Criação do documento		

1. OBJETIVO

A Política de *Compliance* de Proteção de Dados tem como principais objetivos:

- I. **Definir** controles e processos que garantam a proteção dos dados pessoais, sejam da CEABS, de clientes, parceiros ou de terceiros, sob domínio de nossa empresa;
- II. **Estimular** a cultura da conformidade na organização;
- III. **Assegurar** que a CEABS segue os princípios e recomendações da LGPD quanto ao tratamento dos dados pessoais que possuímos em nossas bases;
- IV. **Verificar** a efetividade das orientações deste documento nos procedimentos internos e nas relações que a CEABS mantém, a fim de advertir condutas contrárias.

2. APLICAÇÃO

Esta política aplica-se a todos os colaboradores da CEABS, independentemente de nível hierárquico, também aos parceiros, terceiros ou qualquer outra pessoa que age em nome da organização ou se relaciona conosco.

3. REFERÊNCIAS

Código de Conduta Ética;
 Registro de Operações de Tratamento;
 Normativa de Atendimento às Solicitações de Titulares de Dados Pessoais;
 Política de Propriedade Intelectual;
 Política de Segurança da Informação;

Procedimento - Gestão de crise – incidentes com Dados Pessoais;
Procedimento - *Privacy by Design*;
Regimento - Comitê LGPD;
Relatório de Impacto;
Lei Geral de Proteção de Dados nº 13.709/2018 (LGPD).

4. DEFINIÇÕES

Para fins desta política, alguns termos devem ser entendidos da seguinte forma:

Colaborador: Qualquer pessoa que faça parte do corpo colaborativo da CEABS, independentemente de nível hierárquico.

Parceiros: Qualquer pessoa, física ou jurídica, que se relacione com a CEABS e participe do negócio afim de obter interesses comuns à atividade empresarial.

Terceiros: Qualquer pessoa, física ou jurídica, que presta serviços à CEABS, participando de uma parte da atividade empresarial, típica ao negócio jurídico, ou serviços em geral. Caracterizam-se por fontes de contratação externa.

LGPD: Lei Federal nº 13.709/2018, também chamada de Lei Geral de Proteção de Dados.

Dado Pessoal: Qualquer “informação relacionada a uma pessoa natural identificada ou identificável” (Art. 5º, I, LGPD). Exemplos: nome, CPF, número de telefone, foto.

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” (Art. 5º, II, LGPD).

Dado Anonimizado: “dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (Art. 5º, III, LGPD).

Titular: “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (Art. 5º, V, LGPD).

Controlador: “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (Art. 5º, VI, LGPD).

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Art. 5º, VII, LGPD).

Encarregado de Proteção de Dados ou DPO (*Data Protection Officer*): pessoa indicada pela empresa para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (Art. 5º, VIII, LGPD).

Agente de Tratamento: “o controlador e o operador” (Art. 5º, IX, LGPD).

Autoridade Nacional de Proteção de Dados (ANPD): “órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento” da Lei Geral de Proteção de Dados em todo o território nacional (Art. 5º, XIX, LGPD).

Tratamento: “toda operação efetuada com Dados Pessoais, por meios automatizados ou não automatizados, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (Art. 5º, X, LGPD).

Hipótese de Tratamento de Dados Pessoais ou Base Legal: requisito legal que possibilita que o tratamento de dados pessoais seja realizado pelo agente. São exemplos de hipóteses de tratamento: consentimento, cumprimento de obrigação legal ou regulatória, execução de contrato ou de procedimentos preliminares a um contrato, exercício regular de direitos em processos judiciais, administrativos ou arbitrais, legítimo interesse, proteção do crédito e garantia de prevenção à fraude e à segurança do titular.

Incidente de Violação de Dados Pessoais: qualquer evento adverso, confirmado ou sob suspeita, que pode causar acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, ou seja, gerar o comprometimento das características de confidencialidade, integridade e disponibilidade dos dados pessoais.

Anonimização: “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” (Art. 5º, XI, LGPD).

Eliminação: “exclusão de dado ou de conjunto de dados armazenados em banco de dados (em suporte físico ou eletrônico), independentemente do procedimento empregado”. (Art. 5º, XIV, LGPD).

