

Bolsas	Pontuação B3	Dólar	Salário mínimo	Euro	CDI	CDB	Inflação
Na sexta-feira	Ibovespa nos últimos dias	Na sexta-feira	Últimos	Comercial, venda na sexta-feira	Ao ano	Prefixado 30 dias (ao ano)	IPCA do IBGE (em %)
0,99% São Paulo	0,51% Nova York	157.981	160.766	R\$ 5,410 (+0,12%)	R\$ 1.518	R\$ 6,354	14,90%
	9/12 9/12 10/12 12/12	8/dezembro 9/dezembro 10/dezembro 11/dezembro	5,420 5,436 5,468 5,404				Julho/2025 -0,26 Agosto/2025 -0,11 Setembro/2025 0,48 Outubro/2025 0,09 Novembro/2025 0,18

SISTEMA FINANCEIRO

Aliança nacional combina ações do Ministério da Justiça e do Banco Central e cria barreiras contra contas falsas. Ofensiva inclui 23 ações coordenadas, além de medidas para dificultar a atuação de quadrilhas. Especialistas aprovam

Governo e bancos apertam cerco a golpes digitais

Pilares da estratégia

6 eixos centrais do plano nacional de combate a fraudes digitais

- 

**1. PREVENÇÃO A FRAUDES E GOLPES**

  - Aperfeiçoamento dos mecanismos de segurança.
  - Monitoramento reforçado das transações digitais e identificação de padrões de risco.
- 

**2. REPRESSÃO A CRIMES CIBERNÉTICOS**

  - Ações mais rápidas de investigação e rastreamento de recursos.
  - Suporte técnico ampliado às forças de segurança e autoridades policiais.
- 


**3. COMPARTILHAMENTO DE DADOS**

  - Integração entre bancos, governo e empresas de tecnologia.
  - Protocolos padronizados para troca segura de informações.
- 

**4. CAPACITAÇÃO**

  - Treinamento contínuo de agentes públicos e privados.
  - Atualização sobre novas modalidades de golpes e práticas de proteção.
- 

**5. ATENDIMENTO ÀS VÍTIMAS**

  - Diretrizes unificadas para acolhimento e orientação.
  - Rotinas operacionais e jurídicas para agilizar o suporte após o golpe.
- 

**6. CONSCIENTIZAÇÃO DA POPULAÇÃO**

  - Campanhas educativas nacionais.
  - Materiais de letramento digital para prevenção e identificação de fraudes.

**Sofri um golpe. E agora?**  
Novo portal do MJSP para vítimas de fraudes bancárias digitais

- O que o portal oferece:**
- Passo a passo sobre como agir após o golpe.
  - Orientações operacionais e jurídicas.
  - Vídeos educativos.
  - Glossário com 41 tipos de fraudes.
  - Painel interativo com dados atualizados sobre ocorrências, perfis de vítimas e tendências de golpe.

Fonte: MJSP e BC.

**BC PROTEGE+**

- Bloqueio preventivo contra fraudes de identidade.
- O BC Protege+ é um serviço gratuito que permite a pessoas físicas e jurídicas informar ao sistema financeiro que não autorizam a abertura de contas ou sua inclusão como titular/representante em contas de terceiros.
- A ferramenta funciona como uma trava preventiva, consultada obrigatoriamente por todas as instituições antes de abrir novas contas.

**Como funciona na prática**

- Bancos consultam automaticamente o sistema antes de abrir contas ou cadastrar chaves Pix.
- Se houver bloqueio ativo, a contratação é impedida.
- Reduz fraudes de identidade, criação de contas laranja e golpes com uso indevido de CPF ou CNPJ.

