CARTILHA DE FRAUDES

GERÊNCIA DE RISCOS E CONTROLES

JAN/23

SICOOB
Central Crediminas

ÍNDICE

Conceito Técnico de Fraude e Erro • NBC T 11

1. O termo **fraude** refere-se a ato intencional de omissão ou manipulação de transações, adulteração de documentos, registros e demonstrações contábeis. A fraude pode ser caracterizada por:

a) manipulação, falsificação ou alteração de registros ou documentos, de modo a modificar os registros de ativos, passivos e resultados;

b) apropriação indébita de ativos;

c) supressão ou omissão de transações nos registros contábeis;

d) registro de transações sem comprovação; e

e) aplicação de práticas contábeis indevidas.

2. O termo **erro** refere-se a ato não-intencional na elaboração de registros e demonstrações contábeis, que resulte em incorreções deles, consistente em:

a) erros aritméticos na escrituração contábil ou nas demonstrações contábeis;

b) aplicação incorreta das normas contábeis;

c) interpretação errada das variações patrimoniais.

Conceito Técnico de Fraude e Erro • NBC T 11

A RESPONSABILIDADE DA ADMINISTRAÇÃO

3. **A responsabilidade primeira na prevenção e identificação de fraudes e/ou erros é da administração da entidade**, mediante a manutenção de adequado sistema de controle interno, que, entretanto, não elimina o risco de sua ocorrência.

A RESPONSABILIDADE DO AUDITOR

4. **O auditor não é responsável nem pode ser responsabilizado pela prevenção de fraudes ou erros.** Entretanto, deve planejar seu trabalho avaliando o risco de sua ocorrência, de forma a ter grande probabilidade de detectar aqueles que impliquem efeitos relevantes nas demonstrações contábeis.

5. **Ao planejar a auditoria, o auditor deve** indagar da administração da entidade auditada sobre qualquer fraude e/ou erro que tenham sido detectados.

FRAUDES

são atos intencionais praticados por indivíduos externos à entidade ou internos com o objetivo de apropriar indevidamente de valores financeiros e bens físicos.

Eletrônica:

Consiste na ação de enganar a vítima, por intermédio de dispositivos de informática, ou seja, perdas com operações financeiras no ambiente do App Sicoob, Internet Banking e Internet Banking Empresarial realizadas por ação de malware, violações ou acessos não autorizados por meio de interceptação de informações nos canais eletrônicos de atendimento e por meio de falsa atualização de segurança.

Eletrônica - Invasão de máquina:

Quando o cooperado desconhece débitos realizados em sua conta tratando-se, portanto, de ação de malware, proveniente de download de arquivo malicioso recebido por e-mail ou por meio da navegação em páginas da internet. Ou ainda por meio de violações ou acessos não autorizados por intermédio da interceptação de informações nos canais eletrônicos, por exemplo, um phishing que geralmente simulam o App Sicoob, Internet Banking ou Internet Banking Empresarial.

Golpe da Falsa Central - Vishing

Vishing é uma abreviação de Voice Phishing - uma variação de golpe aplicada por áudio. Um exemplo de Vishing é quando a pessoa recebe uma ligação para "confirmar" informações. Na verdade, quem está ligando não tem informação nenhuma -ou tem muito pouca, mas vai, de alguma forma, te convencer a passar os dados.

Como funciona o golpe da falsa central de atendimento:

O telefone toca. Do outro lado da linha, o atendente informa ser da Central de Atendimento do seu banco. O telefone que aparece em seu celular é o da central de atendimento do seu banco (tecnologia VOIP). O suposto atendente informa que há algum problema em sua conta, como compras suspeitas, necessidade de liberação de dispositivos ou atualização de módulo de segurança, transações realizadas etc.
O criminoso pede a pessoa/vítima que desligue e ligue para o número da central de atendimento que aparece no site da empresa, ou do verso do cartão. Ao fazer isso, a ligação retornará para o criminoso em razão deles conseguirem prender ligações em números para telefone fixo por até 5 minutos.
As gravações que a vítima ouve, os menus para você selecionar: tudo parece indicar que a ligação é realmente da Central de Atendimento do seu banco.
Até alguns dos seus dados pessoais ou financeiros podem ser usados na ligação.

O Sicoob **não entra em contato com cooperados para solicitar** cancelamento ou estorno de PIX, instalação de aplicativos não oficiais do Sicoob e nem realização de reconhecimento facial para cancelar operações.

Documental:

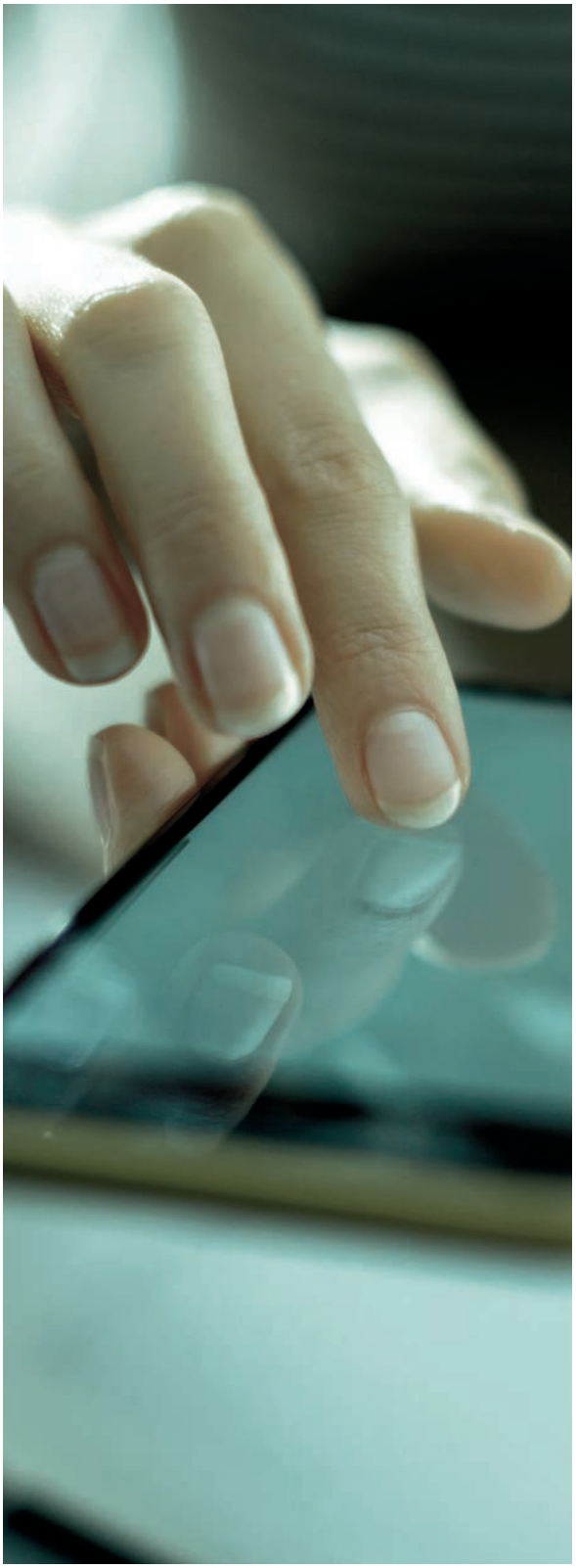
Perda financeira que a cooperativa obteve com crédito enviado para outra instituição e após inadimplência identificada solicita a devolução para a instituição recebedora. Ou transações, por exemplo, transferências, que utilizaram o limite do "cheque especial" da conta após identificação de que a respectiva conta corrente ou poupança foi aberta com documentação de identificação falsa.

Documental - Abertura de conta:

Conta aberta com documento falso: contas abertas presencialmente pela cooperativa.

TIPIFICAÇÃO FRAUDES E GOLPES

Golpes



Quando o cooperado é enganado por meio de persuasão aplicada por terceiros que geralmente utilizam de mensagens de texto, e-mails e telefonemas para obter dados pessoas e senhas, bem como convencê-lo a realizar transações financeiras.

A maior parte dos golpes está relacionado à **Engenharia social**, que é um método de ataque no qual o fraudador faz uso da **persuasão** para obter as credenciais de acesso do cooperado (nº da cooperativa, conta, senha de oito dígitos, senha de seis dígitos) e até mesmo convencer o cooperado a realizar a leitura de QR Codes, com o intuito de realizar operações financeiras em suas contas.

Vide CCI 385/2019 DO SICOOB CONFEDERAÇÃO

Golpes – Engenharia Social

Boleto falso recebido por e-mail:

E-mail recebido contendo boleto adulterado ou solicitando a substituição sob justificativa de concessão de desconto.

Recebimento de código de barras por SMS:

Linha digitável adulterada recebida por SMS pelo cooperado.

Boleto atualizado na internet:

Segunda via de boleto atualizado pelo cooperado em sites de terceiros.

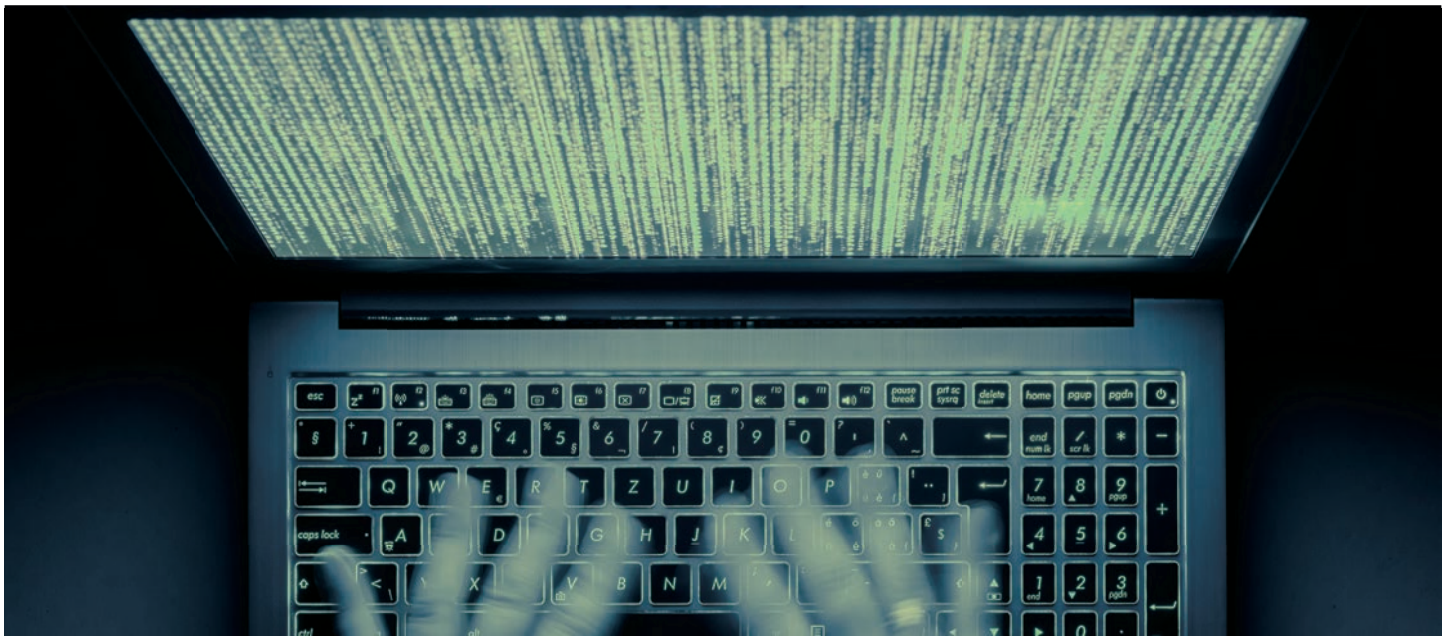
Boleto falso recebido por correspondência:

Boleto adulterado ou com a justificativa de concessão de desconto recebido, por meio de correspondência física.

Falsa quitação de débito:

O golpista convence a vítima de que ela possui uma dívida; ou a vítima procura negociar dívida existente, em canais não oficiais e recebe condições para quitá-la. A forma de abordagem pode ser por meio de mensagens de texto, WhatsApp, e-mail ou por

Golpes – Engenharia Social



Falsa atualização de módulo de segurança:

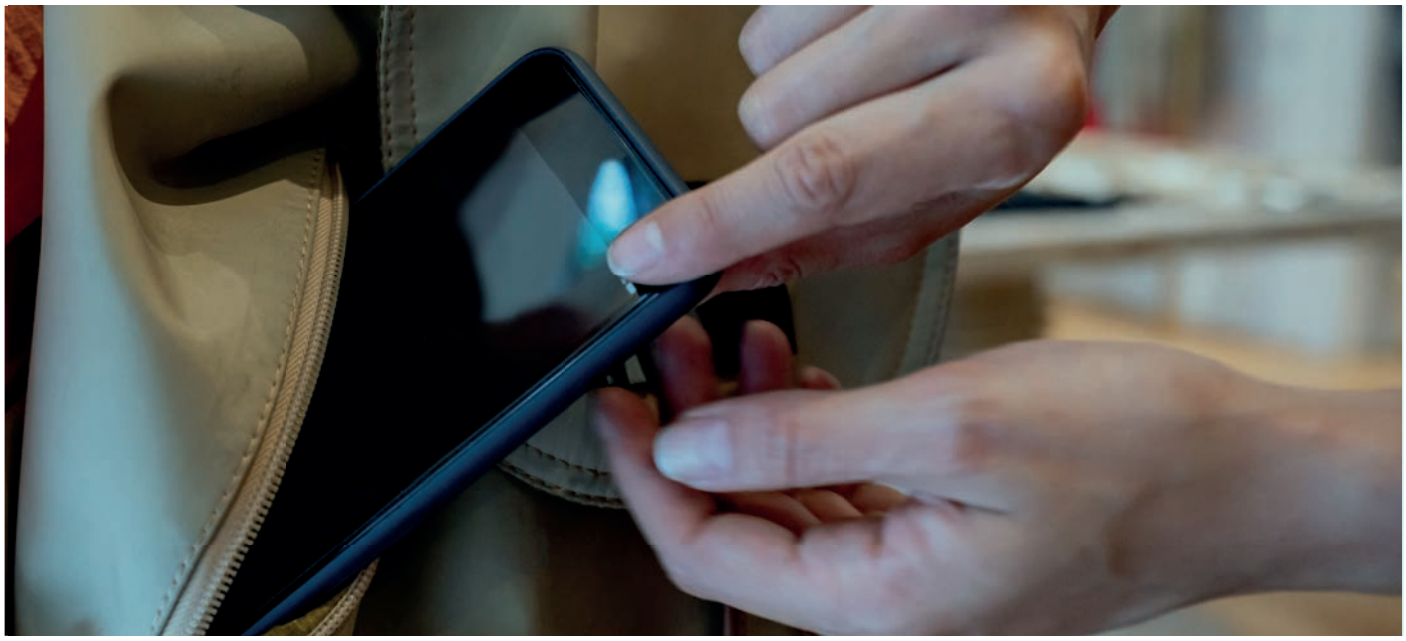
No momento da utilização do Sicoobnet, no computador é apresentada para o cooperado uma tela, supostamente do Sicoob, que induz o cooperado a realizar uma atualização do "módulo de segurança", ou similar, e em seguida é apresentado um QR Code.

