REGULAMENTO SELO DE PREVENÇÃO A FRAUDES
Ciclo 04/2026

1. DAS DISPOSIÇÕES PRELIMINARES

Com o objetivo de trazer aperfeiçoamento das melhores práticas, maturidade, segurança e um ambiente de negócios mais seguro e confiável no mercado financeiro em relação à prevenção a fraudes, a Federação Brasileira de Bancos (FEBRABAN), junto à Fin – Confederação Nacional das Instituições Financeiras, estabeleceu o Selo de Prevenção a Fraudes para que as instituições possam comprovar a aderência em relação aos requisitos apresentados neste documento, elaborado com base em resoluções, normativos e melhores práticas do mercado.

A instituição que solicitar o Selo, deverá:

- Acessar o site https://selo.fin.org.br e realizar a pré-inscrição da instituição para **acesso à plataforma**;
- Para prosseguir com a inscrição no processo de avaliação do Ciclo 04/2026, a instituição deve fornecer, na própria plataforma, as **informações preliminares** da instituição;
- Após essa etapa, será necessário assinar o **Termo de Inscrição** e realizar o pagamento da **Taxa de Inscrição**, ambos disponíveis na plataforma;
- Para concluir a inscrição, o representante legal, conforme autorizado em seus atos societários, deverá **assinar a documentação**:

- **Carta de Abertura**, atestando que está ciente e de acordo com o início do trabalho. Comprometendo-se com a disponibilização de informações/recursos, evidências necessárias para avaliação, declaração de conhecimento das regras deste Regulamento, e que aceitam seguir com o processo de certificação, com a divulgação do resultado positivo ou negativo à Fin. (Anexo ao final deste regulamento);
- **NDA**, onde as partes se comprometem com a confidencialidade das informações. (Anexo ao final deste regulamento);
- **Carta de Encerramento**, atestando que está ciente e de acordo com todas as informações e/ou evidências prestadas presencialmente ou incluídas em questionário para obtenção do Selo de Prevenção a Fraudes, atestando, para todos os fins de direito, a veracidade das mesmas.

Após a solicitação, assinaturas e entrega dos documentos necessários para a inscrição, a EY

formalizará o início do processo de avaliação por meio da **Carta Comunicação - Início das Atividades**, e será iniciado o processo de avaliação de conformidade para obtenção do Selo.

- O processo consiste em 9 pilares para aferir a conformidade de políticas, estruturas físicas e sistêmicas, procedimentos, controles e informativas sobre a instituição.
- O não cumprimento de qualquer um dos requisitos mencionados acima, resulta a inegibilidade do Selo de Prevenção a Fraudes para a empresa solicitante.

2. REQUISITOS DE CONFORMIDADE

Os requisitos de conformidade definidos para cada pilar abrangem o desenvolvimento de controles, procedimentos e formalizações de processo, para identificar o cumprimento às exigências e diretrizes dos órgãos reguladores, além da adoção de boas práticas de mercado, de forma a elevar o nível de prevenção e gestão de riscos. Assim, nos critérios de revisão, serão considerados tanto a aderência às regulamentações quanto a implementação efetiva de boas práticas, evidenciando maturidade e compromisso com a excelência.

Além disso, o processo considera a evolução contínua, avaliando as oportunidades de melhoria identificadas em ciclos anteriores, incentivando avanços consistentes e a busca por inovação.

Abaixo as resoluções as quais os pilares e o questionário foram baseados:

- Resolução CMN n° 4.557 de 23/2/2017
- Resolução CMN n° 4.753 de 26/9/2019
- Resolução Bacen n° 1 de 12/8/2020
- Resolução CMN n° 4.859 de 23/10/2020
- Resolução Bacen n° 96 de 19/5/2021
- Resolução Bacen n° 142 de 23/9/2021
- Resolução Bacen n° 147 de 28/9/2021
- Resolução CMN n° 4.949 de 30/9/2021
- Resolução Bacen n° 198 de 11/3/2022
- Instrução Normativa Bacen n° 331 de 1/12/2022

- Resolução Bacen Conjunta n° 6 de 23/5/2023
- Resolução Bacen n° 343 de 4/10/2023
- Resolução BCB n° 457 de 06/03/2025
- Instrução Normativa BCB n° 661 de 11/9/2025
- Resolução BCB n° 501 de 11/09/2025
- Instrução Normativa BCB n° 669 de 29/9/2025
- Resolução BCB n° 518 de 3/11/2025
- Resolução CMN n° 5.261 de 3/11/2025
- Resolução CMN n° 5.274 de 18/12/2025
- Autorregulação FEBRABAN - NORMATIVO SARB nº 28/2025, em vigor a partir de 27/10/2025.

Demostramos as frentes dos 9 pilares que serão avaliados:

1. Avaliar a existência de serviços especializados em prevenção a fraudes, análises e *score* de risco;
2. Avaliar a existência de ações de cooperação, parceria e compartilhamento de informações com parceiros externos;
3. Avaliar a existência e a adequação dos processos de prevenção a fraudes;
4. Avaliar a existência de requisitos do plano de conscientização e de divulgações recorrentes de ações de prevenção a fraudes;
5. Avaliar a existência das soluções e boas práticas para abertura de contas corrente;
6. Avaliar a existência e adequação de estrutura mínima, ferramentas, procedimentos e governança na gestão do processo transacional;
7. Avaliar a existência e adequação de estrutura mínima, ferramentas, procedimentos e governança no tratamento de fraudes;
8. Avaliar a existência e a adequação do processo de prevenção a fraudes interna; e
9. Avaliar a existência do envolvimento de cyber em prevenção a fraudes.

3. MODELO DE AVALIAÇÃO UTILIZADO

As instituições serão classificadas conforme os seguintes parâmetros:

Classificação	Score
Não aderente	0% → 74%
Parcialmente aderente	75% → 89%
Aderente (Selo)	90% → 100%

A instituição participante deverá atingir o percentual de conformidade mínimo de 90% para adquirir o Selo de Prevenção a Fraudes**.**

- **Não aderente:** caso a instituição queira se adequar, será necessário refazer todo processo com custo adicional;
- **Parcialmente aderente:** a instituição terá o prazo de 60 dias para verificar os itens não atendidos, realizar os procedimentos de adequação e encaminhar as evidências para reavaliação.

4. DO CANCELAMENTO DO SELO

O Selo não deve ser considerado ou utilizado como garantia ou evidência de que a instituição financeira ou a entidade certificada não tenha infringido, em qualquer momento, a legislação ou regulamentação de fraudes vigentes, uma vez que se baseia em situação configurada no período abrangido na revisão dos processos. Nesse sentido, o Selo poderá ser sumariamente cancelado nos casos em que comprovadamente se verifique, após a sua concessão, o descumprimento de quaisquer dos seus requisitos.

Por se tratar de instrumento destinado exclusivamente à aferição de conformidade às normas, será também passível de cancelamento a utilização indevida do Selo insinuando qualquer vínculo com a qualidade dos serviços prestados pela instituição ou pela entidade que o tenha obtido.

5. PILARES

PILAR 1: Avaliar a existência de serviços especializados em prevenção a fraudes, análises e *score* de risco

Este pilar estabelece exigências e boas práticas que devem ser incorporadas aos processos de prevenção a fraudes, abrangendo governança, análises, indicadores e *score* de risco.

A instituição é responsável por garantir a segurança, a integridade e a padronização das práticas adotadas, assegurando proteção tanto para a organização quanto para seus clientes.

