RESOLUÇÃO CA N.º 2.852

Estabelece a Política de Prevenção e Combate à Fraude e à Corrupção do BRDE.

Revoga a Resolução CA n° 2.727, de 24/08/2022.

O **PRESIDENTE** do **CONSELHO DE ADMINISTRAÇÃO** do **BANCO REGIONAL DE DESENVOLVIMENTO DO EXTREMO SUL – BRDE**, no uso de suas atribuições regimentais, faz saber que o **CONSELHO DE ADMINISTRAÇÃO**, em reunião de 18/06/2025, tendo aprovado o VOTO PRESI/CA-2025/043, **RESOLVE**:

Art. 1º Estabelecer a Política de Prevenção e Combate à Fraude e à Corrupção do BRDE, nos termos do Anexo.

Art. 2º. Determinar a inclusão da Política de Prevenção e Combate à Fraude e à Corrupção do BRDE como componente do Programa de Integridade estabelecido pela Resolução CA n.º 2.669, de 25/08/2021.

Art. 3º. Atribuir à SURIS a gestão e a proposição de revisão periódica, no mínimo a cada três anos, da Política de Prevenção e Combate à Fraude e à Corrupção do BRDE.

Art. 4°. Revogar a Resolução CA n° 2.727, de 24/08/2022.

Florianópolis, 18 de junho de 2025.

RANOLFO VIEIRA JUNIOR:45412200087

Assinado de forma digital por RANOLFO VIEIRA JUNIOR:45412200087
Dados: 2025.06.18 17:17:40 -03'00'

RANOLFO VIEIRA JÚNIOR
Presidente do Conselho de Administração

ANEXO À RESOLUÇÃO CA N.° 2.852

POLÍTICA DE PREVENÇÃO E COMBATE À FRAUDE E À CORRUPÇÃO

1. OBJETIVO

A Política de Prevenção e Combate à Fraude e à Corrupção tem por objetivo sistematizar os princípios norteadores, a governança e as regras e procedimentos para o enfrentamento proativo e preventivo à fraude nas atividades desenvolvidas pelo BRDE, fortalecendo os compromissos já assumidos pelo Banco para conservação de um elevado nível de ética nos seus negócios.

Esta Política integra o Programa de Integridade do BRDE, em consonância com o disposto na Lei nº 12.846/2013 (Lei Anticorrupção). Por sua vez, o Programa de Integridade consiste no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva do Código de Conduta Ética do BRDE, das políticas e diretrizes com objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra o BRDE ou à Administração Pública.

São componentes do Programa de Integridade:

- Regulamento Administrativo Disciplinar;
- Código de Conduta Ética do BRDE;
- Canal de Denúncias;
- Ouvidoria;
- Política de Conformidade;
- Política de Divulgação de Informações;
- Política de Gerenciamento Integrado de Riscos do BRDE;
- Política de Porta-Vozes;
- Política de Prevenção e Combate a Fraudes e à Corrupção;
- Política de Prevenção e Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção;
- Política de Relacionamento com Clientes;
- Política de Responsabilidade Social. Ambiental e Climática – PRSAC;
- Política de Segurança da Informação, Cibernética e de Comunicações – PoSIC;
- Política de Transações com Partes Relacionadas;
- Regulamento do Portal da Transparência.

A Política de Prevenção e Combate a Fraude e à Corrupção está em consonância com os princípios e diretrizes dos instrumentos acima relacionados, com destaque para o Código de Conduta Ética, a Política de Gerenciamento Integrado de Riscos (em especial no que se relaciona com o Risco Operacional), a Política de Prevenção e

Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção e aos canais de comunicação e denúncia estabelecidos no Programa de Integridade (Fale Conosco, Ouvidoria e Canal de Denúncias).

2. ABRANGÊNCIA

Este Programa expressa o compromisso do Conselho de Administração e da Diretoria com a promoção da prevenção e combate às fraudes, e suas determinações aplicam-se aos gestores, colaboradores, prestadores de serviços, fornecedores e parceiros do BRDE. Sua aplicação busca apoiar ainda o combate a fraudes contra seus clientes efetivos e potenciais e à sociedade em geral.