A abordagem do fraudador também pode ocorrer por meio do envio de SMS que contém um link malicioso que induz o cooperado a acessá-lo e fornecer suas informações pessoais e senha para realizar a atualização do Sicoobnet. Nesses casos, o QR Code apresentado ao final da suposta atualização trata-se de confirmação de uma transação financeira e não de uma atualização de segurança ou transação de teste.

Falsa atualização/liberação de dispositivo:

O golpista entra em contato com a vítima se passando por funcionário do Sicoob ou não, solicitando que sejam realizados alguns procedimentos operacionais, e ao final, um dispositivo é liberado na conta.

Golpes – Outros



Roubo/furto de celular:

Transações realizadas a partir de um aparelho celular roubado/furtado.

Extorsão ao caixa da cooperativa:

Ocorre quando alguém coage o operador de caixa da cooperativa para realizar uma transação financeira contrária à sua vontade, utilizando da violência ou de qualquer outro tipo de intimidação contra a pessoa extorquida.

Clonagem de WhatsApp:

Mensagem recebida pelo cooperado, supostamente enviada por um familiar ou amigo, que teve o WhatsApp clonado, solicitando deste uma quantia emprestada que foi depositada em conta de titularidade de terceiro.

Extorsão - Pagamento de sequestro:

Trata-se do ato de privar ilicitamente uma pessoa de sua liberdade, geralmente, durante um determinado tempo, até conseguir o resgate.

Extorsão ao cooperado:

Ocorre quando alguém coage o cooperado para ele realizar uma transação financeira contrária à sua vontade, utilizando da violência ou de qualquer outro tipo de intimidação contra a pessoa extorquida.

Golpes – Outros

Venda falsa - Compra pela internet

Compra de mercadoria realizada em sites de lojas falsas e por isso não entregues.

Falso empréstimo

É a oferta de empréstimo para pessoas negativadas com a promessa de não consultar órgãos de proteção ao crédito, por meio de anúncios em outdoors, rádios, jornais, Internet, mídias sociais, etc., no qual os golpistas solicitam pagamento antecipado de taxas administrativas e seguros prestamistas e, quando recebem o pagamento, que geralmente é por TED, cortam o contato com a vítima.

Troca da Maquininha

Fraudador se passa por comprador num estabelecimento comercial e efetua a troca da maquinha da loja por outra, sem que o vendedor/lojista perceba o ato, passando os créditos das compras a ser desviados para outro beneficiário.

Venda falsa - Falso leilão, OLX ou mercado livre:

Compra de veículos, animais, eletrônicos, terrenos, dentre outros realizadas em sites falsos e por isso nunca entregues.

PIX Simulado

Vem sendo aplicado intensamente no comércio, quando de entregas em domicílio, em que o consumidor fraudador simula uma transação de transferência (PIX), no valor da compra, sem efetivamente concretizá-la, imprimi a tela e remete ao Empreendedor. Crendo da legitimidade do comprovante e sem efetuar a conferência do efetivo crédito em sua conta-corrente, o Empreendedor acaba por autorizar a entrega da mercadoria/produto, sendo lesado.

TÉCNICAS DOS FRAUDADORES

SAIBA COMO VOCÊ PODE SER MANIPULADO

As técnicas e variações na engenharia social são tantas, que é muito difícil fornecer uma lista completa. Estas são algumas das coisas mais importantes a serem observadas:

• Pressão do tempo:

todos os ataques de engenharia social têm mais sucesso se a vítima acredita que é preciso tomar uma decisão rapidamente.

• Medo da perda:

o fenômeno “medo da perda” impulsiona o sucesso das redes sociais, mas também se torna uma tática de manipulação avançada.

• Direção errada:

nem todas as técnicas de engenharia social são puramente psicológicas. Um invasor pode usar vulnerabilidades em sites para redirecionar você para uma página mal-intencionada, na esperança de que você insira informações pessoais ou financeiras.

TÉCNICAS DOS FRAUDADORES

• Avaliações falsas:

isso não se aplica apenas a empresas que pagam pelas avaliações em lojas de aplicativos, para tornar seu produto mais atraente. Avaliações falsas podem ser usadas para fazer com que um site ou serviço pareça mais confiável, o que incentiva a enviar informações pessoais.

• Identidade falsa:

este é o elemento fundamental de todos os golpes de phishing. Os invasores se apresentam como uma organização ou pessoa confiável para que você se sinta à vontade e divulgue informações confidenciais.

• Informações parciais:

para tornar seu pretexto mais convincente, os cibercriminosos costumam usar algumas informações públicas ou facilmente obtidas para encorajá-lo a divulgar ainda mais. Por exemplo, golpistas com seu endereço, número de telefone e quatro dígitos finais do cartão de crédito podem se apresentar como uma loja on-line. Eles podem solicitar que você “atualize” suas informações de pagamento para o cartão que termina com estes quatro números.

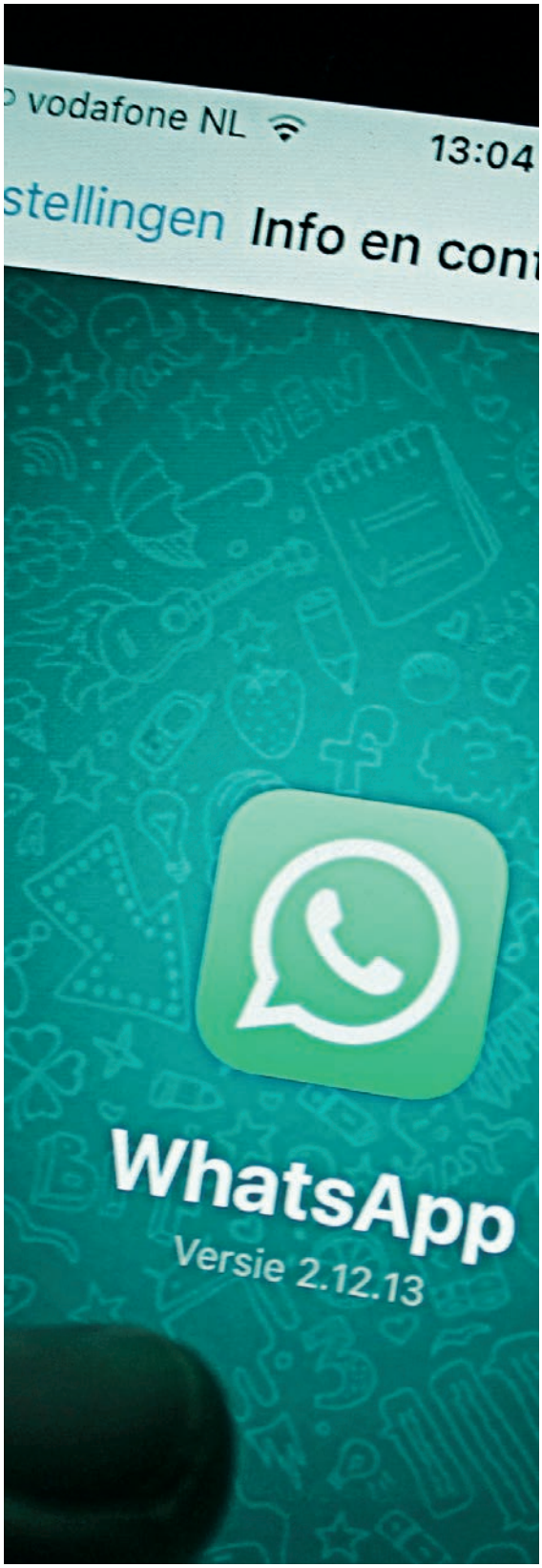
Kevin Townsend, 3 de Maio de 2019 10h0min0s CEST

Golpe do WhatsApp

Nessa modalidade, os golpistas utilizam mensagens do WhatsApp e fingem ser de alguma empresa ou serviço em que a vítima já é cadastrada. Depois disso, eles pedem o código de segurança do app, dizendo que é necessário uma atualização, manutenção ou confirmação de cadastro.

Com a posse do código, eles replicam a conta do WhatsApp em outro dispositivo. Desse modo, passam a enviar mensagens para os contatos da vítima, fazendo-se passar por ela e solicitando dinheiro emprestado por transferência, PIX ou outros métodos.

A melhor forma de evitar esse golpe é habilitar a opção de "Verificação em duas etapas", oferecida pelo próprio app. Basta ir até a aba "Configurações/Ajustes", depois "Conta" e, por último, "Verificação em duas etapas". Ali você cadastra uma senha que será solicitada regularmente, como forma de proteção. Lembre-se de não compartilhar essa senha ou digitá-la em links suspeitos.



Golpe do boleto falso

Esse golpe também é bastante comum e pode ser aplicado de diversas maneiras. Uma delas é por meio de um boleto legítimo, com selo de um banco conhecido, mas com destinatário errado. Nesse caso, a vítima envia seu dinheiro diretamente para um estelionatário.

Isso pode acontecer com bancos, com lojas falsas de produtos ou com a chegada de boletos diretamente no seu e-mail.

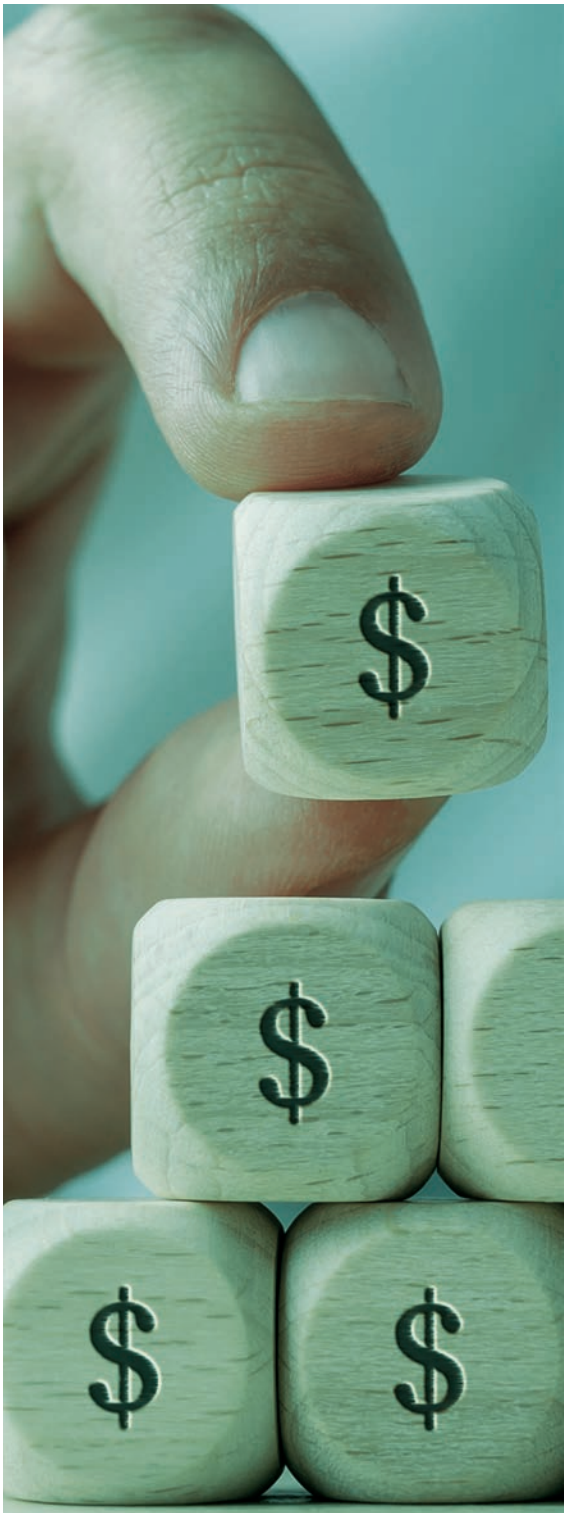
Para escapar dessa armadilha, é fundamental prestar atenção em todos os campos antes de pagar um boleto, conferir o beneficiário e só realizar o pagamento quando tiver certeza de que o dinheiro vai para o lugar certo.

