Relatório de Impacto à Proteção de Dados Pessoais

Setembro de 2020

BANCO CENTRAL DO BRASIL

Relatório de Impacto à Proteção de Dados Pessoais

Setembro de 2020

BANCO CENTRAL DO BRASIL

Sumário

1 Identificação dos agentes de tratamento e do encarregado

Controlador
Banco Central do Brasil

Operador
Não se aplica

Encarregado
Eugênio Pacceli Ribeiro – Coordenador do Comitê de Governança da Informação (CGI)

E-mail Encarregado	Telefone Encarregado
eugenio.ribeiro@bcb.gov.br	145 (custo de ligação local)

2 Necessidade de elaborar o Relatório

A Política de Conformidade (*Compliance*) do Banco Central do Brasil (PCO-BCB) tem entre seus objetivos assegurar que as atividades do Banco Central sejam conduzidas em conformidade com as normas aplicáveis à Instituição, sob a coordenação do Departamento de Riscos Corporativos e Referências Operacionais (Deris).

Nesse sentido, de acordo com o art. 38, *caput*, da Lei 13.709, de 14 de agosto de 2018, ou Lei Geral de Proteção de Dados Pessoais (LGPD), a qualquer momento, a Autoridade de Proteção de Dados Pessoais (ANPD) pode determinar ao BCB que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis. Surgiu, assim, a necessidade de se confeccionar este documento.

O Banco Central do Brasil (BCB), diariamente, realiza o tratamento[1] de dados pessoais que se relacionam a pessoa natural identificada ou identificável (art. 5º, I, LGPD). Existem também os dados pessoais sensíveis, que dizem respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (art. 5º, II, LGPD).

1 Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X, LGPD).

Considerando os fundamentos[2] da proteção de dados pessoais (art. 2º e incisos, LGPD), a boa-fé e os demais princípios[3] a serem observados nas atividades de tratamento de dados pessoais (art. 6º e incisos, LGPD), o BCB dispõe de diferentes sistemas de controles internos, que variam de acordo com a natureza do dado pessoal, para mitigar eventuais riscos de falha na proteção de dados pessoais.

Entretanto, apesar do elevado grau de maturidade da gestão de riscos do BCB, não se pode garantir a eliminação total dos riscos que, em caso de materialização, causariam impacto à privacidade dos dados pessoais existentes na instituição.

3 Descrição do tratamento

A Política de Segurança da Informação do Banco Central do Brasil (PSIBC), divulgada pela Portaria 95.673, de 23 de novembro de 2017, visa evitar que os riscos aos quais estão sujeitos os ativos de informação comprometam as atividades do BCB e o cumprimento de sua missão institucional.

Os ativos de informação compreendem "os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal e os locais onde se encontram esses meios" (art. 5º, III, PSIBC).

No que se refere especificamente às informações de caráter pessoal, os sistemas de controle interno implantados no BCB variam de acordo com o tipo de suporte (físico ou digital), bem como com a natureza da informação (comum ou sensível).

---

2 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

3 Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Nesta seção são descritos os processos de tratamento de dados pessoais, digitais ou físicos, que podem gerar riscos às liberdades civis e aos direitos fundamentais, envolvendo a especificação de natureza,[4] escopo,[5] contexto[6] e finalidade[7] do tratamento.

3.1 Dados digitais

3.1.1 Natureza do tratamento

São adotadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O acesso às bases de dados é controlado por grupos de rede e acesso limitado a determinados perfis de usuários. Há contínua busca por segurança da informação ao se fazer uso de sistemas corporativos no BCB e ao dar cumprimento às disposições contidas na Política de Segurança da Informação (PSIBC) e no Código de Conduta dos Servidores do BCB, especialmente no que se refere ao acesso à informações, arts. 8°, 9° e 13° do Código. Como medidas administrativas adotadas, citam-se: (i) assinatura de acordos de responsabilidade para acesso a sistemas, por requisição formal ou por *e-mail*; (ii) registro dos acessos concedidos; e (iii) destacamento de servidores dedicados às respostas das demandas de outros poderes, com criação de diretórios de acesso exclusivo para guarda de documentos digitais.

3.1.2 Tratamento dos dados

Existem diversas formas de tratamento dos dados pessoais no BCB, considerando a definição da LGPD:

- Coletados/Enviados

Os dados são coletados principalmente por meio de sistemas de informação e por captação de informações de entidades externas, seja por força de regulação seja por acordos e convênios firmados. Os dados de captações são recebidos, em geral, por meio do Sistema de Transferência de Arquivos (STA).

- Retidos/Armazenados

Os dados são mantidos das seguintes formas:

  - bancos de dados corporativos (utilizando os sistemas gerenciadores de banco de dados DB2, SQL Server, Teradata, Adabas, Oracle);
  - bancos de dados departamentais (utilizando os sistemas gerenciadores de banco de dados SQL Server, Teradata, Datalab, SAS);
  - arquivos (p. ex.: planilhas Excel).

4 A natureza representa como a instituição pretende tratar ou trata os dados pessoais.

5 O escopo diz respeito à abrangência do tratamento de dados.

6 O contexto destaca um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

7 A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais, justifica o tratamento e fornece os elementos para informar o titular dos dados.

- Usados

Os dados são usados em processos de trabalho das unidades do BCB (também chamadas neste Relatório de Departamentos) de diversas formas. Pode-se citar a utilização de sistemas de informação desenvolvidos pelo Departamento de Tecnologia da Informação (Deinf), pelas próprias unidades ou adquiridos de terceiros; ferramentas de análise de dados (p. ex.: Microstrategy, Reporting Services, PowerBI); ferramentas de análise estatística (p. ex.: R, Stata, Python, Matlab).

- Eliminados

Os dados podem ser eliminados por meio de ações em sistemas de informação, comandos SQL nos bancos de dados (no caso de bases de dados departamentais) e exclusão de arquivos.

No caso de base de dados departamentais, o curador[8] indica no Catálogo de Informações[9] que uma base de dados deve ser desativada (seção 7.4 do Manual do Agente de Curadoria). Nesse caso, deve-se optar por arquivamento (com a criação de um *backup* e manutenção de curadoria) ou por descarte, quando os dados são apagados.

O Escritório de Governança da Informação (Eginf), vinculado ao Deinf, possui processo para a desativação de bases de dados, que inclui avaliação do uso dos dados no BCB. Inicialmente, retiram-se os acessos de escrita, em seguida, os de leitura e, por fim, são eliminadas todas as conexões, para posterior exclusão dos dados. Esse procedimento permite a descoberta de eventuais usuários dos dados antes da eliminação.

3.1.3 Fonte dos dados

As formas de coleta de dados no BCB são:

- captações de informações externas: são enviados arquivos de dados com informações pessoais pelo STA. Os arquivos são remetidos por entidades supervisionadas e por outras instituições que possuem acordo ou convênio com o BCB (p. ex.: Receita Federal do Brasil);
- sistemas de informação: de acesso interno (p. ex.: Sistema Integrado de Administração de Recursos Humanos – Siarh) e de acesso externo (p. ex.: Censo de Capitais Estrangeiros);
- recebimento de documentos e formulários: eletronicamente ou em papel;
- registro de informações pelos atendimentos institucionais: presencial e telefônico.

3.1.4 Compartilhamento dos dados

O compartilhamento de dados pessoais ocorre com as instituições reguladas pelo BCB, apenas com autorização expressa ou presumida do titular. Também ocorre compartilhamento dos dados protegidos pelo sigilo bancário com órgãos dos Poderes Judiciário, Executivo e Legislativo, e do Ministério Público, para fins de instrução de processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como com autorização judicial.

8 Responsável pela base de dados departamental.

9 Catálogo de metadados sobre as bases de dados divulgadas, para permitir o entendimento necessário à utilização dos dados, abrangendo também a indicação dos responsáveis pela sustentação de cada base de dados divulgada, de acordo com a Política de Governança da Informação (PGI) do BCB.

O envio de dados com incidência de hipóteses de sigilo, do BCB para outros órgãos, é realizado geralmente por meio de arquivos, utilizando-se o STA. Alguns dados também são coletados e enviados por meio da Plataforma de Integração de Entidades Reguladoras (Pier).

No Catálogo de Informações, o curador pode definir os canais de publicação externa de cada base de dados. São informações sobre a base de dados como um todo, mas o curador pode informar se existem dados pessoais.
O Cadin é uma base mantida no BCB por força de lei e também contém informações enviadas por vários órgãos da administração pública, porém, o BCB não tem poder de decisão sobre o tratamento dos dados pessoais.

3.1.5 Adoção de nova tecnologia para tratamento dos dados

A tecnologia Blockchain é utilizada para compartilhamento de dados com outros reguladores do SFN (p. ex.: Comissão de Valores Mobiliários – CVM, Superintendência de Seguros Privados – Susep, e Superintendência Nacional de Previdência Complementar – Previc).

De forma geral, para ser compatível com a LGPD, os dados pessoais não devem ser armazenados em nenhuma Blockchain, por ser uma estrutura em que os dados somente são adicionados, não havendo possibilidade de exclusão ou modificação. Dessa forma, não há como um dado apenas "transitar" pelo sistema sem que seja gravado definitivamente. Logo, o uso de Blockchain não é compatível com o previsto no art. 18, incisos II, IV e VI da LGPD. Porém, essa lei lista, no art. 16, as exceções que isentam o controlador de atender a uma demanda por exclusão de dados.

Entende-se, portanto, que, se o dado for coletado para atender uma obrigação legal, por exemplo, ele pode ser armazenado em Blockchain; caso contrário, a tecnologia não deve ser usada nesse sistema, justamente devido a seu caráter de imutabilidade.

No que se refere ao âmbito interno do BCB, as linguagens de programação R e Python são cada vez mais utilizadas para tratamento dos dados pelos departamentos.

3.1.6 Medidas de segurança

As medidas de segurança adotadas pelo BCB têm validade para qualquer tipo de informação. Elas são definidas pela Política de Segurança da Informação do BCB (PSIBC), a qual contém os Procedimentos Operacionais de Segurança em Tecnologia da Informação (Posti). A PSIBC define informação sensível como aquela que necessita de proteção contra revelação não autorizada, e o Posti normatiza o uso dos recursos de TI.