3. DEFINIÇÕES

- Boa Fé: acreditar estar agindo com honestidade e com motivos verdadeiros para tanto;

- Má Fé: agir de forma intencional de modo a enganar ou induzir alguém em erro;

- Canais de Comunicação do BRDE: ferramentas disponibilizadas para contato com o público-alvo do banco (clientes ou funcionários do BRDE);

- Conflito de Interesses: incompatibilidade entre a vontade e a independência e objetividade na tomada de decisões;

- Denúncia: relato de algum fato relacionado a desvio de conduta, ou seja, de algum ato que estiver em desacordo com as leis, com o Código de Ética e Conduta do BRDE ou com as demais políticas e procedimentos de compliance;

- Fraude: entende-se como fraude qualquer ação promovida de má fé visando vantagens indevidas ou injustas, podem ser citadas entre suas características: intuito de enganar, ocultação da verdade, prejuízo a terceiros, malícia etc.

- Fraude externa: realizada por terceiros, sem envolvimento de funcionários do banco. Pode ser realizada contra clientes do banco ou com a sua participação. Pode ser citado como exemplo o crime de estelionato (Art. 171 do Código Penal);

- Fraude interna: é realizada por funcionários e nem sempre tendo com o objetivo a obtenção de vantagem financeira;

- Partes envolvidas: todos aqueles passíveis de prejuízo financeiro ou não financeiro em decorrência da fraude;

- Situações Suspeitas:qualquer situação que gere desconfiança, incerteza, ou suscite dúvidas quanto ao seguimento da lei e/ou regimentos internos do BRDE.

4. PRINCÍPIOS

São princípios da Política de Prevenção e Combate à Fraude e à Corrupção:

a. O comprometimento e a atuação permanente no enfrentamento proativo e preventivo à fraude nos produtos, atividades, processos e sistemas do BRDE;

b. A busca pelo aperfeiçoamento constante dos padrões de conduta, de qualidade dos produtos, dos níveis de segurança e da eficiência dos serviços;

c. A obrigatoriedade de todos os colaboradores abrangidos por esta Política de reportar quaisquer situações suspeitas ou informação que tenha recebido sobre possíveis atividades fraudulentas;

d. A orientação de que todos os colaboradores devem atuar para a identificação de possíveis falhas nos processos e sistemas que possam ser utilizadas como meios para a efetivação de fraudes internas ou externas, comunicando prontamente aos gestores ou à SURIS;

e. A garantia de que o reporte de suspeitas de fraude não implicará em sanções de nenhuma espécie a quem o realizar de boa-fé, mesmo quando for constatada a realização de denúncia infundada;

f. A confidencialidade das informações recebidas e proteção à reputação dos questionados, mantendo o acesso restrito somente àqueles que legitimamente necessitam ter conhecimento;

g. A imparcialidade e objetividade na análise dos casos apresentados.

5. GOVERNANÇA

5.1. As unidades organizacionais são responsáveis por prevenir e combater fraude e corrupção conforme esta Política, o Código de Conduta Ética e suas atribuições definidas pelo Regimento Administrativo e a Estrutura Organizacional.

5.2. A relação abaixo, não-exaustiva, traz as atribuições das unidades organizacionais relacionadas com o combate à fraude e à corrupção, sem prejuízo de outras:

Conselho de Administração

- Aprovar políticas e diretrizes estratégicas, incluindo o Programa de Integridade e o Regimento Administrativo;
- Supervisionar a atuação das unidades organizacionais e da Comissão de Ética.

Diretoria

- Definir e implementar políticas de integridade, conformidade e combate à corrupção;.
- Normatizar e acompanhar a execução de ações de prevenção e combate à fraude e à corrupção pelas unidades organizacionais.

Auditoria Interna (AUDIN)

- Em conformidade com a Estrutura Organizacional, compete à AUDIN, dentre outras atribuições, avaliar as estruturas, processos e efetividade das atividades de Controles Internos, Prevenção à Lavagem de Dinheiro, Programa de Integridade, Ouvidoria, Portal de Transparência, entre outros instrumentos elencados como parte deste Programa de Prevenção à Fraudes e Corrupção, em especial quanto ao cumprimento de dispositivos legais e regulamentares e quanto à adequação e eficácia de políticas, metodologias, processos e procedimentos implementados, manifestando-se expressamente, quando necessário, e recomendando medidas para seu aprimoramento;
- A AUDIN, conforme determinado na Estrutura Organizacional, deve avaliar o potencial de ocorrência de fraudes bem como o processo de gerenciamento do risco de fraude, contudo, o foco de seu trabalho não será detectar e investigar fraudes, uma vez que atua na prevenção a fraudes por meio do exame e avaliação da adequação e eficácia dos controles preventivos, detectivos e de combate a fraudes.