Golpe da pirâmide financeira

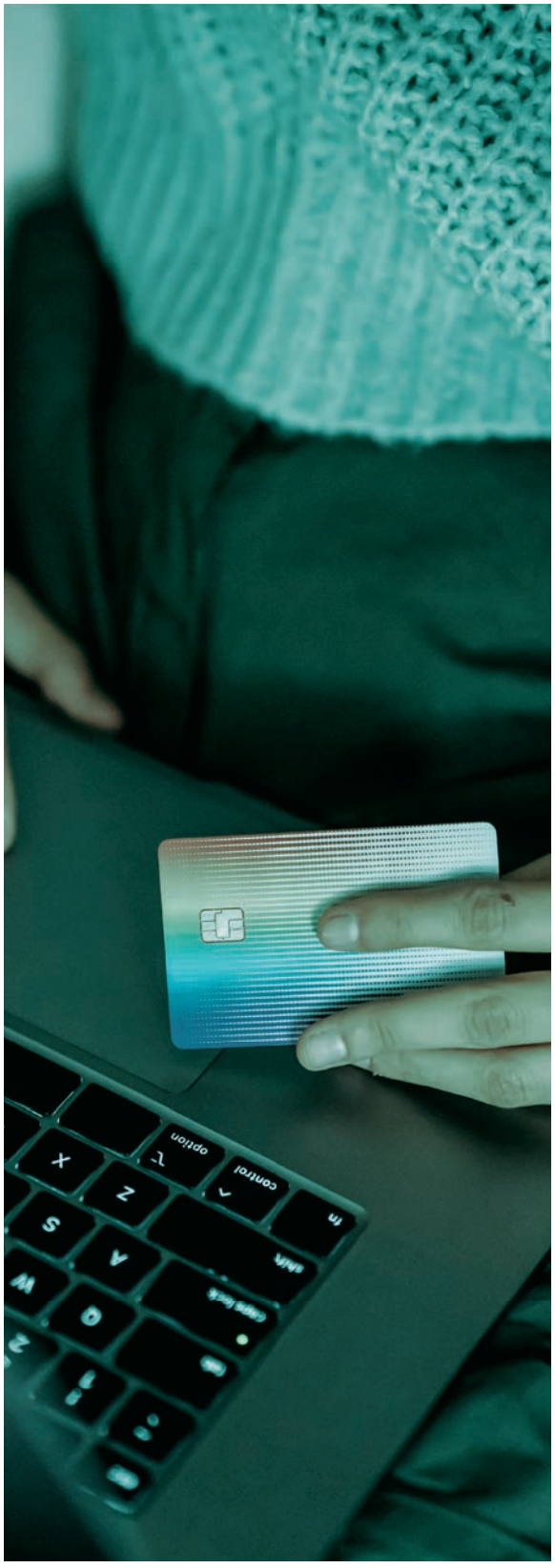
A pirâmide financeira é uma prática ilegal e que traz prejuízos para a grande maioria dos investidores. Esse golpe começa com a promessa de ganhar muito dinheiro de forma simples, rápida e garantida. Outra característica relevante para identificar essa prática é a falta de um produto que seja a principal fonte de renda.

De modo geral, os esquemas são negócios de fachada inventados com a intenção de passar credibilidade para as vítimas.

A melhor forma de evitar esse golpe é desconfiar de propostas que ofereçam ganhos fáceis e rápidos, sem muito esforço. Agindo assim, você não dará espaço para que os golpistas o enganem.



COMO DIFICULTAR AS AÇÕES DE FRAUDADORES



Golpe da clonagem do cartão de crédito

Um dos golpes financeiros mais conhecidos é a clonagem do cartão de crédito. Isso pode acontecer tanto no meio digital quanto no mundo offline, sendo importante estar protegido nos dois ambientes para não ser surpreendido.

Por outro lado, no offline, os golpistas estão sempre procurando por novas formas de aplicar suas táticas. Uma prática comum é a vítima receber uma ligação, supostamente do banco ou da empresa do cartão de crédito, afirmando que uma compra suspeita foi realizada e que, por isso, é preciso digitar o código de segurança, o que dá informações relevantes para os criminosos.

Alguns estabelecimentos também aplicam golpes, por isso é preciso saber **como usar o cartão de crédito** de forma segura. Nessas situações, a máquina é usada apenas para captar os dados do cliente que está pagando uma compra. O operador do caixa, distante da visão da vítima, tira uma foto do cartão de crédito para utilizar no futuro.

A principal maneira de evitar esses problemas é não informar a senha ou o número de cartão de crédito para ninguém. Ao receber ligações, procure diretamente a central de relacionamento do seu cartão, não passando seus dados para quem está do outro lado. Além disso, é essencial sempre visualizar o seu cartão em transações presenciais, pois isso diminui a chance de que alguém clone os seus dados.

COMO DIFICULTAR AS AÇÕES DE FRAUDADORES

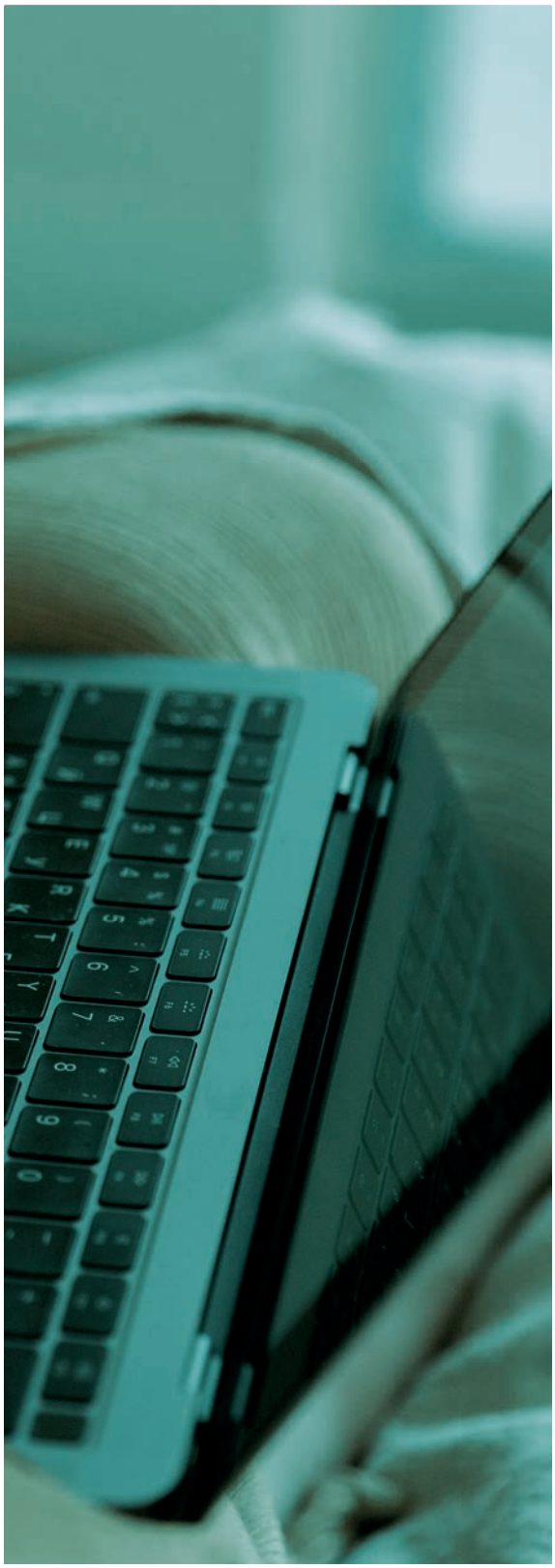
Golpe do e-mail do banco (Phishing)

Nesse tipo de ação, os golpistas enviam um e-mail com mensagens fraudadas, usando um modo de comunicação intimidador e com links e informações que buscam imitar os bancos, o que se define como phishing.

Mensagens desse tipo afirmam que a vítima deve buscar uma solução para que sua conta não seja bloqueada. A ação, por sua vez, é realizada em um site falso, disponibilizado para acesso no próprio e-mail enviado pelo criminoso, que tem a aparência idêntica ao verdadeiro.

O objetivo dos golpistas é roubar informações sigilosas, como senhas de acesso, dados de cartão de crédito ou pagamento de boletos fraudulentos. Para convencer, o site de destino do ataque é muito semelhante ao original, levando as vítimas a não perceberem o golpe.

Para evitar esse tipo de ação criminosa, é essencial verificar as informações e conferir a confiabilidade do e-mail. Se houver problema com a sua conta, procure diretamente o banco pelos canais de atendimento oficiais, pois isso trará mais segurança para as operações e diminuirá a probabilidade de fraude.



Empréstimos e financiamento

Todo mundo sabe muito bem o quanto é importante proteger os nossos dados pessoais, não é verdade? Tanto é que criaram a Lei Geral de Proteção de Dados Pessoais. Mas, mesmo com uma legislação específica, muitas pessoas ainda são vítimas de golpes com o uso indevido de suas informações.

Assim como há casos de operadores tirarem fotos do cartão de crédito de alguém, há também quem tire ou roube fotos de documentos com informações (como RG e CPF) e use para receber crédito ou fazer um pedido de empréstimo com o CPF da vítima.

Para não cair nesse tipo de golpe, é importante sempre verificar a segurança dos sites em que você está inserindo os seus dados, assim como a conexão de internet em que você está logado.

Para o mundo offline, se você perdeu ou teve os seus documentos roubados, faça o registro de ocorrência na polícia o mais breve possível. Também informe o SPC Brasil para que, no caso de ser solicitado algum crédito em seu nome, seja realizada uma dupla verificação.

Promoções com muitos benefícios

Quando estamos contratando um serviço ou comprando algum produto, a gente sempre busca por preços e condições de pagamento mais em conta e de acordo com a nossa capacidade financeira, concorda? Mas tome muito cuidado! Na hora de fazer o pagamento ou negociar um financiamento, o desejo por valores atraentes pode fazer com que você seja vítima de um golpe financeiro, **fazendo depósitos prévios para garantir o benefício.**

Sempre que o preço de um produto ou serviço for muito atrativo, abaixo da média do mercado, ou que as condições de pagamento forem muito vantajosas para o cliente, desconfie! Busque informações sobre a empresa na internet, entre em contato por diversos canais de comunicação e faça uma rápida pesquisa entre família e amigos para verificar se alguém conhece a marca antes de investir o seu suado dinheirinho nessa enrascada.

COMO DIFICULTAR AS AÇÕES DE FRAUDADORES

- √ **Fique atento nos postos de atendimento.**
- √ **Saiba como evitar vazamentos de dados.**
- √ **Implemente e dissemine ações de conscientização aos cooperados.**
- √ **Mais destaque nas mensagens de alertas aos cooperados.**
- √ **Reforce as mensagens de alerta nos canais de atendimento.**
- √ **Oriente seus cooperados em relação ao uso de smartphones e sobre o cuidado com seus cartões.**

COMO DIFICULTAR AS AÇÕES DE FRAUDADORES

√ Orientações quanto ao uso de smartphones e cartões

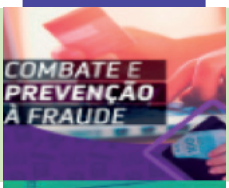
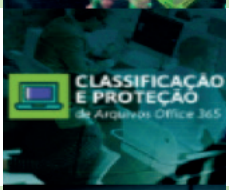
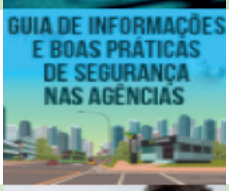
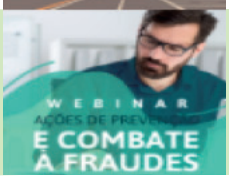
• não utilizar a funcionalidade Lembrar Senha de navegadores e demais aplicativos instalados no dispositivo;
• não utilizar a mesma senha em diferentes serviços ou aplicativos, principalmente os financeiros;
• anotar o código IMEI (International Mobile Equipment Identity) assim que comprar um aparelho, pois com ele será mais fácil bloquear o celular em caso de roubo ou furto. Basta digitar *#06# no celular e o número aparecerá;
• não usar senhas frágeis, como datas de aniversário própria ou de familiares ou qualquer coisa facilmente identificável a partir de seus dados pessoais;
• não transmitir senhas por meio dos aplicativos do celular, pois muitos aparelhos têm recursos que permitem pesquisar tudo que já foi transmitido, dando acesso à senha ao criminoso;
• não utilizar o bloco de notas do celular para guardar senhas ou informações sensíveis;
• não guardar fotos de cartões de crédito;
• usar sempre uma configuração de bloqueio da tela de início do celular e optar pela opção de bloqueio automático mais rápida;
• manter o sistema operacional do celular atualizado, assim como os aplicativos financeiros;
• inibir informações das notificações da tela inicial quando o celular estiver bloqueado.