- Transferência de Arquivos

Para a transferência de arquivos eletrônicos, para destinatários internos, com informação sensível, devem ser utilizadas:

- pastas compartilhadas localizadas em servidor de arquivos sigilosos;
- biblioteca de documentos no portal da Intranet com o recurso de Gerenciamento de Direitos de Informação habilitado e localizada na Intranet com configurações de auditoria habilitadas para todos os eventos;
- mensagem de *e-mail* com anexo criptografado, com a senha do arquivo sendo transmitida por outro meio, como telefone, por exemplo.

Para a transferência de arquivos eletrônicos de/para destinatários externos, podem ser utilizados:

- o sistema STA, para arquivos transferidos entre o Banco Central e instituições cadastradas no Sisbacen, de forma rotineira;
- o sistema https://upload.bcb.gov.br, para a transferência esporádica de arquivos entre o BCB e instituições externas;
- anexos de *e-mail*, caso não haja necessidade de garantia de entrega. Se a informação for sensível, o anexo deve estar criptografado, com a senha do arquivo sendo transmitida por outro meio, como telefone.

Mídias removíveis (*pendrive*, CD, DVD ou HD externo) podem ser utilizadas para a transferência de arquivos corporativos mediante justificativa e com a anuência da chefia imediata, em especial em caso de impossibilidade de uso dos meios tecnológicos descritos acima. Nesse caso, é obrigatória a aplicação de criptografia para proteção da informação sempre que viável tecnologicamente.

Não são considerados meios adequados para a transferência de arquivos eletrônicos: pastas compartilhadas em estações de trabalho (*desktops* e *notebooks*), *e-mail* particular e serviços de terceiros na Internet (ex.: Dropbox, Google Drive e Onedrive).

- Servidores de arquivos

Os servidores de arquivos possuem áreas de armazenamento reservadas para cada unidade. Os másters[10] de cada unidade são responsáveis por conceder permissão de acesso às pastas e arquivos, observados os princípios da necessidade de conhecer e do privilégio mínimo.

Para as informações sigilosas, existe um servidor de arquivos sigilosos (com criptografia no tráfego de rede e auditoria completa de acessos). Esse servidor é administrado e acessado exclusivamente pela unidade gestora da informação.

- Impressão de documentos

Não deverão ser impressos arquivos eletrônicos corporativos com informação sensível fora das dependências do BCB.

- Descarte de informações

O descarte de informações corporativas gravadas em qualquer mídia deverá ser feito de maneira a impedir a sua recuperação.

- Monitoramento

O Deinf poderá monitorar, para fins de trilhas de auditoria, os acessos e gravações de arquivos e as transferências e impressões de arquivos eletrônicos corporativos.

10 Gestores setoriais de segurança da informação.

É de responsabilidade de cada unidade do BCB assegurar o uso correto e eficiente da área de armazenamento reservada a ela, verificando periodicamente se:

- apenas arquivos necessários aos processos de trabalho da unidade estão armazenados;
- não existem arquivos que infrinjam direitos autorais ou que apresentem outros riscos jurídicos, como músicas, filmes e livros que não tenham sido adquiridos pelo BCB.

A segurança da informação é constantemente revista e aprimorada com novas medidas de segurança. Uma das abordagens em discussão atualmente é garantir que os dados estejam protegidos durante todo o seu tratamento (desde a coleta até o descarte). Nesse processo, são utilizados diversos sistemas, tecnologias e ferramentas para permitir a criptografia e o controle de acesso de forma integrada.

3.1.7 Fluxo de dados

A seguir, será mostrado o fluxo de dados de três sistemas de comunicação com usuários externos ao BCB: o Protocolo Digital, o BacenJud e o Pix (Pagamentos Instantâneos Brasileiro). O Protocolo Digital é um sistema que permite que o cidadão envie documentos digitais ao BCB. O BacenJud é a principal plataforma de comunicação eletrônica entre o Poder Judiciário e as instituições financeiras bancárias. Por meio do BacenJud, as ordens judiciais são transmitidas eletronicamente e têm suas respostas visíveis para o juízo emissor na manhã do segundo dia útil após a instituição executar a demanda. O Pix estará em funcionamento a partir de novembro de 2020 e permitirá a realização de transações financeiras instantâneas.

O Protocolo Digital determina um fluxo de informações transitadas a partir de reclamação do cidadão, conforme ilustrado na Figura 3.1.

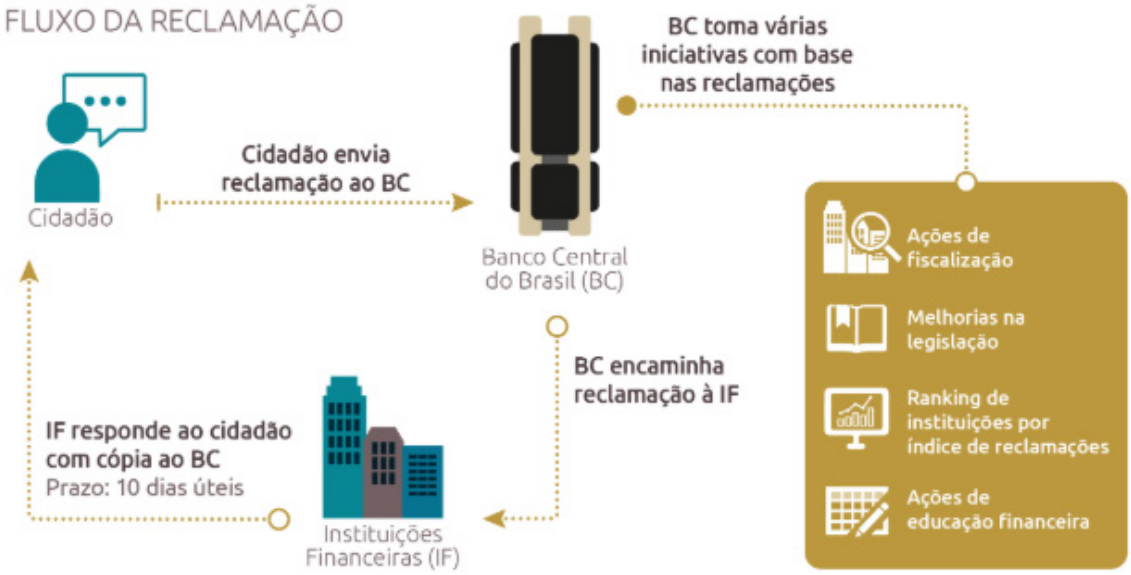

Figura 3.1 – Fluxo de informações no Protocolo Digital

O fluxo de dados no BacenJud é mostrado na Figura 3.2.

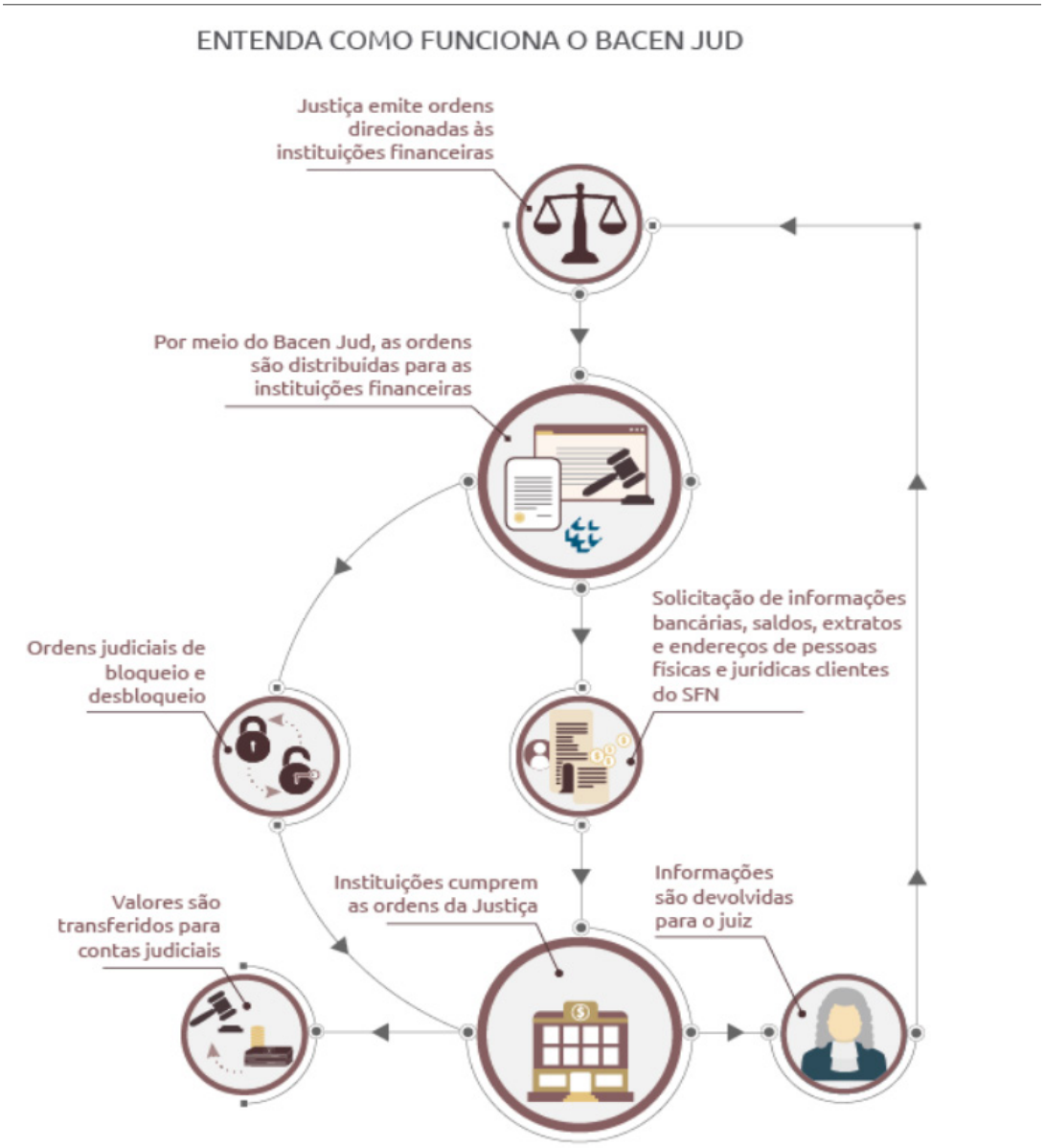

Figura 3.2 – Fluxo de informação no BacenJud

O Pix se caracteriza como um sistema de transferências monetárias eletrônicas no qual a transmissão da ordem de pagamento e a disponibilidade de fundos para o usuário recebedor ocorrem em tempo real, com operação durante 24 horas por dia, sete dias por semana e em todos os dias do ano. As transferências ocorrem diretamente da conta do usuário pagador para a conta do usuário recebedor, sem a necessidade de intermediários, o que propicia custos de transação menores. A Figura 3.3 ilustra como ocorre o fluxo de informações no Pix.