5. DIRETRIZES ESPECÍFICAS

Todos os colaboradores da CEABS devem pautar suas atividades e relações na ética e integridade. É de sua responsabilidade conduzi-las em observância a esta política. Desta forma, violações através de condutas contrárias aos direcionamentos aqui presentes serão devidamente apuradas e, se comprovada a violação, medidas disciplinares serão aplicadas.

A presente política possui como diretrizes básicas:

- Reforçar a vedação e compromisso da CEABS, a todos os seus colaboradores, independentemente de nível hierárquico, em banir todo e qualquer tipo de conduta contrária que fere essa política;
- Orientar nossos colaboradores, terceiros e parceiros quanto às diretrizes de proteção de dados pessoais na CEABS;
- Definir os principais requisitos a serem seguidos ao processar dados pessoais, nas operações de tratamento na CEABS, levando em conta as disposições da LGPD.

6. PRINCÍPIOS DA LGPD

Quaisquer tratamentos de dados pessoais realizados pela CEABS, seja na condição de controlador ou de operador, deverão sempre levar em conta a boa-fé, bem como observar os princípios orientadores previstos na LGPD a seguir:

Princípio da finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (Art. 6º, I, LGPD).

Princípio da adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. (Art. 6º, II, LGPD).

Princípio da 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 (Art. 6º, III, LGPD).

Princípio do livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integridade de seus dados pessoais (Art. 6º, IV, LGPD).

Princípio da 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 (Art. 6º, V, LGPD).

Princípio da 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 (Art. 6º, VI, LGPD).

Princípio da 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 (Art. 6º, VII, LGPD).

Princípio da prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (Art. 6º, VIII, LGPD).

Princípio da não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (Art. 6º, IX, LGPD).

Princípio da 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 (Art. 6º, X, LGPD).

A CEABS pode demonstrar a qualquer momento a adoção e cumprimento dos princípios acima, através de políticas, procedimentos, 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 execução destes princípios.

7. HIPÓTESES PARA O TRATAMENTO DE DADOS PESSOAIS

Quando da realização de tratamento de dados pessoais pela CEABS, a organização precisa atentar-se ao disposto no art. 7º da LGPD. Este dispositivo contempla as hipóteses para o tratamento, quais sejam:

- i. Mediante o fornecimento de consentimento pelo titular;
- ii. Para o cumprimento de obrigação legal ou regulatória pelo controlador;

- iii. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do capítulo IV da lei;
- iv. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- v. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- vi. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- vii. Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- viii. Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- ix. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- x. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- xi. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

8. DIREITOS DOS TITULARES DE DADOS PESSOAIS

Nos termos da LGPD, o titular terá garantido o exercício dos seus direitos, conforme abaixo:

- i. Titularidade de seus dados pessoais e garantia dos direitos fundamentais de liberdade, de intimidade e de privacidade (art. 17);
- ii. Confirmação da existência do tratamento e acesso a dados (art. 18, I e II);
- iii. Correção de dados incompletos, inexatos ou desatualizados (art. 18, III);
- iv. Direito à anonimização, bloqueio ou eliminação (art. 18, IV);
- v. Direito à 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 (art. 18, V);
- vi. Direito à eliminação dos dados tratados com consentimento (art. 18, VI). PS: Hipóteses de conservação dos dados pessoais (art. 16);
- vii. Direito à informação de entidades públicas ou privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII);
- viii. Direito de revogação do consentimento (art. 18, IX);
- ix. Direito de oposição (art. 18, IX, § 2º);
- x. Direito de revisão de decisões automatizadas (art. 20);
- xi. Direito de não utilização dos seus dados pessoais, tratados com base no exercício regular de direitos, em seu prejuízo (art. 21).

9. REGISTRO DE OPERAÇÕES DE TRATAMENTO

Disponível no art. 37 da LGPD, o registro de operações de tratamento consiste em uma ferramenta de controle que retrata todo o ciclo de vida do dado pessoal, desde o ingresso na CEABS até o momento de seu descarte. Deve estar sempre atualizado de acordo com a mudança de procedimentos da organização. A manutenção deste documento deve ser realizada pelo DPO com informe aos outros controlares e operadores.