COMO DIFICULTAR AS AÇÕES DE FRAUDADORES

Capacitação

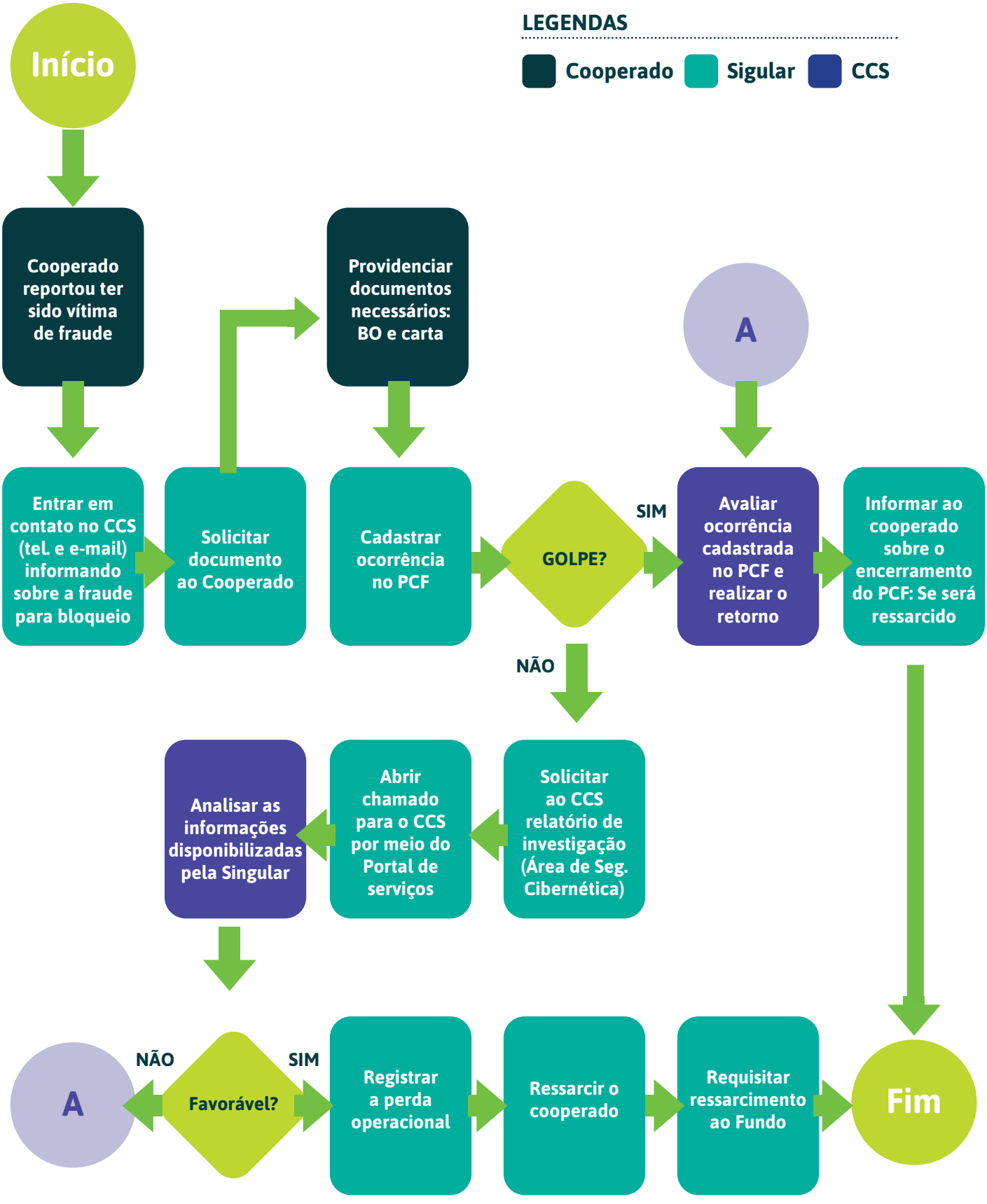
Cursos disponíveis no Sicoob Universidade:

ID: PREVENT-COMBATE-FRAUDE
Esclarecer os conceitos, normas e diretrizes que norteiam os processos de prevenção e combate às fraudes no Sicoob.

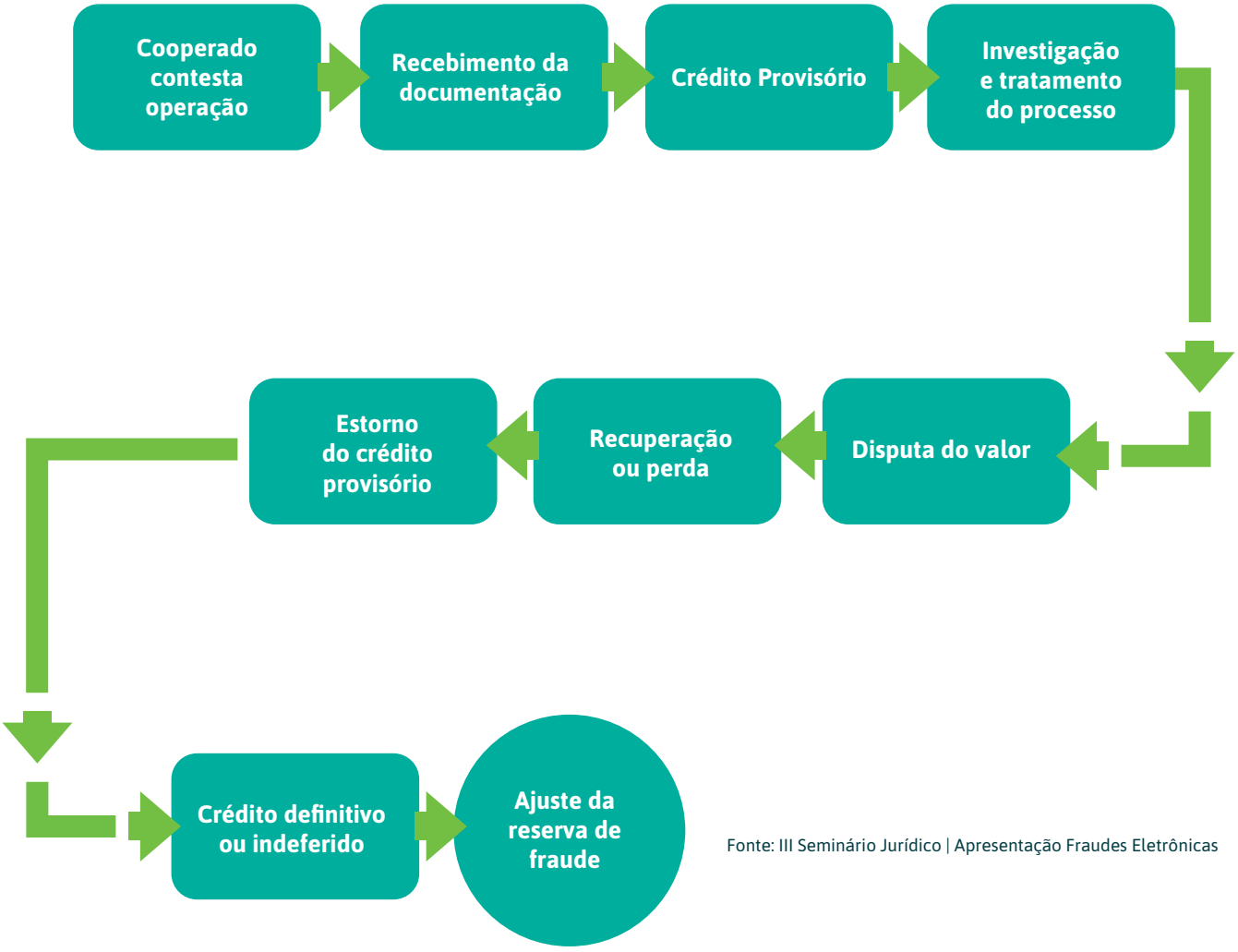
ATRIBUIÇÕES		
1		**OBRIGATÓRIO** Combate e Preveção à Fraude - AVANÇADO ONL 117101
2		**OBRIGATÓRIO** Segurança da Informação ONL 7103
3		**OBRIGATÓRIO** Lei Geral de Proteção de Dados - LGPD ONL 155105
4		**OBRIGATÓRIO** Classificação e Proteção de Arquivos Office 365 ONL 147106
5		**OBRIGATÓRIO** Engenharia Social ONL 143125
6		**OBRIGATÓRIO** Guia de Informação e Boas Práticas de Segurança nas agências ONL 98102
7		**OBRIGATÓRIO** Webinar: Ações de Prevenção e Combate a Fraudes ONL 151110

FLUXOS OPERACIONAIS

Esquema simplificado da atuação da Credi no processo de fraude

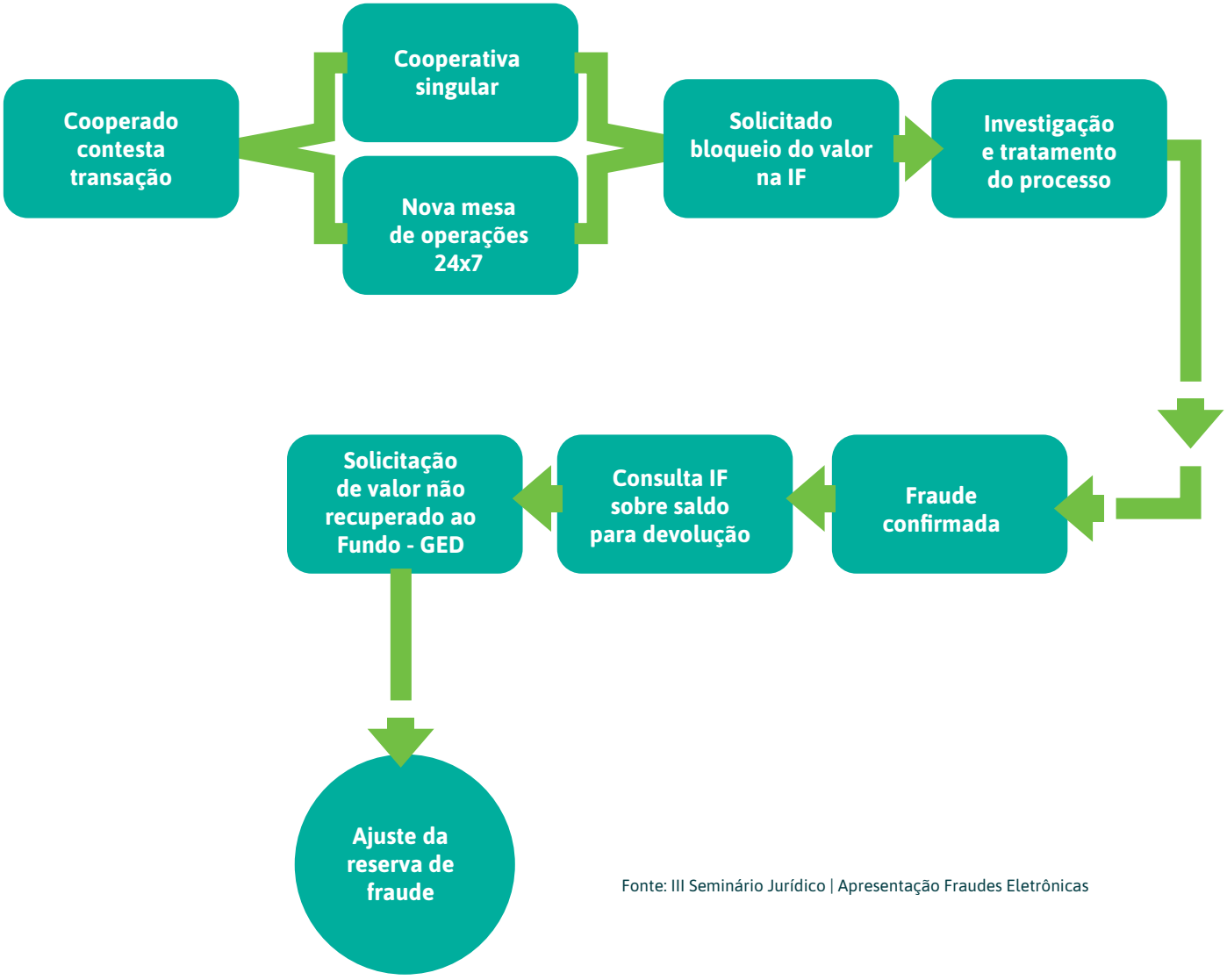


Fluxo de ressarcimento Produto cartão



Fonte: III Seminário Jurídico | Apresentação Fraudes Eletrônicas

Fluxo de ressarcimento Canais



Fonte: III Seminário Jurídico | Apresentação Fraudes Eletrônicas

BLOQUEIO DE RECURSO

CCI - 258/2020 - Sicoob Confederação

1. A partir de 1°/8/2022, os atendimentos relacionados às ocorrências de fraudes serão realizados da seguinte maneira:
a) das 8h às 9h, pela Área de Prevenção a Fraudes, por meio do telefone **(61) 3771- 6500**;
b) das 9h às 18h, pela Central de Atendimento à Cooperativa, por meio do telefone (**61) 3771-6600**, opção 9, item 3.
2. Ressaltamos que o contato será exclusivo para as cooperativas.
3. O número **(61) 3217-8000 será desativado**.

Fora do horário comercial a solicitação de bloqueio deverá ser realizada por meio do seguinte endereço eletrônico:

Analisedefraude@sicoob.com.br *

Com cópia (Cc) para
prevencaoafraudes@sicoobcrediminas.com.br

* Por este e-mail deverão ser formalizados posteriormente os contatos efetuados por telefone

ATENDIMENTO AO COOPERADO

CCI - 736/2021 - CCS

O canal de atendimento ao cooperado relativo à prevenção à Fraudes na Central de Atendimento ao Sicoob está disponível 24 horas por dia em todos os dias da semana e feriados

0800 724 4420

Opção 5

Golpes
Formalização da ocorrência

Caso o cooperado informe à Cooperativa ter sido vítima de golpe, o mesmo deverá ser orientado que aquela situação não é de responsabilidade da cooperativa e solicitar os documentos necessários:
Boletim de Ocorrência e carta de próprio punho.
Embora, não seja sua responsabilidade é obrigação da cooperativa envidar esforços para reaver os valores, solicitando o bloqueio dos recursos de acordo com o fluxo apresentado.

Essas ocorrências também deverão ser cadastradas no módulo PCF e reportadas aos seguintes endereços eletrônicos:

Analisedefraude@sicoob.com.br

Com cópia (Cc) para
prevencaoafraudes@sicoobcrediminas.com.br

Identificação de potenciais golpes ou fraudes por colaboradores da Singular ou cooperados deverá a Cooperativa notificar o CCS e a Central nos seguintes endereços eletrônicos:

PrevencaoaFraude@sicoob.com.br

Com cópia (Cc) para
prevencaoafraudes@sicoobcrediminas.com.br

Cadastro ocorrência de fraude

Antes de iniciar o cadastro da ocorrência de fraude a cooperativa deve colher do cooperado a documentação necessária relacionadas na CCI 258/2018 do CCS, quais sejam:

A **Boletim de Ocorrência Policial – BO registrado pelo cooperado;**

B **Carta, de próprio punho, elaborada pelo cooperado, se identificando (nome e número da conta) e descrevendo o fato ocorrido;**

C **Comprovante da transação, gerado por colaborador da própria cooperativa, acessando o SSPB ou Módulo Conta Corrente → Movimentação → Agendamento.**

Importante!
Cabe à Cooperativa orientar o Cooperado para obtenção desses documento

Cadastro ocorrência de fraude

As instruções para realização do cadastramento da ocorrência de fraude estão disponíveis no MANUAL DO USUÁRIO: MÓDULO PCF – OCORRÊNCIA DE FRAUDE

Uma ocorrência de fraude deve ser cadastrada para um único número de conta do cooperado. Portanto, caso o cooperado tenha sido vítima em duas ou mais contas distintas, será necessária a abertura de duas ou mais ocorrências correspondentes.