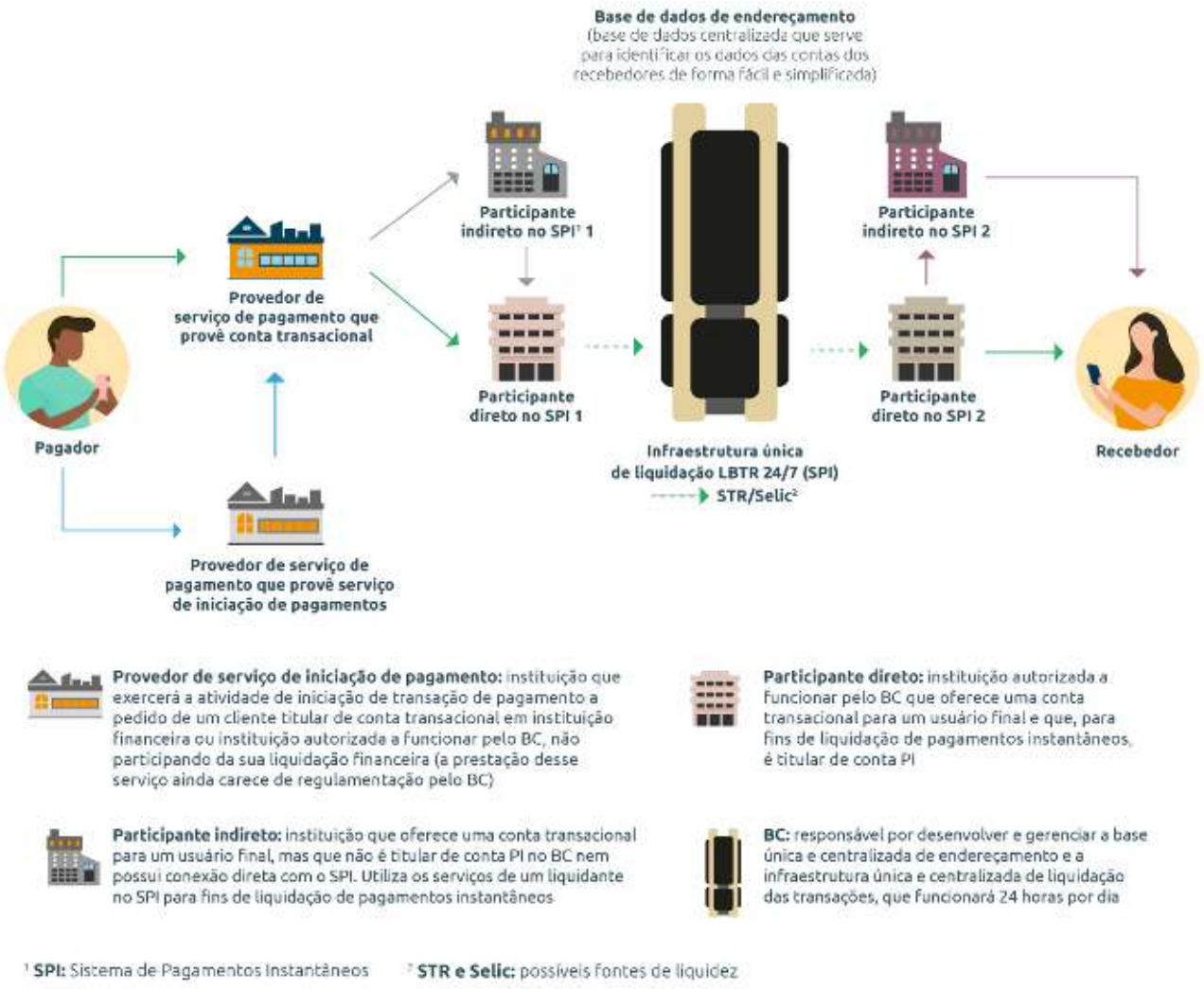

Figura 3.3 – Fluxo de informação do Pix

3.2 Dados físicos

O BCB possui aproximadamente 200 mil caixas contendo processos físicos abertos ao longo de sua história. Entretanto, esse montante não aumenta desde 2018, podendo inclusive ser reduzido por meio da eliminação de documentos físicos, obedecidas as regras estabelecidas na Tabela de Temporalidade publicada pelo Conselho Nacional de Arquivos (Conarq). Todavia, existem documentos de guarda permanente, o que impossibilita a eliminação completa da quantidade de documentos físicos sob a guarda do BCB.

A partir de 2018, com a adoção da retenção dos documentos físicos no protocolo, os servidores do BCB trabalham com a versão digitalizada desses papéis, ou seja, com uma cópia autenticada cadastrada com seus metadados (remetente e destinatário). Os documentos físicos são mantidos em dossiês nos arquivos do BCB até que cumpram seu prazo de guarda e possam ser eliminados ou enviados para guarda permanente.

Nenhum dado pessoal é cadastrado pelo protocolo ou gerenciado pelos arquivos físicos do BCB. Todas as operações relativas a documentos físicos (localização, retirada da caixa, envio para caixa, entrega para o

servidor, recebimento do servidor, arquivamento e eliminação) são feitas pela equipe do protocolo e do arquivo, composta por servidores e terceirizados.

Os documentos físicos do BCB são arquivados pelo tempo definido pela Tabela de Temporalidade do BCB. Somente pessoas lotadas nas áreas que cuidam de determinado assunto (de acordo com os Códigos de Classificação de Assunto do Conarq) podem pedir para consultar um documento físico arquivado. Há casos excepcionais, como documentos do Departamento de Gestão de Pessoas, Educação, Saúde e Organização (Depes), que podem ser consultados também pelo servidor titular dos dados.

As cópias dos documentos físicos, autenticadas e enviadas para as áreas de destino, são classificadas como restritas, cabendo ao destinatário reclassificá-las como ostensivas, se for o caso. Documentos restritos somente podem ser visualizados por seu possuidor. Caso um documento físico recebido pelo protocolo seja classificado, pelo remetente, como sigiloso, seu envelope é encaminhado lacrado para o destinatário, cabendo a ele o devido tratamento da informação. Esses documentos são armazenados pelas áreas-fim do BCB, não sendo enviados para o arquivo.

A Figura 3.4 ilustra o fluxo de informações dos documentos físicos protocolados no arquivo.

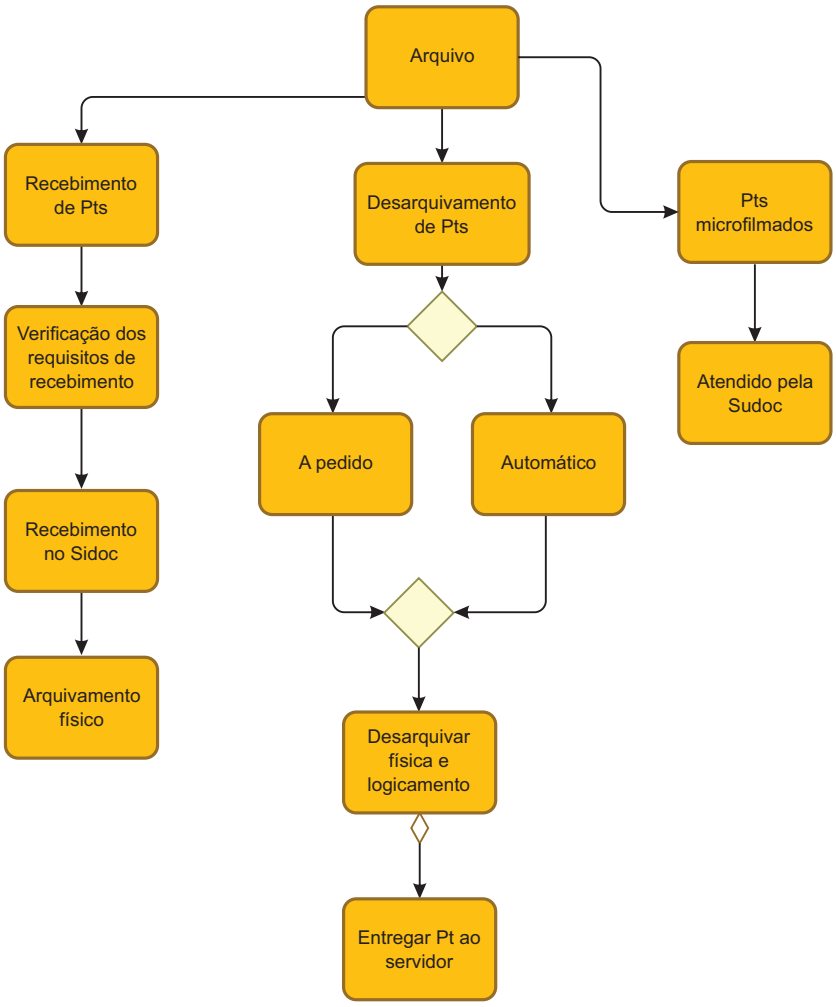

Figura 3.4 – Fluxo de informação de documentos físicos

3.3 Escopo do tratamento

O escopo representa a abrangência do tratamento de dados. As seções seguintes mostram detalhes sobre a extensão do escopo para os dados digitais. Com relação aos dados contidos em documentos físicos, conforme visto anteriormente, recebem o mesmo tratamento dos digitais, pois são digitalizados assim que adentram o Protocolo do BCB.