Superintendência de Riscos, Controles Internos e Compliance (SURIS)

- Coordenar o Programa de Integridade e o Sistema de Controles Internos, bem como outras ações relacionadas;
- Reportar indícios de fraude à Diretoria e o Conselho de Administração.

Departamento de Riscos Operacionais, Controles Internos e Compliance (DEROC)

- Executar atividades operacionais de controle e conformidade sob coordenação da SURIS;
- Realizar a gestão do Canal de Denúncias e a coordenação da Comissão de Ética;
- Reportar indícios de fraude nos termos da normatização emanada dos orgãos reguladores[1];
- Registrar perdas incorridas com fraude ou corrupção na base de Perdas Operacionais;
- Promover, com apoio da SUPIN, treinamentos e capacitações aos colaboradores relacionados com a temática da integridade e prevenção e combate à fraude e à corrupção.

[1] No momento da entrada em vigência desta Política, merece destaque a Resolução Conjunta n° 6, emitida pelo CMN e pelo Banco Central.

Comissão de Ética

- Receber e apurar denúncias de infrações éticas e conflitos de interesse, reportando à Diretoria e ao Conselho de Administração situações que tragam indícios de fraude ou corrupção;
- Revisar periodicamente e propor alterações no Código de Conduta Ética que possam aprimorar a prevenção e o combate à fraude e à corrupção no BRDE.

Superintendência de Infraestrutura (SUPIN)

- Promover a realização de treinamentos e capacitações ao público abrangido por esta Política sobre os temas da integridade e prevenção e combate à fraude e à corrupção;
- Zelar pela integridade nos contratos administrativos e na relação do BRDE com fornecedores;
- Normatizar e operacionalizar os procedimentos de entrega e guarda das Declarações de Bens e Rendimentos dos colaboradores.

Consultoria Jurídica (CONJUR)

- Emitir pareceres sobre atos normativos e contratos considerando os aspectos de integridade e conformidade;
- Apoiar juridicamente todas as áreas do BRDE, inclusive em processos administrativos e judiciais relacionados a fraudes.

Assessoria de Comunicação (ASCOM)

- Atuar na comunicação institucional de riscos e alertas à sociedade em casos de fraude que envolvam clientes ou terceiros.

Superintendência de Crédito e Controle (SUCEC)

- Normatizar e fiscalizar a adoção de cláusulas de integridade e de prevenção à lavagem de dinheiro nos instrumentos contratuais;
- Zelar pelo levantamento cadastral de clientes e potenciais clientes com apoio da SURIS - em especial em relação à inscrição em listas de exclusão relacionadas com improbidade administrativa;
- Em caso de detecção de indícios de fraude, realizar a comunicação com o cliente eventualmente vitimado - com apoio da SURIS, da CONJUR e da Agência respectiva.

Superintendência de Acompanhamento e Recuperação de Créditos (SUARC)

- Zelar pelo monitoramento cadastral da base de clientes, com apoio da SURIS - em especial em relação a inscrição em listas de exclusão.
- Normatizar e fiscalizar a adoção de cláusulas de integridade e de prevenção à lavagem de dinheiro nos instrumentos contratuais;
- Realizar os procedimentos relacionados com a prevenção da lavagem de dinheiro e financiamento do terrorismo no âmbito de suas atividades.

Superintendência de Tecnologia e de Segurança da Informação e Comunicações (SUTEC)

- Coordenar, supervisionar, acompanhar, controlar e avaliar a execução das atividades relacionadas com a segurança da informação e comunicações;
- Propor iniciativas de Segurança da Informação, no âmbito do Plano Diretor de Segurança da Informação e Comunicações do BRDE – PDSEG, em consonância com o Planejamento Estratégico;
- Elaborar, propor, manter atualizada e executar a Política de Segurança da Informação, Cibernética e de Comunicações – PoSIC;
- Elaborar, propor, executar e manter atualizadas as normas relativas à tecnologia e segurança da informação e comunicações.