Para cumprimento do pilar, serão revisados os seguintes requisitos:

I. Envolvimento da área de prevenção a fraudes no desenvolvimento de canais, sistemas, transações, produtos e serviços:

- Existência de documento formalizado, atualizado, aprovado e publicado na *intranet* corporativa, acessível a todos os colaboradores. O documento deve contemplar todas as etapas e procedimentos realizados pela área de prevenção a fraudes durante o desenvolvimento de novos produtos, serviços, canais ou sistemas, incluindo análises, pareceres e acompanhamento de condicionantes.

- Demonstração de que a área de prevenção a fraudes está envolvida no ciclo de desenvolvimento dos canais, sistemas, transações, produtos e serviços. Deverá ser evidenciado o acionamento e o envolvimento da área de fraudes de casos reais dentro do período de escopo avaliado, bem como, evidências do acompanhamento da implementação dos requisitos identificados (ex.: *prints* sistêmicos/relatórios/atas de reuniões).

- Existência de sistema automatizado que registre os pareceres e condicionantes emitidos pela área, incluindo justificativas e análises detalhadas para cada decisão.

- Existência de acompanhamento das condicionantes, de forma a evidenciar que o banco realiza o monitoramento sistemático das exigências estabelecidas pelas áreas responsáveis, assegurando que o respectivo produto somente seja colocado em produção após a integral implementação e validação das condicionantes aplicáveis.

II. Governança, com expectativas claras do conselho diretor:

- Estabelecimento de estrutura formalizada de governança de fraudes, por meio de documento atualizado, aprovado e disponibilizado em sistema interno e disponível a todos os colaboradores, contendo diretrizes claras e definição de papéis e responsabilidades para todas as partes envolvidas, incluindo Prevenção a Fraudes, Conselho Diretor, Auditoria Interna, Riscos e Controles Internos. Esse documento deve descrever responsabilidades, como apoiar a governança e promover transparência, implementar medidas e controles (como treinamentos e campanhas), monitorar e investigar casos de fraude, além de avaliar a eficácia da política e propor melhorias.

III. Indicadores de fraudes externas e internas:

- Existência de *dashboards* e gráficos para monitoramento dos indicadores de fraude, bem como a metodologia adotada para definição, obtenção, construção e acompanhamento desses indicadores.

- Existência do acompanhamento dos principais tipos de fraudes e suas volumetrias para todos os produtos/serviços/transações: indicadores de perdas financeiras devido a fraudes, % de Fraudes Detectadas/Total de Fraudes Ocorridas, alertas falso-positivo/total de alertas, alertas falso-negativo/total de alertas, % de alertas gerados por regra/total de alertas, % *chargebacks* por fraude (cartão); *chargebacks* por fraude aprovados/*chargebacks* por fraude solicitados (cartão), % fraudes por Canal, % fraudes por Meio de Pagamento, % de Fraudes confirmadas ("*true positive*"), % fraudes resolvidas/total de fraudes identificadas, fraudes com análise concluída/total de alertas, fraudes com valor recuperado/total de fraudes, valor recuperado/valor total perdido, % fraudes internas/total de fraudes, fraudes internas confirmadas/denúncias ou alertas de fraudes internas, % funcionários envolvidos em fraude interna/total de funcionários;

- Compartilhamento dos indicadores com as instâncias competentes, incluindo:

    a. Descrição completa do processo, indicando momentos e fóruns de apresentação

(comitês, *dashboards*, reuniões);

b. Evidências do compartilhamento com diretoria e conselho, assegurando a validação da participação dessas instâncias.

IV. Canais de Denúncias:

- Existência de um documento que descreva detalhadamente os procedimentos aplicáveis aos canais de denúncia, devidamente atualizado, aprovado e divulgado para todos os colaboradores envolvidos no processo. Além disso, será avaliado também, se é definido um processo para controlar o atendimento das demandas externas realizadas pelo canal de denúncias, contendo informações do sistema utilizado e a formalização dos procedimentos e prazos adotados pela instituição.

- Prazos claros e formalizados para atendimento das demandas recebidas pelos canais de denúncia, bem como evidências de mecanismos de controle que assegurem o monitoramento e a rastreabilidade dessas demandas.

- Utilização de um canal de denúncias para clientes para recebimento de contestações relacionadas a transações fraudulentas; evidência da existência do canal; apresentar relatório ou controle consolidado das contestações recebidas com periodicidade definida; e evidenciar a divulgação do canal aos clientes por meio de comunicação oficial ou material informativo.

- Demonstração de como é realizada a formalização das contestações de clientes relacionadas a transações fraudulentas. O procedimento deverá ser descrito de forma detalhada, incluindo a informação de onde são registradas as contestações, quais dados são capturados, existência de classificação das contestações, e as etapas realizadas. Ainda, deverão ser fornecidas evidências dos processos de controle das contestações recebidas via canal no período de escopo avaliado, bem como a periodicidade definida.

V. Contato com o cliente para confirmação/esclarecimento de transações atípicas e/ou suspeitas e eventuais bloqueios:

- Existência de documento que descreva detalhadamente os critérios que determinam quando o contato com o cliente deve ocorrer (incluindo orientações sobre como conduzir a comunicação e informações que devem ser coletadas e registradas, bem como a definição do um prazo para que os funcionários atendam as demandas recebidas pelo canal de denúncias). O documento deve estar devidamente atualizado, aprovado e divulgado para todos os colaboradores envolvidos no processo.

- Existência de registros de todos os contatos realizados, independentemente do meio utilizado (como *push notifications* ou ligações), garantindo que estejam devidamente armazenados e formalizados no sistema interno, com rastreabilidade completa do histórico.

- Existência de um processo estruturado para comunicação clara e segura ao cliente em casos de bloqueios ou suspeitas. A comprovação deverá incluir descrição detalhada do processo, contemplando responsáveis pela execução, forma de comunicação e frequência, além de documento formalizado com os procedimentos e critérios aplicáveis, devidamente atualizada, aprovada e disponibilizada a todos os colaboradores em ferramenta interna. Também será necessário apresentar evidências práticas, como *prints* sistêmicos ou exemplos reais de comunicação, garantindo transparência e aderência às diretrizes estabelecidas.

PILAR 2: Avaliar a existência de ações de cooperação, parceria e compartilhamento de informações com parceiros externos

Este pilar tem como objetivo garantir que a instituição desenvolva e mantenha iniciativas estruturadas de colaboração com entidades externas, promovendo integração, troca de informações relevantes e sinergia para fortalecer processos, reduzir riscos e ampliar a eficiência operacional.

É responsabilidade da instituição assegurar o cumprimento integral dos requisitos e exigências estabelecidos pelos órgãos reguladores, bem como adotar as boas práticas avaliadas neste regulamento.

Para cumprimento do pilar, serão revisados os seguintes requisitos:

I. Compartilhamento de dados com as instituições financeiras:

- Formalização dos procedimentos de forma detalhada em documento específico, devidamente atualizado, aprovado e acessível em repositório interno para todos os colaboradores envolvidos no processo.

- Existência de procedimentos de compartilhamento de dados e informações relacionados a indícios de fraude para terceiros. Adicionalmente, será solicitado evidências sistêmicas de compartilhamento de dados, não limitado apenas a informações de indícios realizado no período de escopo avaliado, contendo a data do alerta, bem como a data do início e fim da investigação, e a data do encaminhamento.