3.3.1 Tipos de dados

O BCB, por meio de um convênio com a Receita Federal do Brasil (RFB), recebe dados de pessoas físicas, que contemplam as seguintes informações: número do CPF; nome completo; data de nascimento; sexo; nome completo da mãe; endereço completo; telefone; indicativo de estrangeiro; situação cadastral; data de óbito (atualmente apenas o ano é recebido); indicativo de residente no exterior; código do país e nome do país, caso seja residente no exterior; código e descrição da natureza da ocupação principal; código e descrição da ocupação principal; exercício a que se referem os códigos de natureza da ocupação e código da ocupação principal; data de inscrição; data da última operação de atualização e nacionalidade. Esses dados são armazenados em um banco de dados (DB2) e copiados para outros ambientes diariamente (p. ex.: SQLServer, Teradata e Adabas) para atender às necessidades das unidades do BCB.

Por sua vez, o Departamento de Operações Bancárias e de Sistema de Pagamentos (Deban) possui dados pessoais armazenados no Datawarehouse e no SqlServer departamental. Essas informações são recebidas pelo Sistema de Transferência de Reservas (STR) ou pelo Sistema de Pagamentos Instantâneos (SPI).

O STR contém as seguintes informações: nome completo, CPF, banco,[11] agência, conta, tipo de conta para o STR; quanto ao SPI, esse possui nome completo, CPF, banco, agência, conta, tipo de conta e id da conta – telefone, *e-mail*, endereço virtual para pagamento (EVP).

As mensagens que trafegam no STR e no SPI possuem informações incluídas externamente, portanto, sem controle do BCB (podem conter desde a finalidade da transferência até dados pessoais).

Há ainda os dados do Programa de Assistência à Saúde dos Servidores do Banco Central (PASBC) que são sensíveis.

Diversas outras bases de dados possuem dados pessoais no BCB. A seguir são elencados alguns exemplos de sistemas e seus respectivos dados:

- RDR – registros de reclamação do cidadão – Informações da atividade financeira do titular, tais como extratos bancários, movimentações de cartão de crédito, dados específicos de operações de crédito;
- RDR – pedidos de informação do cidadão – Armazenamento de dados replicados de outras bases mediante solicitação específica do cidadão (p. ex.: CCS, SCR, CCF, Cadin e Câmbio);
- CCS – Relacionamentos mantidos com bancos e outras instituições autorizados a funcionar pelo Banco Central;
- SCR – Informações como saldo devedor, modalidade (p. ex.: empréstimo consignado, cartão de crédito, cheque especial) e *status* (a vencer ou vencida) de empréstimos e financiamentos contratados em cada banco ou outra instituição autorizada a funcionar pelo Banco Central;

11 Por banco entende-se qualquer instituição participante do SPI.

- Câmbio – Informações sobre as operações de câmbio ou de transferências de valores com o exterior em determinado período;
- Cadin – Informações das dívidas com órgãos e entidades credores da Administração Pública Federal, direta e indireta;
- CCF – Informações sobre cheques devolvidos, que geram inclusão nesse cadastro;
- Capitais Brasileiros no Exterior (CBE) – valores de qualquer natureza mantidos fora do país por residentes no Brasil (atendimento exclusivo aos Poderes da República).

No âmbito do Pix, teremos dados de natureza bancária e dados de cunho pessoal. Os dados bancários são referentes às informações específicas da transação (pagador, recebedor, valor, frequência, descrição). As transações contarão com os mecanismos de segurança hoje utilizados para as transações que cursam no STR para a realização de Docs e TEDs, tais como mensageria e criptografia. Esses dados são protegidos pela legislação de sigilo bancário vigente.

Por sua vez, informações de cunho pessoal envolvem dados do pagador e do recebedor. São informações tais como nome, CPF, telefone ou *e-mail*, que são mantidos no Diretório de Identificadores de Contas Transacionais (DICT) para fins de cadastramento e manutenção das chaves de pagamento. O DICT possui mecanismos próprios para proteção da base, p. ex.: ataques de leitura à base de dados.

3.3.2 Volume de dados

Há diversas bases que possuem dados pessoais no BCB. Uma das mais relevantes é a que recebe diariamente dados cadastrais de pessoas físicas enviados pela RFB. Essa base possui aproximadamente 254 milhões de registros, sendo recebidos diariamente entre 30 e 50 mil registros. Em alguns períodos, como no de declaração do IRPF, esse número pode subir para alguns milhões por dia. Os dados recebidos são descritos em convênio firmado entre os órgãos e foram informados na seção 3.3.1.

Os dados de pessoas físicas recebidos do convênio com a RFB, armazenados em um banco de dados principal (DB2), possuem aproximadamente 79 gigabytes. Esses dados são copiados diariamente para outros ambientes (p. ex.: SQLServer, Teradata, Adabas) para atender às necessidades dos departamentos do BCB.

3.3.3 Frequência de tratamento dos dados

O BCB recebe diariamente atualizações de dados cadastrais de pessoas físicas, seja por demandas de registros de reclamação e pedidos de informação no atendimento ao cidadão, seja por demandas dos órgãos públicos ou relacionamento com o Sistema Financeiro Nacional (SFN).

3.3.4 Retenção dos dados

No Catálogo de Informações, o curador pode definir o tempo de retenção e de descarte para cada base de dados. Essas informações dizem respeito a toda a base de dados e não especificamente aos dados pessoais nela contidos.

As informações presentes nas bases de dados do RDR e nos outros sistemas listados na seção 3.3.1 não são eliminadas. Os documentos físicos recebidos no atendimento ao cidadão possuem guarda permanente.

Todos os dados utilizados para atendimento aos órgãos públicos são armazenados pelo BCB e não são eliminados.

3.3.5 Titulares afetados pelo tratamento de dados

Qualquer pessoa física ou jurídica, cliente ou usuária de serviços financeiros/bancários, pode ser afetada pelo tratamento de dados no BCB.

3.4 Contexto do tratamento

O BCB trata os dados pessoais de acordo com os propósitos legítimos e específicos de modo compatível com a sua finalidade, cujo caráter é de interesse público, e objetiva executar as competências legais ou cumprir as atribuições legais do serviço público.

3.4.1 Natureza do relacionamento do BCB com os cidadãos

As informações apresentadas pelo cidadão no RDR ajudam no processo de regulação e fiscalização do SFN. Além disso, o BCB organiza e disponibiliza para o cidadão informações financeiras, como saldos de operações de empréstimos e financiamentos, e relação de instituições que mantêm contas e relacionamentos.

3.4.2 Métodos de controle pelo cidadão

O cidadão pode acessar seus dados pessoais por meio de pedidos de informação via RDR. Quanto à alteração de dados, isso deve ser realizado diretamente na instituição supervisionada pelo BCB, da qual o cidadão seja cliente.

O cidadão pode ainda consultar seus dados por meio de sistemas de informação (p. ex.: o Registrato) ou contatar o BCB pelos canais existentes (p. ex.: Fale Conosco ou presencialmente).

3.4.3 Tratamento de dados que envolvem crianças, adolescentes ou outro grupo vulnerável

Esses grupos podem realizar operações e manter relacionamento com as instituições do sistema financeiro e, consequentemente, podem ter seus dados pessoais no BCB. Contudo, para acesso aos dados, devem ser observados requisitos de representação legal, no caso de civilmente incapazes.

Há também dados de dependentes de servidores do BCB referentes ao PASBC que envolvem crianças e adolescentes.

3.4.4 Tratamento de dados conforme determinação legal

O tratamento de dados é aquele previsto em regras públicas e comunicados transparentes. No caso do CCS, por exemplo, haverá cruzamento de dados entre a sua base, no banco de dados Teradata, e outras bases existentes no BCB, que registram relacionamentos bancários, com o objetivo de melhorar a qualidade das informações, detectar inconsistências, corrigir falhas e fornecer subsídios à fiscalização quando detectadas possíveis fraudes.

3.4.5 Experiências anteriores

O BCB já demonstra ter precaução com as informações que coleta e manuseia, tendo em vista não somente a importância desses dados para a economia e o sistema financeiro do país, mas também a natureza sigilosa de boa parte deles. As obrigações previstas na Lei Complementar (LC) 105, 10 de janeiro de 2001, conhecida

como Lei do Sigilo Bancário, criam um regime de restrição ao acesso não autorizado a muitas das informações pessoais regidas pela LGPD.

3.4.6 Avanços em tecnologia e segurança

As seguintes ferramentas de proteção de dados estão em avaliação:

- Microsoft – permite configurar políticas para classificar, rotular e proteger dados com base em seu nível de confidencialidade. A classificação pode ser totalmente automática, coordenada pelos usuários ou baseada em recomendação. Também é possível definir quem pode acessar dados e o que as pessoas podem fazer com eles – por exemplo, permite a exibição e edição de arquivos, mas não o seu encaminhamento e impressão. Os dados são protegidos, estejam eles armazenados em infraestruturas locais ou na nuvem;
- Informática PowerCenter/TDM – permite a anonimização dos dados;
- Guardium – possui funcionalidades de anonimização de dados armazenados em DB2 ou SQL Server.

Questões práticas em relação ao desempenho no uso dos dados e espaço de armazenamento ainda estão sendo avaliadas.

3.5 Finalidade do tratamento

A finalidade do tratamento dos dados pelo BCB relaciona-se ao estrito cumprimento de obrigação legal ou regulatória, assim como à execução de políticas públicas no âmbito da atuação regulatória do SFN.

4 Partes interessadas consultadas

Para confecção deste Relatório, todas as unidades do BCB foram consultadas. A partir de março de 2020, realizaram-se avaliações de conformidade à LGPD, segundo padrão metodológico desenvolvido pelo Departamento de Riscos Corporativos e Referências Operacionais (Deris), baseado nas melhores práticas de gerenciamento de conformidade. Até o momento, foram realizadas 109 avaliações de conformidade à LGPD por mais de 40 unidades componentes organizacionais do BCB.

