TECNOBANK
SOLUÇÃO TEM A NOSSA DIGITAL



PL.CMP.019.02
Uso Interno ou Público

Política Integrada de *Compliance*, Anticorrupção e Antissuborno

Compliance

Sumário

1. OBJETIVO 5
2. ABRANGÊNCIA 5
3. DIRETRIZES 6
   3.1 Tolerância Zero 6
   3.2 Suborno e Corrupção 7
   3.3 Conformidade legal e regulatória 7
   3.4 Integridade, ética e transparência 7
   3.5 Proibição de Suborno Direto ou Indireto 7
   3.6 Proibição Irrestrita de Pagamentos de Facilitação 8
   3.7 Registros contábeis 8
   3.8 Segregação de funções e controles internos robustos 9
   3.9 Confidencialidade e não retaliação 9
   3.10 Governança Corporativa 9
4. SISTEMA DE GESTÃO INTEGRADA DE *COMPLIANCE*, ANTICORRUPÇÃO E ANTISSUBORNO (SGICA) 10
   4.1 Gestão de Obrigações de *Compliance* 10
   4.2 Gestão de Oportunidades de *Compliance* 11
   4.3 Avaliação de Riscos 11
   4.4 Políticas, Normas e Procedimentos 13
   4.5 Suporte da Alta Administração 13
   4.6 Comunicação e Treinamento 13
   4.7 *Due Diligence* (KYS, KYE, KYC) 13
   4.8 Canal de Ética 15
   4.9 Investigação e Resposta 16
   4.10 Melhoria Contínua 16
   4.11 Gestão de Mudanças 16
5. SANÇÕES INTERNACIONAIS – OFAC E OUTRAS LISTAS 17
6. MONITORAMENTO E AUDITORIAS 17

7. INFORMAÇÕES RELEVANTES E PRIVILEGIADAS – *INSIDER TRADING* 18
8. TEMAS ESPECÍFICOS DE INTEGRIDADE 18
8.1. Presentes, Brindes, Hospitalidades e Entretenimento 18
8.2. Doações e Patrocínios 18
8.3. Conflitos de interesse e partes relacionadas 19
8.4. Contribuições Políticas 19
8.5. Relação com Agentes Públicos 19
8.6. Contratação de Terceiros e Intermediários 20
8.7. Fusões, Aquisições e Integrações 20
8.8. Extorsão e Situações de Coação 21
9. CONDUTAS VEDADAS 21
10. ESTRUTURA DE GOVERNANÇA 22
10.1 Órgão Diretivo 22
10.2 Alta Administração 22
10.3 Comitê de Ética 23
10.4 Diretoria de Governança Corporativa 24
10.5 Área de *Compliance* 25
10.6 Função de *Compliance* (*Compliance Officer*) 26
10.7 Diretores 28
10.8 Liderança 29
10.9 Colaboradores 30
10.10 Multiplicadores 31
10.10.1 Compras 31
10.10.2 Comunicação & *Marketing* 31
10.10.3 Financeiro 32
10.10.4 Jurídico 32
10.10.5 Pessoas & Cultura 33
10.10.6 Privacidade e Proteção de Dados e Segurança da Informação 33
11. MEDIDAS DISCIPLINARES 34
12. DISPOSIÇÕES FINAIS 35

13. GLOSSÁRIO 35
14. DOCUMENTOS DE REFERÊNCIA 35
15. GESTÃO DO DOCUMENTO 36
15.1 REVISÃO 36
15.2 HISTÓRICO DE ATUALIZAÇÃO 36
15.3 APROVAÇÃO 36

1.OBJETIVO

A Política Integrada de *Compliance,* Anticorrupção e Antissuborno da Tecnobank estabelece os princípios, diretrizes, responsabilidades e mecanismos necessários para assegurar que todas as atividades da organização sejam conduzidas com ética, integridade, transparência, responsabilidade corporativa e conformidade com a legislação aplicável.

Esta política integra os requisitos das normas ISO 37301:2021 e ISO 37001:2025, bem como as diretrizes da Lei Anticorrupção Brasileira, Lei nº 12.846/2013 e Decreto nº 11.129/2022. Também considera legislações anticorrupção internacionais aplicáveis, incluindo, mas não se limitando ao FCPA (*Foreign Corrupt Practices Act*), UK *Bribery Act* (Lei Antissuborno do Reino Unido) e diretrizes internacionais e convenções anticorrupção relevantes.

A política visa promover a prevenção, detecção e resposta a riscos de *Compliance*, corrupção, suborno (no setor público e privado), fraude, conflitos de interesse, lavagem de dinheiro e demais irregularidades, fortalecendo a cultura de integridade em toda a Companhia.

2. ABRANGÊNCIA

Esta Política aplica-se a todas as pessoas que se relacionam e ajam em nome da Tecnobank, abrangendo colaboradores, administradores, prestadores de serviços, fornecedores e parceiros de negócio que, em razão de suas atividades, tenham acesso a instalações, sistemas, informações ou quaisquer ativos da empresa.

O cumprimento desta Política é obrigatório e integra as práticas de *Compliance* e Governança Corporativa, devendo ser observado por todos aqueles que mantêm vínculo direto ou indireto com a Companhia.

3. DIRETRIZES

As diretrizes fundamentais da Tecnobank estabelecem os princípios e padrões de conduta que orientam a atuação de todos os públicos abrangidos por esta Política Integrada, promovendo uma cultura organizacional pautada na integridade, ética, transparência, conformidade e prevenção à corrupção e ao suborno em todas as relações corporativas.

Para fins desta Política, considera-se suborno a oferta, promessa, concessão, autorização, solicitação, aceitação ou recebimento, de forma direta ou indireta, de qualquer vantagem indevida, de natureza financeira ou não financeira, com a finalidade de influenciar indevidamente uma ação, decisão ou omissão no exercício de atribuições ou responsabilidades, independentemente de envolver agentes públicos ou privados, em operações nacionais ou internacionais.

A vantagem indevida pode se manifestar por meio de pagamentos em dinheiro, presentes, brindes, viagens, hospitalidades, doações, patrocínios, concessão de benefícios, oportunidades de emprego ou qualquer outro favorecimento, inclusive quando destinado a familiares, pessoas próximas ou terceiros relacionados ao beneficiário.

