Relatório de Impacto à Proteção de Dados Pessoais

Outubro de 2022

BANCO CENTRAL DO BRASIL

Relatório de Impacto à Proteção de Dados Pessoais

Outubro de 2022

BANCO CENTRAL DO BRASIL

Sumário

1 Identificação dos Agentes de Tratamento e do Encarregado

Controlador
Banco Central do Brasil

Operador
Não se aplica

Encarregado
Leonardo Martins Nogueira – Secretário-Executivo

E-mail Encarregado	Telefone Encarregado
https://www.bcb.gov.br/acessoinformacao/faleconosco	145 (custo de ligação local)

2 Necessidade de Elaborar o Relatório

A Política de Conformidade (*Compliance*) do Banco Central do Brasil (PCO-BC) tem entre seus objetivos assegurar que as atividades do Banco Central do Brasil (BC) 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, Lei Geral de Proteção de Dados Pessoais (LGPD), a qualquer momento a Autoridade de Proteção de Dados Pessoais (ANPD) pode determinar ao BC que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis. Surgiu, assim, a necessidade de se confeccionar este documento.

O BC realiza diariamente o tratamento[1] dos dados pessoais que se relacionam a pessoa natural identificada ou identificável (art. 5º, I, da 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, da 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, da LGPD).

Considerando os fundamentos[2] da proteção de dados pessoais (art. 2º da LGPD), a boa-fé e os demais princípios[3] a serem observados nas atividades de tratamento de dados pessoais (art. 6º da LGPD), o BC 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 BC, 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 Resolução BC 115, de 14 de julho de 2021, visa orientar as ações necessárias à garantia da segurança da informação, o que resulta na mitigação de riscos aos quais estão sujeitos os ativos de informação e que poderiam comprometer as atividades do BC e o cumprimento de sua missão institucional.

Os ativos de informação compreendem "os meios, os locais, os equipamentos e os sistemas de armazenamento, transmissão e processamento da informação" (art. 4º, III, da PSIBC).

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

O BC também conta com a Política de Governança da Informação (PGI-BC), divulgada pela Portaria 90.187, de 17 de agosto de 2016, que contempla segurança e privacidade entre os seus princípios. A PGI-BC define uma estrutura de governança da informação, que inclui entre os seus componentes o Comitê de Governança da Informação (CGI), um colegiado deliberativo de nível executivo, o Escritório de Governança da Informação (Eginf), área de apoio e secretariado técnico ao CGI, e a Auditoria de Observância (AO), que supervisiona as obrigações de remessa e prestação de informações ao BC pelas instituições integrantes do Sistema Financeiro Nacional (SFN). Algumas ferramentas são utilizadas como base para as ações de governança da informação, sendo uma delas o Catálogo de Informações, que mantém registro de todas as bases de dados da instituição.

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.

Nessa ferramenta, são mantidos diversos metadados para cada uma das bases de dados, sendo alguns deles relativos ao tratamento e à proteção de dados pessoais.

Adicionalmente, como órgão regulador e supervisor do SFN, o BC mantém, com as instituições reguladas e supervisionadas, contratos de utilização de serviços para o ecossistema denominado Sisbacen, conforme Circular 3.913, de 5 de setembro de 2018, que assegura a finalidade e o sigilo dos dados enviados a esta Autarquia.

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 BC e ao dar cumprimento às disposições contidas na PSIBC e no Código de Conduta dos Servidores do BC, especialmente no que se refere ao acesso a informações, arts. 8º, 9º 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 BC, considerando a definição da LGPD:

- Coletados/Enviados

Os dados são coletados principalmente por meio de sistemas de informação pertencentes ao Sisbacen, conforme regulamento estabelecido pela Circular 3.913, de 5 de setembro de 2018, e por captação de informações de entidades externas, seja por força de regulação, seja por acordos e convênios firmados. Os dados de captações, por arquivos, são recebidos, em geral, por meio do Sistema de Transferência de Arquivos (STA). Tanto as novas captações de informação quanto as novas bases de dados criadas são objeto de análise no âmbito da governança da informação, observando a devida adequação à LGPD.

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.

O BC, por meio de seus serviços digitais, pode ainda captar informações fornecidas por pessoas físicas, usuárias desses serviços. A captação e o uso desses dados se sujeitam à Política de Privacidade e Termos de Uso do *site*, dos aplicativos e dos serviços digitais do BC.