5 Necessidade e proporcionalidade

O tratamento de dados é limitado ao mínimo necessário para a realização das finalidades informadas ao titular. Quando necessário, tem abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

O tratamento é feito apenas quando é indispensável e com propósito de cumprimento de obrigação legal e regulatória, monitoramento do sistema financeiro, pesquisa e divulgação de estatísticas para cálculo e divulgação de indicadores agregados (sem consultas individualizadas).

Com o objetivo de assegurar que o operador realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição, todo servidor ou terceirizado deve seguir o Código de Conduta dos servidores do BCB. Além disso, os sistemas de informação possuem logs e controles de acesso.

6 Riscos à Proteção de Dados Pessoais

Os riscos podem ser divididos em riscos de origem financeira – risco de mercado, crédito e liquidez – e riscos de origem organizacional – risco operacional e estratégico – e têm diferentes dimensões de impacto – como impacto financeiro, reputacional e de negócio. Conforme definido por Basileia II, os riscos operacionais contemplam a possibilidade de ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas.

Dentre os tipos de risco operacional, destacam-se os riscos à proteção de dados e informações armazenadas pela instituição, em especial aos dados pessoais. Esse tipo de risco pode ser descrito como potencial evento que gera impacto sobre o titular de dados pessoais e sobre o BCB. No Anexo I, “Gerenciamento dos Riscos à Proteção de Dados Pessoais”, a metodologia da gestão de risco no BCB é discutida em detalhes.

6.1 Categorias de riscos

Em virtude da introdução da temática de proteção dos dados pessoais, a metodologia de gestão de riscos operacionais do BCB passou por recente alteração com a inclusão de novas taxonomias para identificação e mensuração dos riscos específicos a esse assunto. No levantamento dos riscos operacionais à proteção de dados pessoais, os eventos potenciais são analisados nas categorias a seguir:

1. Acesso não autorizado	Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.
2. Modificação não autorizada	Modificação de dados pessoais sem a anuência do titular. Viola o princípio da segurança.
3. Perda	Destruição ou extravio de dados pessoais. Viola os princípios da segurança e da prevenção.
4. Apropriação	Apropriação ou uso indébito de dados de pessoais. Possibilidades de fraude e vazamento intencional de dados. Viola os princípios da segurança e da prevenção.
5. Remoção não autorizada	Retirada de dados pessoais sem autorização do titular.
6. Coleção excessiva	Extração de mais dados do que o necessário para a realização do trabalho, ou do que é previsto em Lei ou foi autorizado pelo usuário. Viola o princípio da necessidade.
7. Informação insuficiente sobre a finalidade do tratamento	A finalidade declarada para o uso das informações pessoais é insatisfatória, não é específica ou pode suscitar interpretações diversas.
8. Tratamento sem consentimento do titular dos dados pessoais	Tratamento dos dados pessoais sem a devida prévia permissão expressa, inequívoca e informada do titular, salvo exceções legais.
9. Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Compartilhamento dos dados pessoais com outras entidades privadas (fora da administração pública federal) sem a devida permissão do titular.
10. Retenção prolongada de dados pessoais sem necessidade	Manter os dados pessoais do titular para além do necessário ou do que estava consentido/autorizado. Viola o princípio da necessidade.

11. Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Erro ao vincular dados do verdadeiro titular a outro. Viola o princípio da qualidade dos dados.
12. Falha ou erro de processamento	Processamento dos dados de forma imperfeita ou equivocada. Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc. Viola o princípio da qualidade dos dados.
13. Reidentificação de dados pseudonimizados	Anonimização insatisfatória de dados pessoais sensíveis possibilitando inferir quem é a pessoa em questão. Viola o direito à anonimização.

6.2 Identificação dos riscos

Apresentam-se a seguir exemplos iniciais não exaustivos de riscos identificados e mensurados, de acordo com a metodologia de gerenciamento de riscos operacionais à proteção de dados pessoais:

- vazamento intencional de dados pessoais;
- alteração intencional de dados pessoais;
- permissão indevida para acesso a dados pessoais;
- furto de informações confidenciais;
- divulgação não autorizada de dados pessoais contidos nos documentos e arquivos;
- quebra não autorizada de sigilo bancário;
- invasão de sistemas para coleta de dados pessoais;
- invasão do *site* do BCB por *hackers*.

Uma avaliação completa desse tipo específico de risco está planejada em todos os processos do BC que envolvem o armazenamento de dados pessoais.

6.3 Medidas de tratamento dos riscos

A aplicação da metodologia de identificação e avaliação dos riscos permite classificá-los de acordo com critérios de priorização. Assim, após a validação do tratamento pela alta administração, as ações necessárias para mitigar os riscos são formalizadas pelos departamentos em Planos de Mitigação de Riscos (PMR). A elaboração desses PMR, quando os planos forem necessários, cabe à unidade do BC responsável pelo processo na cadeia de valor. Dessa forma, vários planos de mitigação estão em andamento com o objetivo de reduzir a probabilidade de ocorrência e/ou os impactos dos riscos mapeados. A condução desses planos possui suporte organizacional, em termos de recursos, e apoio da alta administração.

7 Conformidade à Lei Geral de Proteção de Dados Pessoais

Com a publicação da LGPD, que dispõe sobre tratamento de dados pessoais por pessoa natural ou jurídica de direito público ou privado, surgiu a necessidade do Banco Central do Brasil (BCB) rever seus processos no intuito de verificar o estágio atual de conformidade à referida norma.

Dessa forma, ao longo desse ano, as unidades realizaram avaliações de conformidade à LGPD. No Anexo II, "Resumo da Metodologia de Gestão de Conformidade", a metodologia da gestão de conformidade no BCB é apresentada em detalhes.

Conforme mencionado anteriormente, até o momento, foram realizadas 109 avaliações de conformidade à LGPD pelas unidades do BCB. Os principais resultados dessas avaliações podem ser conhecidos nas seções seguintes.

7.1 Impacto da não conformidade e urgência para ação

De acordo com a Figura 7.1, 35% das possíveis não conformidades gerariam impactos de níveis consideráveis (muito alto e alto) para a instituição. Entretanto, para uma melhor medição do grau de conformidade a uma obrigação, a efetividade dos controles implantados, que é representada pela urgência para ação, também deve ser considerada.

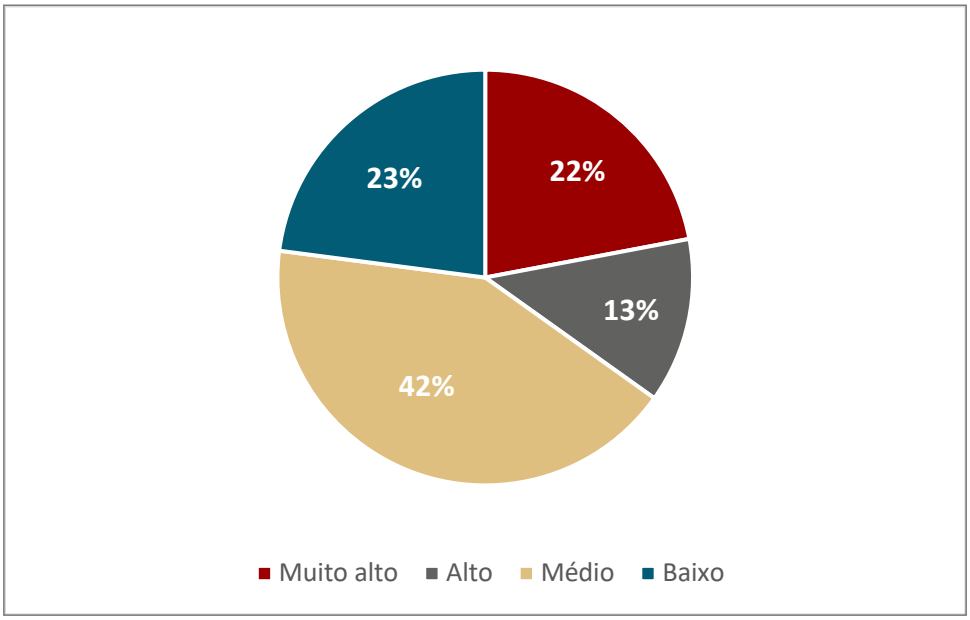

Figura 7.1 – Distribuição das avaliações por nível de impacto de não conformidade

Assim, ao analisar o gráfico da Figura 7.2, verifica-se que grande parte das avaliações (90%) foi aferida com grau de urgência para ação média ou baixa, ou seja, na percepção das unidades, os controles implantados são considerados adequados para garantir o razoável cumprimento da LGPD.

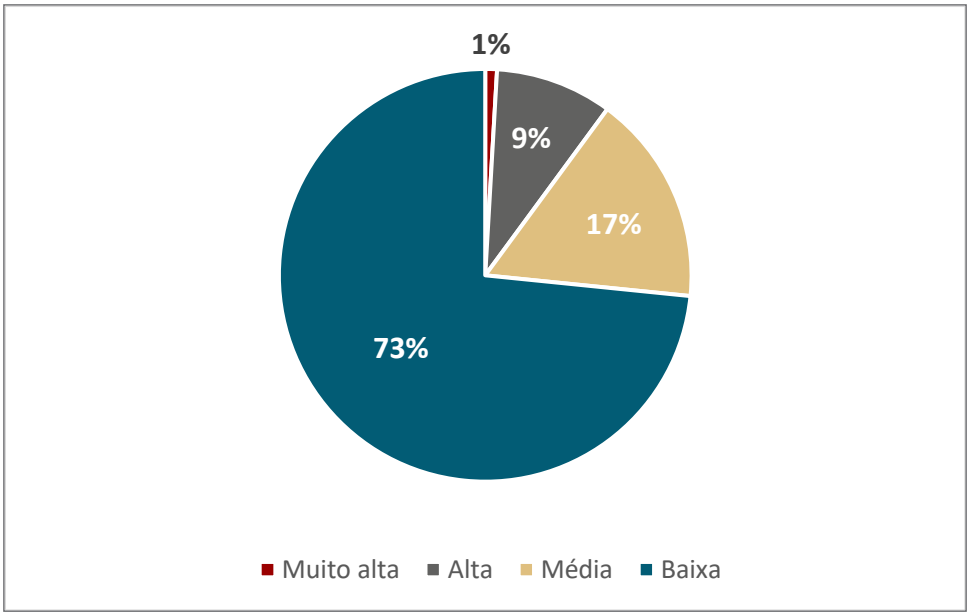

Figura 7.2 – Distribuição das avaliações por nível de urgência para ação

7.2 Criticidade

A partir da composição do impacto da não conformidade e da urgência para ação, encontra-se o grau de criticidade da obrigação avaliada. Conforme a Figura 7.3, somente 4% das avaliações podem ser consideradas críticas.[12] Ressalta-se que o BCB tem implementado ações para reduzir a criticidade dessas avaliações.