Considera-se corrupção, para fins desta Política, a prática de atos ilícitos relacionados à obtenção, concessão ou manutenção de vantagens indevidas, incluindo práticas de suborno, fraude ou outras condutas que comprometam a integridade das relações públicas ou privadas, observadas as definições e disposições da legislação aplicável.

3.1 Tolerância Zero

A Tecnobank adota tolerância zero a qualquer forma de corrupção, suborno, fraude ou vantagem indevida.

É proibida, em todas as circunstâncias, a oferta, promessa, solicitação, aceitação ou recebimento de qualquer benefício indevido, direta ou indiretamente, no setor público ou privado.

3.2 Suborno e Corrupção

Qualquer proposta de custeio de pagamentos de viagens, hospedagem ou despesas correlatas destinadas a agentes públicos deverá, obrigatoriamente, ser submetida à análise e aprovação da área de *Compliance*. A avaliação considerará critérios de transparência, legalidade, finalidade institucional legítima e vinculação direta às atividades do órgão público envolvido.

É vedado, em qualquer hipótese, o pagamento direto de valores a agentes públicos para que estes custeiem suas próprias despesas, incluindo viagens, hospedagem ou quaisquer outras relacionadas.

3.3 Conformidade legal e regulatória

A Tecnobank cumpre rigorosamente legislações aplicáveis, regulamentos setoriais, normas internas, requisitos das normas ISO 37301 e ISO 37001 e diretrizes da Lei 12.846/2013 e Decreto 11.129/2022, FCPA, *UK Bribery Act* e demais legislações aplicáveis.

Adicionalmente, a Companhia observa compromissos voluntários e boas práticas de integridade, incluindo iniciativas relacionadas a ESG e ao Pacto Brasil pela Integridade, quando aplicáveis ao seu contexto de atuação.

3.4 Integridade, ética e transparência

Todos os destinatários devem atuar de forma íntegra, ética, transparente e responsável, sem qualquer forma de favorecimento indevido, fraude, ocultação de informação ou condutas que possam comprometer a reputação da Companhia.

3.5 Proibição de Suborno Direto ou Indireto

É proibido suborno direto e por meio de terceiros (intermediários, consultores, parceiros, clientes, fornecedores ou quaisquer pessoas associadas). Nenhuma pessoa pode ser utilizada como “interposta pessoa” para atos ilícitos.

3.6 Proibição Irrestrita de Pagamentos de Facilitação

A Companhia proíbe integralmente pagamentos de facilitação (*facilitation payments*), entendidos como pagamentos ou vantagens indevidas oferecidos, prometidos ou concedidos com a finalidade de acelerar, facilitar ou assegurar a realização de atos, serviços ou procedimentos, ainda que sejam considerados rotineiros ou devidos.

A proibição aplica-se às relações com agentes públicos e privados, no Brasil ou no exterior, independentemente do valor envolvido ou da prática eventualmente adotada no local da operação.

Essa prática é considerada forma de corrupção e é proibida por diversas legislações anticorrupção internacionais, especialmente o *UK Bribery Act*, e tratada como risco relevante pelo FCPA e pela ISO 37001.

3.7 Registros contábeis

A Tecnobank mantém controles internos e mecanismos de segregação de funções destinados a assegurar a integridade, a precisão, a completude e a rastreabilidade dos registros contábeis e financeiros, observando a legislação brasileira e os requisitos legais e regulatórios efetivamente aplicáveis às suas atividades.

Em decorrência de sua integração ao Grupo Evertec, a Companhia também observa, conforme o escopo e as responsabilidades formalmente estabelecidos pelo Grupo, as diretrizes corporativas relacionadas à Lei *Sarbanes-Oxley* (SOX), aos controles internos sobre informações financeiras e aos requisitos associados à *Securities and Exchange Commission* (SEC), órgão regulador do mercado de capitais dos Estados Unidos.

A Companhia estabelece e mantém controles destinados a:

- Assegurar a completude, a precisão e o detalhamento dos registros e lançamentos contábeis.

- Formalizar os controles internos, incluindo segregação de funções e alçadas de aprovação.
- Garantir a manutenção e a conservação dos registros, observados os prazos legais, regulatórios e corporativos aplicáveis.
- Prevenir falsificações, omissões e alterações indevidas nos registros.
- Promover a rastreabilidade e a proteção dos registros físicos e eletrônicos.
- Atender aos controles e às evidências requeridos pelo Grupo Evertec, conforme o escopo corporativo estabelecido e os requisitos aplicáveis.

3.8 Segregação de funções e controles internos robustos

A Companhia assegura que processos sensíveis possuam:

- controles adequados;
- aprovações formais;
- mitigação de riscos operacionais e de integridade;
- rastreabilidade documental.

3.9 Confidencialidade e não retaliação

As análises e apurações serão conduzidas de forma confidencial, técnica e restrita a quem necessite conhecer. É expressamente vedada qualquer forma de retaliação contra colaboradores ou terceiros que reportem suspeitas de boa-fé, ainda que a apuração conclua pela inexistência de irregularidade.

3.10 Governança Corporativa

A Tecnobank reforça práticas de governança que assegurem transparência, responsabilidade, prestação de contas e alinhamento estratégico do SGICA.

A Companhia assegura a adequada retenção, integridade, rastreabilidade e confidencialidade dos registros relacionados ao Sistema de Gestão de *Compliance*, conforme requisitos legais e internos aplicáveis.

4. SISTEMA DE GESTÃO INTEGRADA DE *COMPLIANCE*, ANTICORRUPÇÃO E ANTISSUBORNO (SGICA)

O Sistema de Gestão Integrada de *Compliance*, Anticorrupção e Antissuborno da Tecnobank (SGICA) estabelece princípios, regras e mecanismos destinados à prevenção, identificação e tratamento de desvios de conduta, riscos de integridade, corrupção, suborno e descumprimento de obrigações de *Compliance*.

O SGICA busca assegurar que as atividades e os relacionamentos da Companhia sejam conduzidos em conformidade com os requisitos legais, regulatórios, contratuais e normativos aplicáveis, promovendo a cultura ética, a gestão de riscos e a melhoria contínua.

São pilares do SGICA:

4.1 Gestão de Obrigações de *Compliance*

A Tecnobank estabelece a gestão estruturada das obrigações de *Compliance*, compreendendo a identificação, análise, monitoramento e atualização de:

- legislações e regulamentações aplicáveis;
- requisitos contratuais;
- compromissos voluntários e institucionais assumidos pela Companhia;
- diretrizes nacionais e internacionais de integridade aplicáveis às suas atividades e relacionamentos.