Se o cooperado foi vítima de uma mesma modalidade de fraude, como por exemplo, invasão de máquina, mas as saídas de recursos da mesma conta foram em dias diferentes, todas as transações devem ser cadastradas na mesma ocorrência de fraude, independente da data de ocorrência dela.

No entanto, se no dia "X" o cooperado foi vítima de "invasão de máquina" e no dia "Y" foi vítima de venda falsa, a cooperativa deve registrar 2 ocorrências distintas, mesmo que a conta e data de ocorrência sejam as mesmas, pois o que prevalece é o registro do tipo de fraude. Portanto, cada ocorrência dessa deve ser classificada com a respectiva modalidade (invasão de máquina e venda falsa).

Uma ocorrência de fraude corresponde no sistema a um número identificador único, denominado de "ID da Ocorrência", dentro de uma ocorrência podem existir mais de uma saída de recurso, portanto cada transação deve ser cadastrada na mesma ocorrência de fraude. Desse modo, cada transação possuirá um identificador único denominado de "Número de processo".

Cadastro ocorrência de fraude

As ocorrências de fraude serão efetivamente tratadas após o cadastramento no PCF. O contato telefônico e e-mail se destinam apenas à dar celeridade ao processo possibilitando o CCS de entrar em contato com a outra IF e garantir o bloqueio "sob confiança". E, caso a cooperativa não cadastre a ocorrência no PCF ou demore, esse bloqueio pode ser desfeito.

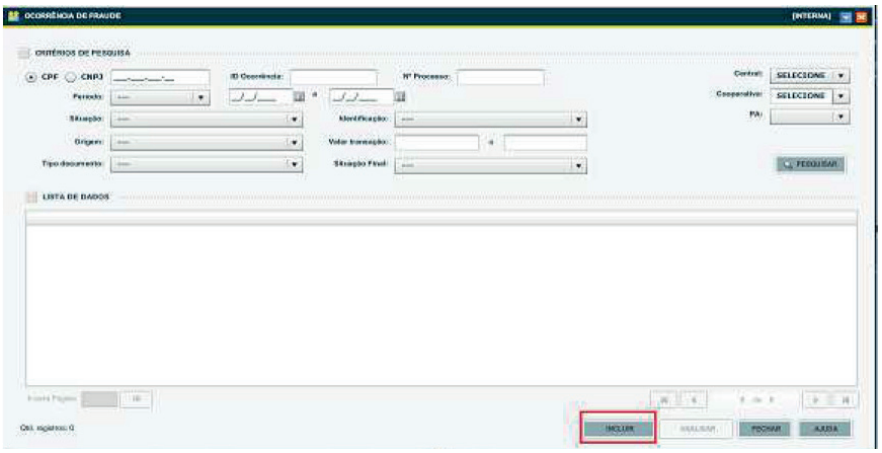
Por meio do menu **OCORRÊNCIA DE FRAUDE** o usuário poderá realizar o cadastro da ocorrência de fraude. Para realizar o procedimento citado, deverá acessar o módulo PCF, em seguida selecionar o menu **"PCF" → "Ocorrência de Fraude"**.

O **módulo PCF** está disponível no **Sisbr 2.0** e o acesso poderá ser realizado apenas por colaboradores com permissão, em função dos cargos que ocupam.

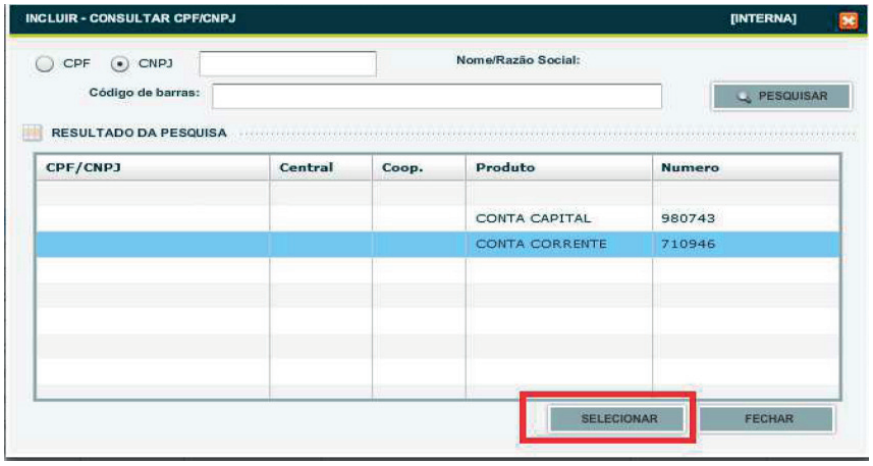
REGISTRO DAS OCORRÊNCIAS

Cadastro ocorrência de fraude

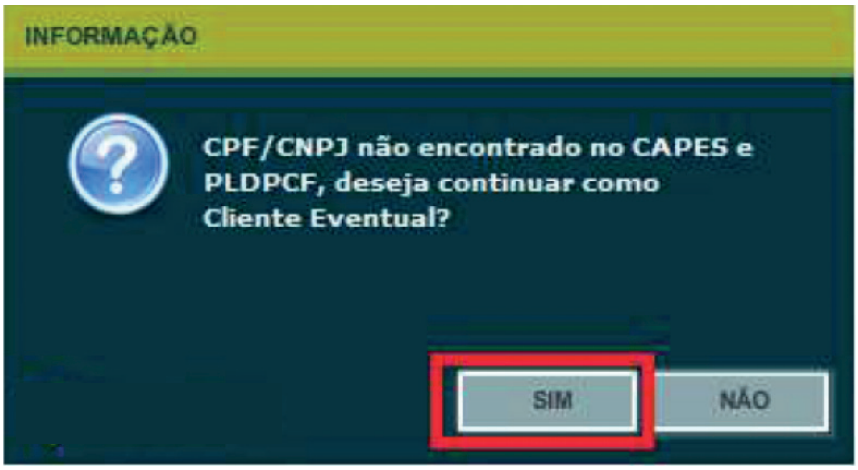
Nesta tela apresentada, o usuário deve informar o número do CPF/CNPJ do cooperado e clicar em pesquisar.



Caso o CPF/CNPJ de um cliente não for encontrado na base do CAPES, a funcionalidade emitirá o alerta abaixo.



Nesta tela de alerta selecionar a opção “SIM”.

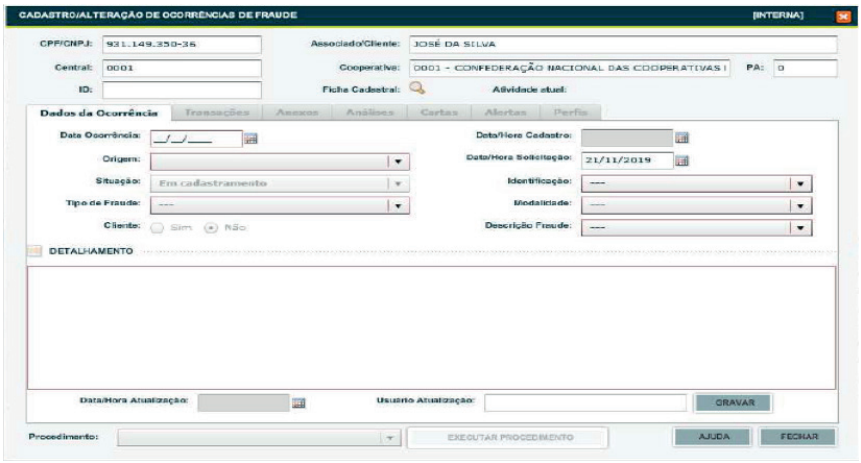


Informar o nome do cliente, número da central, número da cooperativa responsável pelo atendimento e clicar no botão prosseguir.

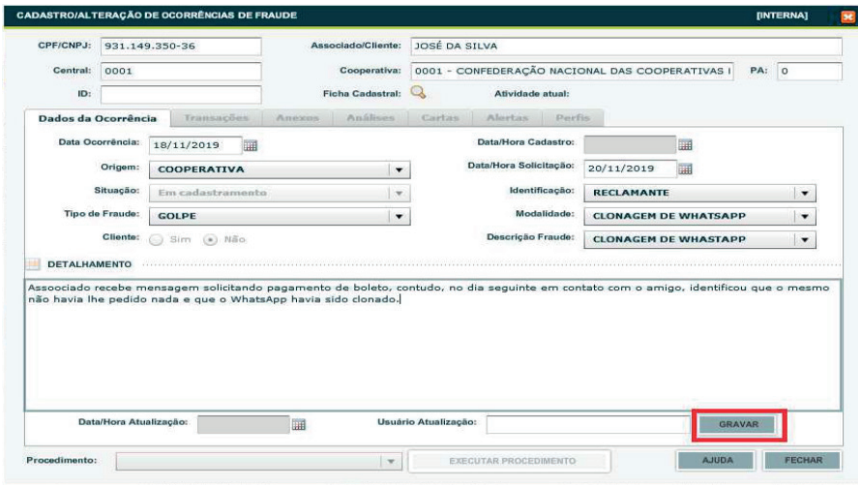
REGISTRO DAS OCORRÊNCIAS

Cadastro ocorrência de fraude

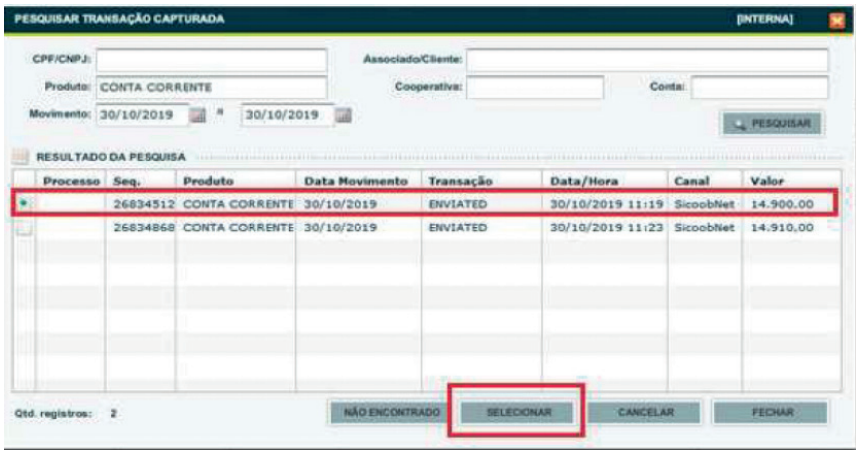
Nesta aba “Dados da Ocorrência” deverão ser preenchidas as informações relacionadas a contestação.



Após preencher todos os campos de “tipo de fraude”, “modalidade”, “descrição da fraude” e “detalhamento” o usuário deve clicar no botão “gravar”.

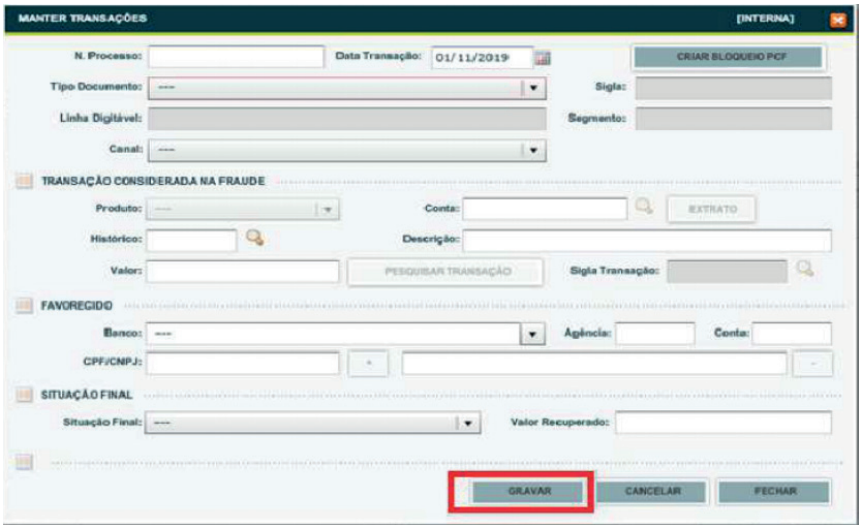


Para adicionar uma transação financeira na ocorrência o usuário deve utilizar o botão.



Cadastro ocorrência de fraude

Se por algum problema de sistema a transação contestada não aparecer na pesquisa por meio da captura automática, o usuário deverá utilizar o botão “não encontrado”, para cadastro manual.



As transações inseridas manualmente ficarão com um destaque em vermelho para análise da Confederação. O objetivo é que todas as transações sejam capturadas automaticamente para reduzir a possibilidade de erro. Assim, a inclusão manual só deve ocorrer em casos pontuais de não captura automática, portanto em hipótese alguma esta opção deverá ser utilizada para cadastrar transações já capturadas.

Em caso de cliente eventual, por ele não dispor de produto no Sicoob, a tela “Manter transações”, para cadastro manual, será habilitada automaticamente para preenchimento dos dados da transação.

Encerramento de ocorrência de fraude

Contestações de Cooperativas:
O CCS encaminhará ao Banco a Carta de Responsabilidade e com base na resposta encaminhada pela IF, irá preencher a situação final do processo. A cooperativa será notificada, por e-mail.

Contestações de outros Bancos:
Com base na existência de saldo oriundo da transação contestada, a cooperativa deve realizar uma análise de perfil e do cadastro do cooperado e aplicar a "política do conheça seu associado/cliente" e após a conclusão desta análise deve-se preencher a "situação final" do processo.

Após selecionar a situação final e gravar, na aba anexos, estarão disponíveis os documentos da ocorrência e os anexos no CAPES.

Na sequência, na aba "análises", estarão disponíveis todas as análises realizadas pelo CCS. No caso de contestações encaminhadas por outros Bancos, a cooperativa deve incluir uma nova análise justificando a devolução ou não do recurso e "encaminhar para análise no CCS" para responder o Banco que contestou a transação. O CCS irá responder o Banco e na sequência encerrará a ocorrência de fraude.