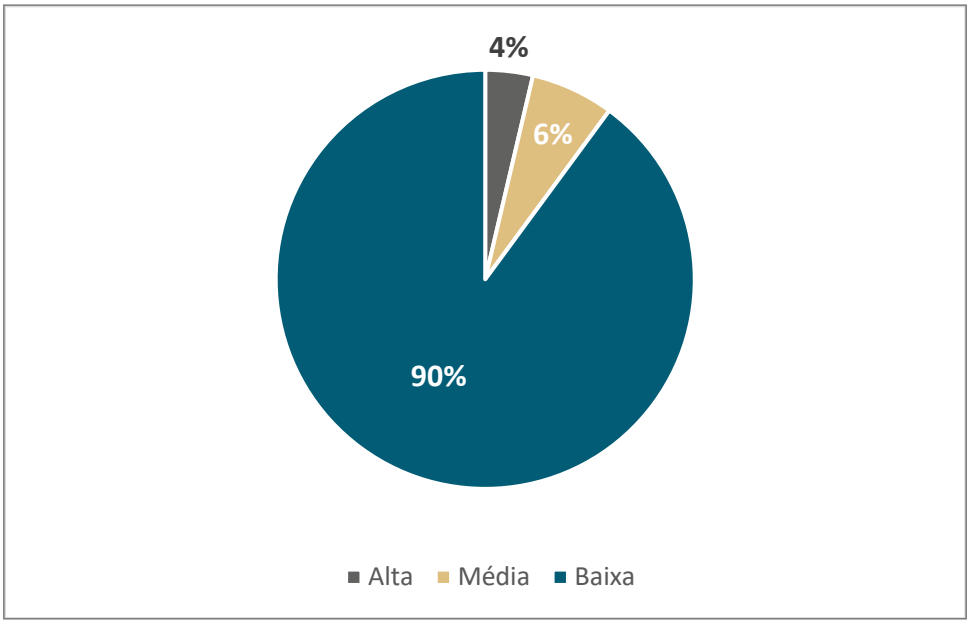

Figura 7.3 – Distribuição das avaliações por nível de criticidade

12 Consideram-se críticas as avaliações aferidas com graus de criticidade muito alto e alto.

7.3 Possíveis causas de não conformidade

Outro fator importante para auxiliar o planejamento de ações pelas unidades é a identificação de possíveis causas de não conformidade. Na Figura 7.4 podem ser vistas as distribuições das causas apontadas nas avaliações críticas. Destacam-se, por representarem cerca de 80% das causas identificadas, organização interna do BCB,[13] tecnologia da informação,[14] e gerenciamento.[15]

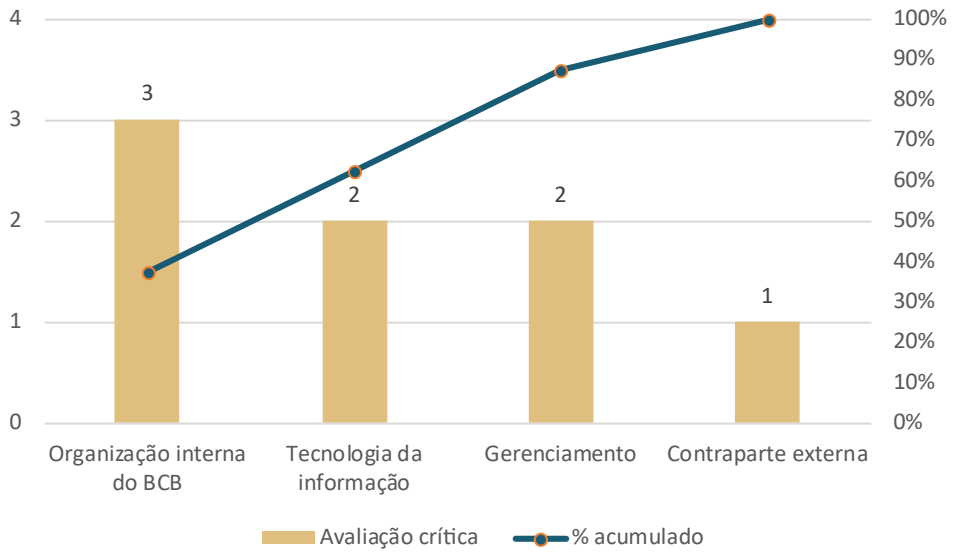

Figura 7.4 – Possíveis causas de não conformidade apontadas nas avaliações críticas

A Tabela 7.1 traz detalhes das possíveis causas de não conformidades indicadas pelas unidades nas avaliações críticas.

Taxonomia de causa	Observações
Organização interna do BCB	- Ainda não foi levantada a base de dados pessoais objeto de tratamento pelas áreas do BCB ou de compartilhamento com outros órgãos. A definição depende de análise jurídica da Procuradoria-Geral do Banco Central (PGBC). - Não há informações do BC sobre dados tratados de forma automatizada (inteligência artificial, algoritmos, tratamentos sem intervenção humana)
Tecnologia da informação	- Deve ser implementada a funcionalidade para distribuição, entre as áreas do BCB, de dúvidas, pedidos de confirmação de tratamento e acesso a dados, pedidos de retificação de dados e pedidos de informações sobre compartilhamento com outros órgãos.
Gerenciamento	- Ainda não definimos os procedimentos para retificações.

Tabela 7.1 – Causas apontadas nas avaliações críticas

13 Não conformidade decorrente de falhas na integração entre unidades e/ou componentes organizacionais.

14 Não conformidade decorrente da indisponibilidade de recursos apropriados de TI.

15 Não conformidade decorrente do gerenciamento no âmbito da própria unidade ou componente organizacional, o qual pode se originar das atividades de planejamento, controle, organização dos recursos, liderança etc.

Ressalta-se ainda que todas as possíveis causas apontadas nas avaliações críticas já estão sendo tratadas, de acordo com o apresentado na Figura 7.5.

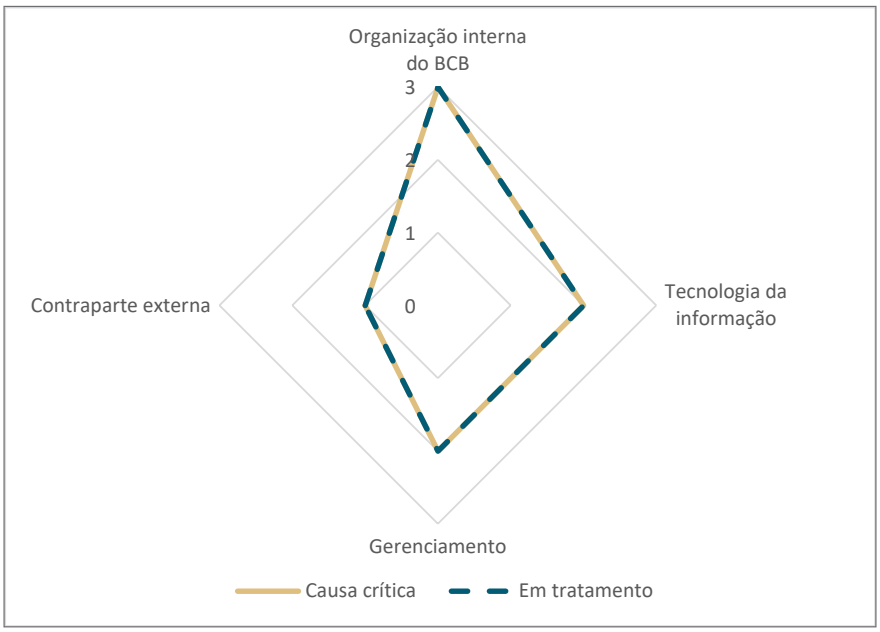

Figura 7.5 – Possíveis causas críticas em tratamento

7.4 Ações de conformidade

Como resultado das avaliações realizadas, as unidades planejaram 63 ações de conformidade, sendo que 17 (ou 27%) já foram concluídas. Daquele total, 11% referem-se às avaliações críticas, como pode ser visto na Figura 7.5. Destacamos, ainda, que todas as avaliações críticas possuem ações de tratamento em implantação no BCB.

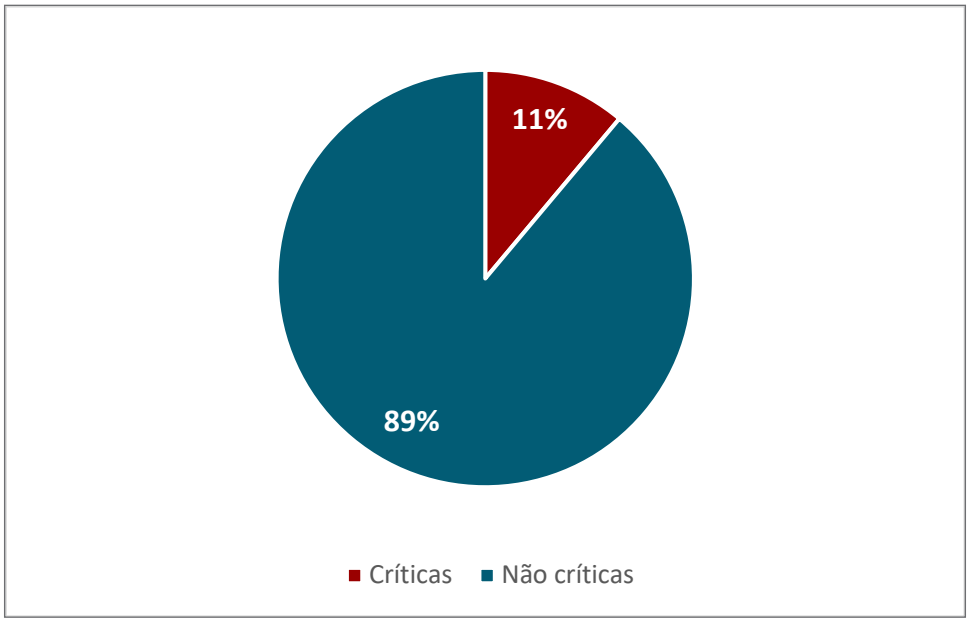

Figura 7.5 – Distribuição de ações de conformidade pela criticidade das avaliações

8 Considerações finais

Este documento demonstra, em linhas gerais, como os dados pessoais são coletados, tratados, usados, compartilhados, bem como as medidas adotadas para o tratamento dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares desses dados. Além disso, foram apresentadas informações que denotam o estágio atual de conformidade do BCB à LGPD.