- Retidos/Armazenados

Os dados são mantidos em sistemas gerenciadores de banco de dados e em servidores de arquivos, nos quais os acessos são restritos, de acordo com os conteúdos armazenados.

- Usados

Os dados são usados em processos de trabalho das unidades do BC (também chamadas neste relatório de Departamentos), em agregações analíticas ou em análises singulares, quando pertinente ao processo de trabalho do departamento e com justificada finalidade.

- Eliminados

O curador[8] pode indicar no Catálogo de Informações[9] que uma base de dados deve ser desativada. 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, e deve ser fornecida uma justificativa para a desativação.

O Eginf, vinculado ao Departamento de Tecnologia da Informação (Deinf), executa processo para a desativação de bases de dados, que inclui avaliação do uso dos dados no BC. 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 BC são:

- captações de informações externas: são enviados arquivos de dados com informações pessoais pelo STA. Os arquivos são remetidos por entidades supervisionadas, participantes do Sisbacen, e por outros entes que possuem acordo ou convênio com o BC;
- sistemas de informação: *site*, aplicativos e serviços digitais ao cidadão, sistemas de mensageria em tempo real e demais sistemas eletrônicos do ecossistema do Sisbacen;
- 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 segue o determinado pelo Decreto 10.046, de 9 de outubro de 2019, e os preceitos expressos na PGI do BC, aderentes à LGPD. O BC compartilha dados com as instituições reguladas pelo BC apenas com autorização expressa ou presumida do titular. O BC também pode compartilhar os dados protegidos pelo sigilo bancário com órgãos dos Poderes Judiciário, Executivo e Legislativo, e do Ministério Público, para fins de

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 PGI do BC.

instrução de processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como com autorização judicial.

No Catálogo de Informações do BC, 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.

3.1.5 Adoção de nova tecnologia para tratamento dos dados

A adoção de novas tecnologias para tratamento dos dados é objeto de permanente atenção do BC, no sentido de garantir a conformidade com a LGPD, em particular os direitos dos titulares dos dados pessoais.

3.1.6 Medidas de segurança

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 a eliminação). Nesse processo, são utilizados diversos sistemas, tecnologias e ferramentas para permitir a criptografia e o controle de acesso de forma integrada.

A PSIBC é regida pelos seguintes princípios da segurança da informação: disponibilidade; integridade; confidencialidade; autenticidade; irretratabilidade; privilégio mínimo; necessidade de conhecer; proteção dos dados pessoais; e proteção da privacidade.

Esses princípios e as diretrizes constantes na PSIBC visam à garantia da segurança da informação do BC, independentemente do meio em que ela se encontre. Além disso, a PSIBC ainda prevê que o Deinf poderá publicar normas complementares relacionadas ao segmento de TIC que priorizem a segurança da informação, bem como os princípios e diretrizes que a norteiam, ou seja, os normativos de segurança da informação do BC fornecem o arcabouço necessário para que os dados pessoais estejam protegidos durante seu tratamento.

Ressalta-se que os ativos de informação destinados à eliminação, seja em meio físico ou digital, são devidamente inutilizados, assegurando a segurança da informação e o atendimento aos princípios que regem a PSIBC.

3.1.7 Fluxo de dados

Os dados coletados e, eventualmente, compartilhados pelo BC trafegam pelo Sistema de Transferência de Arquivos (STA) na Internet; por sistemas de informação do ecossistema Sisbacen, na Internet ou em rede privada, conforme cada serviço; e por mensageria, pela Rede do Sistema Financeiro Nacional (RSFN).

Os usuários de serviços digitais fornecidos pelo BC podem, ainda, informar seus dados pessoais, conforme cada serviço e de acordo com os seus termos de uso. Cabe destacar que o BC pode oferecer e consumir serviços de dados com outros entes governamentais. A Figura 3.1 ilustra o fluxo genérico de dados.