Para as ocorrências encaminhadas pela Cooperativa, o CCS irá notificar a Cooperativa com a resposta do Banco e na sequência encerrar a ocorrência.

Após a ocorrência encerrada, ela ficará disponível somente na "consulta gerencial". Caso a cooperativa necessite reabrir uma ocorrência já encerrada, a solicitação deve seguir por e-mail para a Área de Prevenção e Combate à Fraude.

Considerações importantes sobre o cadastro de ocorrência de fraudes

Para cada transação gravada, o sistema atribuirá um número de processo correspondente.

Em caso de documentação pendente de envio a ocorrência será devolvida à cooperativa para correção.

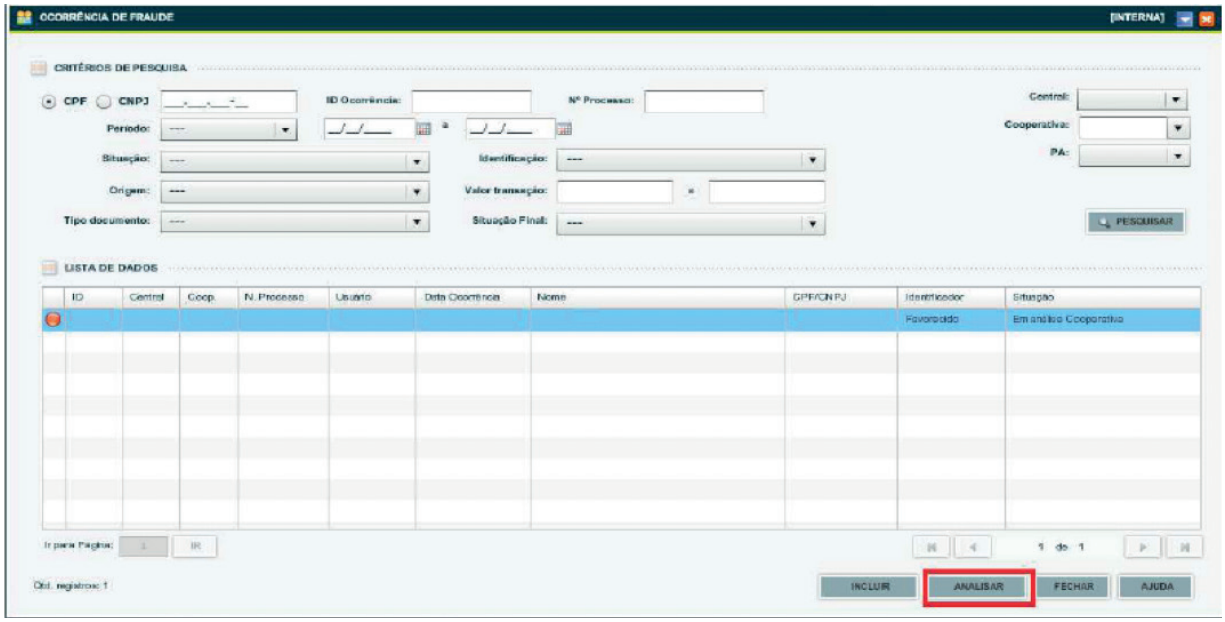
Após recebimento da ocorrência de fraude e estando correto o cadastro realizado pela cooperativa, a Área de Prevenção e Combate à Fraude emite e encaminha para a instituição financeira envolvida a Carta de Responsabilidade solicitando a devolução do valor. Conforme CCI 241/2019, a cooperativa não possui acesso a Carta de Responsabilidade.

O andamento de cada processo pode ser acompanhado consultando pelo número informado ou quando houver qualquer alteração os usuários com permissão nos fluxos serão notificados por e-mail.

Encerramento de ocorrência de fraude

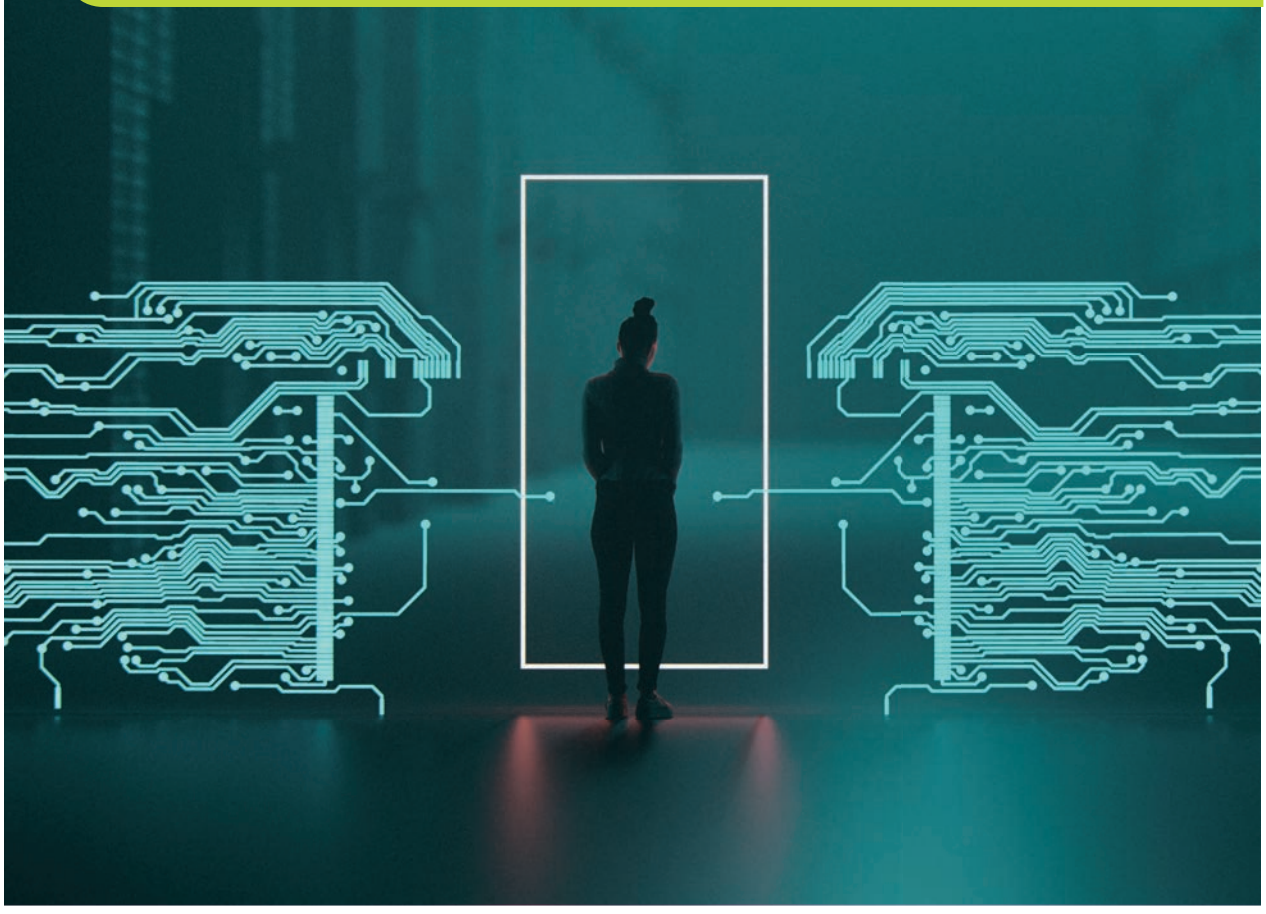
A Área de Prevenção e Combate à Fraude da Confederação é responsável por recepcionar as contestações de fraudes vindas de outros bancos cujos recursos foram creditados em cooperativas do Sicoob

Quando for recebida uma ocorrência ela será cadastrada no módulo PCF e os usuários com permissão no fluxo, serão notificados por e-mail e deverão abrir a ferramenta para realizar o tratamento. Essa contestação ficará na tela inicial da ferramenta com a marcação em vermelho até ser aberta. Para tratar a ocorrência o usuário deverá clicar no botão “analisar”.



Após a análise o responsável irá preencher a situação final.

Quando a Cooperativa pode atuar em casos de fraude sem a intervenção do CCS?



CANCELAMENTOS

DOC

Para **DOC** até o fechamento da cooperativa e de convênios, desde que não sejam do tipo baixa on-line, ou de Secretarias Estaduais de Fazendas.

As IC estão disponíveis no PORTAL DE SERVIÇOS DO CCS

Ocorrências passíveis de cancelamento no mesmo dia ic 14108

Por meio do menu CANCELAMENTO, o usuário poderá consultar e cancelar pagamento de convênios e/ou transferência via DOC e TED, no caso de solicitação do cooperado, por iniciativa da Cooperativa ou em caso de suspeita de fraude.

O cancelamento poderá ser realizado, mesmo que a transação esteja na situação “Efetivado”, desde que, os documentos não tenham sido transmitidos, por meio das remessas diárias ou de remessa on-line.

As Cooperativas Centrais que optarem por realizar o cancelamento dessas transações em suas Cooperativas singulares, deverão por meio do módulo CTA, executar a replicação do usuário.

Para realizar os procedimentos citados, o usuário deverá acessar o módulo Conta-Corrente, em seguida, selecionar o menu “Movimentação” → “Agendamento” → “Cancelamento”.

IC 6682

Para títulos, desde que os documentos não tenham sido transmitidos por meio das remessas diárias ou de remessa on-line, conforme contido na CCI 024/2019 - Procedimentos de envio de 'Registro Automático de Nossa Remessa Cobrança' e 'Exclusão de Boletos.

Ocorrências passíveis de cancelamento no mesmo dia ic 14108

Por meio do menu TÍTULOS, o usuário poderá realizar a consulta e agendamento de títulos pelo Sisbr2.0.

Título ou boleto bancário são documentos emitidos por alguém que presta serviços ou vende produtos e que têm como função a cobrança destes, geralmente podem ser pagos em qualquer instituição financeira conveniada, até o seu vencimento.

Para realizar os procedimentos citados, o usuário deverá selecionar o menu "Movimentação" → "Agendamento" → "Títulos".

IC 5403

Faturas de cartão de crédito

As faturas de cartões de crédito Sicoob, por serem de baixa on-line, não são passíveis de cancelamento. Havendo a necessidade de cancelamento, a cooperativa deverá solicitar o estorno do pagamento, realizado pelo cooperado, por meio da Central de Suporte e Serviços do Sicoob, siga o caminho: Atendimento à Cooperativa → Cartões → Operacional → Faturamento → Faturas e boleto.

Comprovantes de transações

Os comprovantes para as transações na situação efetivados são emitidos como documentos pagos, portanto, quando a solicitação de cancelamento for por erro ou pagamento em duplicidade, por solicitação do cooperado, a cooperativa deverá solicitar que ele assine o termo de responsabilidade pelo cancelamento e a inutilização do comprovante, com o objetivo de evitar possíveis questionamentos judiciais.

Transações canceladas

Para ocorrência de fraude com transação(ões) cancelada(s), a cooperativa deverá proceder conforme item 1.2.3 - Coleta da documentação necessária e registrar a ocorrência de fraude. (Conforme IC 14068)

IC 14018

NORMATIVOS

CCI - 607/2021 - CCS | Pix, TED e Boletos de Cobrança

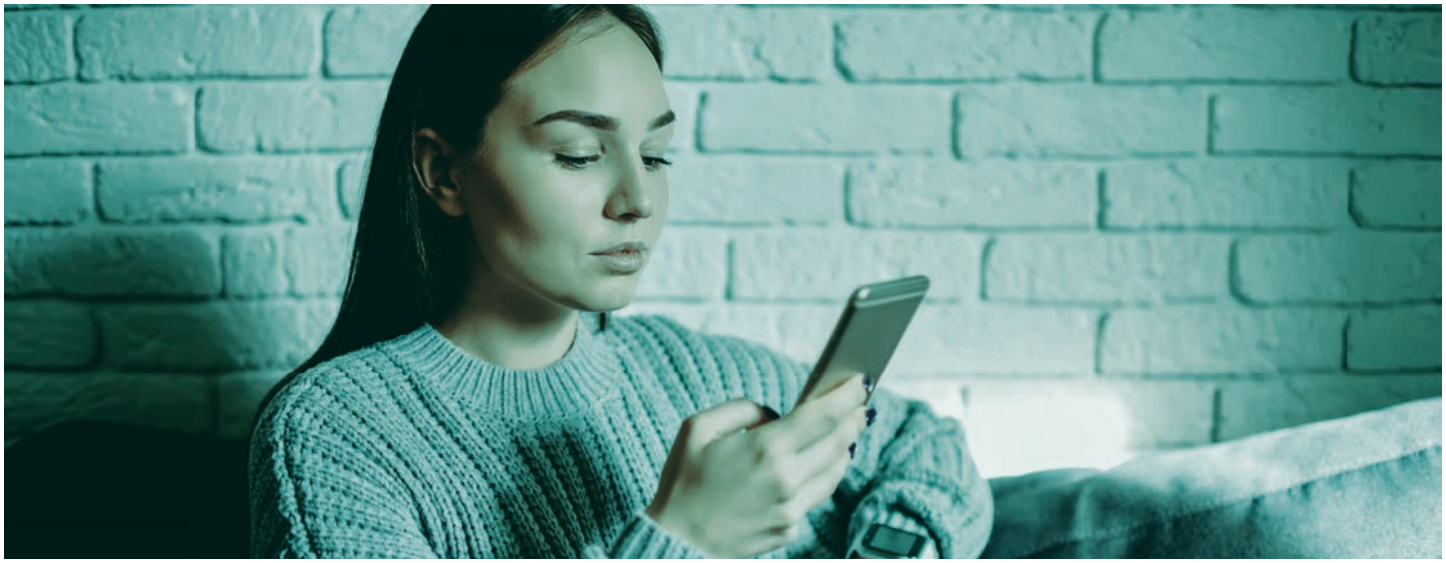
Foram disponibilizadas na Plataforma de Combate a Fraudes (PCF) as seguintes funcionalidades:

A serviço responsável por avaliar Pix enviados pelos cooperados nos canais de atendimento que possuam características de comprometimento de legitimidade;

B serviço responsável por avaliar boletos de cobrança pagos pelos cooperados nos canais de atendimento que possuam características de comprometimento de legitimidade.