Este Relatório será revisto e atualizado anualmente ou sempre que a Instituição implementar qualquer tipo de mudança que afete o tratamento dos dados pessoais. O BCB preocupa-se em avaliar continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

9 Aprovação

Responsável pela elaboração do Relatório de Impacto	**Encarregado**
Isabela Ribeiro Damaso Maia Chefe do Deris Brasília-DF, 18 de setembro de 2020	Eugênio Pacceli Ribeiro Secretário-Executivo (interino) Brasília-DF, 18 de setembro de 2020

Autoridade representante do controlador	**Autoridade representante do operador**
Roberto Campos Neto Presidente Brasília-DF, 18 de setembro de 2020	Não se aplica

Anexo I – Gerenciamento dos Riscos à Proteção de Dados Pessoais

De acordo com a ISO 31.000, o risco pode ser definido como o efeito – positivo ou negativo – das incertezas nos objetivos da organização. A gestão de riscos, por sua vez, é o conjunto de ações coordenadas que buscam garantir que os objetivos sejam perseguidos dentro de limites aceitáveis de risco.

O início da formalização de técnicas de gestão de riscos no BCB ocorreu em 1997, com a aplicação de ferramentas de gerenciamento de risco de mercado para a gestão das reservas internacionais. Em 2000, foi desenvolvida abordagem de gerenciamento de riscos financeiros para administração desses ativos e, em 2006, foram criadas uma política e uma estrutura para a gestão de riscos financeiros envolvendo unidades operacionais na área de política monetária. Em 2011, foi formalizada a Política de Gestão de Riscos para toda a Instituição, englobando tanto os riscos financeiros quanto os riscos organizacionais. A Política de Gestão de Riscos do BCB é pautada por diretrizes e recomendações apresentadas nos principais documentos de referência em gestão de riscos nas organizações, e posiciona o BCB entre as instituições que apresentam as melhores práticas.

A seguir é apresentada a metodologia para gerenciamento de riscos operacionais à proteção de dados pessoais adotada pelo BCB e, de forma preliminar, os principais riscos aos quais a Instituição está exposta.

Riscos Corporativos

A gestão integrada de riscos corporativos aplica-se a todos os níveis e unidades do BCB. As informações provenientes da gestão de riscos servem de apoio à tomada de decisão e buscam o fortalecimento da defesa dos processos organizacionais, conforme ilustrado na Figura I.1.

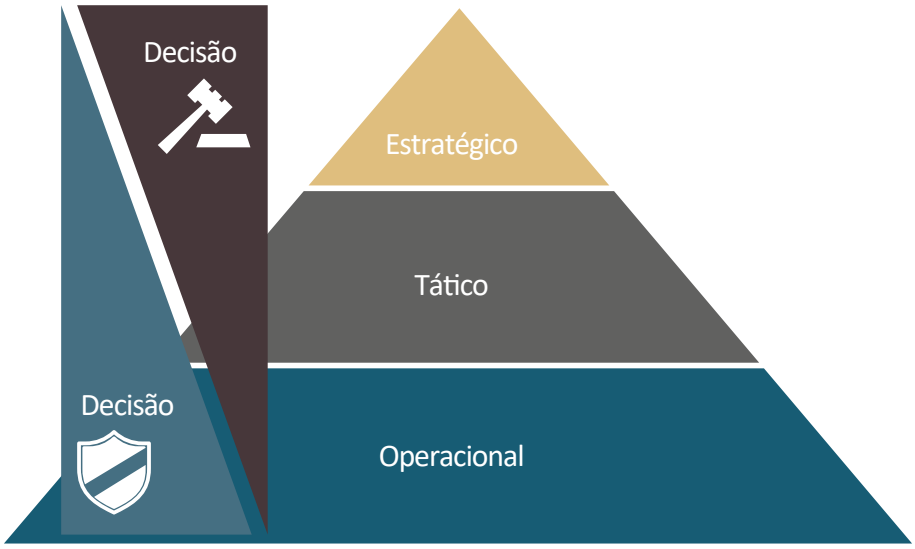

Figura I.1 – Aplicação das informações de gestão de riscos

No nível estratégico, o uso das informações de risco se apresenta como subsídio para a tomada de decisão, como, por exemplo, de alocação de recursos e de definição de ações estratégicas.

No nível operacional, por outro lado, as informações de risco se oferecem especialmente para implantação de medidas adicionais de mitigação e para análise dos potenciais impactos em caso de materialização de eventos de risco.

No nível tático da organização, por sua vez, esses dados de risco servem como abordagens complementares entre as visões de decisão e de defesa.

Metodologia de Gerenciamento dos Riscos à Proteção de Dados Pessoais

O processo de identificação e avaliação de riscos na metodologia de gestão de riscos corporativos do Banco Central do Brasil realiza-se com resultados integrados e analisados por meio de três modelos principais de informações:

i) **modelos de percepção: modelos de avaliação de riscos e controles baseados na percepção dos gestores de cada processo, em que os riscos associados a cada processo, e suas possíveis causas, são identificados e classificados segundo uma taxonomia de risco baseada em eventos. São classificados pela natureza dos eventuais incidentes de impacto negativo como, por exemplo: fraude, furto, erro, interrupção de sistema etc.;**
ii) **modelos de confirmação: modelos que permitem identificar novos riscos, visualizar tendências e conhecer detalhes do comportamento do risco ao longo do tempo, a partir do sistemático registro tanto dos eventos de risco quanto dos quase-eventos, independentemente da severidade da perda;**
iii) **modelos de reconhecimento: modelos que antecipam a evolução de determinada exposição ao risco e que podem ser usados para identificar a exposição de risco atual e as tendências de risco futuras, por meio de técnicas de reconhecimento de padrões e aprendizagem automática.**

A aplicação de modelos de percepção, sob coordenação da equipe do Deris, é realizada pela área gestora do processo no qual se busca compreender as atividades e seus objetivos, identificar os riscos e mensurá-los.

A autoavaliação de riscos, em uma primeira abordagem, é conduzida por entrevistas nas quais são identificados os riscos mais relevantes associados a cada processo de negócio e classificados segundo taxonomia de risco baseada em eventos. Em seguida, é levantada a probabilidade de ocorrência, são avaliados os impactos nas dimensões financeira, reputacional e de negócio, bem como a efetividade dos controles, e apuradas as causas.

O resultado da identificação e da mensuração de riscos organizacionais, ao final dessa etapa, é apresentado na forma de uma matriz de riscos. Pela facilidade de compilação e de visualização, essa matriz estabelece relações entre processos e riscos associados de forma integrada, gerando um panorama geral sobre os graus de exposição de risco. Dessa forma, permite que se tenha uma ampla visão dos processos, ações e projetos, relacionando-os com os potenciais eventos e subsidiando a implantação de medidas de mitigação de riscos por parte da organização.

Os riscos podem, dessa forma, ser classificados nas escalas: “I”, maior prioridade; “II”, prioridade média; e “III”, menor prioridade, em função do impacto e da probabilidade de ocorrência. A Figura I.2 ilustra o processo de elaboração dessa matriz de risco, construída em dois eixos: ocorrência e impacto.

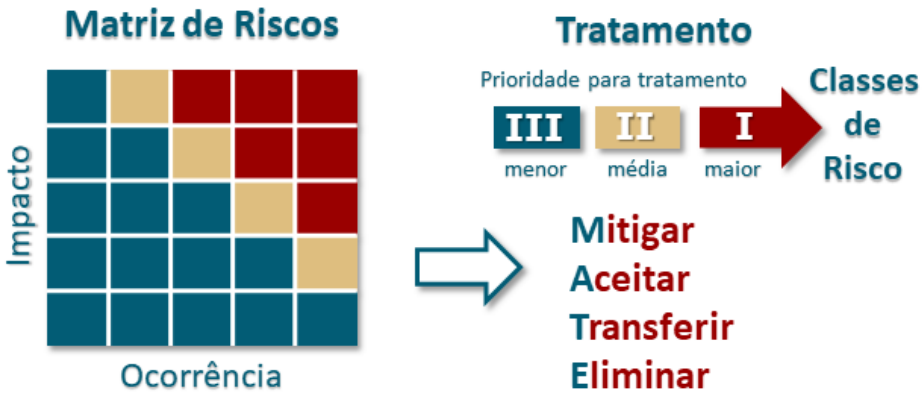

Figura I.2 – Matriz de riscos e definição do tratamento

A partir dos dados da matriz de risco, os gestores do processo devem avaliar a resposta apropriada a cada risco identificado, com o objetivo de adequar a exposição a risco a níveis aceitáveis. Dessa forma, deve-se indicar a ação de tratamento para cada risco, dentre as listadas a seguir:

a) **mitigar o risco: planejar ações de resposta visando reduzir a ocorrência e/ou o impacto do risco, podendo ser, por exemplo, por meio da melhoria dos controles. As ações de mitigação podem envolver mais de uma unidade;**
b) **aceitar a exposição ao risco: o risco residual está no nível aceitável ou o risco é conhecido e não haverá um tratamento devido a fatores como relação custo-benefício não favorável;**
c) **transferir o risco a uma terceira parte: repasse total ou parcial do risco para outra unidade de negócio, órgão ou terceiro; e**
d) **eliminar o risco: implica a decisão de eliminar a atividade geradora do risco. Esse tratamento pode ser entendido como um instrumento de gestão que permite identificar um processo ou uma atividade desnecessária, sendo uma fonte causadora de risco e, assim, deve ser descontinuado.**

A metodologia desse processo de avaliação de risco, ferramenta fundamental para a gestão de riscos, traz como vantagens: facilitar o entendimento do negócio e suas vulnerabilidades, apontar atividades críticas com controles frágeis ou inexistentes, gerar maior qualidade nas informações de risco e trazer flexibilidade ao processo de avaliação.