As obrigações identificadas são avaliadas quanto à sua aplicabilidade e consideradas na definição de responsabilidades, processos, controles e medidas de monitoramento, observadas as competências das áreas envolvidas.

A gestão dessas obrigações é realizada de forma integrada ao SGICA, conforme os critérios e procedimentos internos aplicáveis.

4.2 Gestão de Oportunidades de *Compliance*

A Tecnobank promove a identificação e avaliação de oportunidades relacionadas ao fortalecimento e à melhoria contínua do Sistema de Gestão de *Compliance*, considerando seu contexto organizacional, as necessidades das partes interessadas, os resultados de auditorias, monitoramentos, avaliações de riscos e mudanças internas e externas.

As oportunidades identificadas podem contemplar melhorias de processos, fortalecimento de controles, eficiência operacional, inovação, aperfeiçoamento da governança e evolução da cultura ética e de integridade.

As ações decorrentes das oportunidades consideradas relevantes são planejadas e acompanhadas conforme sua natureza, prioridade e viabilidade, com definição das responsabilidades aplicáveis e avaliação dos resultados alcançados, utilizando os mecanismos de gestão e monitoramento existentes.

4.3 Avaliação de Riscos

A Tecnobank realiza identificação, análise, avaliação e tratamento dos riscos de *Compliance*, anticorrupção, antissuborno e integridade, considerando:

- a probabilidade de ocorrência e o impacto dos riscos;
- a existência, a maturidade e a eficácia dos controles aplicáveis;
- o contexto interno e externo da Companhia;
- as necessidades e expectativas das partes interessadas pertinentes;
- as obrigações de *Compliance* aplicáveis;
- as mudanças organizacionais, regulatórias, tecnológicas e operacionais;
- os riscos emergentes e os resultados das atividades de monitoramento e auditoria.

A avaliação dos riscos observa a metodologia estabelecida na Política de Gestão de Riscos e nos instrumentos internos aplicáveis, considerando os riscos inerentes, os controles existentes e os riscos residuais.

Os riscos identificados são avaliados para definição das medidas de tratamento apropriadas, considerando sua criticidade, o apetite a riscos estabelecido pela Companhia e as estratégias de aceitação, mitigação, transferência ou prevenção da exposição ao risco, conforme aplicável.

As ações de tratamento são planejadas e acompanhadas pelas áreas responsáveis, com definição de medidas, responsabilidades e prazos.

A aceitação de riscos residuais, quando permitida pelos critérios internos, não autoriza a prática de atos ilícitos, corrupção, suborno ou quaisquer condutas expressamente proibidas pelas políticas corporativas e pela legislação aplicável.

A eficácia dos controles e das ações implementadas é avaliada por meio das atividades de monitoramento, testes de controles, auditorias e demais mecanismos de avaliação do SGICA, subsidiando a revisão das classificações de riscos e a adoção de medidas adicionais, quando necessárias.

A Matriz de Riscos de Integridade deve ser revisada, no mínimo, a cada dois anos ou sempre que ocorrerem mudanças relevantes no ambiente regulatório, organizacional ou operacional, sem prejuízo do monitoramento e das atualizações necessárias durante esse período.

Antes do ingresso da Tecnobank em novos mercados ou da implementação de novos negócios, produtos ou serviços, deverá ser realizada avaliação dos riscos de *Compliance*, corrupção e suborno relacionados à iniciativa, com participação das áreas de *Compliance* e Jurídico e apoio das áreas responsáveis, conforme a natureza e a relevância dos riscos envolvidos.

Os riscos identificados devem ser considerados nos processos decisórios relevantes da Companhia, observadas as responsabilidades e autoridades estabelecidas na estrutura de governança e os critérios de registro definidos nos procedimentos internos.

4.4 Políticas, Normas e Procedimentos

A Companhia mantém documentos normativos claros, objetivos e atualizados, assegurando alinhamento com:

- legislações vigentes;
- ISO 37301 e ISO 37001;
- Lei 12.846/2013 e Decreto 11.129/2022;
- FCPA, *UK Bribery Act* e normativas aplicáveis;
- melhores práticas de mercado.

4.5 Suporte da Alta Administração

A Alta Administração garante recursos, liderança pelo exemplo *(tone from the top*), aprovação de políticas aplicáveis, supervisão do SGICA, definição de apetite de risco e avaliação periódica de eficácia.

4.6 Comunicação e Treinamento

A Companhia implementa ações contínuas de comunicação e treinamentos obrigatórios, proporcionais ao risco, incluindo:

- trilhas de capacitação por público;
- reforço para áreas sensíveis;
- campanhas institucionais;
- registros de participação;
- avaliação de efetividade.

A Tecnobank avalia a efetividade de suas ações de comunicação e treinamento por meio de métricas de engajamento, avaliação de conhecimento e monitoramento de comportamento.

4.7 *Due Diligence* (KYS, KYE, KYC)

A Tecnobank realiza procedimentos de *Due Diligence* de Integridade de fornecedores (KYS), colaboradores (KYE) e clientes (KYC), observando critérios de

elegibilidade, classificação de riscos e proporcionalidade definidos na Política de *Due Diligence* de Integridade e nos procedimentos internos aplicáveis.

As avaliações têm como finalidade identificar e mitigar riscos de *Compliance*, corrupção, suborno, fraude, conflitos de interesses e demais riscos de integridade associados aos relacionamentos da Companhia.

A realização das diligências considera a natureza do relacionamento, o perfil da parte avaliada, as atividades envolvidas, a exposição a agentes públicos, os riscos associados e demais critérios estabelecidos nos instrumentos normativos específicos.

As diligências são realizadas previamente ao estabelecimento do relacionamento, quando exigidas pelos critérios internos e reavaliadas periodicamente ou diante de eventos relevantes, conforme os critérios aplicáveis a cada modalidade de avaliação.

Para o processo de KYS, a periodicidade de reavaliação observa a classificação de risco atribuída:

- Risco Alto: anualmente;
- Risco Médio: a cada dois anos;
- Risco Baixo: a cada três anos.

Para os processos de KYC e KYE, as avaliações seguem critérios específicos de elegibilidade e atualização previstos nos procedimentos internos, não estando sujeitas à periodicidade estabelecida para KYS.