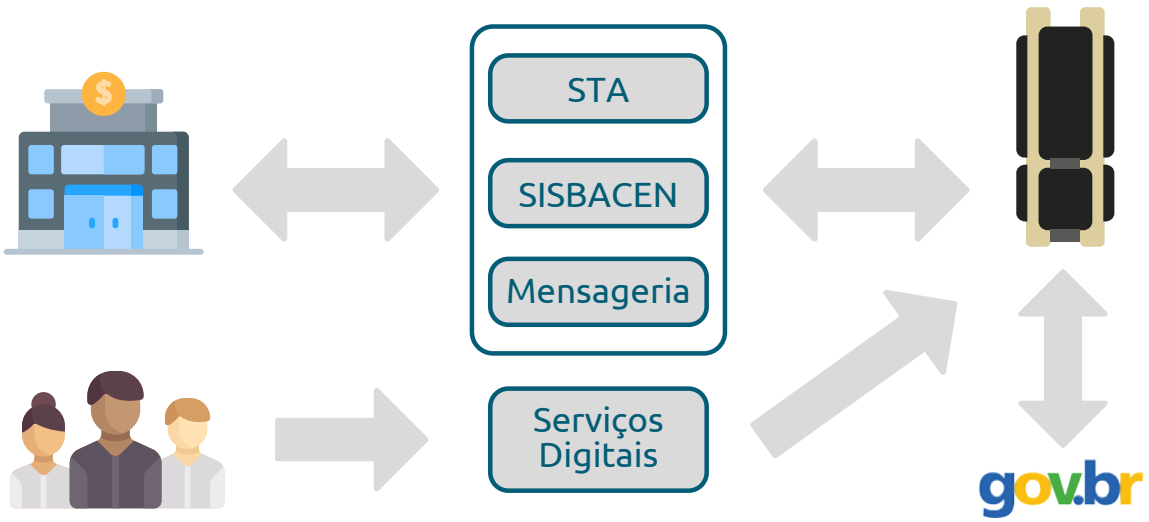

Figura 3.1 – Fluxo genérico de dados

3.2 Dados físicos

O BC 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 BC.

A partir de 2018, com a adoção da retenção dos documentos físicos no protocolo, os servidores do BC 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 BC 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 BC. 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 BC são arquivados pelo tempo definido pela Tabela de Temporalidade do BC. 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 este o devido

tratamento da informação. Esses documentos são armazenados pelas áreas-fim do BC, não sendo enviados para o arquivo.

A Figura 3.2 ilustra o fluxo de informações dos documentos físicos protocolados no arquivo.

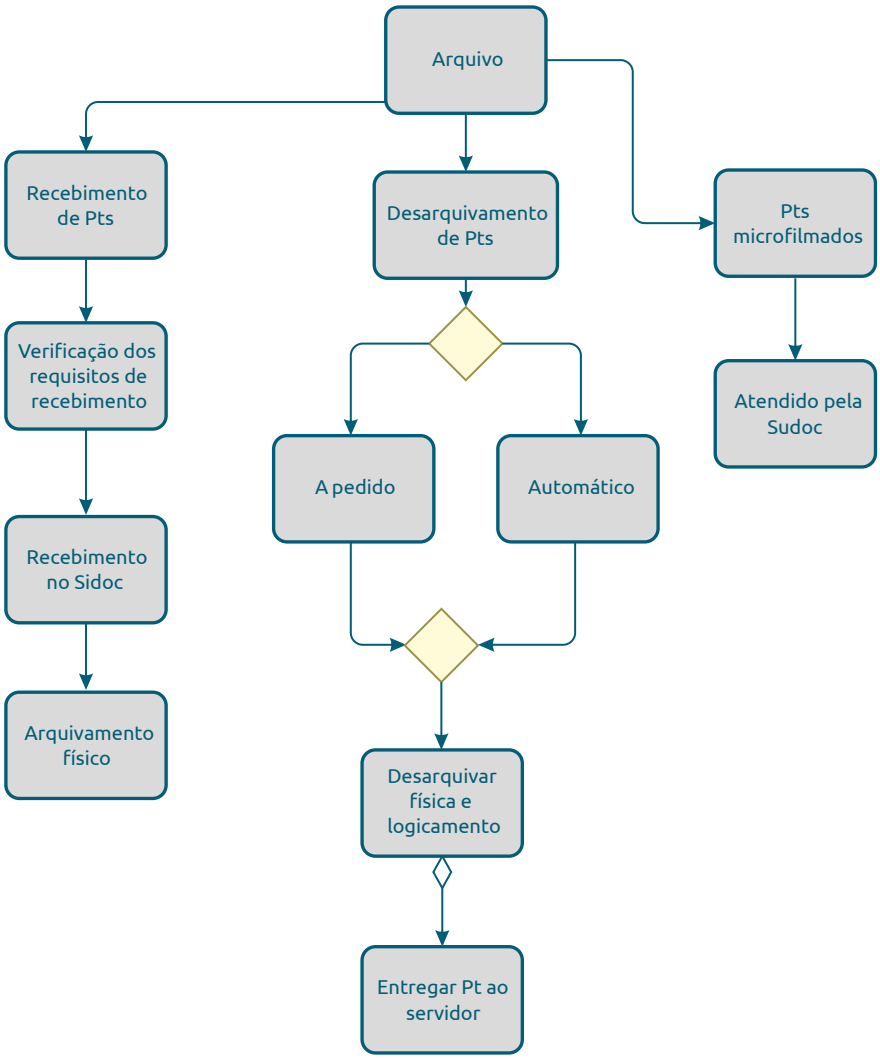

Figura 3.2 – Fluxo de informação de documentos físicos

3.3 Escopo do tratamento

O escopo representa a abrangência do tratamento de dados.

