

POLÍTICA DE PREVENÇÃO
E GESTÃO DO RISCO
DE FRAUDE EXTERNA

DEZEMBRO 2021





ÍNDICE

1 – Enquadramento	3
2 – Definição de Fraude	3
3– As Dimensões do Processo de Prevenção e Gestão da Fraude	3
3.1 Planeamento e Prevenção.....	3
3.1.1 Onboarding	3
3.1.2 Autenticação	4
3.1.3 Cibersegurança	4
3.1.4 Clientes Vulneráveis.....	4
3.1.5 Sensibilização dos Clientes	4
3.2 Deteção, Diagnóstico, Análise e Resolução	4
3.3 Controlo e Avaliação.....	5
3.3.1 Avaliação de Risco.....	5
3.3.2 Avaliação da eficácia, melhoria contínua e <i>reporting</i>	5
3.3.3 Arquivo.....	5

1 – Enquadramento

A presente Política define princípios, responsabilidades e regras gerais em matéria de Prevenção e Gestão do Risco de Fraude Externa na Caixa Geral de Depósitos (doravante designado por “CGD” ou “Banco”).

De modo a proteger a sua reputação e ir ao encontro das obrigações legais e regulamentares, a CGD adota medidas responsáveis para minimizar o risco de fraude externa e de outras infrações conexas em toda a sua organização. Nesse âmbito, são internamente definidos os riscos de fraude externa e implementados os controlos internos adequados, de forma atempada, que permitam prevenir, detetar e responder à fraude e a outras infrações conexas.

A Política adotada é suportada por um ambiente de controlo, que inclui um programa onde a gestão de topo do Banco dá o exemplo e onde são promovidas ações de formação e comunicação para sensibilizar os colaboradores, bem como para criar uma cultura ética e aberta.

A Política de Prevenção e Gestão do Risco de Fraude Externa providencia diretrizes sobre a identificação de fraude, os controlos a implementar para prevenir e detetar a fraude e as etapas a completar no sentido de construir uma resposta robusta para proteger os interesses do Banco e dos seus clientes.

2 – Definição de Fraude

Podemos definir fraude como a prática de uma ação ilícita, intencional e de má-fé, punível por Lei, por parte de um fraudador, com o objetivo de enganar ou prejudicar uma pessoa ou organização, para proveito próprio ou de terceiros, evitar uma determinada obrigação ou causar perdas para determinada organização.

Relativamente à Fraude Externa, poderá definir-se como perdas potenciais resultantes de atividades com intenção fraudulenta levada a cabo por clientes CGD e terceiros (outros *stakeholders*, excluindo colaboradores).

Neste sentido, a Fraude Externa ocorre quando os atos definidos no conceito de Fraude são perpetrados por pessoas ou entidades externas ao Grupo CGD.

3 – As Dimensões do Processo de Prevenção e Gestão da Fraude

Os Processos de Prevenção e Gestão da Fraude encontram-se representados por três dimensões:

- i) Planeamento e Prevenção;
- ii) Detecção, Diagnóstico Análise e Resolução; e,
- iii) Controlo e Avaliação.

3.1 PLANEAMENTO E PREVENÇÃO

De modo a promover uma cultura de gestão de risco e controlos mais robusto, a CGD está estruturada em conformidade com as boas práticas para a Prevenção do Risco de Fraude (“PRF”), tendo claramente definidas as funções e responsabilidades das respetivas áreas afetas, bem como dos Fóruns onde a PRF é analisada e avaliada de forma regular e preventiva.

3.1.1 Onboarding

No âmbito do estabelecimento da relação de negócio com um novo cliente ou com uma nova contraparte, o Banco procede às diligências já preconizadas nos requisitos de *Know Your Customer* (“KYC”) relativos a Prevenção de Branqueamento de Capital e Combate ao Financiamento do Terrorismo (“PBC/CFT”).

Estes procedimentos de KYC, para além da prevenção dos riscos de Branqueamento de Capitais e de Financiamento ao Terrorismo (“BC/FT”), mitigam também a exposição aos riscos financeiros, regulamentares e/ou reputacionais.



3.1.2 Autenticação

De modo a prevenir riscos de fraude, riscos reputacionais e regulatórios, bem como violações ou roubos de dados, o Banco tem implementado controlos que permitem minimizar o risco de acesso não autorizado às contas e transações dos clientes.

Desta forma, os métodos de autenticação em vigor na CGD fundamentam-se numa abordagem baseada no risco, pelo que são aplicadas medidas de autenticação mais robustas (autenticação forte) para operações consideradas de risco acrescido.

3.1.3 Cibersegurança

A CGD, através do seu *site* institucional, www.cgd.pt, divulga permanentemente alertas e recomendações de segurança sobre a proteção contra os riscos de fraude informática (“*phishing*” e outros), para promover uma utilização segura da internet e dos serviços de pagamento através de meios eletrónicos.

Adicionalmente, os serviços de *homebanking* da Caixa dispõem de sistemas de monitorização permanente que previnem e detetam tentativas de fraude.

A utilização destes sistemas de verificação e prevenção de fraudes permite identificar atividades suspeitas, ajudando a proteger as contas e interesses dos clientes CGD.