Departamento de Segurança da Informação e Comunicações (DESEG)

- Planejar, desenvolver e supervisionar a implantação da PoSIC, suas normas complementares, do PDSEG, e da Política de Privacidade, esta última no que se referir à segurança da informação e comunicações;
- Elaborar, propor e manter atualizado o Plano de Contingência de Infraestruturas Tecnológicas e o Plano de Ação e de Resposta a Incidentes;
- Administrar, monitorar e operar os sistemas de proteção dos ativos de informação do BRDE, incluindo o firewall, anti-malware, DLP, dentre outros que o BRDE vier a adotar para proteção da informação;
- Monitorar e mitigar vulnerabilidades técnicas;
- Atuar em conjunto com a SURIS na gestão de incidentes cibernéticos e fraudes digitais;
- Realizar testes de vulnerabilidade, revisão de acessos, monitoramento de logs e gestão de riscos cibernéticos;
- Coordenar campanhas de conscientização em segurança cibernética.

Gerência de Estratégia e de Governança de Tecnologia e de Segurança da Informação e Comunicações (GEGOV)

- Identificar, reportar e gerenciar os riscos de tecnologia e de segurança da informação e comunicações, atuando como segunda linha de defesa na prevenção, mitigação e eliminação de riscos operacionais relativos à tecnologia e segurança da informação e comunicações;
- Atuar em conjunto com a SURIS na gestão de incidentes cibernéticos e fraudes digitais.

Comitê de Governança de Segurança da Informação e Comunicações (COSEG)

- Assegurar que a governança de segurança da informação e comunicações seja devidamente integrada à governança corporativa, mitigando riscos operacionais e a ocorrência de incidentes de segurança, e aconselhando a Administração do BRDE quanto ao direcionamento estratégico e o plano de investimentos e despesas na área de segurança da informação e comunicações, incluindo as contratações de soluções e serviços;

- Apreciar e recomendar a Política de Segurança da Informação, Cibernética e de Comunicações – PoSIC, inclusive quanto às propostas de alteração, com posterior encaminhamento à alçada competente para apreciação, monitorando e avaliando periodicamente sua execução;
- Acompanhar e recomendar ações de resposta e de recuperação de incidentes de segurança da informação, orientando-se pelo PCIT e pelo Plano de Ação e de Resposta a Incidentes.

Agências (SUCUR, SUFLO e SUPOA)

- Os analistas devem observar os aspectos cadastrais dos clientes e potenciais clientes, bem como registrar e reportar eventuais indícios de fraude ou corrupção verificados durante o relacionamento com o cliente ou potencial cliente;
- Efetuar os procedimentos de levantamento cadastral, verificação da autenticidade de documentos e preenchimento da Avaliação Interna de Risco (AIR) para lavagem de dinheiro e financiamento do terrorismo, de acordo com as normatizações, atentando para que sejam criteriosos e tempestivos.

6. PROCEDIMENTOS DE PREVENÇÃO

A relação abaixo, não-exaustiva, traz os principais procedimentos de prevenção à fraude e à corrupção, os quais são objetos de normatizações próprias:

- Monitoramento de listas cadastrais e de exclusão;
- Procedimentos de prevenção à lavagem de dinheiro e financiamento do terrorismo em liquidações atípicas;
- Práticas de “conheça seu cliente” e “ conheça seu funcionário”;
- Código de Conduta Ética do BRDE;
- Canal de Denúncias e Ouvidoria;
- Obrigatoriedade de entrega de Declarações de Imposto de Renda dos colaboradores;
- Procedimentos de conformidade e controle em processos licitatórios;
- Política de Segurança Cibernética;
- Treinamentos obrigatórios sobre integridade, prevenção à fraudes e à corrupção, ética e controles internos.

6.1. Ações de promoção da Ética e da Integridade

6.1.1. Para promoção da ética e da integridade, devem ser amplamente divulgados e explicados a todos os colaboradores os instrumentos componentes do Programa de Integridade, em especial o Código de Conduta Ética, o Regulamento Administrativo Disciplinar, a Política de Gerenciamento Integrado de Riscos (em especial no que se relaciona com o Risco Operacional), a Política de Prevenção e Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção e o funcionamento dos canais de comunicação e denúncia (Ouvidoria e Canal de Ética). As ações de divulgação são

de competência primária da SURIS, através do DEROC, com o apoio das demais áreas conforme demandadas.