Conforme visto na seção 3.2 deste Relatório, os dados contidos em documentos físicos recebem o mesmo tratamento dos digitais, pois são digitalizados assim que adentram no Protocolo do BC.

Os dados digitais são aqueles de sistemas previstos no Sisbacen (incluídos os de captações de arquivos), nos serviços digitais do gov.br e nos sistemas de mensageria, todos previstos em normativos específicos e públicos, cujas bases de dados são divulgadas no *site* do BC.

As seções seguintes mostram detalhes sobre a extensão do escopo para os dados digitais.

3.3.1 Tipos de dados

O inventário das bases de dados do BC está disponível em: https://www.bcb.gov.br/acessoinformacao/dadosabertos.

3.3.2 Frequência de tratamento dos dados

O BC trata dados pessoais diariamente, por seus sistemas de informação, conforme estabelecido pelas finalidades e pelos regulamentos de cada sistema.

3.3.3 Retenção dos dados

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

3.3.4 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 BC.

3.4 Contexto do tratamento

O BC 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 BC com os cidadãos

O BC presta importantes serviços aos cidadãos, especialmente por meio de canais digitais. A lista completa desses serviços pode ser consultada no portal gov.br. Em alguns casos, há coleta e tratamento de dados pessoais, de acordo com a finalidade descrita no item 3.5 deste Relatório e em conformidade com a legislação.

Os demais dados coletados pelo BC, que são provenientes de entidades supervisionadas ou outros órgãos públicos, também são tratados conforme destacado no parágrafo anterior.

3.4.2 Métodos de controle pelo cidadão

O cidadão pode consultar seus dados pessoais e financeiros custodiados no BC por meio do sistema Registrato. Mais detalhes podem ser obtidos na página “Minha Vida Financeira”. Outras informações podem ser consultadas pelo cidadão por meio do serviço “Fale Conosco” do BC.

Em relação a dados que sejam enviados ao BC por entidade supervisionada no qual o cidadão seja cliente, quando necessário, este deve solicitar à própria entidade ajustes em dados incompletos, inexatos ou desatualizados.

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 BC. Contudo, para acesso aos dados, devem ser observados requisitos de representação legal, no caso de civilmente incapazes.

3.4.4 Tratamento de dados conforme determinação legal

O tratamento de dados pessoais é aquele previsto em normas públicas e comunicados transparentes. A criação de bases de dados obedece ao disposto na PGI-BC, e os curadores devem informar a base legal para o tratamento, no Catálogo de Informações, como pré-condição.

3.4.5 Experiências anteriores

O BC 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 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

Atualmente, estudos e provas de conceito estão sendo realizados pelas áreas técnicas no que se refere ao aprimoramento da gestão de metadados, da classificação/rotulação de informações e da prevenção de vazamentos de dados.

3.5 Finalidade do tratamento

O tratamento de dados pessoais é uma atividade essencial para a prestação de serviços públicos. No BC, os dados são usados principalmente para:

- executar políticas públicas previstas em leis e regulamentos ou permitidas em contratos, convênios ou instrumentos similares;
- cumprir alguma norma;
- avaliar os serviços, identificar problemas, melhorar a segurança e a navegação nas páginas, aplicativos e serviços digitais; e
- dar proteção ao crédito.

4 Partes Interessadas Consultadas

Para a elaboração deste Relatório, todas as unidades do BC foram consultadas. As avaliações de conformidade à LGPD iniciaram em março de 2020, segundo padrão metodológico desenvolvido pelo Deris, baseado nas melhores práticas de gerenciamento de conformidade. Até o momento, foram realizadas 104 avaliações de conformidade à LGPD por mais de quarenta unidades componentes organizacionais do BC.

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 o 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 BC. 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 BC. No Anexo I, “Gerenciamento dos Riscos à Proteção de Dados Pessoais”, a metodologia da gestão de risco no BC é discutida em detalhes.