3.1.4 Clientes Vulneráveis

No âmbito da abordagem baseada no risco, o Banco considera os clientes potencialmente mais vulneráveis na *framework* de gestão de risco de fraude.

Um cliente potencialmente mais vulnerável é alguém que, devido a circunstâncias pessoais, é especialmente suscetível a ameaças de fraude, particularmente se o Banco não atuar com o nível de cuidado apropriado.

Entre os clientes potencialmente mais vulneráveis, destacam-se:

- i) clientes idosos;
- ii) clientes com deficiência mental / física; e,
- iii) clientes marginalizados.

A abordagem considera

- i) os possíveis indicadores de vulnerabilidade; e,
- ii) de que forma as diferentes áreas evitam, inadvertidamente, a exclusão de clientes ou a colocação de barreiras que impactem a capacidade do mesmo em utilizar os produtos e serviços oferecidos pelo Banco.

3.1.5 Sensibilização dos Clientes

A CGD providencia materiais de sensibilização sobre PRF aos seus clientes e outras contrapartes, nomeadamente através do seu *website* institucional e outros meios de publicação, partilhando informações relativas a temáticas de fraude, como tendências, campanhas em vigor e alertas para situações recorrentes.

3.2 DETEÇÃO, DIAGNÓSTICO, ANÁLISE E RESOLUÇÃO

A CGD documenta, no âmbito da abordagem baseada no risco, a identificação de práticas potenciais de fraude e atividades suspeitas. A abordagem utilizada inclui os processos, tecnologias e sistemas utilizados para detetar atividades suspeitas de fraude.

Com vista à deteção das práticas de fraude e atividades suspeitas, a CGD tem implementados controlos, sendo estes proporcionais ao nível de risco de fraude identificado.

Todos os casos de fraude detetados são geridos em linha com os processos internos definidos no âmbito da PRF e revistos, tendo por base toda a informação disponível para determinar se é considerado um potencial incidente de fraude e os casos com suspeita de fraude são reencaminhados para um nível superior de revisão, juntamente com a documentação suporte.

A CGD dispõe do registo de *audit trail* de todos os casos de fraude analisados, bem como das decisões e ações realizadas com vista a mitigar o risco associado, possibilitando o reporte periódico dos casos identificados.

No âmbito da atividade de PRF, caso existam suspeitas de incidentes de fraude externa e caso seja aplicável, o Banco procede ao reporte às autoridades.

Adicionalmente, o Banco mantém uma relação efetiva com as autoridades, que facilita a partilha de informação, o apoio à resposta a ataques de fraude e uma melhor cooperação na investigação de casos de fraude externa e todos os requisitos das autoridades policiais são respondidos dentro dos períodos definidos pelas mesmas.

3.3 CONTROLO E AVALIAÇÃO

3.3.1 Avaliação de Risco

A CGD realiza, periodicamente, uma avaliação de riscos de negócio, no que diz respeito a fraude externa.

Esta avaliação, para além determinar os riscos inerentes de fraude externa, permite determinar a eficácia dos controlos em vigor, bem como identificar oportunidades de melhoria existentes.

A CGD tem tolerância zero sobre incidentes de fraude externa.

A avaliação dos riscos inclui, no mínimo, a:

- i) identificação dos riscos na área de negócio baseados na sua estrutura, produtos, serviços e canais de distribuição;
- ii) identificação de processos e controlos em prática para mitigar os riscos;
- ii) identificação de falhas ou debilidades na estrutura de controlos que enfrenta os riscos.

3.3.2 Avaliação da eficácia, melhoria contínua e reporting

Os Departamentos e áreas afetos à PRF realizam testes de controlo para avaliar a adequabilidade, o desenho e a efetividade operacional dos seus procedimentos, sistemas e controlos de fraude.

Estes testes são baseados no risco e personalizados de acordo com os riscos específicos de cada unidade orgânica afeta à PRF, com maior foco nas transações, vulnerabilidades do cliente e atividades que possuem um risco mais elevado de fraude.

No âmbito dos incidentes de fraude detetados, a CGD procede à análise de causas relativas à revisão de alertas, resolução e resposta ao cliente. Os resultados e conclusões destas análises suportam alterações aos controlos ou procedimentos e às avaliações de risco realizadas.

As métricas de fraude são ferramentas críticas para quantificar e reportar a natureza dos riscos de fraude aos quais a CGD se encontra exposta. A recolha e análise periódica e atempada da informação é essencial para uma gestão efetiva, o reporte e supervisão dos riscos de fraude.

É elaborado um relatório com a periodicidade trimestral de reporte à Administração das principais atividades desenvolvidas no âmbito da prevenção e gestão da fraude externa.

3.3.3 Arquivo

Em linha com as boas práticas no que diz respeito ao arquivo de documentação, a CGD conserva a documentação relativa a Prevenção e Gestão do Risco de Fraude Externa, por um período mínimo de 7 anos.

A CGD estabelece procedimentos, sistemas e controlos documentados de modo a assegurar a conservação e acesso apropriado dos documentos acima listados.

Todos os documentos deverão ser legíveis, auditáveis e recuperáveis e toda a legislação aplicável referente à confidencialidade, sigilo e proteção de dados é cumprida.

Luís Saraiva Martins

Head of Compliance