6.1.2. Para prevenção da ocorrência de situações de conflitos de interesse, o BRDE orienta-se pelas determinações do Código de Conduta Ética, em especial quanto ao exercício de atividades paralelas; e do Regulamento Administrativo Disciplinar.

6.2. Controles preventivos

6.2.1. Como integrante da Política de Gerenciamento do Risco Operacional, o combate à fraude está inserido na estrutura do Sistema de Controles Internos do BRDE. Os meios utilizados para a identificação, avaliação, monitoramento, controle e mitigação do risco operacional devem prever também a prevenção de fraudes internas e externas.

6.2.2 Na elaboração das Matrizes de Riscos Operacionais e de Controles Internos, a SURIS deve considerar o risco da ocorrência de fraudes internas ou externas e da prática de corrupção.

6.2.3. Como integrante da Política para Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção o BRDE, o combate à fraude utiliza-se das ações de controle adotadas, compreendendo: conheça seu cliente, conheça seu funcionário, conheça seu fornecedor, conheça seu parceiro, avaliação de novos produtos e serviços.

6.2.4. Em atendimento à legislação que trata do registro das declarações de bens e o controle da variação patrimonial e de sinais de enriquecimento ilícito por agente público no exercício de cargo ou emprego público e ao Regulamento Administrativo Disciplinar do BRDE, é obrigação dos Diretores, membros do Quadro de Pessoal do BRDE, funcionários de carreira e gabinete, e pessoal cedido, entregar, anualmente, a Declaração de Bens e Rendimentos que compõem seu patrimônio particular em 31 de dezembro do ano anterior, acompanhada do correspondente Recibo de Entrega, aos cuidados da SUPIN.

Compete à SUPIN a normatização dos procedimentos de entrega e guarda das Declarações de Bens e Rendimentos, por meio de Instrução Normativa. As declarações devem ser criptografadas no envio, somente podendo seus dados serem acessados pelos órgãos legalmente competentes e habilitados, para fins de realização de auditoria.

6.2.5. As regras para hospitalidade, brindes e presentes estão estabelecidas no Código de Conduta Ética do BRDE, sendo dever funcional a sua observância.

6.2.6. Todos os colaboradores têm o dever de reportar a identificação de possíveis falhas nos processos e sistemas que possam ser utilizadas como meios para a efetivação de fraudes internas ou externas.

6.3. Transparência: Portal da Transparência

Em consonância com seu comprometimento com a ética, com o zelo pelo patrimônio público e com as melhores práticas de governança corporativa, o BRDE estabeleceu, em obediência às disposições da Lei Federal nº 12.527 de 2011, seu Portal da Transparência como o canal de comunicação entre o BRDE e a sociedade em geral na prestação de contas e na divulgação de informações, assegurando o acesso a informações e à transparência, observadas as disposições da Política de Divulgação de Informações. A normatização do funcionamento do Portal da Transparência é contemplada pelo Programa de Integridade

No Portal da Transparência devem ser divulgadas ao público as informações mais relevantes sobre a atuação do BRDE, respeitadas as informações abrangidas pelo sigilo bancário estabelecido na Lei Complementar nº 105 de 2001.

Devem ser disponibilizados à sociedade canais de comunicação para a solicitação de informações que porventura não constem do Portal da Transparência e sejam de interesse público.

7. PROCEDIMENTOS DE DETECÇÃO E RESPOSTA À FRAUDE E À CORRUPÇÃO

7.1. Recebimento e tratamento de denúncias

7.1.1. O reporte de fraudes ou indícios de fraude é obrigatório a todos os colaboradores e demais abrangidos por esta Política, e deve ser feito pelos meios de comunicação disponibilizados pelo BRDE (Canal de Ética, Ouvidoria) ou diretamente ao Departamento de Riscos Operacionais, Controles Internos e Compliance (e-mail: deroc@brde.com.br).