**COMO ATIVAR**

1. Cidadão acessa a área logada do Meu BC com sua conta gov.br, nível prata ou ouro, com verificação em duas etapas habilitada
2. Clica no botão Gerenciar a proteção no card BC Protege+
3. Ativa a proteção no card Contas – abertura e inclusão
4. Antes de abrir uma conta ou incluir um titular ou representante em uma conta, a instituição deve consultar opção registrada para o CPF ou CNPJ; se a proteção estiver ativada, ela não poderá fazer a contratação
5. O cidadão pode ativar e desativar a proteção a qualquer momento, inclusive durante a jornada de contratação
6. O cidadão também pode ver qual instituição realizou a consulta dos seus dados no sistema
7. Para empresas, o serviço está disponível para sócios, representantes e colaboradores devidamente cadastrados no módulo de empresas da plataforma gov.br



» RAFAELA GONÇALVES

O governo federal e o sistema financeiro deram início a uma nova ofensiva contra fraudes digitais no país. O Ministério da Justiça e Segurança Pública (MJSP), em parceria com entidades do setor financeiro, lançou um plano de ação integrado para enfrentar golpes e crimes cibernéticos que se multiplicam nas transações digitais. Paralelamente, o Banco Central (BC) anunciou novas medidas para dificultar a abertura de contas falsas usadas por quadrilhas para movimentar dinheiro de forma irregular, reforçando a estratégia nacional de contenção às fraudes e ao avanço das organizações criminosas no ambiente virtual. À medida que as operações on-line ultrapassam as presenciais no sistema financeiro, o Brasil se tornou um dos países com maior número de tentativas de fraude digital, atrás apenas da China, de acordo com o estudo *The Emotional Undercurrent of Financial Scams*. A iniciativa, batizada de Aliança Nacional de Combate a Fraudes Bancárias Digitais, reúne 23 ações articuladas e é fruto de um acordo de cooperação técnica entre o MJSP e a Federação Brasileira de Bancos (Febraban). O ministro da Justiça e Segurança Pública, Ricardo Lewandowski, destacou como a digitalização transformou o cenário da criminalidade. “A crescente complexidade da criminalidade, exacerbada pela digitalização, tem transformado profundamente o cenário da segurança pública. O combate ao crime exige uma abordagem que transcende as ações estatais. É imprescindível que a sociedade

participe ativamente”, disse no lançamento da Aliança. Segundo Lewandowski, a Aliança tem horizonte de cinco anos e reúne iniciativas já em execução, como o novo portal voltado às vítimas de golpes. “Já existem diversas ações concretas em andamento, como a criação de um site hospedado no Ministério da Justiça. Este portal tem como objetivo fornecer informações claras e confiáveis aos cidadãos, especialmente às vítimas de fraudes, que muitas vezes não sabem como agir ou a quem recorrer”, explicou. O objetivo é fortalecer ações de prevenção, detecção e repressão a fraudes, além de oferecer apoio direto às vítimas. “Esta Aliança é essencial, porque demonstra algo que o crime não terá, que é a capacidade de integrar setores distintos, público e privado, com agendas próprias, em torno de um objetivo comum”, destacou Isaac Sidney, presidente da Febraban. Segundo ele, o esforço conjunto inaugura uma nova etapa na resposta às ameaças digitais. “Assim, mostramos ao Brasil que, para combater a criminalidade digital, podemos romper barreiras históricas e criar soluções coletivas para enfrentar um dos desafios mais graves e complexos, que são os golpes, as fraudes e os ataques cibernéticos nas transações financeiras.” O plano se apoia em seis pilares: aprimoramento dos processos de prevenção de golpes, intensificação da repressão, compartilhamento de dados, capacitação de agentes públicos e privados, atendimento às vítimas e conscientização da população.