Independentemente da periodicidade prevista, poderão ser realizadas diligências extraordinárias diante da identificação de fatos novos, alterações relevantes no perfil da parte avaliada, mudanças nas condições do relacionamento ou outras circunstâncias que possam modificar a exposição aos riscos de integridade.

As avaliações poderão contemplar, conforme aplicabilidade, consultas a bases públicas, listas de sanções nacionais e internacionais, identificação de pessoas expostas politicamente, análise reputacional, vínculos societários e outros elementos necessários à avaliação de integridade.

Os resultados das diligências deverão ser registrados e considerados nos processos de aprovação, contratação, manutenção ou revisão dos relacionamentos, observadas as alçadas de decisão e as medidas de tratamento previstas nos procedimentos internos.

A identificação de riscos relevantes poderá resultar na adoção de diligências reforçadas, controles adicionais, restrições ou recomendação de não estabelecimento ou descontinuidade do relacionamento, conforme os critérios e responsabilidades definidos nos procedimentos internos aplicáveis.

4.8 Canal de Ética

A Tecnobank mantém Canal de Ética operado por empresa externa independente, disponível aos colaboradores, terceiros e público externo, assegurando a possibilidade de relatos anônimos, a confidencialidade das informações e a proteção contra retaliação, observados os requisitos legais e os procedimentos internos aplicáveis.

Suspeitas de violações ao Código de Conduta, a esta Política ou às demais diretrizes de integridade devem ser comunicadas por meio dos canais oficiais disponibilizados pela Companhia, incluindo:

- Telefone: 0800 602 6911;
- Portal de *Compliance* da Tecnobank;
- Plataforma externa independente: https://www.contatoseguro.com.br/pt/tecnobank.

As comunicações recebidas serão tratadas conforme os critérios de confidencialidade, imparcialidade, proteção dos envolvidos e não retaliação estabelecidos nos instrumentos normativos aplicáveis.

4.9 Investigação e Resposta

A Tecnobank mantém mecanismos estruturados para o recebimento, a avaliação, a apuração e o tratamento de relatos de possíveis irregularidades, observando critérios de confidencialidade, imparcialidade, proporcionalidade e proteção contra retaliação.

As apurações são conduzidas conforme a natureza, a gravidade e a complexidade dos fatos, podendo contemplar triagem, coleta e análise de evidências, registros documentais, recomendações, medidas corretivas e disciplinares, quando aplicáveis, e encaminhamento às instâncias competentes, observadas as responsabilidades estabelecidas nos procedimentos internos.

4.10 Melhoria Contínua

A Tecnobank promove a melhoria contínua do Sistema de Gestão Integrada, por meio de auditorias e monitoramentos, revisão de riscos, ações corretivas, lições aprendidas, atualização de políticas, normas e procedimentos.

4.11 Gestão de Mudanças

A Tecnobank assegura que mudanças relevantes, incluindo alterações organizacionais, novos produtos, serviços, mercados ou requisitos regulatórios, sejam previamente avaliadas quanto aos riscos de *Compliance*, com a devida adequação dos controles internos.

5. SANÇÕES INTERNACIONAIS – OFAC E OUTRAS LISTAS

A Tecnobank observa as restrições e obrigações relacionadas a sanções econômicas e financeiras nacionais e internacionais efetivamente aplicáveis às suas atividades, operações e relacionamentos, incluindo, quando pertinente, aquelas estabelecidas pela Organização das Nações Unidas (ONU), União Europeia (UE) e *Office of Foreign Assets Control* (OFAC).

A identificação de pessoas, entidades, países ou operações sujeitas a sanções deverá ser avaliada conforme a natureza da restrição, sua aplicabilidade e os procedimentos internos pertinentes, com apoio das áreas competentes, antes da adoção de decisões relacionadas ao estabelecimento, à manutenção ou à continuidade dos relacionamentos e operações.

É vedada a realização de operações ou relacionamentos que contrariem proibições legais ou restrições sancionatórias efetivamente aplicáveis à Companhia.

6.MONITORAMENTO E AUDITORIAS

A Tecnobank estabelece mecanismos de monitoramento e avaliação do desempenho do Sistema de Gestão de *Compliance*, por meio de indicadores, auditorias, análises críticas e acompanhamento de planos de ação.

Não conformidades são tratadas por meio de processo estruturado que inclua registro formal, análise de causa raiz, definição de ações corretivas e preventivas, definição de prazos e responsáveis e verificação de eficácia das ações implementadas.

7. INFORMAÇÕES RELEVANTES E PRIVILEGIADAS – *INSIDER TRADING*

Colaboradores que tenham acesso à informação privilegiada devem zelar por sua confidencialidade e não podem:

- divulgar informação a terceiros não autorizados;
- utilizar informação para obtenção de vantagem indevida;
- negociar ativos com base em informação não pública.

O uso indevido de informação privilegiada pode configurar infração grave e violação legal.

8.TEMAS ESPECÍFICOS DE INTEGRIDADE

8.1. Presentes, Brindes, Hospitalidades e Entretenimento

É permitido somente quando:

- for razoável, proporcional e esporádico;
- não gerar expectativa de contrapartida;
- não influenciar decisões;
- estiver alinhado às políticas internas;
- for registrado e aprovado quando aplicável.

É proibido oferecer ou aceitar qualquer item de valor em contextos sensíveis, incluindo:

- Licitações / credenciamentos;
- renovações contratuais;
- fiscalizações;
- negociações críticas.

8.2. Doações e Patrocínios

Somente são permitidos quando:

- possuírem finalidade legítima;
- forem transparentes;
- sejam submetidos às avaliações de integridade e aos procedimentos de *Due Diligence* aplicáveis, conforme os critérios estabelecidos nas políticas e nos procedimentos internos;
- tenham seus riscos identificados, avaliados e tratados antes da aprovação, observadas as competências e alçadas pertinentes;
- não representarem benefício indireto a agente público ou pessoa associada.

8.3. Conflitos de interesse e partes relacionadas

A Tecnobank exige que colaboradores e administradores:

- declarem conflitos reais, potenciais ou aparentes;
- se abstenham de decisões quando conflitados;
- sigam o fluxo formal de avaliação;
- mantenham transparência sobre vínculos pessoais, familiares ou societários.

Relações com partes relacionadas devem ser avaliadas e registradas conforme normas internas aplicáveis.

8.4. Contribuições Políticas

A Tecnobank proíbe contribuições políticas institucionais.