7.1.2. Todos os colaboradores (funcionários, estagiários, aprendizes, parceiros e terceirizados) têm o dever de reportar quaisquer situações suspeitas ou informação que tenha recebido sobre possíveis atividades possivelmente caracterizadas como fraudulentas.

7.1.3. A denúncia de fraude, bem como a identidade do denunciante serão classificadas como informação restrita. Caso o denunciante deseje realizar a denúncia de forma anônima, ele deverá necessariamente utilizar o Canal de Ética.

7.1.4. O reporte de suspeitas de fraude não poderá implicar em sanções a quem o realizar de boa-fé, mesmo quando for constatada a realização de denúncia infundada.

7.1.5. A área que receber uma denúncia de fraude (GADIR no caso da Ouvidoria; DEROC no caso do Canal de Ética ou por e-mail), deverá dar o encaminhamento previsto no Programa de Integridade. O prazo máximo para a adoção das providências diante da constatação de ocorrência de fraude ou corrupção é de dez (10) dias úteis.

7.1.6. A unidade organizacional que receber a denúncia deverá, quando for o caso, alertar as áreas relacionadas, visando a adoção tempestiva de ações corretivas e preventivas, seguindo, quando for o caso, o rito já previsto nos normativos que compõem o Programa de Integridade.

7.1.7. Caso aplicável, a SURIS deverá emitir ordem aos funcionários para sustar qualquer destruição de documentos físicos e eletrônicos, para garantir sua preservação.

7.1.8. Dependendo da natureza e severidade do caso, a SURIS deverá notificar os setores internos pertinentes ao caso (CONJUR, SUPIN/DERHU, SUTEC, etc) e às instâncias de investigação adequadas (ex. Polícias, Ministério Público, Tribunais de Contas etc.).

7.1.9. A SURIS deverá avaliar a situação detectada e poderá recomendar à Diretoria a designação de uma equipe de resposta para examinar a ocorrência com mais profundidade.

7.1.10. Na hipótese de a possível fraude afetar especificamente algum cliente ou outra contraparte externa ao BRDE, deverá ser estabelecida comunicação com os mesmos por meio dos canais oficiais de comunicação do Banco prestando esclarecimentos e orientações.

7.1.11. No caso de possível fraude que possa afetar os clientes e demais contrapartes do BRDE, a SURIS e a ASCOM deverão promover ações de comunicação no site e por outros meios para alertar sobre o assunto.

8. REGISTRO E REPORTE DE DENÚNCIAS

8.1. Âmbito interno

8.1.1. A SURIS deverá manter o registro de todas as fraudes e tentativas de fraude investigadas, e incluí-las no Relatório de Riscos Operacionais, dando ciência à Diretoria, ao Comitê de Riscos e ao Conselho de Administração.

8.1.2. Havendo a constatação de perdas associadas à fraude, estas deverão ser relatadas à SURIS pelas unidades organizacionais envolvidas e serão registradas na base de Perdas Operacionais e reportadas no Relatório de Riscos Operacionais.

8.2. Âmbito Externo

8.2.1. O BRDE deve compartilhar os dados e informações sobre indícios de fraude de acordo com a normatização da legislação e dos orgãos reguladores[2].

8.2.2. O registro de que trata o item 8.2.1 não se aplica aos dados e às informações sigilosos, nos termos de legislação especial, relacionados a indícios da prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores e de financiamento do terrorismo.

2 No momento da entrada em vigência desta Política, deverão ser observadas as determinações da Resolução Conjunta n° 06, de 23/05/2023, do Conselho Monetário nacional e do Banco Central: compartilhar os dados e informações sobre indícios de fraude por meio de sistema eletrônico que permita, no mínimo, (i) o registro de dados e informações sobre ocorrências ou tentativas de fraudes identificadas pelas instituições em suas atividades, (ii) a alteração e exclusão desses registros conforme o caso, e (iii) a consulta aos dados e informações registrados. O registro dos dados e das informações sobre indícios de fraudes deverá conter, no mínimo, (i) a identificação de quem, segundo os indícios disponíveis, teria executado ou tentado executar a fraude, quando aplicável; (ii) a descrição dos indícios da ocorrência ou tentativa de fraude; (iii) a identificação da instituição responsável pelo registro; e (iv) os dados da conta destinatária e de seu titular, nos casos de transferência ou pagamento de recursos.