- Estabelecimento de procedimentos realizados com a ferramenta utilizada para acesso à base

de dados compartilhada sobre ocorrências de fraude, como também os procedimentos realizados. A instituição deverá evidenciar, de maneira não exaustiva, a forma de acesso, incluindo registros visuais das etapas do processo, mesmo quando executadas via API, e disponibilizar a listagem dos colaboradores que possuem acesso à plataforma.

- Existência de sistema de compartilhamento de fraudes contendo trilha de auditoria provida pelo fornecedor, contendo demonstração dos registros de alterações realizadas.
- Existência de procedimentos relacionados a declaração de conformidade referente aos registros de dados e informações sobre indícios de fraude, evidenciando a existência ou inexistência de alterações.
- Estabelecimento de controle realizado pela instituição para fins de acompanhamento das alterações, correções e exclusões realizadas no sistema de compartilhamento, a fim de verificar se as correções foram aplicadas corretamente.
- Existência de contrato firmado com a empresa fornecedora do sistema de compartilhamento de dados, completo, atualizado e acessível em repositório interno. O contrato deverá descriminar o percentual mínimo de disponibilidade do sistema, garantindo a eficácia do compartilhamento dos dados.
- Existência de participação em fóruns, grupos de trabalho, comitês ou outras iniciativas setoriais voltadas à prevenção e ao combate a fraudes, bem como ao compartilhamento estruturado de informações relevantes, indicando, quando pertinente, a natureza da participação e os objetivos das iniciativas.

II. Comunicação tempestiva com a instituição destinatária dos recursos objetos da fraude ou do golpe:

- Existência de documento formalizado para os procedimentos de compartilhamento de dados (Resolução R6), atualizado, aprovado e publicado aos colaboradores envolvidos no processo. O documento deverá contemplar o detalhamento de todo o processo, como por exemplo: as responsabilidades das equipes envolvidas, os critérios que acionam a comunicação para cada arranjo de pagamento e os métodos utilizados para realizar a comunicação, como e-mail, telefone ou sistema de mensagens.
- Existência de evidências (de forma não exaustiva) de exemplos reais de comunicação com outras instituições, abrangendo tanto o envio quanto o recebimento de solicitações relacionadas a indícios ou ocorrências de fraude ou golpe. Ademais, deve ser detalhado como o procedimento é realizado, incluindo as etapas do fluxo operacional, a equipe ou área responsável pela execução e o momento em que o procedimento é acionado no ciclo.

- Utilização do MED para o âmbito do Pix e, para os demais arranjos de pagamento, deverá evidenciar a existência dispor de um sistema interno automatizado para controle das repatriações. Esse sistema deve permitir o acompanhamento completo de todas as solicitações, retornos, pagamentos, recebimentos, itens em aberto e conclusões.

- Existência de sistema interno automatizado para o controle das repatriações de valores, incluindo aquelas decorrentes de fraudes entre instituições financeiras, que permita o acompanhamento completo e histórico de todas as solicitações (entrada e saída), retornos, pagamentos, recebimentos, itens em aberto e conclusões, bem como demonstrar se possui sistema próprio para armazenamento desse histórico. Adicionalmente, deverá evidenciar o controle e o monitoramento da destinação e utilização dos valores, que comprovem o acompanhamento realizado ao longo de todo o processo.

PILAR 3: Avaliar a existência e a adequação dos processos de prevenção a fraudes

Este pilar tem como objetivo garantir que a instituição disponha de mecanismos robustos para prevenir, detectar e mitigar fraudes, assegurando a integridade das operações e a proteção dos clientes.

É responsabilidade da instituição assegurar o cumprimento integral dos requisitos e exigências estabelecidos pelos órgãos reguladores, bem como implementar práticas robustas que garantam excelência na prestação de serviços e mitigação de riscos relacionados a fraudes.

Para cumprimento do pilar, serão revisados os seguintes requisitos:

I. Formalizações de procedimentos:

- Existência de documento formalizado que estabeleça diretrizes voltadas à prevenção e à vedação de práticas fraudulentas e outras condutas indevidas, aplicáveis a todos os colaboradores, devidamente aprovado pelas alçadas competentes, mantido atualizado e acessível a todos.

- Existência de documento formalizado que descreva os procedimentos de monitoramento, controle e prevenção de fraudes, incluindo a revisão periódica da base de regras. Esse documento deve estar devidamente atualizado, aprovado pelas alçadas competentes e divulgado aos colaboradores envolvidos no processo.

II. Estabelecimento de limites transacionais:

- Estabelecimento de limites transacionais para cada arranjo de pagamento do Sistema

Financeiro Brasileiro (Pix, TED, boleto bancário, cartão de crédito, cartão de débito, cartão pré-pago, transferência interna, débito automático, DDA, cheque). Esses limites devem ser definidos com base em critérios claros e documentados, contemplando o procedimento para alteração ou revisão.

- Existência dos limites pré-estabelecidos por segmentos, devidamente publicados.
- Existência de procedimento formalizado que define os limites de valor para todas as transações realizadas no período noturno. O documento que trata o procedimento deve especificar os tipos de transações abrangidos, os valores máximos permitidos e o prazo para efetivação segura. Além disso, será necessário apresentar evidências do compartilhamento dessas diretrizes com os colaboradores e comprovar a execução do procedimento, demonstrando que os controles estão sendo aplicados conforme estabelecido.
- Existência de procedimento e documento formalizado relacionado a aprovação/reprovação de solicitações de alteração de limite de clientes contendo controles adicionais que assegurem a execução conforme os critérios definidos. Adicionalmente, o documento que trata o procedimento deve detalhar os critérios utilizados na análise, as etapas do processo, os responsáveis por cada fase e as ferramentas empregadas.
- Existência de procedimentos realizados referentes a solicitações de aumento de limite efetuadas por clientes, contemplando ao menos uma solicitação analisada no período de escopo avaliado. As evidências devem demonstrar o processo de análise e deliberação, incluindo os pareceres emitidos, por meio de *prints* sistêmicos.
- Existência de procedimento formalizado que defina os limites de valor para alteração de limite diurnos/noturnos para todas as transações realizadas. O documento deve conter diretrizes para identificar os procedimentos de alteração de limites. Além disso, será necessário apresentar evidências do compartilhamento dessas diretrizes com os colaboradores e comprovar a execução do procedimento, demonstrando que os controles estão sendo aplicados conforme estabelecido.

III. Sistema interno de histórico de fraudes:

- Utilização de sistema interno que registre o histórico de fraudes, incluindo fraudes eletrônicas, documentais e por falsidade ideológica, contendo, no mínimo, as seguintes informações: Nome, CPF, Razão Social, CNPJ, Classificação da Modalidade, Data da Ocorrência e prazo mínimo de retenção do histórico. Serão solicitadas evidências quanto ao procedimento adotado para armazenar essas informações, incluindo passo a passo do processo e registros visuais (*prints* de tela) do sistema interno que demonstrem claramente

todos os dados exigidos.

IV. Regras e mecanismos de segurança:

- Estabelecimento de processo estruturado para diagnóstico e calibração das regras e mecanismos de segurança, utilizando como base o histórico das ocorrências de fraudes, com o objetivo de aprimorar continuamente as estratégias adotadas. Esse processo deve ser formalizado e descrito com riqueza de detalhes, contemplando todas as etapas, os racionais aplicados, os ajustes realizados e os níveis de gestão autorizados para aprovar mudanças, além de possuir fluxo completo do processo.

- Existência de documento formalizado que descreva o processo de diagnóstico e calibração de regras e/ou mecanismos de segurança, com base no histórico de ocorrências de fraude, visando ao aprimoramento contínuo das estratégias adotadas. O documento deverá detalhar os critérios utilizados na análise, as etapas do processo, os responsáveis pela execução e a periodicidade das revisões.