8.5. Relação com Agentes Públicos

Interações com agentes públicos devem:

- ser transparentes;
- ter finalidade legítima;
- ser registradas quando aplicável;

- respeitar normas e controles internos;
- vedar qualquer promessa de vantagem.

8.6. Contratação de Terceiros e Intermediários

É proibida contratação de terceiros com finalidade ilícita ou sem diligência adequada.

A Companhia aplica controles reforçados para:

- representantes comerciais;
- consultores;
- despachantes;
- agentes;
- parceiros de canal;
- *joint ventures* e parcerias comerciais.

A Tecnobank espera que os terceiros e intermediários com os quais se relaciona tenham procedimentos de conduta e ética e os façam valer. Para os terceiros ou intermediário que não possuem tais diretrizes a Tecnobank espera que estes sigam os padrões éticos estabelecidos no Código de Conduta da Tecnobank.

Além disso, o time Jurídico deve assegurar que todos os contratos estabelecidos com terceiros ou intermediários contenham as disposições de anticorrupção e antissuborno.

8.7. Fusões, Aquisições e Integrações

Nos casos de fusões, aquisições ou reestruturações societárias conduzidas pela controladora, a organização deverá avaliar os impactos dessas operações em seu Sistema de Gestão Integrada de *Compliance*, Anticorrupção e Antissuborno (SGICA).

Essa avaliação deve contemplar, no mínimo, a identificação e análise de riscos de *Compliance*, a adequação de controles internos, bem como a atualização do contexto organizacional e dos processos afetados, em alinhamento com as diretrizes estabelecidas pela controladora.

8.8. Extorsão e Situações de Coação

Em caso de ameaça à integridade física do colaborador, a prioridade é a segurança.

O fato deve ser comunicado imediatamente à liderança e à área de *Compliance*, com registro formal e avaliação de riscos.

9. CONDUTAS VEDADAS

São vedadas, entre outras condutas:

- oferecer ou receber vantagem indevida;
- fraudar licitações;
- manipular contratos públicos;
- financiar práticas ilícitas;
- ocultar beneficiários por interpostas pessoas;
- realizar pagamento de facilitações;
- utilizar informações privilegiadas para obter vantagem em negociações financeiras – *Insider Trading*.

A simples promessa, aceitação ou oferecimento já configuram ato indevido.

10.ESTRUTURA DE GOVERNANÇA

10.1 Órgão Diretivo

Considerando o porte e a estrutura organizacional da Tecnobank, não existe um órgão que se enquadre formalmente na definição de "Órgão Diretivo", conforme previsto nas normas ISO 37001 e ISO 37301.

Dessa forma, para fins do Sistema de Gestão Integrada de *Compliance*, Anticorrupção e Antissuborno (SGICA), as responsabilidades atribuídas ao Órgão Diretivo pelas referidas normas são exercidas pela Alta Administração, observadas as competências e autoridades estabelecidas na estrutura de governança da Companhia.

10.2 Alta Administração

Para fins do SGICA, a Alta Administração da Tecnobank é representada pela Presidência, responsável pela liderança, comprometimento e supervisão estratégica do Sistema.

A Vice-Presidência, a Diretoria de Governança Corporativa e as demais Diretorias participam da implementação, manutenção e melhoria contínua do SGICA, conforme suas respectivas responsabilidades e autoridades, sem se confundirem com a Alta Administração definida para fins do Sistema.

- Compete à Alta Administração: demonstrar liderança e comprometimento com o SGICA e promover a cultura de ética, integridade e conformidade em todos os níveis da Companhia;
- aprovar as políticas, diretrizes e documentos de natureza estratégica, institucional, estruturante ou mandatória, observadas as alçadas definidas no Manual do SGICA e na Lista Mestra;
- assegurar a disponibilização dos recursos humanos, tecnológicos, financeiros e organizacionais necessários à implementação, manutenção e melhoria contínua do Sistema;

- assegurar a autonomia, a independência técnica e a autoridade da Função de *Compliance*, incluindo seu acesso direto à Presidência;
- supervisionar o desempenho do SGICA, considerando os resultados de monitoramentos, auditorias, avaliações de riscos, indicadores, não conformidades e ações corretivas;
- realizar a análise crítica periódica do Sistema, avaliando sua adequação, suficiência e eficácia;
- apoiar a melhoria contínua do SGICA e assegurar que eventuais deficiências relevantes sejam tratadas.

10.3 Comitê de Ética

O Comitê de Ética constitui instância colegiada de governança, com atuação pautada pela imparcialidade, confidencialidade e independência de julgamento, observadas as competências, regras de funcionamento e alçadas estabelecidas em seu Regimento Interno.

O Comitê contribui para a supervisão de aspectos relevantes da integridade corporativa, sem substituir as responsabilidades da Alta Administração ou da Função de *Compliance*.

Compete ao Comitê de Ética:

- fomentar cultura ética na Tecnobank;
- zelar pelo cumprimento do Código de Conduta, políticas e diretrizes de integridade da Companhia;
- avaliar e deliberar sobre casos de potenciais violações éticas submetidas à sua apreciação, conforme as competências estabelecidas em seu Regimento;
- analisar riscos de retaliação e acompanhar a adoção de medidas de proteção cabíveis;

- deliberar ou recomendar medidas disciplinares e de responsabilização, observadas as competências e alçadas aplicáveis;
- acompanhar o tratamento adequado das situações submetidas ao Comitê, respeitados os princípios de confidencialidade, imparcialidade e não retaliação;
- analisar informações consolidadas sobre denúncias e tendências de risco;
- acompanhar aspectos críticos do SGICA que sejam submetidos à sua apreciação;
- recomendar medidas preventivas, corretivas ou de aprimoramento dos mecanismos de integridade, quando aplicável.

10.4 Diretoria de Governança Corporativa

A Diretoria de Governança Corporativa é responsável pela coordenação estratégica e pela supervisão gerencial do SGICA, incluindo sua integração com os programas de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLDFT), Anticorrupção e Gestão de Riscos, observadas as atribuições e responsabilidades das áreas competentes.

A estrutura sob sua gestão contempla as áreas de *Compliance*, Controles Internos, Privacidade e Proteção de Dados e Segurança da Informação, promovendo a atuação coordenada dessas funções, a segregação adequada de responsabilidades e o acompanhamento da eficácia dos controles implementados.