10. 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 abrangem 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 documento “**Procedimento - Privacy by Design**” detalha o processo de avaliação do desenho de novas operações de tratamento de dados pessoais.

11. TÉRMINO DO TRATAMENTO DOS DADOS PESSOAIS

Por determinação da LGPD, em seu art. 15, o término do tratamento dos dados pessoais ocorre nas seguintes hipóteses:

- i. Restar verificado que a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade;
- ii. Tiver findado o período de tratamento;
- iii. Houver comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
- iv. Mediante determinação da autoridade nacional, quando houver violação da lei.

Conforme mencionado acima, na cláusula VI, A CEABS, por respaldo do art. 16 da LGPD, poderá conservar os dados pessoais, mesmo após pedido de eliminação do titular, para as seguintes finalidades:

- i. Cumprimento de obrigação legal ou regulatória pelo controlador;
- ii. Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- iii. Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
- iv. Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

12. AVALIAÇÃO DE IMPACTO DE PROTEÇÃO DE DADOS (DPIA)

Deve ser elaborado o relatório da avaliação de impacto de processamento da proteção de dados pessoais para as atividades de tratamento de dados da CEABS (DPIA).

Esta avaliação destina-se a:

- Descrever o tratamento de dados pessoais;
- Avaliar a necessidade e a proporcionalidade de tais processos com relação aos objetivos relevantes;
- Ajudar a gerenciar os riscos para os direitos e liberdades dos Titulares dos Dados que possam surgir em conexão com tal tratamento.

13. GESTÃO DE VIOLAÇÃO DE DADOS PESSOAIS

A gestão das violações de dados pessoais deve seguir o estabelecido no documento **“Procedimento – Gestão de Crise – Incidentes com dados pessoais”**, que obedece ao tratamento de violações de dados pessoais, incluindo a tomada de medidas adequadas, o que pode incluir a comunicação aos titulares dos dados e à Autoridade Nacional.

14. OBRIGAÇÃO DE REPORTAR

A CEABS reforça a exigência que todos os seus colaboradores, terceiros e parceiros adotem todas as medidas necessárias para prevenir a ocorrência de violações às normas estabelecidas nesta política ou pelas legislações vigentes. Caso esteja ciente de algum ato ilícito, utilize nosso Canal de Denúncia para reporte. Nosso objetivo é atingir o mais alto nível de compromisso da CEABS com a ética e com o exercício de condutas morais.

Quaisquer situações, exceções e/ou esclarecimentos sobre a aplicação desta política deverão ser reportadas a área de *Compliance* através do e-mail compliance@ceabs.com.br.

15. RESPONSABILIDADES

15.1 CEABS

Sempre que a CEABS atuar como Controlador de dados pessoais, deve:

- Processar os dados pessoais de acordo com os princípios estabelecidos na cláusula IV deste documento e de acordo com a legislação aplicável;
- 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 internacional de Dados Pessoais, aplicar as medidas de proteção conforme o documento “**Manual – Privacidade e Proteção de dados**”;
- 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;
- Auxiliar o Controlador de Dados em suas obrigações cooperando em tempo hábil com qualquer DPIA realizada pelo Controlador de Dados e no cumprimento de quaisquer obrigações relacionadas a ANPD;
- 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.

15.1. Colaboradores, parceiros e terceiros

Cabe aos colaboradores da CEABS, parceiros e terceiros cumprir com as orientações desta política e assegurar que todos de seu relacionamento profissional sejam informados sobre seu conteúdo.

Os usuários externos devem entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes.

Deverão, ainda:

- Utilizar o e-mail de contato do encarregado de dados, dpo@ceabs.com.br, para sinalizar novos projetos, mudanças em procedimentos, sinalizar situações de vulnerabilidade em sua máquina que possam comprometer o armazenamento dos dados pessoais manipulados por sua área;
- Contribuir com o encarregado de dados para possibilitar atendimento célere às solicitações dos titulares de dados;
- Não compartilhar com terceiros ou extrair dados pessoais manipulados em decorrência de suas atividades no âmbito da CEABS;
- Não compartilhar ou deixar visível a terceiros suas credenciais de acesso.