- Existência de revisões periódicas da base de regras, seguindo um procedimento formal que detalhe passo a passo como a revisão é conduzida e especifique a periodicidade definida. Esse procedimento deverá indicar claramente as etapas, os responsáveis e os prazos para execução. Além disso, é necessário apresentar evidências que comprovem que a base foi revisada conforme a periodicidade estabelecida, garantindo aderência aos controles internos e à governança.

- Estabelecimento de regras que exijam validação adicional da identidade do cliente em transações consideradas de maior risco. Essas diretrizes devem estar descritas em documento formalizado, detalhando os parâmetros utilizados para classificação de risco do cliente, contendo a classificação do cliente, os mecanismos de autenticação aplicáveis, os fluxos de aprovação e os controles complementares. É essencial apresentar evidências que comprovem a execução dessas validações, incluindo registros de cada etapa, além de anexar um fluxograma que represente todo o processo.

- Estabelecimento de dupla aprovação ou definição de alçadas para inclusão, exclusão e calibragem de regras, garantindo que as mudanças ocorram dentro do sistema de regras estabelecido e com segregação de funções, evitando que a mesma pessoa realize solicitações e aprovações. O procedimento deve estar formalizado, descrevendo claramente como ocorre a dupla aprovação e permitindo identificar os responsáveis pela execução.

- Existência de controles e regras para monitorar excesso de transações, seja por quantidade ou valor, bem como tipologias e ações mitigatórias para prevenção de fraudes é essencial

apresentar evidências que demonstrem a aplicação prática desses controles.

- Existência de evidências dos controles existentes, bem como demonstração dos critérios utilizados na análise, as etapas do processo, os responsáveis pela execução e a periodicidade das revisões.
- Estabelecimento de procedimentos de desenvolvimento, homologação e produção das regras, que devem ser realizados em ambientes segregados e por colaboradores distintos, de forma a garantir a confiabilidade do processo e mitigar conflitos de interesse.
- Existência de avaliação prévia das regras antes de sua efetivação em produção, como testes de desempenho, simulações ou validação da eficácia, assegurando sua adequação ao objetivo proposto.

V. Ferramentas de segurança e monitoramento de transações:

- Estabelecimento de procedimento de segurança e monitoramento de transações não financeiras com suspeita de fraude, contendo documento específico formalizado (política, manual, regulamento, normativo etc.), devidamente atualizado, aprovado pelas alçadas competentes e acessível em repositório interno para todos os colaboradores envolvidos no processo. Esse documento deve conter de forma detalhada os procedimentos aplicáveis, deve detalhar quem executa o procedimento, como e onde é executado, bem como a frequência das atividades. Também deve descrever as ações específicas a serem tomadas em casos de suspeita de fraude, garantindo resposta rápida e eficaz.
- Estabelecimento de procedimentos formais de segurança e monitoramento para transações não financeiras com suspeita de fraude, abrangendo casos como alterações cadastrais, ajustes de segurança e acesso, gestão de canais digitais, cartões e produtos, vinculações, mandatos e representações, contratação ou cancelamento de serviços, bloqueios, restrições, atualizações legais e fiscais e configurações operacionais. Será necessário apresentar evidências que comprovem a execução dos processos de segurança e identificação de possíveis fraudes em transações não financeiras.
- Existência de monitoramento via geolocalização nos processos de análise de riscos, incluindo um controle ou mapa das regiões consideradas críticas, como áreas com alta incidência de fraudes ou presídios. O procedimento deverá possuir documento formalizado e descrever passo a passo como o monitoramento é realizado, incluindo os responsáveis, ferramentas utilizadas, frequência etc. Além disso, deverá possuir documentação que especifique: (a) como a instituição avalia locais considerados críticos, (b) quais locais são

classificados como críticos; (c) como ocorre o controle, por exemplo, por meio de alertas, bloqueios temporários ou restrições. Por fim, é necessário apresentar evidências que comprovem a aplicação do processo, como, por exemplo, transações bloqueadas devido à geolocalização.

- Existência de procedimentos para atender clientes de público vulnerável. Deverá ser evidenciado o procedimento adotado, bem como evidências de como os atendimentos aparecem no sistema (indicador de prioridade/vulnerabilidade).

- Existência de documento formalizado que descreva procedimentos de monitoramento, controle e prevenção de fraudes relativos ao produto “cartões”, contendo medidas preventivas e corretivas relacionadas a situações envolvendo o produto. Devem ser apresentadas evidências que comprovem que o documento está publicado e é disponibilizado aos colaboradores envolvidos.

- Adoção de medidas eficazes para mitigação de riscos relacionados ao extravio de cartões. Para comprovação, deverá ser apresentado documento formalizado contendo as ações preventivas e corretivas aplicáveis, além de evidências práticas da execução dessas medidas, como bloqueio automático ou alertas sistêmicos. Também será necessário disponibilizar relatório consolidado com registros de ocorrências e as respectivas ações de mitigação implementadas.

- Adoção de análise das solicitações de aumento de limite ou desbloqueio imediato de cartões. Para comprovação, deverá ser apresentada descrição detalhada do procedimento, incluindo responsáveis, forma de execução, local e frequência, além de documento formalizado contendo critérios e regras aplicáveis. Também será necessário anexar evidências práticas, como *prints* sistêmicos que demonstrem uma análise real, e disponibilizar prova do fluxo completo, contemplando todas as etapas de aprovação e validação.

- Existência de procedimentos formalizados e detalhados para a análise de *chargeback*, considerando a complexidade e os riscos associados a esse processo. Para comprovação, deverá ser apresentado documento oficial que estabeleça políticas, critérios e responsabilidades, como manuais ou regulamentos, acompanhado da evidência de sua atualização, aprovação e divulgação aos colaboradores envolvidos no processo. Além disso, será necessário demonstrar o fluxo completo de análise, incluindo etapas, prazos e responsáveis, bem como apresentar evidências práticas de todas as etapas da execução real, como *prints* sistêmicos ou protocolos de *chargeback*.

PILAR 4: Avaliar a existência de requisitos do plano de conscientização e de divulgações recorrentes de ações de prevenção a fraudes

Este pilar abrange a disseminação de informações e a promoção da conscientização por meio de treinamentos e campanhas voltadas à prevenção de fraudes internas e externas. Compreende a implementação de práticas educativas que fortaleçam a cultura organizacional, assegurando que colaboradores e clientes estejam preparados para identificar e mitigar riscos relacionados a fraudes.

É responsabilidade da instituição zelar pelo compartilhamento contínuo de informações, garantindo que todos os envolvidos compreendam os procedimentos e adotem condutas seguras. Para isso, deverão ser realizados treinamentos específicos, abordando temas como prevenção a fraudes, riscos nos processos de abertura de contas (presencial e remota), utilização de ferramentas antifraude e documentoscopia.

Além dos treinamentos, serão avaliadas as campanhas direcionadas à conscientização dos clientes e colaboradores, abordando medidas preventivas, segurança cibernética, boas práticas no compartilhamento de informações sensíveis e reforço de valores éticos para reduzir comportamentos que possam resultar em fraude.