**Identidade segura**

Também entrou em vigor na última semana o BC Protege+,



**O golpe também envolve engenharia social, vazamento de dados e falhas humanas. É uma ferramenta essencial, mas não suficiente sozinha”**

**Stefano Ribeiro Ferri, especialista em Direito do Consumidor**

novo sistema do Banco Central que permite aos clientes bloquear a abertura de contas em seus nomes, ampliando a proteção contra fraudes e golpes no sistema financeiro. A partir da ferramenta, todas as instituições financeiras são obrigadas a consultá-la antes de abrir contas de depósito, poupança ou contas de pagamento pré-pagas, garantindo que apenas titulares autorizados possam movimentar recursos. A adesão ao serviço é voluntária e pode ser feita pelo portal Meu BC, que já reúne funcionalidades como o Registrato e o Sistema de Valores a Receber (SVR). Segundo resolução do Banco Central, a consulta ao BC Protege+ é obrigatória e deve ocorrer de forma prévia à formalização de qualquer nova conta. Gratuito, o serviço permite que pessoas físicas e jurídicas bloqueiem a abertura de novas contas em seus nomes ou como representantes, obrigando as instituições a conferir a restrição antes de concluir qualquer contratação, reduzindo golpes de identidade. Para o especialista em Direito do Consumidor Stefano Ribeiro Ferri, o recurso adiciona uma nova camada de proteção, ao oferecer

**Contas-bolsão**

Além da nova ferramenta, entrou em vigor o fim das chamadas contas-bolsão, utilizadas para movimentar recursos de terceiros sem identificação individual dos titulares. Comuns em plataformas de comércio eletrônico, essas contas passaram a ser exploradas por organizações criminosas para ocultar operações financeiras e lavar dinheiro, motivando a restrição do seu uso. As instituições financeiras serão obrigadas a encerrar esse tipo de conta, que dificulta o rastreamento de recursos e já apareceu em investigações como as operações Carbono Oculto, ligada ao PCC, e Poço de Lobato, sobre o Grupo Refit, apontado como maior sonegador de impostos do país. Ao regulamentar a terceirização de serviços bancários pelo modelo Banking as a Service (BaaS), o Banco Central deixou claro que as contas abertas, mantidas ou encerradas nesse sistema devem ter titularidade de individualizada e só podem ser movimentadas pelos clientes finais.

**Adequação à LGPD**

O avanço das fraudes de identidade e dos crimes cibernéticos tem impulsionado instituições financeiras e reguladores a reforçar mecanismos de prevenção no país. Para especialistas, a combinação entre ferramentas públicas, governança robusta e adequação à Lei Geral de Proteção de Dados (LGPD) é decisiva para garantir segurança sem comprometer direitos de privacidade. Segundo Luiz Fernando Plastino, advogado especialista em Privacidade, Proteção de Dados e Direito da Informática no Barcellos Tucunduva

Advogados, o Brasil possui algumas das regras mais desenvolvidas do mundo em relação à segurança das instituições financeiras, e o Banco Central atualiza constantemente essas normas para responder ao surgimento de novas ameaças. O especialista alerta que falhas na prevenção podem gerar responsabilização. “As instituições podem responder por perdas e danos se falharem em endereçar adequadamente o risco de fraude, inclusive quando o incidente envolver prestadores de serviços”, diz. A depender da causa, também podem ser aplicadas sanções administrativas por descumprimento de normas de segurança e governança. Quando houver vazamento ou uso indevido de dados pessoais, a Agência Nacional de Proteção de Dados (ANPD) pode investigar e atuar a instituição, aplicando multas ou até determinando a suspensão de atividades. Plastino destaca que biometria e inteligência artificial reforçam a segurança, mas exigem base legal, transparência e controles humanos para evitar erros e garantir monitoramento contínuo. De acordo com ele, a tecnologia pode identificar padrões suspeitos e prevenir fraudes de forma automática, mas deve operar com “controles humanos para evitar falsos positivos e negativos, além de monitoramento contínuo.” Em sua avaliação, o país dispõe hoje de um ecossistema regulatório e tecnológico capaz de reduzir de forma significativa a superfície de ataque das fraudes. “O Brasil está na vanguarda da proteção contra fraudes, combinando normas robustas, ferramentas públicas e tecnologias avançadas, sempre com atenção aos direitos de privacidade e à segurança jurídica.”