Governança das Informações de Riscos Organizacionais

Para o levantamento de riscos operacionais, a realização dos trabalhos conta com a colaboração do Agente de Gestão de Risco, que é o ponto de contato entre o Deris e cada unidade de negócio. Após a devida identificação e mensuração, os riscos mapeados são apresentados e homologados pelo chefe da unidade em que tais riscos foram levantados. Posteriormente, a unidade, por meio da chefia, propõe o tratamento adequado para cada risco mapeado. Esse tratamento de risco considera as quatro possíveis alternativas mencionadas anteriormente: mitigar, aceitar, transferir e eliminar.

Na sequência do processo de gestão de riscos operacionais, todos os riscos identificados e as respectivas propostas de tratamento são submetidos ao diretor da área responsável, o qual valida as indicações de tratamento, inclusive os riscos aceitos, de forma que as ações de mitigação possam ser iniciadas. Além do

diretor da área em que o levantamento foi realizado, o Diretor de Assuntos Internacionais e o de Gestão de Riscos Corporativos tomam conhecimento dos riscos de cada unidade.

Cada unidade, após a validação do diretor da área, deve registrar os Planos de Mitigação de Riscos, ou seja, o conjunto de ações de resposta aos riscos identificados no Sistema de Planejamento e Gestão. Por meio desse registro em sistema corporativo, os PMR podem ser acompanhados pelas chefias e pela Diretoria Colegiada, e integram o planejamento da unidade e o orçamento do BCB.

Finalmente, os riscos transversais, ou seja, aqueles que podem ocorrer em diversas funções do BC e/ou causar impacto em diversas áreas de negócio, assim como a existência de ações adotadas para mitigação, são apresentados à Diretoria Colegiada, por meio do relatório anual da Gestão Integrada de Riscos. A Figura I.3 resume o processo de governança das informações de riscos operacionais.

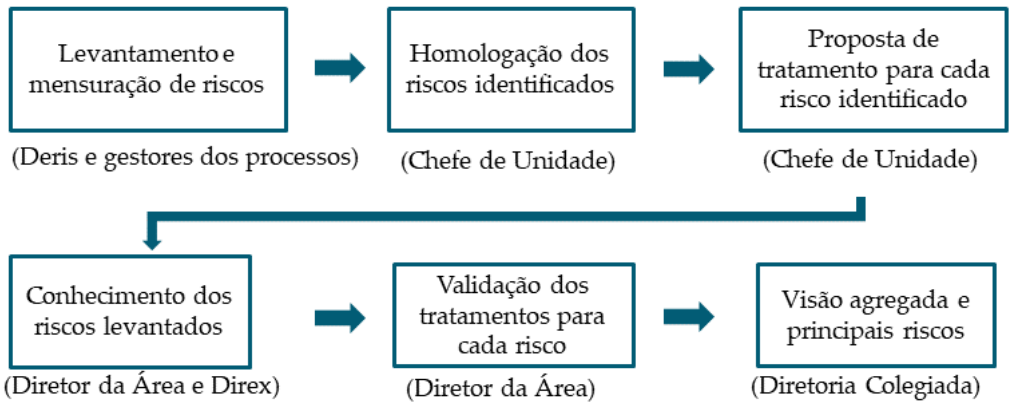

Figura I.3 – Informações de Riscos Operacionais

Anexo II – Resumo da Metodologia de Gestão de Conformidade

O gerenciamento de conformidade, cuja coordenação cabe ao Deris, visa garantir que as atividades executadas por servidores e demais colaboradores sejam conduzidas de acordo com as normas, como leis, decretos e votos, bem como com as fontes não normativas, a exemplo de padrões e procedimentos aplicáveis à Instituição.

Para isso, conforme a Figura II.1, as unidades devem identificar e avaliar a criticidade de suas obrigações. Em seguida, caso necessário, deve-se decidir acerca da implementação de ações de conformidade no intuito de melhorar seus controles internos. O Deris pode auxiliar as unidades nessa atividade por meio de recomendações de conformidade. As informações de conformidade devem ser registradas no sistema *Compliance* e serão monitoradas pela Divisão de Controles Internos da Gestão e Conformidade.

Figura II.1 – Etapas do processo de gerenciamento de conformidade

O grau de criticidade de cada obrigação é obtido a partir da composição do impacto da não conformidade e da urgência para ação. Para isso, as unidades devem observar, em cada avaliação, as escalas descritas na Tabela II.1.

Nível	Impacto da não conformidade	Urgência para ação
Muito alto	Pode acarretar implicações jurídicas à alta administração, colocar indivíduos em risco ou ocasionar restrições significativas ao livre exercício das atividades, violar o dever de cuidado, provocar grandes perdas financeiras (acima de R$1 milhão) e/ou danos prolongados à imagem do Banco.	Não há controles que garantam a observância da obrigação de conformidade, o que requer o planejamento/execução de ação imediata.
Alto	Pode ensejar suspensão temporária de atividades, advertências e/ou outras penalidades, bem como a abertura de sindicâncias ou inquéritos, provocar perdas financeiras (entre R$100 mil e R$1 milhão) e/ou danos à imagem do Banco.	Os controles existentes são inefetivos e insuficientes para garantir a observância da obrigação de conformidade, o que requer o planejamento/execução de ação em momento oportuno ou acompanhamento contínuo da situação.
Médio	Pode deflagrar inspeções, sindicâncias ou inquéritos administrativos, bem como violar o Código de Conduta e/ou ato normativo assemelhado, provocar pequenas perdas financeiras (entre R$10 mil e R$100 mil) e/ou danos de curta duração à imagem do Banco.	Os controles existentes são efetivos, porém insuficientes, para garantir a observância da obrigação de conformidade, o que requer planejamento/execução de ação sem prazo determinado.
Baixo	Pode causar impacto reduzido ao Código de Conduta e/ou ato normativo assemelhado. Não provoca significantes perdas financeiras (abaixo de R$10 mil) e/ou danos à imagem do Banco.	Os controles existentes são efetivos e suficientes, o que não requer o planejamento/execução de ação adicional.

Tabela II.1 – Escalas de impacto da não conformidade e de urgência para ação

Glossário

BCB	Banco Central do Brasil
BacenJud	Instrumento de comunicação eletrônica entre o Poder Judiciário e instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central – https://www.bcb.gov.br/acessoinformacao/bacenjud.
Cadin	Cadastro Informativo de Créditos não Quitados do Setor Público Federal – https://www.bcb.gov.br/acessoinformacao/relatoriodividasetorpublico.
Câmbio	Relatório de Câmbio e transferências internacionais (Operações de Câmbio e Transferências Internacionais) – https://www.bcb.gov.br/acessoinformacao/relatoriocambiotransferencias.
Catálogo de Informações	Catálogo de metadados sobre as bases de dados divulgadas para permitir o entendimento necessário à utilização dos dados, abrangendo também a indicação dos responsáveis pela sustentação de cada base de dados divulgada, de acordo com a Política de Governança da Informação (PGI) do BCB.
CBE	Capitais Brasileiros no Exterior – https://www.bcb.gov.br/estabilidadefinanceira/cbe.
CCF	Cadastros de Emitentes de Cheques sem Fundos – https://www.bcb.gov.br/acessoinformacao/relatoriochequesemfundos.
CCS	Cadastro de Clientes do Sistema Financeiro – https://www.bcb.gov.br/acessoinformacao/relatoriocontasrelacionamentos.
CDNR	Cadastro Declaratório de Não Residente – (um módulo do sistema RDE) – https://www.bcb.gov.br/estabilidadefinanceira/registrocapitaisestrangeiros.
Censo	Censo de Capitais Estrangeiros no País – https://www.bcb.gov.br/estabilidadefinanceira/censocapitaisestrangeiros.
CIP	Câmara Interbancária de Pagamentos.
CONARQ	Conselho Nacional de Arquivos. Órgão colegiado, vinculado ao Arquivo Nacional do Ministério da Justiça e Segurança Pública que tem por finalidade definir a política nacional de arquivos públicos e privados.
DICT	Diretório de Identificadores de Contas Transacionais. Armazena as informações que servem para identificar as contas dos usuários recebedores no Pix.
PASBC	Programa de Assistência à Saúde dos Servidores do Banco Central.
POSTI	Procedimentos Operacionais de Segurança em TI.
PSIBC	Política de Segurança da Informação do BCB.
RDR	Sistema de Registro de Demandas do Cidadão – https://www.bcb.gov.br/acessoinformacao/registrar_reclamacao.
RDE	Registro Declaratório Eletrônico. Registro de capitais estrangeiros no país – https://www.bcb.gov.br/estabilidadefinanceira/registrocapitaisestrangeiros.
Registrato	Ferramenta que permite ao cidadão solicitar, via internet, relatórios com dados do SCR e do CCS.
RFB	Receita Federal do Brasil.

SCR	Relatório de Empréstimos e Financiamentos (Sistema de Informações de Créditos) – https://www.bcb.gov.br/acessoinformacao/relatorioemprestimofinanciamento
SFN	Sistema Financeiro Nacional
Sitraf	Sistema de Transferência de Fundos operado pela CIP.
SPI	Sistema de Pagamentos Instantâneos.
STR	Sistema de Transferência de Reservas.
Tabela de Temporalidade	Ferramenta Essencial na Gestão Documental, pois determina prazos para a eliminação de dados de forma racional. A eliminação de documentos de arquivos deve obedecer às normas do Conarq, especialmente os documentos produzidos por todos os órgãos integrantes do poder público.

BANCO CENTRAL
DO BRASIL