Atualmente, todas as transações Pix passam pela validação da Plataforma de Combate a Fraudes (PCF) para verificar se o CPF ou CNPJ envolvido na operação possui restrição por suspeita de fraude. Em caso positivo, a transação não é enviada/recebida e ocorre automaticamente o bloqueio das credenciais de acesso do cooperado aos canais digitais.

CCI - 607/2021 - CCS | Pix, TED e Boletos de Cobrança



PIX E BOLETOS DE COBRANÇA

As transações de Pix ou boletos de cobrança serão submetidas a nova avaliação na PCF, de acordo com critérios e regras prudenciais e de identificação de vícios que possam comprometer a legitimidade da transação.

No caso de Pix, se houver indícios de comprometimento, será emitido um alerta e a transação será retida por até 30 minutos, aguardando decisão da cooperativa para aprovação ou cancelamento. Se a cooperativa não realizar nenhuma ação (aprovação ou cancelamento) no prazo citado, o Pix será automaticamente cancelado.

No caso de boletos de cobrança, se houver indícios de comprometimento, será emitido um alerta e a cooperativa deverá proceder a análise e, caso não seja realizada nenhuma ação (aprovação ou cancelamento), o boleto não será compensado/liquidado e ocorrerá o estorno da transação na conta do cooperado.

Os demais Pix ou boletos que não forem alertados seguem o fluxo normal de envio para o destinatário/beneficiário.

Para análise das transações de Pix e boletos, serão disponibilizadas funcionalidades na PCF para visualização e detalhamento dos alertas, que apresentarão os dados relacionados ao perfil de movimentação do cooperado remetente da operação.

NORMATIVOS

Regulamento do fundo para ressarcimento de fraudes externas e perdas operacionais do Sicoob

O Fundo para Ressarcimento de Fraudes Externas e Perdas Operacionais do Sicoob foi criado na Assembleia Geral Ordinária do Sicoob Confederação de 11/3/2015, conforme art. 28, § 1°, da Lei n° 5.764/1971 e art. 23 do Estatuto Social do Sicoob Confederação.

O Regulamento do Fundo de Ressarcimento foi atualizado em 20/12/2022 por meio da Resolução CCS 138028.

O Fundo tem como objetivo reunir recursos financeiros para ressarcimentos às cooperativas de eventuais prejuízos, nos termos e limites deste Regulamento, decorrentes de:

I. fraudes nos canais eletrônicos de atendimento, mediante violação ou acesso não autorizado, ocorridos nas entidades do Sicoob, doravante denominados Fraudes Externas, no plural ou no singular;

II. erros e/ou falhas nos processos sistêmicos sob reponsabilidade do CCS, que possam afetar as cooperativas, doravante denominados Perdas Operacionais, no plural ou no singular.

Formação do Fundo

O saldo do Fundo observa o piso de 12 (doze) vezes e o teto de 18 (dezoito) vezes, calculados sobre a média mensal das solicitações de ressarcimento de fraudes e perdas operacionais ocorridas nos 6 (seis) meses anteriores à data-base de cálculo.
A contribuição total mensal para o Fundo observa a tabela a seguir, multiplicando-se o Fator da Média Mensal de Fraudes e Perdas pela média mensal das solicitações de ressarcimento de fraudes e perdas operacionais dos últimos 6 (seis) meses, considerando o saldo do fundo em relação ao teto.

% de reserva constituída	Fator da média mensal de fraudes e perdas
até 25%	2
até 50%	1,75
até 75%	1,5
até 100%	1,25
> 100%	1

Para o cálculo do valor da contribuição mensal das cooperativas singulares para o Fundo, será utilizada a média mensal da movimentação financeira dos últimos 6 (seis) meses como base, considerando a participação de cada cooperativa singular na movimentação.
A movimentação financeira considera as transferências (saídas) realizadas internamente ou para outras instituições nas modalidades: TED, DOC, Intercredis, PIX, convênio, débito automático e cobrança.
Serão segregados 10% (dez por cento) da contribuição mensal da cooperativa singular, que passará a ser acumulada e controlada separadamente, para ressarcimento da cooperativa aos seus cooperados em eventos de golpes, à sua discricionariedade.
A cooperativa singular, nos ressarcimentos realizados conforme o previsto no art. 6°, poderá ficar com saldo negativo em até 100% da contribuição mensal média dos últimos 6 (seis) meses.
Para a recomposição do saldo negativo, a contribuição mensal da cooperativa será de 130% (cento e trinta por cento) do valor previsto para o mês.

Regulamento do fundo para ressarcimento de fraudes externas e perdas operacionais do Sicoob

Os recursos arrecadados serão utilizados para ressarcimento às cooperativas que tiverem perdas decorrentes de:

I. Fraudes Externas, até o limite padronizado para as respectivas transações;

II. Perdas Operacionais.

O valor mínimo de Perda Operacional ou de Fraude Externa a ser coberto pelo Fundo é de R$ 100,00 (cem reais).

O Banco Sicoob efetuará o repasse ao Fundo dos recursos mediante débito nas contas das cooperativas centrais, com base em relatório de valores individualizado por cooperativas, a ser apresentado pelo CCS.

Fica estabelecida carência de 6 (seis) meses para a cooperativa, contada da sua primeira contribuição, ter direito ao ressarcimento de perdas por Fraudes Externas.

Nenhum ressarcimento de perdas por Fraudes Externas será concedido antes do cumprimento da carência e a ocorrência da Fraude Externa a ser ressarcida deverá ser posterior a essa data.

Os recursos financeiros para ressarcimento de Fraudes Externas destinam-se à reparação das cooperativas que reembolsaram seus cooperados por perdas com operações financeiras no ambiente do Internet Banking (Sicoobnet) e nos demais canais de atendimento do Sicoob, realizadas por ação de malware ou mediante violações ou acessos não autorizados, tais como: fraudes eletrônicas por meio da obtenção de identidade e credencial de acesso por meio de interceptação de informações nos canais eletrônicos de atendimento.

Regulamento do fundo para ressarcimento de fraudes externas e perdas operacionais do Sicoob

Os recursos destinados a ressarcimento de Fraudes Externas não se destinam ao ressarcimento de perdas decorrentes de:

• fraudes internas;

• fraudes externas ocorridas em produtos e canais de uso específicos de cooperativas, por exemplo: Ura, VipService;

• erro operacional;

• eventos físicos que gerem prejuízos para as cooperativas ou cooperados

• inobservância de decisões, políticas, diretrizes, regulamentações, normas e procedimentos emitidos pelo CCS, inclusive de contratos e manuais relativos aos produtos e serviços disponibilizados;

• não cumprimento de controles e limites padronizados estabelecidos pelo CCS para os processos de negócio;

• transações fraudulentas realizadas durante o período de liberação, por parte da cooperativa, de regras de prevenção a fraudes implementadas pelo CCS;

• pagamento de cheque falso, adulterado ou com erro na assinatura;

• operações legítimas realizadas pelo próprio cooperado;

• operações financeiras realizadas por meio de cartão (débito ou crédito) clonado, cujo assunto é tratado no Fundo específico para cartões;

• pagamento de boleto falso por falha humana na confirmação do número do banco e dados do favorecido nos canais de atendimento, exceto boletos relacionados a produtos do Sicoob;

Regulamento do fundo para ressarcimento de fraudes externas e perdas operacionais do Sicoob

• operações financeiras realizadas com documentação falsa, inclusive fraude originada de abertura de conta com documentação falsa, exceto a associação digital realizada com documentação falsa, devido a falha no processo de avaliação dos documentos de identificação, sendo ressarcido de acordo com normativo específico complementar, limitado aos valores dos limites de cheque especial e cartão de crédito padrão concedidos pelo App;

• fraudes ocorridas em redes de parceiros, por exemplo: rede Banco 24 Horas, rede Cirrus;

• casos fortuitos ou força maior;

• vendas falsas ou falsos leilões, clonagem/golpes de WhatsApp e falso funcionário/falsa central de atendimento;

• fraudes em que as operações foram realizadas mediante uso do QR Code para autorização/aprovação;

• operações realizadas mediante autorização de colaboradores da cooperativa.

Os recursos destinados a ressarcimento de Perdas Operacionais não se destinam ao ressarcimento de perdas decorrentes de:

• Falha, deficiência ou inadequação nos processos internos, pessoas e sistemas ou eventos internos sob responsabilidade das cooperativas;

• lucro cessante;

• prejuízo por queda de link, casos fortuitos ou força maior;

• horas-extras realizadas para continuidade das atividades da cooperativa;

• ação ou omissão de cooperativa ou de empresa ou entidade do Sicoob,

em que o evento de perda tenha sido originado. Nesse caso cumprirá à própria cooperativa, entidade ou empresa do Sicoob, assumir o encargo;

• utilização indevida de software ou hardware por parte de cooperativa ou de empresa ou entidade do Sicoob que acabe por gerar dano financeiro aos associados pelo não atendimento aos normativos internos;

• assaltos, violências físicas, roubos, furtos ou qualquer outro evento que não tenha conotação de perda nos termos definidos no inciso II art. 2º do presente Regulamento, assim como a não realização de transações em decorrência desses eventos;

• inobservância de políticas, procedimentos, manuais, normas e orientações emitidas pelo CCS;

• não cumprimento de controles e/ou procedimentos padronizados;

• interrupção do serviço de energia na região da cooperativa, da empresa ou entidade do Sicoob;

• Sicoob como demandante;

• ocorrência com mais de 360 dias no momento do registro da solicitação no Sistema GED.

Art. 20 Para ressarcimento de eventuais prejuízos pelo Fundo, a cooperativa deve estar em situação regular com as contribuições.

Art. 21 Para ressarcimento de eventuais prejuízos decorrentes de Fraudes Externas, a cooperativa, além de cumprir o disposto no art. 19, deve:

I. ter registrado a ocorrência na ferramenta específica, Sisbr PCF, e

cumprido os procedimentos do protocolo de devolução de recursos;

II. para as ocorrências tratadas via protocolo de devolução de recursos sem resposta da instituição sobre a possibilidade de recuperação a cooperativa pode realizar a solicitação em até 10 dias após a emissão da carta de responsabilidade;

III. se a solicitação de ressarcimento for encaminhada via Plataforma de Gestão de Documentos (GED), anexar os arquivos digitalizados por:

a) formulário de pedido de ressarcimento (disponível na opção Download de anexos () deste Regulamento, na intranet do Sicoob) devidamente preenchido e assinado por, pelo menos, um diretor da cooperativa e acompanhado da documentação comprobatória

b) formulário de tratamento de ocorrência de fraude (disponível na opção Download de anexos ( ) deste Regulamento, na intranet do Sicoob) devidamente preenchido e assinado por empregado da cooperativa;

c) relatório de investigação de incidentes ou parecer emitido pela Área de Segurança Cibernética do CCS, ou pelas áreas técnicas ou de desenvolvimento da Diretoria de Tecnologia da Informação do CCS, nos casos de operações realizadas em meios eletrônicos, em que o cooperado conteste operações realizadas em equipamentos cadastrados, em que houver indícios de invasão ou da existência de softwares maliciosos.

Art. 22 Para ressarcimento de eventuais prejuízos decorrentes de Perdas Operacionais, a cooperativa, além de cumprir o disposto no art. 19, deverá encaminhar a solicitação de ressarcimento pela Plataforma de Gestão de Documentos (GED), e:

I. anexar, no campo do GED Formulário de Pedido de Ressarcimento, o arquivo digitalizado do formulário de pedido de ressarcimento (disponível na opção Download de anexos () deste Regulamento, na intranet do Sicoob) devidamente preenchido, contendo um breve relato que explique de forma clara e consistente a ocorrência, assinado por pelo menos um diretor da cooperativa;

II. anexar a documentação de suporte que comprove o relatado no item anterior, devendo conter no mínimo:
a) relatório de atendimento do Portal de Serviços do CCS que contenha a confirmação da ocorrência, emitida por empregado da área de Atendimento a Cooperativas do CCS, ou parecer emitido pela área técnica de TI ou área técnica de negócios, que deverá ser anexado no campo do GED Relatório da Área de Suporte Operacional;

b) comprovação do valor do ressarcimento solicitado, contendo os valores individuais e o respectivo total, incluindo a memória de cálculo e comprovantes de pagamentos, de agendamentos, recibos etc., que devem ser anexados no campo GED Extrato da Conta Corrente.

Art. 23. Ocorrendo o ressarcimento, pelo Fundo, de evento de perda operacional abrangida por este Regulamento, a cooperativa do Sicoob deverá adotar todas as medidas necessárias para a recuperação do prejuízo indenizado.

Art. 24 - Responsabilidades

Nos casos de análise sobre possível ressarcimento de perdas decorrentes de Fraudes Externas compete:

I. à cooperativa:

a) reembolsar o cooperado;
b) estar em dia com as contribuições para o Fundo;
c) cumprir os requisitos mínimos estabelecidos no art. 20 deste Regulamento;
d) solicitar o ressarcimento conforme descrito no art. 20 deste Regulamento.

II. à Área de Segurança Cibernética do CCS:

a) emitir relatório de investigação de incidentes.

III. à Área de Prevenção a Fraudes do CCS:

a) examinar a documentação encaminhada pela entidade requisitante;
b) emitir parecer para subsidiar decisão da Diretoria Executiva do CCS;
c) aprovar o ressarcimento, conforme alçada;
d) detectar movimento específico que ocasione aumento de perdas com fraudes ou nova modalidade de fraude;

e) verificar a necessidade de atualização do presente Regulamento e propor alteração à Diretoria Executiva do CCS;

f) avaliar e promover ações e projetos relativos à prevenção e combate a fraudes;

g) apresentar à Diretoria Executiva e ao Conselho de Administração do Sicoob Confederação, semestralmente, prestação de contas sobre a utilização dos recursos específicos para ressarcimento de Fraudes Externas do Sicoob.