Compete à Diretoria de Governança Corporativa:

- supervisionar o desempenho do SGICA por meio de relatórios, indicadores, avaliações e resultados de monitoramento;
- gerenciar estrategicamente as áreas sob sua responsabilidade, promovendo a integração das atividades de Governança, Riscos e *Compliance* (GRC), Privacidade e Proteção de Dados, Segurança da Informação e Controles Internos;

- promover alinhamento entre os objetivos estratégicos da Companhia e as obrigações de *Compliance* aplicáveis;
- apoiar a disponibilização dos recursos necessários à manutenção e à melhoria contínua do SGICA;
- aprovar documentos de natureza gerencial, metodológica ou de governança relacionados ao SGICA, observadas as competências da Alta Administração e os critérios de alçada estabelecidos no Manual do SGICA e na Lista Mestra;
- submeter à aprovação da Alta Administração os documentos de natureza estratégica, institucional, estruturante ou mandatória, conforme os critérios de alçada aplicáveis;
- acompanhar os resultados das atividades relacionadas ao SGICA, assegurando o devido reporte ao Comitê de Ética e à Alta Administração;
- apoiar a implementação de ações de melhoria e o acompanhamento dos planos de ação relacionados ao SGICA, respeitadas as responsabilidades das áreas executoras;
- preservar as condições necessárias para que a Função de *Compliance* exerça suas atribuições com autonomia e independência técnica.

10.5 Área de *Compliance*

A área de *Compliance* da Tecnobank integra a estrutura organizacional da Diretoria de Governança Corporativa e é responsável por coordenar e executar atividades técnicas relacionadas à implementação, manutenção, monitoramento e melhoria contínua do SGICA, conforme as responsabilidades estabelecidas nos instrumentos normativos internos.

Sua atuação observa os princípios de integridade, imparcialidade, confidencialidade, autonomia técnica e abordagem baseada em riscos, com acesso às informações necessárias ao desempenho de suas atribuições, respeitadas as disposições legais aplicáveis.

No âmbito da Governança Corporativa, *Compliance* e Controles Internos constituem áreas distintas e complementares, com atribuições e responsabilidades próprias.

As áreas atuam de forma integrada e coordenada, respeitadas suas competências e a segregação de funções, contribuindo para o fortalecimento da governança, da gestão de riscos, da conformidade e da eficácia dos controles corporativos.

10.6 Função de *Compliance* (*Compliance Officer*)

A Função de *Compliance* é exercida pela *Compliance Officer*, responsável pela coordenação técnica do SGICA, com autoridade, autonomia e independência necessárias ao desempenho de suas atribuições.

A vinculação administrativa da Função de *Compliance* à Diretoria de Governança Corporativa não compromete sua independência técnica, autonomia de atuação, imparcialidade ou autoridade para realizar análises, emitir recomendações e reportar situações relevantes.

A Função de *Compliance* possui acesso direto e independente à Presidência, inclusive para comunicar riscos significativos, potenciais violações, conflitos de interesses, deficiências relevantes do SGICA e demais assuntos que demandem apreciação da Alta Administração, sem necessidade de autorização prévia ou intermediação de outras instâncias.

Compete à Função de *Compliance*:

- coordenar tecnicamente a implementação, manutenção, monitoramento e melhoria contínua do SGICA;
- orientar as áreas da Companhia quanto à interpretação e à aplicação dos requisitos de *Compliance*, Anticorrupção e Antissuborno;

- apoiar a identificação, a avaliação e o tratamento dos riscos de *Compliance*, corrupção e suborno, em conjunto com os responsáveis pelos processos;
- acompanhar o atendimento às obrigações de *Compliance* aplicáveis e apoiar sua tradução em controles, responsabilidades e medidas de monitoramento;
- coordenar ou acompanhar as avaliações de integridade e os procedimentos de *Due Diligence*, conforme os critérios e responsabilidades definidos nos instrumentos normativos específicos;
- promover ações de comunicação, conscientização e treinamento relacionadas ao SGICA, incluindo a avaliação de sua eficácia, conforme os critérios internos;
- monitorar o desempenho do SGICA e comunicar os resultados às instâncias competentes;
- acompanhar não conformidades, ações corretivas e oportunidades de melhoria relacionadas ao Sistema;
- apoiar a realização de auditorias internas e externas e o acompanhamento dos respectivos resultados;
- emitir pareceres, orientações e recomendações técnicas sobre questões relacionadas ao SGICA;
- aprovar documentos técnicos e operacionais de sua competência, observadas as alçadas estabelecidas no Manual do SGICA e na Lista Mestra;
- reportar diretamente à Alta Administração assuntos relevantes relacionados à integridade e à eficácia do Sistema, sempre que necessário.

A Função de *Compliance* exerce suas atividades sem assumir a responsabilidade operacional pelos processos e controles pertencentes às demais áreas, preservando a segregação de funções e a responsabilidade dos respectivos gestores.

Durante ausências temporárias, férias, licenças ou impedimentos da titular da Função de *Compliance,* a continuidade das atividades essenciais do SGICA será organizada pela estrutura de Governança Corporativa, mediante distribuição das demandas entre os profissionais da área de *Compliance* e a Diretoria de Governança Corporativa, conforme suas respectivas atribuições, competências e níveis de autoridade.

As atividades operacionais e de acompanhamento poderão ser conduzidas pelos profissionais da área, enquanto situações que demandem decisões, autorizações ou escalonamento serão direcionadas às instâncias competentes, observadas a criticidade, a segregação de funções, a confidencialidade e a independência técnica da Função de *Compliance*. As atividades programáveis poderão ser antecipadas ou reagendadas, desde que respeitados os prazos aplicáveis e que não haja comprometimento da eficácia do SGICA.

A distribuição das atividades não implica transferência automática da designação formal, das autoridades ou dos acessos restritos atribuídos à titular, devendo eventuais necessidades específicas ser avaliadas e tratadas conforme a natureza, a criticidade e a urgência da demanda.

10.7 Diretores

Compete aos Diretores, no âmbito de suas respectivas áreas de atuação:

- promover elevados padrões éticos e de integridade, demonstrando comprometimento com as diretrizes do SGICA;
- assegurar o cumprimento das leis, regulamentos, obrigações de *Compliance* e políticas internas aplicáveis aos processos sob sua responsabilidade;
- identificar, avaliar, tratar e acompanhar os riscos relacionados às atividades de suas áreas;
- assegurar a implementação, a execução e a manutenção dos controles internos aplicáveis;

- disponibilizar informações e evidências necessárias às atividades de monitoramento, auditoria e avaliação de *Compliance*;
- assegurar o tratamento tempestivo de não conformidades e a implementação das ações corretivas sob sua responsabilidade;
- apoiar a disseminação da cultura de integridade e a participação das equipes nas ações de treinamento e conscientização;
- comunicar à Função de *Compliance* riscos relevantes, potenciais irregularidades e situações que possam comprometer a eficácia do SGICA.