6.1 Identificação de riscos

Em virtude da introdução da temática de proteção dos dados pessoais, a metodologia de gestão de riscos operacionais do BC 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 seguintes categorias:

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 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 LGPD

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 de o BC rever seus processos no intuito de verificar o estágio atual de conformidade à referida norma. Para isso, foi implantada metodologia da gestão de conformidade apresentada em detalhes no Anexo II, "Resumo da Metodologia de Gestão de Conformidade".

Conforme mencionado anteriormente, até o momento, foram realizadas 104 avaliações de conformidade à LGPD pelas unidades do BC, sendo que houve cinco cancelamentos de avaliações, entre a emissão do relatório anterior e o atual, em virtude de mudança de percepção da análise realizada pelas unidades. Os principais resultados dessas avaliações podem ser conhecidos nesta seção.

7.1 Impacto da não conformidade e urgência para ação

De acordo com a Figura 7.1, 27% das possíveis não conformidades poderiam gerar impactos de níveis consideráveis (muito alto e alto) para a instituição. Entretanto, para 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.

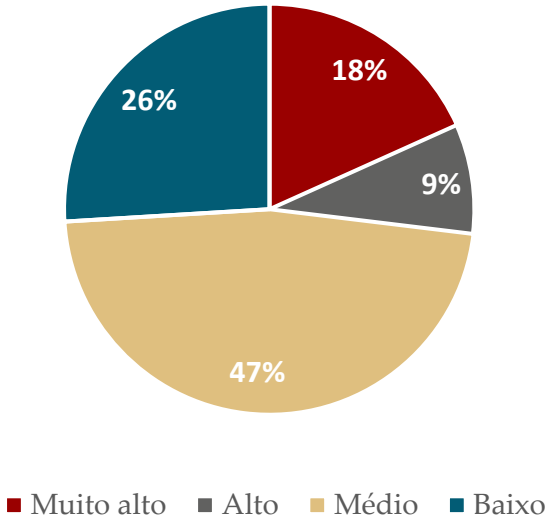

Figura 7.1 – Distribuição das avaliações por nível de impacto de não conformidade

Assim, ao analisar o gráfico da Figura 7.2, verifica-se que todas as avaliações foram aferidas 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.

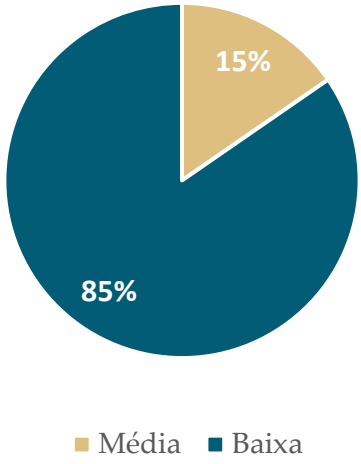

Figura 7.2 – Distribuição das avaliações por nível de urgência para ação

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. Atualmente todas as avaliações possuem criticidade baixa, fruto da implantação de ações de conformidade.[10]

7.3 Possíveis causas de não conformidade

Outro fator importante para auxiliar o planejamento de ações de conformidade pelas unidades é a identificação de possíveis causas de não conformidade. Na Figura 7.3, pode ser vista a distribuição das causas apontadas nas avaliações, que atualmente, em sua totalidade, são não críticas.[11] Destacam-se por representarem cerca de 80% das causas identificadas, tecnologia da informação,[12] recursos humanos,[13] gerenciamento[14] e contraparte externa.[15]

10 Ação definida para prevenção, identificação e correção de procedimentos que facilitem a ocorrência de falhas de conformidade, como por exemplo, implantação ou melhoria de controles e alterações normativas.

11 Consideram-se não críticas as avaliações aferidas com graus de criticidade médio e baixo.

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

13 Não conformidade decorrente de questões relacionadas à gestão dos servidores do BC, tais como alto turnover, insuficiência de quantidade de servidores, greves, desvios de conduta de servidores etc.

14 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.