IV. à Diretoria Executiva do CCS:

a) aprovar o ressarcimento, conforme alçada;

b) analisar proposta de alteração deste Regulamento, encaminhando-a para deliberação do Conselho de Administração do CCS.

V. ao Conselho de Administração do Sicoob Confederação:

a) deliberar sobre ações e projetos apresentados, relativos à prevenção e combate a fraudes;

b) deliberar sobre proposta de alteração deste Regulamento.

Art. 25 - Responsabilidades

Nos casos de análise sobre possível ressarcimento de Perdas Operacionais, compete:

I. à cooperativa:

a) reembolsar o cooperado;
b) estar em dia com as contribuições para o Fundo;
c) cumprir os requisitos mínimos estabelecidos no art. 20 deste Regulamento;
d) solicitar o ressarcimento conforme descrito no art. 20 deste Regulamento.

II. à Área de Risco Operacional e GCN do CCS:

a) examinar a documentação encaminhada pela cooperativa requisitante;

b) identificar e tratar o risco que deu origem à perda operacional;

c) registrar a perda operacional na Plataforma de Gestão de Processos e Controles (PGPC) do Sisbr 2.0;
d) emitir parecer para subsidiar a decisão da Diretoria Executiva do CCS;

e) aprovar o ressarcimento, conforme a alçada;

f) propor à Diretoria Executiva do CCS alteração deste Regulamento, quando for o caso;

g) apresentar à Diretoria Executiva e ao Conselho de Administração do Sicoob Confederação, semestralmente, prestação de contas sobre a utilização dos recursos específicos para ressarcimento de Perdas Operacionais.

III. às Superintendências do CCS:

a) analisar e aprovar o parecer emitido pelas áreas de negócios ou de Tecnologia da Informação (TI).

IV. à Diretoria Executiva do CCS:

a) aprovar ressarcimento, conforme alçada;

b) analisar proposta de alteração deste Regulamento e encaminhá-la para deliberação do Conselho de Administração do Sicoob Confederação.

IV. ao Conselho de Administração do Sicoob Confederação:

a) deliberar sobre os recursos interpostos;

b) aprovar o ressarcimento conforme alçada;

c) deliberar sobre proposta de alteração deste Regulamento.

AUTORIZAÇÃO DO PAGAMENTO E ALÇADAS

O pagamento, pelo Fundo, de ressarcimento decorrente de Fraudes Externas será autorizado:

• pelo Gerente da Área de Prevenção a Fraudes do CCS e, na sua ausência, pelo Superintendente de Controles do CCS, quando o valor estiver entre

R$ 100,00 (cem reais) e R$ 10.000,00 (dez mil reais);

• pelo Superintendente de Controles do CCS e, na sua ausência, pelo Superintendente de Gestão Integrada de Riscos do CCS, e pelo Gerente da Área de Prevenção a Fraudes do CCS, ou substitutos, quando o valor a ser ressarcido estiver entre R$ 10.000,01 (dez mil reais e um centavo) e R$ 30.000,00 (trinta mil reais);

• pelo Diretor de Riscos e Controles do CCS e pelo Superintendente de Controles do CCS e, na sua ausência, pelo Superintendente de Gestão Integrada de Riscos do CCS, ou substitutos, quando o valor a ser ressarcido estiver entre R$ 30.000,01 (trinta mil reais e um centavo) e R$ 100.000,00 (cem mil reais);

• por 2 (dois) diretores executivos do CCS, quando o valor do ressarcimento for entre R$ 100.000,01 (cem mil reais e um centavo) e R$ 300.000,00 (trezentos mil reais), sendo eles o Diretor de Riscos e Controles e o de Operações do CCS;

• pela alçada da Diretoria Executiva do CCS, quando o valor do ressarcimento for superior a R$ 300.000,00 (trezentos mil reais).
O pagamento, pelo Fundo, de ressarcimento decorrente de Perdas Operacionais será autorizado:

• pelo Gerente da Área de Risco Operacional e, na sua ausência, pelo Superintendente de Gestão Integrada de Riscos, quando o valor estiver entre R$ 100,00 (cem reais) e R$ 10.000,00 (dez mil reais);

• pelo Superintendente Gestão Integrada de Riscos do CCS e, na sua ausência, pelo Superintendente de Controles do CCS, e pelo responsável pela Área de Risco Operacional e GCN do CCS, ou substitutos, quando o valor a ser ressarcido estiver entre R$ 10.000,01 (dez mil reais e um centavo) e R$ 30.000,00 (trinta mil reais);

• pelo Diretor de Riscos e Controles e pelo Superintendente de Gestão Integrada de Riscos do CCS e, na sua ausência, pelo Superintendente de Controles do CCS, ou substituto, quando o valor a ser ressarcido estiver entre R$ 30.000,01 (trinta mil reais e um centavo) e R$ 100.000,00 (cem mil reais);

• por 2 (dois) diretores executivos do CCS, quando o valor do ressarcimento for entre R$ 100.000,01 (cem mil reais e um centavo) e R$ 300.000,00 (trezentos mil reais), sendo o Diretor de Riscos e Controles e o de Operações do CCS;

• pela alçada da Diretoria Executiva do CCS, quando o valor do ressarcimento for superior a R$ 300.000,00 (trezentos mil reais).

Disposições Finais

Serão cobradas da cooperativa incorporadora, no mês da incorporação, as contribuições para o Fundo devidas pela cooperativa incorporada.

Deixarão de ser devidas contribuições ao Fundo, a partir do mês de desligamento da cooperativa, seja por demissão, eliminação ou exclusão. Não será devolvida qualquer contribuição à cooperativa no caso de sua demissão, eliminação ou exclusão.

A administração dos recursos financeiros do Fundo é de competência do CCS, que deverá aplicá-los integralmente no Banco Sicoob, devendo ser garantida a liquidez imediata desses valores.

A Superintendência Financeira do CCS disponibilizará, mensalmente, arquivo que permitirá à cooperativa central acompanhar o aporte pelas cooperativas singulares.

Regulamento do fundo para ressarcimento de fraudes externas e perdas operacionais do Sicoob

Os recursos do Fundo não poderão ser utilizados para ressarcimento de:

I. processos judiciais;
II. viagens;
III. indenizações;
IV. honorários.

Poderão ser ressarcidos processos judiciais vinculados a golpes/fraudes, com sentença favorável ao associado/cliente, não ressarcidos previamente pelo Fundo.

Todo prejuízo financeiro decorrente de perda que tenha sido ressarcida pelo Fundo e que venha a ser recuperada pela cooperativa do Sicoob beneficiada pela cobertura, deverá ser imediatamente devolvido ao Fundo.

Para ter direito ao ressarcimento, as cooperativas do Sicoob não poderão ter concorrido, ainda que culposamente, para a ocorrência da perda verificada, bem como ter realizado tempestivamente todas as ações necessárias para a recuperação dos recursos ou para evitar o prejuízo, inclusive executar as orientações repassadas pelo CCS para este fim.

Este Regulamento foi aprovado pelo Conselho de Administração do Sicoob Confederação na 49ª reunião ordinária, realizada em 15/4/2015, e passa a vigorar a partir da data de publicação, conforme autorização da Assembleia Geral Ordinária do Sicoob Confederação realizada em 11/3/2015. Suas atualizações passam a viger a partir de sua publicação.

CCI - 264/2018 do Sicoob Confederação estabelece, os valores máximos a serem ressarcidos pelo Fundo para Ressarcimento de Fraudes Externas e de Perdas Operacionais do Sicoob quando da ocorrência de fraudes.

Para ocorrências superiores ao valor de R$ 2.000,00 (dois mil reais), a cooperativa deverá:

a) possuir Termo de Cessão de Licenças Sisbr e Instrumento particular de Licenciamento de Software (Sisbr) válidos vigentes;

b) estar em situação regular no custeio das despesas de manutenção do Sisbr cobradas pelo Sicoob Confederação.

Valores para ressarcimento do fundo, para ressarcimento de fraudes externas e perdas operacionais do Sicoob

Para ter direito ao ressarcimento, a cooperativa não poderá ter concorrido, ainda que culposamente, para a ocorrência da perda verificada.
Portanto a cooperativa precisará:

a) certificar-se de que os montantes envolvidos não são superiores aos limites globais diários definidos pelo Comunicado Bancoob 1.085/2008 e pela CCI 241/2015 - Sicoob Confederação:

Transação	Limite global
Valor máximo para agendamento de Título PJ	R$ 30.000,00
Valor máximo para agendamento de Título PF	R$ 5.000,00
Valor máximo para agendamento de convênios PJ	R$ 10.000,00
Valor máximo para agendamento de convênios PF	R$ 2.000,00
Valor máximo para transferência sem o cadastro de favorecido	R$ 1.000,00
Valor máximo para transferência com o cadastro de favorecido	R$ 30.000,00

b) No caso de valor superior, o ressarcimento ocorrerá até o limite global estabelecido;
c) não haverá ressarcimento de transferências emitidas a favorecido não cadastrado de valores superiores ao limite global e/ou com aprovação de empregado da cooperativa;
d) não haverá ressarcimento de operações financeiras provenientes de extorção, cheques, golpes aplicados por terceiros associados por meio de engenharia social ou operações que foram realizadas mediante o uso do QR Code para autorização/aprovação, entre outros, conforme artigo 17° do Regulamento do Fundo para ressarcimento de Fraudes Externas e de Perdas Operacionais do Sicoob.

RISCOS OPERACIONAL: Possibilidade de ocorrência de perdas resultantes, falha, deficiência ou inadequação de processos internos, pessoas, sistemas ou eventos externos.

Conforme MIG - Risco Operacional, as fraudes são eventos de risco operacional, portanto, deverão ser mapeados e tratados de acordo com as normas sistêmicas e boas práticas de mercado.

7. Os registros de perdas operacionais e recuperação de perdas operacionais referem-se aos eventos de risco operacional, conforme listado abaixo:

Fraudes Internas:

Perdas devido aos atos intencionais com a participação de pelo menos uma pessoa interna à entidade com o objetivo de apropriar, indevidamente, de valores financeiros e bens físicos por meio de violação intencional de normas e controles internos, mediante a troca de senhas e perfis de acesso, ou ainda pela forja de documentos ou assinaturas, suborno, propina, negociação com empregados que possuem acessos a informações privilegiadas;

Fraudes Externas:

Perdas devido aos atos intencionais praticados pelo indivíduo externo à entidade por meio de adulteração de documentos, roubos, furtos, invasão de máquinas/equipamentos com o objetivo de apropriar indevidamente de valores financeiros e bens físicos.

NORMATIVOS

ATENÇÃO AOS NORMATIVOS

Documento	Descrição	Data
CCI 092/2022	Evolução das funcionalidades Suspeita de Fraude, Entradas e Saídas e Relatório TEDs PCF na Plataforma SSPB do Sisbr 2.0.	28/01/2022
CCI 189/2022	Revisão das estações de trabalho habilitadas para uso no Sicoob	18/02/2022
CCI 287/2022	Implantação do QR Code como duplo fator de autenticação (2FA) no login da Plataforma de Caixa	18/03/2022
CCI 343/2022	Prazo para adoção de segundo fator de autenticação para conexão de VPN	07/04/2022
CCI 340/2022	Requisitos técnicos e de segurança para utilização do Plataforma de Serviços Financeiros do Sicoob (Sisbr)	13/04/2022
CCI 406/2022	Diagnóstico para implementação da gestão sistêmica de risco e segurança cibernética	14/04/2022
CCI707/2022	Evolução da funcionalidade Suspeita de Fraude, na Plataforma SSPB do Sisbr 2.0	05/07/2022
Resolução CCS 110	Atualiza a Política Institucional de Prevenção e Combate a Fraudes	19/07/2022
CCI 803/2022	Alteração do número do telefone de contato da Área de Prevenção a Fraudes	27/07/2022
CCI 856/2022	Disponibilização das funcionalidades Relatórios de Acompanhamento em Ocorrência de Fraude e Pesquisa Cooperado, na Plataforma de Prevenção e Combate a Fraudes (PCF) do Sisbr 2.0.	12/08/2022
CCI 955/2022	Implementação de novas soluções antifraude no onboarding da associação digital	05/09/2022
Resolução CCS 123	Atualiza o Regulamento do Fundo para Ressarcimento de Fraudes Externas e Perdas Operacionais do Sicoob.	27/09/2022
CCI 1.053/2022	Novas Ações de Segurança e Prevenção a Fraudes	05/10/2022
CCI 1.085/2022	Notificação dos usuários a partir de um novo alerta do Painel de Alertas da Plataforma de Prevenção e Combate a Fraudes (PCF) do Sisbr 2.0.	11/10/2022
CCI - 1.083/2022	Evolução das funcionalidades Suspeita de Fraude e Entradas e Saídas, do Sicoob SPB do Sisbr 2.0, referentes à integração deste módulo à Plataforma de Prevenção e Combate a Fraudes (PCF) do Sisbr 2.0	13/10/2022
CCI 1.103/2022	Orientações sobre complexidade de senhas	17/10/2022
CCI 1.118/2022 e CCI 1.159/2022	Levantamento de infraestrutura de segurança cibernética das cooperativas centrais, singulares e dos PAs	19/10/2022
CCI 1.112/2022	Alteração no processo de liberação de dispositivos no Sicoob para acesso ao Sisbr 2.0 Mobile	20/10/2022
CCI 1.141/2022	Disponibilização da funcionalidade Reversão de Estorno no menu Pesquisa Cooperado	25/10/2022
CCI 1.199/2022	Evolução da funcionalidade Operações DOC/TED na Plataforma de Caixa	09/11/2022
CCI 1.244/2022	Prevenção a Fraudes no Sicoob	22/11/2022

GERÊNCIA DE RISCOS E COMPLIANCE • **GERIC**

GERIC@SICOOBCREDIMINAS.COM.BR

SICOOB
Central Crediminas