Para cumprimento deste pilar, serão revisados os seguintes requisitos:

I. Formalizações de procedimentos:

- Existência de documento formalizado que estabeleça diretrizes claras para a realização de treinamentos em prevenção a fraudes, abrangendo todos os colaboradores. Essa documentação deverá detalhar aspectos essenciais, como formato do treinamento (presencial ou virtual), prazo de tolerância para conclusão após a admissão, periodicidade de atualização e mecanismos de gestão das consequências em caso de não realização. Além disso, deverá contemplar menção aos treinamentos específicos, incluindo documentoscopia e utilização de ferramentas antifraude, assegurando padronização, rastreabilidade e efetividade na conscientização dos funcionários.

II. Treinamentos periódicos:

- Estabelecimento de treinamentos periódicos sobre prevenção a fraudes para todos os funcionários da instituição, garantindo atualização contínua e aderência às boas práticas. Para comprovação, deverá ser disponibilizada a ementa, conteúdo ou material de apoio utilizado nos treinamentos, assegurando que os temas abordem riscos internos e externos. Além disso, será necessário apresentar controles ou *dashboards* que evidenciem a gestão

dos treinamentos, incluindo indicadores como: percentual de colaboradores que concluíram os treinamentos, percentual de pendências, alertas gerados para cobrança de treinamentos não realizados e notificações direcionadas aos superiores sobre treinamentos próximos do vencimento ou vencidos.

- Existência de treinamentos específicos voltados a prevenção e identificação de possíveis fraudes nos processos de abertura de contas, tanto digitais quanto presenciais, direcionados aos colaboradores envolvidos nessas atividades. Para comprovação, deverá ser disponibilizada a ementa, conteúdo ou material de apoio utilizado nos treinamentos, assegurando que os temas abordem riscos e práticas preventivas aplicáveis ao *onboarding*. Além disso, será necessário apresentar controles ou *dashboards* que evidenciem a gestão dos treinamentos, incluindo indicadores como: percentual de colaboradores que concluíram os treinamentos, percentual de pendências, alertas gerados para cobrança de treinamentos não realizados e notificações direcionadas aos superiores sobre treinamentos próximos do vencimento ou vencidos.

- Existência de evidências que comprovem a realização dos treinamentos relacionados a ferramentas utilizadas nos procedimentos de fraude, incluindo a ementa, conteúdo e materiais de apoio utilizados. Além disso, é necessário apresentar controles ou *dashboards* que demonstrem o acompanhamento dos treinamentos pelos funcionários, contendo indicadores como: quantidade de colaboradores que concluíram os treinamentos e sua representatividade em percentual; quantidade de colaboradores pendentes e sua respectiva porcentagem; alertas gerados para cobrança de treinamentos não realizados; e notificações enviadas aos superiores sobre treinamentos próximos do vencimento ou já vencidos.

- Existência de treinamentos específicos de documentoscopia destinados aos colaboradores envolvidos nos processos de mesa com análise manual. A avaliação incluirá: a disponibilização da ementa, conteúdo programático e materiais de apoio utilizados na capacitação; o controle ou *dashboard* que demonstre a realização dos treinamentos pelos funcionários, contendo indicadores como número de colaboradores treinados e sua representatividade percentual, quantidade de pendências e respectivos percentuais; além dos alertas gerados para cobrança de treinamentos pendentes e notificações direcionadas aos superiores sobre treinamentos próximos do vencimento ou já vencidos.

III. Campanhas de conscientização:

- Existência de campanhas voltadas à conscientização e prevenção à fraude junto aos clientes, abordando temas como compartilhamento de senhas, ligações suspeitas e outras práticas

de segurança. A instituição deverá apresentar evidências das campanhas realizadas, incluindo materiais de comunicação utilizados (como folhetos, e-mails, postagens em redes sociais). Além disso, deverá ser demonstrado que as campanhas passam por revisões e atualizações periódicas.

- Realização de campanhas internas voltadas à conscientização sobre prevenção à fraude entre os funcionários. A instituição deverá apresentar evidências das campanhas realizadas, incluindo materiais de comunicação utilizados (como folhetos, cartazes ou apresentações). Além disso, será necessário disponibilizar o calendário da campanha de conscientização, demonstrando sua programação e periodicidade.

- Realização de campanhas internas voltadas à conscientização sobre segurança cibernética para os funcionários. A instituição deverá disponibilizar evidências das campanhas realizadas, incluindo materiais de comunicação utilizados (como folhetos, cartazes ou apresentações). Além disso, será necessário apresentar o calendário da campanha de conscientização, demonstrando sua programação e periodicidade.

- Será avaliada a existência e a efetividade dos mecanismos de acompanhamento dos treinamentos realizados pelos colaboradores. Para isso, a instituição deverá apresentar evidências que comprovem a utilização de *dashboards* ou controles específicos, incluindo prints de tela ou relatórios que demonstrem sua aplicação. Os *dashboards* devem permitir a visualização do status de conclusão, pendências e periodicidade dos treinamentos etc.

PILAR 5: Avaliar a existência das soluções e boas práticas para abertura de contas corrente

Este pilar tem como objetivo garantir que a instituição disponha de processos seguros, eficientes e alinhados às melhores práticas para abertura de contas, assegurando a proteção dos clientes e a mitigação de riscos relacionados a fraudes.

É responsabilidade da instituição assegurar o cumprimento integral dos requisitos estabelecidos pelos órgãos reguladores, bem como implementar práticas robustas que garantam excelência na prestação de serviços e mitigação de riscos relacionados a fraudes.

Para cumprimento deste pilar, serão revisados os seguintes aspectos:

I. Formalização de procedimentos:

- Existência de procedimentos e documento formalizado que estabeleça os procedimentos realizados pelo time antifraude relacionados à abertura de conta ou relacionamento. A

instituição deverá apresentar evidência da publicação do documento formalizado, sua atualização, aprovação e comprovar que ele foi devidamente compartilhado com os colaboradores, garantindo sua disseminação e aplicação.

- Existência de procedimentos e documento formalizado que estabeleça os procedimentos realizados pelos Gerentes de Relacionamentos relacionados à abertura de conta ou relacionamento. A instituição deverá apresentar evidência da publicação do documento formalizado, sua atualização, aprovação e comprovar que ele foi devidamente compartilhado com os colaboradores, garantindo sua disseminação e aplicação.

- Existência de contrato de abertura de conta contemplando, de forma clara e acessível, os seguintes elementos: procedimentos para identificação e qualificação do titular; características e regras básicas da conta, incluindo formas de movimentação, tarifas e prazos; medidas de segurança e situações que ensejam bloqueio da conta e valores; direitos e deveres das partes; eventuais limites de saldo e aporte de recursos; procedimentos para atualização cadastral; regras para encerramento da conta; formas e canais para disponibilização de demonstrativos e faturas; encargos incidentes.

II. Validações realizadas durante abertura de contas:

- Existência de soluções e estratégias especializadas nos processos de abertura de contas digitais e presenciais (para clientes PF, PJ e menores de idade), voltadas à verificação da identidade do cliente/associado e à autenticidade dos documentos apresentados. A instituição deverá detalhar como esses procedimentos são realizados, incluindo quem executa, como executa, a frequência, o nome da solução utilizada e seu modo de operação. Além disso, deverá evidenciar o processo, demonstrando todas as etapas de avaliação de identidade e verificação documental até o resultado final, com prints de tela cheia contendo data e hora do sistema no momento da extração.

- Existência de processos e documentação formal para verificação e classificação do perfil de risco do cliente no momento da abertura de conta ou relacionamento. A instituição deverá apresentar descrição das tecnologias empregadas para cada critério de validação, árvores de decisão, bem como a metodologia, e documentação formalizada contendo esses critérios, além de evidências que demonstrem o processo.