10.8 Liderança

A liderança, compreendida pelos gerentes, coordenadores, supervisores e demais profissionais com responsabilidade pela gestão de equipes, deve atuar como multiplicadora da cultura ética e de integridade, promovendo a aplicação das diretrizes do SGICA nas atividades sob sua responsabilidade.

Compete à liderança:

- atuar pelo exemplo, conduzindo suas equipes de forma ética, íntegra e transparente;
- incentivar o diálogo sobre ética, integridade, conformidade e prevenção à corrupção e ao suborno;
- orientar as equipes quanto à aplicação do Código de Conduta, das políticas e dos procedimentos internos;
- incentivar a comunicação de riscos, dúvidas e suspeitas de irregularidades, respeitando a confidencialidade e a proibição de retaliação;
- assegurar a participação das equipes nos treinamentos obrigatórios de *Compliance*;
- acompanhar a execução dos controles e o cumprimento das obrigações aplicáveis aos processos sob sua responsabilidade;
- apoiar a implementação de medidas preventivas e corretivas relacionadas ao SGICA;
- comunicar situações relevantes às instâncias competentes, conforme os canais e procedimentos internos.

10.9 Colaboradores

Todos os colaboradores da Tecnobank são responsáveis por atuar em conformidade com as diretrizes do SGICA, independentemente do cargo, função ou nível hierárquico.

Compete aos colaboradores:

- zelar pelo nome, pela reputação e pela imagem da Tecnobank;
- atuar de acordo com os valores da Companhia, mantendo conduta ética, íntegra, transparente e responsável;
- conhecer e cumprir o Código de Conduta, as políticas, os procedimentos e as demais diretrizes internas aplicáveis;
- cumprir as leis, os regulamentos e as obrigações de *Compliance* relacionados às suas atividades;
- identificar e comunicar riscos, falhas, não conformidades, potenciais conflitos de interesses e suspeitas de irregularidades;
- reportar, pelos canais apropriados, fatos relevantes ou situações que possam representar violações às diretrizes de integridade;
- participar dos treinamentos e das ações de conscientização de *Compliance*, conforme requerido;
- cooperar com atividades de monitoramento, auditoria, apuração e avaliação de conformidade, observadas as regras de confidencialidade;
- buscar orientação da área de *Compliance* sempre que houver dúvidas relacionadas à aplicação das diretrizes do SGICA;
- executar suas atividades em conformidade com os controles e procedimentos aplicáveis.

O desconhecimento das normas internas não afasta as responsabilidades decorrentes de seu descumprimento, observadas as condições de comunicação, disponibilização e capacitação estabelecidas pela Companhia.

10.10 Multiplicadores

São considerados multiplicadores do Sistema de Gestão Integrada de *Compliance*, Anticorrupção e Antissuborno (SGICA) os profissionais de áreas que, no âmbito de suas atribuições, apoiam a área de *Compliance* na execução de atividades específicas, na disseminação das diretrizes de integridade e no fortalecimento da cultura de ética e conformidade.

Os principais multiplicadores são representantes das áreas de Compras, Comunicação e *Marketing*, Financeiro, Jurídico, Pessoas e Cultura, Privacidade e Proteção de Dados e Segurança da Informação.

A atuação dos multiplicadores ocorre de forma integrada e colaborativa, observadas as competências de cada área, a segregação de funções e as responsabilidades estabelecidas nos procedimentos internos.

10.10.1 Compras

Compete à área de Compras:

- apoiar a área de *Compliance* na realização dos procedimentos de *Due Diligence* de Integridade de fornecedores e parceiros de negócio, conforme os critérios de elegibilidade e as responsabilidades estabelecidas nos procedimentos internos;
- assegurar a observância dos critérios de ética, integridade e transparência nos processos de aquisição e contratação sob sua responsabilidade;
- comunicar à área de *Compliance* situações que possam representar riscos de integridade, conflitos de interesses ou irregularidades nos relacionamentos com fornecedores e parceiros;
- apoiar a implementação e o acompanhamento das medidas de tratamento de riscos relacionadas aos processos de contratação.

10.10.2 Comunicação & *Marketing*

Compete à área de Comunicação e *Marketing*:

- apoiar a área de *Compliance* na elaboração, divulgação e atualização de comunicações internas e externas relacionadas à ética, integridade, anticorrupção e antissuborno;
- contribuir para a disseminação das políticas, diretrizes, campanhas e ações de conscientização relacionadas ao SGICA;
- apoiar a definição dos canais e formatos de comunicação adequados aos públicos envolvidos;
- disponibilizar, quando aplicável, evidências das comunicações realizadas, de forma a contribuir para o acompanhamento de sua abrangência e efetividade.

10.10.3 Financeiro

Compete à área Financeira:

- assegurar que os registros financeiros e contábeis sob sua responsabilidade sejam realizados de forma íntegra, precisa, tempestiva e compatível com a realidade das operações;
- observar os controles e procedimentos aplicáveis às movimentações financeiras, pagamentos, reembolsos e demais operações sob sua responsabilidade;
- disponibilizar informações, registros e evidências necessários às atividades de monitoramento, avaliação e auditoria do SGICA;
- comunicar à área de *Compliance* situações que possam representar irregularidades, inconsistências relevantes ou riscos de fraude, corrupção e suborno.

10.10.4 Jurídico

Compete à área Jurídica:

- monitorar e analisar leis, regulamentos e demais requisitos legais aplicáveis às atividades da Tecnobank, no âmbito de suas competências;

- apoiar a área de *Compliance* na identificação, interpretação e avaliação da aplicabilidade das obrigações legais e regulatórias relacionadas ao SGICA;
- fornecer análises, orientações e pareceres jurídicos sobre situações que envolvam riscos legais, regulatórios e de integridade;
- apoiar a definição e a revisão de cláusulas contratuais de integridade, anticorrupção, antissuborno e conformidade, conforme a natureza e os riscos dos relacionamentos;
- comunicar à área de *Compliance* alterações legais ou regulatórias relevantes que possam demandar revisão de controles, políticas ou procedimentos internos.