15.2. Posição de Liderança

Os gestores da CEABS devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão. Cada gestor deverá manter os processos sob sua responsabilidade aderentes às políticas, normas e procedimentos específicos de segurança da informação da CEABS, tomando as ações necessárias para cumpri-las. A responsabilidade pela gestão das credenciais de usuários externos ou terceiros é do gestor do contrato de prestação de serviços ou do gestor do setor em que este usuário desempenha suas atividades. As posições de liderança também precisam contribuir para a promoção um ambiente de trabalho íntegro. Além disso, deverão:

- Auxiliar na percepção de aderência de seus integrantes ao cumprimento desta política bem como seu monitoramento;
- Fomentar, manter e orientar quanto à aplicação desta política, não somente aos colaboradores já existentes, mas também aos novos;
- Direcionar e salientar aos colaboradores da existência do canal de comunicação para denúncias de não cumprimento desta política.

15.6. DPO

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

Ele pode ser contatado através do e-mail dpo@ceabs.com.br. A identidade e informações de contato do encarregado devem ser divulgadas publicamente.

O encarregado na CEABS tem como atividades:

- Orientar os colaboradores com boas práticas a serem tomadas para garantir a proteção de dados pessoais;
- Receber as comunicações internas referentes a incidentes de violação de dados pessoais;
- Receber comunicações externas referentes a solicitações dos titulares dos dados pessoais;
- Dar seguimento aos procedimentos necessários para retorno aos titulares de dados pessoais, indicando as demais áreas que deverão participar do processo;
- Prestar apoio técnico de proteção de dados à CEABS sempre que solicitado;
- Avaliar a necessidade de comunicação do incidente para a ANPD e para os titulares de dados, bem como providenciar esse feito, conforme o caso;
- Apoiar a organização, em casos de notificação de incidente de violação de dados à ANPD;
- Prosseguir com investigação de incidentes de violação de dados pessoais até a conclusão, indicando atividades para mitigação de riscos, sugestões de monitoramento, controles internos e treinamentos.

15.7. 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 documento: **“Regimento – Comitê LGPD”**.

- Apoiar o Encarregado e gestores de todas as áreas da empresa em temas relativos à proteção de dados pessoais, a fim de atender às exigências da LGPD, da ANPD e dos procedimentos internos;
- Revisar, em conjunto com o Encarregado, políticas, normas e procedimentos da política de governança em privacidade periodicamente, a cada ano, a fim de garantir a melhoria contínua;
- Envolver-se sempre que a tomada de decisões impactar nas atividades de tratamento de dados pessoais de modo a envolver risco para direitos fundamentais e liberdades dos titulares de dados pessoais ou para os interesses da organização.

15.8. Comitê de Ética

Realizar as investigações e aplicar as medidas disciplinares.

15.9. Comitê de Compliance

- Prestar suporte ao Comitê de Ética, quando solicitado;
- Realizar a gestão e atualização desta política;
- Fomentar a cultura da integridade no contexto interno e externo;
- Dirimir dúvidas a respeito da aplicação das diretrizes desta política.

16. CANAL DE DENÚNCIA

Quaisquer atos ou suspeitas de não conformidade com esta política deverão ser relatados imediatamente através do Canal de Denúncias da CEABS. Seu relato pode ser enviado de forma anônima ou identificada.

Nesse sentido, disponibilizamos o link de acesso: <https://www.ceabs.com.br/canal-de-denuncia>.

17. INVESTIGAÇÕES E MEDIDAS

A CEABS considera falta grave qualquer violação às normas e orientações desta política. Portanto, todos os incidentes ou suspeitas de violação desta política serão investigados de forma apropriada. Conselheiros, diretores, empregados e todas as pessoas físicas ou jurídicas que exerçam atividades para ou em nome da CEABS estão sujeitas a medidas disciplinares administrativas ou legais em caso de violação dos princípios e valores estabelecidos por esta política, incluindo o término do vínculo empregatício ou da relação contratual de negócios, conforme o caso.

Qualquer colaborador da CEABS, parceiro ou terceiro que viole alguma disposição desta política estará sujeito a medidas disciplinares, tais como:

- Advertência verbal;
- Advertência por escrito;
- Suspensão;
- Rescisão contratual motivada.

A presente política entra em vigor a partir da sua data de divulgação.