- Estabelecimento de mecanismos eficazes para prevenção à fraude no processo de abertura de contas, incluindo procedimentos para identificação de autores de fraudes registrados em bases específicas como bancos de fraudadores internos e externos (R6, DICT, BCPROTEGE etc.), bem como a descrição detalhada do fluxo de identificação e tratamento desses casos. Além disso, será exigida a apresentação de evidências de aplicação prática do procedimento,

demonstrando a identificação de um autor de fraude e as medidas adotadas após a detecção.

- Existência, nos casos de rejeição de abertura de conta por suspeita ou confirmação de fraude, de sistemas ou mecanismos eficazes para impedir novas tentativas de abertura pelo mesmo titular ou por meio de dados relacionados. Além disso, deverá ser apresentada a descrição detalhada do procedimento adotado para bloqueio e prevenção de reincidência, incluindo critérios técnicos e operacionais. Por fim, será exigida a disponibilização de evidências de aplicação prática dos procedimentos mencionados, contendo etapa de análise, conclusão e registro.

- Estabelecimento de mecanismos de validação biométrica facial 1x1 e 1xN no processo de abertura de contas. Será exigida a descrição detalhada do procedimento, incluindo responsáveis pela execução, ferramentas utilizadas, etapas do processo e frequência da verificação. Além disso, deverá ser disponibilizada evidência prática de aplicação, demonstrando a leitura realizada pelo sistema, as análises efetuadas e os pareceres emitidos.

- Existência de mecanismos de verificação de geolocalização no processo de abertura de contas, garantindo maior segurança e prevenção a fraudes. Será exigida a apresentação de documento formalizado contendo a política ou procedimento que determina a obrigatoriedade dessa verificação, bem como evidências de que a funcionalidade está implementada no sistema, por meio de registros ou capturas que demonstrem a coleta ou validação da localização. Além disso, deverá ser anexada evidência comprovando a aplicação da verificação de geolocalização durante a abertura da conta, incluindo o fluxo executado e os resultados obtidos.

- Existência de procedimento/ferramenta de análise que realize a validação do perfil e a habitualidade comportamental do cliente na abertura de conta, de forma a sinalizar os casos em que houver movimentações fora do padrão comportamental do cliente.

PILAR 6: Avaliar a existência e adequação de estrutura mínima, ferramentas, procedimentos e governança na gestão do processo transacional

Este pilar tem como objetivo garantir que a instituição disponha de uma estrutura sólida e integrada para a gestão segura e eficiente das transações, contemplando recursos tecnológicos adequados, processos padronizados e mecanismos de governança que assegurem confiabilidade e mitigação de riscos.

É responsabilidade da instituição assegurar o cumprimento integral dos requisitos estabelecidos pelos órgãos reguladores, bem como implementar mecanismos robustos que garantam segurança, eficiência operacional e mitigação de riscos.

Para cumprimento deste pilar, serão revisados os seguintes aspectos:

I. Formalização de procedimentos:

- Existência de documento formalizado que estabeleça os procedimentos antifraude relacionados a monitoramento de transações (incluindo restrição a contas bolsão e controles relacionados a concentração indevida de recursos). A instituição deverá apresentar evidência da publicação do documento formalizado, sua atualização, aprovação e comprovar que ele foi devidamente compartilhado com os colaboradores, garantindo sua disseminação e aplicação. O documento deve prever monitoramento para todos os arranjos de pagamentos aplicáveis à instituição.

II. Disponibilidade de sistemas e *backup*:

- Existência de utilização de ferramentas ou tecnologias para monitorar a disponibilidade e o desempenho dos sistemas de prevenção a fraudes. Deverão ser apresentados: nome da ferramenta, sistema ou tecnologia empregada, bem como evidências de sua utilização por meio de *prints* das interfaces e funcionalidades. Além disso, será necessário disponibilizar o último relatório gerado para teste de disponibilidade e desempenho, contendo pareceres e apontamentos, quando existentes, e o diagrama da solução indicando os pontos de coleta das informações.

- Existência do procedimento de realização de *backups* periódicos, contendo o detalhamento sobre como o processo é executado — indicando quem realiza, onde é realizado, a forma de execução e a frequência definida. Além disso, será necessário disponibilizar evidências da ferramenta de *backup* e sua parametrização, bem como evidências do diretório onde os *backups* são armazenados, permitindo identificar todos os *backups* executados.

- Existência de análise de riscos voltada à identificação de possíveis falhas na disponibilidade dos sistemas, bem como a implementação de medidas preventivas. A avaliação deverá incluir o encaminhamento dos relatórios que descrevem as falhas identificadas e as medidas previstas ou implementadas, além de evidências de mecanismos de alerta ou notificação em caso de interrupções sistêmicas, por meio de *prints* de alertas reais, quando existentes. Também será necessário disponibilizar o plano de continuidade de negócios, assegurando que a instituição possua estratégias documentadas para mitigação de riscos e manutenção da operação em cenários críticos.

- Existência de testes realizados pela instituição para validar o funcionamento e a disponibilidade dos sistemas, incluindo práticas como testes de segurança (ex.: *pentest*). A análise deverá contemplar a descrição detalhada do processo, indicando quem executa, como é executado e a frequência estabelecida. Além disso, será necessário encaminhar evidências dos últimos testes realizados, como relatórios, *prints* e demais registros que comprovem a execução e os resultados obtidos.

III. Análises de ambiente transacional:

- Existência de procedimentos de monitoramento de transações, assegurando que esse monitoramento seja estendido a todos os arranjos de pagamento do Sistema Financeiro Brasileiro (Pix, TED, cartões, boletos de depósito e aporte, entre outros). O procedimento deverá incluir a descrição detalhada dos procedimentos adotados, indicando quem executa, como é executado e a frequência estabelecida, bem como a identificação e evidência dos sistemas ou tecnologias utilizados para esse monitoramento. Além disso, será necessário anexar evidências do processo de monitoramento, demonstrando casos reais de transações não realizadas para cada arranjo.

- Existência de procedimento específico para bloqueio cautelar de transações via Pix. A avaliação deverá considerar a documentação que comprove a previsão contratual para realização do bloqueio cautelar, bem como a possibilidade de devoluções e bloqueios de recursos no âmbito do Mecanismo Especial de Devolução (MED), incluindo bloqueios parciais. Também será necessário apresentar evidências práticas do processo, como registros ou telas que demonstrem a execução real do bloqueio cautelar.

- Existência da realização de validação de chave Pix dos clientes. Deverá ser encaminhado evidências do processo de validação, de forma que seja possível observar todo o processo, bem como a avaliação do risco.

- Existência de procedimentos para comunicação ao cliente em casos de bloqueio realizado. A avaliação deverá considerar evidências que demonstrem a execução desse processo, como exemplos reais de comunicações enviadas aos clientes.

- Existência de controles que assegurem que o bloqueio cautelar de transações tenha duração máxima de 72 horas. A avaliação deverá considerar evidências que comprovem a existência desses controles, bem como exemplos reais de casos em que a transação foi bloqueada dentro do prazo estabelecido.

- Existência de procedimentos relacionados à utilização das informações da DICT disponibilizadas pelo Banco Central e R6, bem como os mecanismos aplicados em caso de

apontamentos. A verificação considerará evidências que demonstrem a aplicação dessas informações nos processos internos e registros que comprovem ações decorrentes, como bloqueios de transações.