10.10.5 Pessoas & Cultura

Compete à área de Pessoas e Cultura:

- apoiar a área de *Compliance* no planejamento, na organização e na realização de treinamentos e ações de conscientização sobre ética, integridade, anticorrupção e antissuborno;
- integrar as diretrizes do SGICA ao processo de admissão e integração de novos colaboradores, promovendo o conhecimento do Código de Conduta e das políticas internas aplicáveis;
- apoiar o acompanhamento da participação dos colaboradores nos treinamentos obrigatórios e a disponibilização dos respectivos registros;
- apoiar os procedimentos de *Due Diligence* de Integridade de colaboradores (KYE), conforme os critérios de elegibilidade e as responsabilidades estabelecidas nos instrumentos normativos específicos;
- contribuir para a implementação de medidas relacionadas à cultura organizacional, à conduta ética e à prevenção de irregularidades, respeitadas as competências das instâncias responsáveis.

10.10.6 Privacidade e Proteção de Dados e Segurança da Informação

Compete às áreas de Privacidade e Proteção de Dados e Segurança da Informação, observadas suas respectivas atribuições:

- identificar, avaliar e acompanhar riscos relacionados à proteção de dados pessoais e à segurança da informação;
- implementar, manter e avaliar controles de proteção de dados pessoais e de segurança da informação sob suas responsabilidades;
- apoiar a área de *Compliance* na identificação e no tratamento de riscos que possam impactar a conformidade e a integridade dos processos da Companhia;
- comunicar situações relevantes que possam representar descumprimento de obrigações legais, regulatórias ou normativas relacionadas às suas áreas de atuação;
- apoiar a revisão e a atualização dos documentos normativos de suas respectivas áreas, observados os critérios de aprovação, revisão, controle de versões e gestão documental estabelecidos nos procedimentos internos e na Lista Mestra.

A atuação dos multiplicadores não substitui as responsabilidades dos gestores dos processos, nem transfere a essas áreas a autoridade ou a independência técnica da Função de *Compliance*. Cada área permanece responsável pela execução e pela manutenção dos controles sob sua competência, cabendo à Função de *Compliance* a orientação técnica, o acompanhamento e o monitoramento das atividades relacionadas ao SGICA, conforme os procedimentos internos aplicáveis.

11.MEDIDAS DISCIPLINARES

As violações ao Código de Conduta, políticas, legislação ou procedimentos podem resultar em medidas disciplinares conforme Política de Medidas Disciplinares, observando imparcialidade, proporcionalidade, não retaliação, devido processo e registro formal. Para terceiros, podem ser aplicadas medidas contratuais (suspensão, bloqueio, rescisão) e comunicações às autoridades, quando aplicável.

12. DISPOSIÇÕES FINAIS

A presente Política reflete o compromisso institucional da Tecnobank com a integridade e com a adoção de boas práticas de governança, sendo aplicada de forma proporcional à natureza e complexidade de suas operações. Em caso de dúvidas ou esclarecimentos sobre o conteúdo desta política, ou sobre aplicação deste documento em relação a algum assunto específico, deverão ser direcionadas à área de *Compliance*.

13. GLOSSÁRIO

As definições dos termos utilizados em todas as políticas de *Compliance* estão agrupadas no documento GL.CMP.001 – Glossário de *Governança Corporativa Tecnobank*.

14. DOCUMENTOS DE REFERÊNCIA

- Código de Conduta
- Convenções internacionais contra corrupção
- FCPA (*Foreign Corrupt Practices Act*)
- Legislações setoriais e regulatórias aplicáveis
- Lei nº 12.846/2013 (Lei Anticorrupção) e Decreto nº 11.129/2022
- Manual do Sistema de Gestão Integrada de *Compliance*, Anticorrupção e Antissuborno
- Normas ISO 37301:2021 e ISO 37001:2025
- *Office of Foreign Assets Control* (OFAC)
- Política de Canal de Ética, Não Retaliação e Investigações Internas
- Política de *Due Diligence* de Terceiros
- Política de Medidas Disciplinares
- Política de Presentes, Hospitalidades e Brindes
- Regimento do Comitê de Ética
- *UK Bribery Act*

15. GESTÃO DO DOCUMENTO

15.1 Revisão

Este documento passará por revisão, no mínimo, **a cada dois anos**, conforme determinado pela Lista Mestra da Tecnobank.

Revisões extraordinárias podem ocorrer por mudanças legais, estruturais, operacionais, atualização ISO, recomendações de auditoria, investigações ou avaliação de risco.

15.2 Histórico de Atualização

Versão	Data	Descrição	Autor
01	01/10/2018	Emissão inicial do Documento	Departamento de *Compliance*
02	04/06/2021	Revisão do documento e adequação ao novo *template* da organização	Thais Takagi
03	10/06/2022	Atualização do documento, nomenclatura, versionamento, rodapé, sumário, termos e atualizações gerais.	Joy Neto
04	16/01/2023	Atualização do documento, alteração do texto para nível de maturidade do programa e inclusão de novos tópicos relevantes.	Joy Neto
05	28/09/2023	Atualização do documento de acordo com os apontamentos da auditoria interna e externa.	Joy Neto
06	01/07/2024	Revisão periódica e ajuste de *template*	Sheila Esmeralda
07	14/11/2025	Unificação da Política de *Compliance* (PL.CMP.009.06) e Política Anticorrupção e Antissuborno (PL.CMP.007.05). Revisão, restruturação e aprimoramento dos capítulos objetivo, diretrizes, estrutura de *Compliance*, responsabilidades, multiplicadores, riscos de *Compliance* e medidas disciplinares, criação do Anexo 1.	Thais Takagi
08	30/01/2026	Atualização de definições sobre FCPA e legislações estrangeiras e alinhamento às diretrizes da Evertec	Gabriel Buracoski
09	30/03/2026	Alinhamento às diretrizes da Evertec	Gabriel Buracoski
10	15/10/2026	Revisão dos itens 1, 3, 4, e 10	Thais Takagi

15.3 Aprovação

Atividade	Data	Nome	Função
Aprovação	19/10/2026	Thais Takagi	*Compliance Officer*
Aprovação	19/10/2026	Sabrina Araújo	Diretora de Governança Corporativa
Aprovação	19/10/2026	Renata Herani	Presidente