- Existência de procedimentos relacionados à inteligência de dados aplicada às regras de antifraude, incluindo a utilização de ferramentas de *analytics*. A verificação considerará evidências que demonstrem a aplicação dessas práticas e o uso das ferramentas indicadas, garantindo aderência às normas e efetividade dos controles implementados.
- Existência de procedimentos para análise comportamental dos clientes no ambiente transacional, bem como a utilização de parâmetros ou regras que suportem essa prática. A verificação considerará evidências que demonstrem a aplicação da análise e registros que comprovem os critérios utilizados.
- Existência de procedimentos formais para identificação de prestação de serviços financeiros ou de pagamentos não autorizados pelo cliente, como contas laranja, contas bolsão e contas de passagem. A verificação considerará se há regras implementadas e evidências que demonstrem sua aplicação prática.
- Existência de procedimentos e mecanismos de monitoramento de movimentações incompatíveis com o perfil do cliente, com intuito de identificar prestação de serviços financeiros de pagamento não autorizados. A verificação considerará evidências que demonstrem o processo realizado e a parametrização sistêmica aplicável.
- Existência de procedimentos e mecanismos para análise de comportamento transacional a fim de identificar contas de passagem. A verificação considerará evidências que demonstrem o processo realizado, alertas, relatórios, parametrizações e demais formalizações.
- Existência de documento formalizado contendo os critérios utilizados para identificação de serviços financeiros ou pagamentos não autorizados, aprovado, pela alta administração. A análise buscará confirmar se existe governança adequada para validação desses critérios, garantindo respaldo institucional.
- Utilização de informações provenientes de bases públicas e privadas nos critérios de identificação de serviços financeiros ou pagamentos não autorizados. A verificação considerará se essas fontes são integradas ao processo e se há evidências que comprovem sua utilização.
- Existência de processo formal para revisão periódica dos critérios utilizados na identificação de serviços financeiros ou pagamentos não autorizados. A análise buscará confirmar se há

periodicidade definida e mecanismos que assegurem atualização conforme mudanças regulatórias ou novas ameaças.

- A manutenção da documentação dos critérios utilizados para identificação e encerramento de contas pelo prazo regulamentar, garantindo que as informações estejam disponíveis para órgãos reguladores quando necessário.
- Existência de procedimentos para encerramento de contas identificadas como prestadoras de serviços financeiros ou de pagamentos não autorizados, incluindo comunicação ao cliente. A análise buscará confirmar se há formalização e evidências práticas do processo.
- Existência de dossiês contendo evidências e análises que fundamentam o encerramento de contas de passagem, garantindo rastreabilidade e conformidade com as normas aplicáveis.
- A inclusão das contas de passagem encerradas no DICT, considerando evidências que comprovem a execução dessa obrigação regulatória.
- A realização do compartilhamento das contas de passagem encerradas com a Base RC6, garantindo aderência às exigências normativas.
- Existência de procedimentos para encerramento de contas identificadas como *Bet* Irregular, incluindo comunicação ao cliente e formalização do processo.
- Existência de dossiês contendo evidências e análises que fundamentam o encerramento de contas de *Bet* Irregular, assegurando rastreabilidade e conformidade.
- Realização de comunicação à Secretaria de Prêmios e Apostas (SPA) em casos de *Bet* Irregular, garantindo cumprimento das obrigações regulatórias.
- Existência de declaração emitida por área independente (Auditoria Interna, *Compliance* ou Controles Internos) que comprove conformidade com o SARB 28/2025, assegurando transparência e governança.

PILAR 7: Avaliar a existência e adequação de estrutura mínima, ferramentas, procedimentos e governança no tratamento de fraudes

Este pilar tem como objetivo identificar que a instituição disponha de uma estrutura organizada e eficaz para o tratamento de fraudes, contemplando procedimentos formais, equipe dedicada, sistemas adequados e mecanismos de governança que garantam prevenção, registro e acompanhamento contínuo dos riscos.

É responsabilidade da instituição assegurar o cumprimento integral dos requisitos estabelecidos

pelos órgãos reguladores, bem como implementar mecanismos robustos que garantam segurança, eficiência operacional e mitigação de riscos relacionados a fraudes.

Para cumprimento deste pilar, serão revisados os seguintes aspectos:

I. Formalização de procedimentos e governança:

- Existência de documentos formalizados que estabeleçam os procedimentos para registro de fraudes internas e externas. A análise contemplará o conteúdo do documento com detalhamento das ações, vigência e aprovação pela instância competente, e a identificação de que houve divulgação interna adequada a todos os colaboradores aplicáveis.
- Existência de uma equipe dedicada à prevenção de fraudes, incluindo definição clara de responsáveis pelo tratamento de incidentes e indícios de fraude. A verificação considerará a estrutura organizacional, cargos e funções, bem como políticas internas atualizada, aprovadas e divulgadas que sustentem essa atuação.

II. Registro de fraudes:

- Procedimentos de registro de fraudes internas e externas, considerando a formalização dos procedimentos e os sistemas utilizados para essa finalidade. Além disso, será necessário a instituição evidenciar a existência de documentos normativos que descrevam o processo, a identificação dos sistemas empregados e a clareza do fluxo operacional, incluindo responsáveis, etapas e frequência do registro.

III. Acompanhamento de riscos e auditoria:

- Implementação de auditorias internas em intervalos regulares na área de prevenção a fraudes, conforme período mínimo definido pela instituição (ex.: anual, semestral). A avaliação incluirá a documento formal que mencione o prazo, evidência da última auditoria realizada e cronograma formal das auditorias.
- Implementação de ações de regularização, por parte da área de prevenção a fraudes, decorrentes dos apontamentos das auditorias internas. A análise contemplará planos de ação, prazos para execução e evidências de acompanhamento e conclusão de apontamentos.
- Procedimento realizado pela instituição para monitorar, identificar e atender novas regulações relacionadas à prevenção de fraudes. Deverá descrever e evidenciar o processo, incluindo responsáveis, métodos, frequência e finalidade, bem como a existência de

procedimentos formais e evidências de monitoramento efetivamente realizado.

- Elaboração de relatório mensal consolidado das ocorrências de fraudes e das medidas preventivas e corretivas adotadas. A revisão incluirá verificação da existência do relatório, sua aprovação e utilização em comitês.
- Realização de comunicação periódica das ocorrências de fraudes e das medidas preventivas e corretivas adotadas pela Alta Administração/Conselho. A análise considerará a frequência, os canais utilizados e a abrangência da comunicação.
- Utilização e integração de riscos, indicadores e controles ao processo de gerenciamento de risco, incluindo utilização destes na avaliação dos riscos operacionais e contemplação de fraudes internas e externas no relatório de riscos operacionais. A revisão incluirá relatórios que integrem esses indicadores, a metodologia utilizada, a aprovação pela instância competente e documento da avaliação de riscos de fraude (ex.: matriz de riscos e controles, telas sistêmicas).
- Existência de critérios formalizados para classificação, priorização e definição de prazos no tratamento de ocorrência. A revisão incluirá documentos formais com a formalização do processo e evidências das etapas realizadas.

PILAR 8: Avaliar a existência e a adequação do processo de prevenção a fraudes internas

Este pilar tem como objetivo identificar que a instituição disponha de procedimentos formalizados, controles internos robustos e mecanismos de governança eficazes para prevenir e mitigar fraudes internas, garantindo segurança lógica, segregação de funções e rastreabilidade das ações.

É responsabilidade da instituição implementar controles e práticas que assegurem a integridade dos processos internos, garantindo que acessos, investigações e monitoramentos sejam realizados de forma segura, transparente e auditável.

Para cumprimento deste pilar, serão revisados os seguintes aspectos:

I. Formalização de procedimentos:

- Existência de documento formalizado que estabeleça os procedimentos para recebimento de denúncias, investigação de fraudes internas e definição das sanções aplicáveis em caso de confirmação. O documento deve estar vigente, aprovado pela instância competente e amplamente divulgado aos colaboradores.

- Existência de documento formalizado atualizado, aprovado e amplamente divulgado aos

colaboradores, que defina os procedimentos para revogação imediata e revisão periódica dos acessos, garantindo segregação de funções e prevenção de acessos indevidos.

- Existência de documento formalizado que comunique aos colaboradores as medidas administrativas aplicáveis em casos de envolvimento com fraude, garantindo clareza sobre consequências.

- Formalização da obrigatoriedade da autenticação em dois fatores para acesso a ferramentas e computadores, visando reforçar a segurança lógica.

- Existência de documento formalizado que dispõe sobre os procedimentos realizados em casos de coação a colaboradores. O documento deve estar vigente, aprovado pela instância competente e amplamente divulgado aos colaboradores.

II. Prevenção de fraudes internas:

- Existência de procedimentos de formalização das investigações de fraudes internas em relatório formal ou sistema, garantindo rastreabilidade, transparência e comunicação às instâncias competentes. A análise verificará se os relatórios ou registros sistêmicos contêm informações essenciais, como etapas da investigação, responsáveis, conclusões e evidência de aprovação. Também será avaliado se existe fluxo formal que assegure que as alçadas competentes tenham visibilidade sobre os casos tratados.

- Independência entre as áreas responsáveis por investigação de fraudes internas e pelo canal de denúncias em relação às decisões finais, garantindo segregação de funções e imparcialidade.

- Existência de monitoramento e alertas para acesso físico de funcionários a áreas restritas, utilizando tecnologias adequadas (ex.: acesso a *data centers*, em casos de instituições com agências presenciais: locais de que possuem cofres etc.). Deve existir documento formal que defina o processo e evidência dos alertas gerados.

- Existência de monitoramento e mitigação de fraudes em casos de coação a colaboradores, assim como a verificação de existência de documentação formalizada (ex.: política interna, guia orientativo, manual de procedimentos) contendo a definição clara do que constitui coação de colaboradores, quais sinais devem ser observados, procedimentos passo a passo de como agir ao identificar coação (quem deve ser comunicado - hierarquia, canal de denúncias, áreas envolvidas), prazos para comunicação e tratamento, responsabilidade de

cada área, indicação das medidas de proteção ao colaborador coagido, orientação sobre documentação e registros do caso. O documento deverá estar compartilhado formalmente aos colaboradores.

PILAR 9: Avaliar a existência do envolvimento de *cyber* em prevenção a fraudes.

Este pilar tem como objetivo identificar que a instituição disponha de procedimentos formalizados, controles internos robustos e mecanismos de governança eficazes em segurança da informação e cibernética, visando à proteção dos dados, a prevenção e mitigação de fraudes, bem como a detecção e resposta a incidentes no ambiente tecnológico.

É responsabilidade da instituição implementar controles e práticas que garantam a confidencialidade, integridade e disponibilidade das informações, assegurando que acessos físicos e lógicos, monitoramentos, investigações, gestão de fornecedores, testes de vulnerabilidades e eventos atípicos sejam realizados de forma segura, transparente, rastreável e auditável.

Para cumprimento deste pilar, serão revisados os seguintes aspectos:

I. Procedimentos relacionados a cybersegurança:

- Existência de Política de Segurança da Informação. O documento deve estar vigente, aprovado pela instância competente e amplamente divulgado aos colaboradores.

- Estabelecimento de responsável formal pela segurança cibernética. Deverá ser evidenciado quem são e onde estão publicadas as informações correspondentes.

- Existência de procedimentos relacionados a classificação de dados e regras claras de uso, armazenamento e descarte. Deverá ser evidenciado o inventário de dados anonimizado para análise, cópia do documento formal (ex.: política interna, guia orientativo, manual de procedimentos) e evidência da divulgação aos colaboradores envolvidos nos processos relevantes.

- Existência de monitoramento de transações suspeitas com correlação entre eventos de Segurança da Informação (SI) e fraudes. Deverá ser evidenciado o procedimento executado e o armazenamento de evidências em casos de identificação de fraude.

- Informações quanto aos fornecedores críticos da instituição e os procedimentos de *due diligence* de segurança realizados. Deverá ser evidenciado o passo a passo do procedimento,

demonstrando todas as etapas performadas.

- Implementação de cláusulas contratuais com os fornecedores e terceiros cobrindo proteção de dados, vazamentos e resposta a incidentes. Deverá ser disponibilizado o(s) contrato(s) para análise, quando solicitado.

- Realização de revogação de acessos físicos e lógicos, no prazo máximo de 24h após a rescisão do funcionário, conforme boas práticas de Segurança da Informação. Deverá ser evidenciado o passo a passo do procedimento realizado e o documento formal (ex.: política interna, guia orientativo, manual de procedimentos) com a descrição dos procedimentos.

- Existência de revisão dos direitos de acesso em uma periodicidade mínima definida (em documento formal disponibilizado). Deverá ser evidenciado o documento formal que rege a periodicidade, as 3 últimas revisões realizadas.

- Existência de *tracking*/base de dados armazenadas contendo o histórico das revisões de acessos realizadas. Deverá ser evidenciado o histórico e a política/documento formalizado que rege a retenção de dados.

- Utilização de autenticação multifator (MFA/2FA), para acesso ao ambiente interno, assim como a abrangência (todos os usuários ou grupos específicos) e existência de documento formal que determine a obrigatoriedade.

- Existência de procedimentos e ferramentas para identificar e alertar sobre eventos atípicos no ambiente de produção (ex.: conexões VPN anômalas, acessos privilegiados fora de horário). Deverá ser evidenciada a tecnologia utilizada (VPN, *proxy* etc.), os procedimentos executados e o documento formal que define o processo.

- Estabelecimento de processo de autorização e registro para *download*/instalação de *software* em estações e servidores da instituição. Deverá ser evidenciado o passo a passo do processo, inclusive as informações de registro e aprovação, além de documento formal que estabeleça tal procedimento.

- Realização de testes de intrusão com periodicidade mínima anual, inclusive em prestadores de serviços de processamento de mensagens no âmbito do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamento Brasileiro (SPB). Deverá ser evidenciado documentação formalizada (ex.: política interna, guia orientativo, manual de procedimentos) contendo os procedimentos realizados, o passo a passo dos procedimentos executados e o relatório

contendo a conclusão do teste realizado.

RESSALVAS QUANTO ÀS REVISÕES DAS DOCUMENTAÇÕES:

Todas as documentações solicitadas serão revisadas de forma criteriosa, podendo ser requeridas evidências adicionais, quando necessário.

Para evidências que envolvam extração de dados, é obrigatório o envio acompanhado do IPE correspondente.

Nos casos de evidências apresentadas em formato de *prints* de tela, estas deverão ser enviadas em tela cheia, garantindo a visualização completa da interface, incluindo data e horário do registro.

Para documentações formais, como políticas, manuais, normativos e similares, deverão estar devidamente atualizadas, aprovadas e disponibilizadas (*intranet* ou equivalente), assegurando acesso aos colaboradores aplicáveis. Adicionalmente, os documentos formalizados não serão aceitos em documentos editáveis.