15 Não conformidade decorrente da relação do BC com contraparte externa.

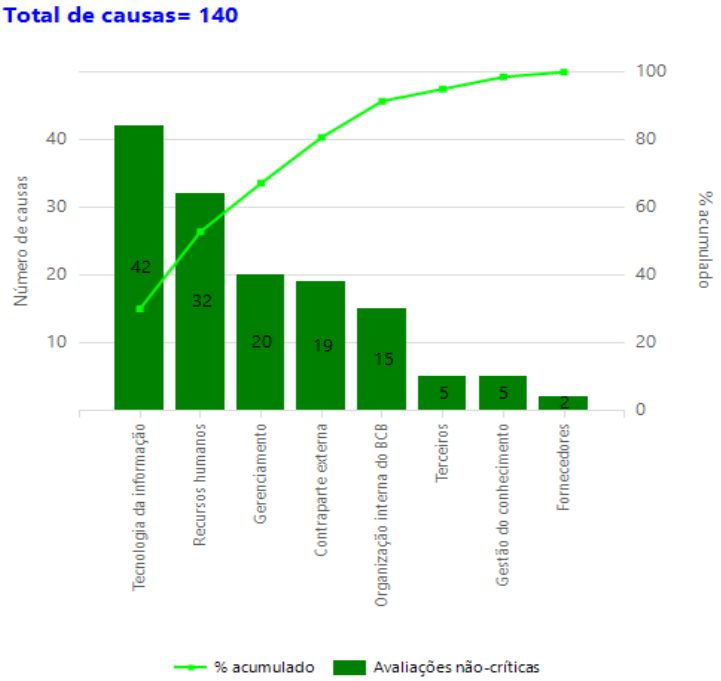

Figura 7.4 – Possíveis causas de não conformidade apontadas nas avaliações não críticas

7.4 Ações de conformidade

Como resultado das avaliações realizadas, as unidades planejaram 66 ações de conformidade, sendo que 60 (ou 91%) dessas já foram realizadas.

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 BC à LGPD

Este Relatório será revisto e atualizado periodicamente ou sempre que a instituição implementar qualquer tipo de mudança que afete o tratamento dos dados pessoais. O BC 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**
José Luiz Barros Fernandes Chefe do Deris Brasília-DF, 16 de setembro de 2022	Leonardo Martins Nogueira Secretário-Executivo Brasília-DF, 16 de setembro de 2022

Autoridade representante do controlador	**Autoridade representante do operador**
Roberto Campos Neto Presidente Brasília-DF, 16 de setembro de 2022	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 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 BC 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 a política e a estrutura para a gestão dos riscos financeiros do BC, envolvendo unidades operacionais na área de política monetária. Em 2011, foi formalizada a Política de Gestão Integrada de Riscos para toda a Instituição, englobando tanto os riscos financeiros quanto os riscos organizacionais. A Política de Gestão Integrada de Riscos do BC é pautada por diretrizes e recomendações apresentadas nos principais documentos de referência em gestão de riscos nas organizações, e posiciona o BC 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 BC 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 BC. 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.

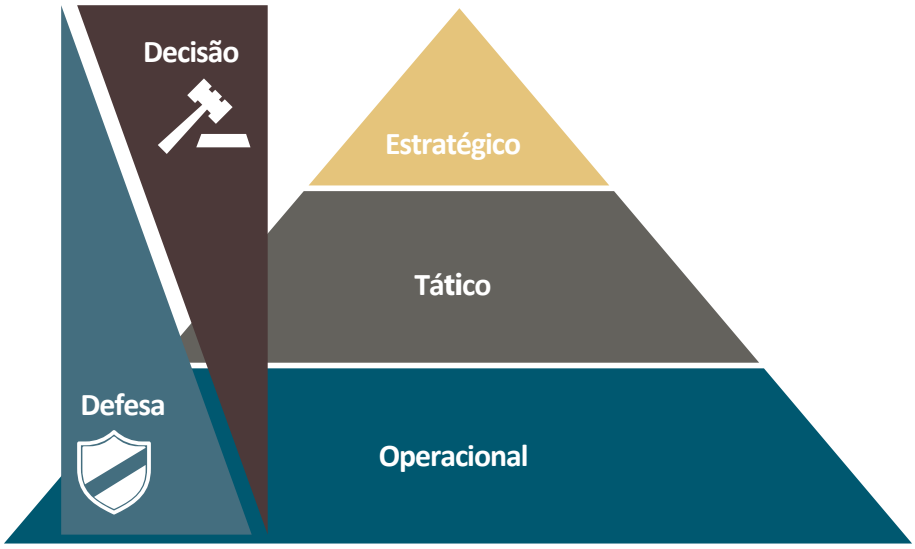

Figura I.1 – Aplicação das informações de gestão de riscos

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 as 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 BC 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 taxonomia de risco baseada em eventos. São classificados pela natureza dos eventuais incidentes de impacto negativo, como 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.

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 ampla visão dos processos, das ações e dos 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.

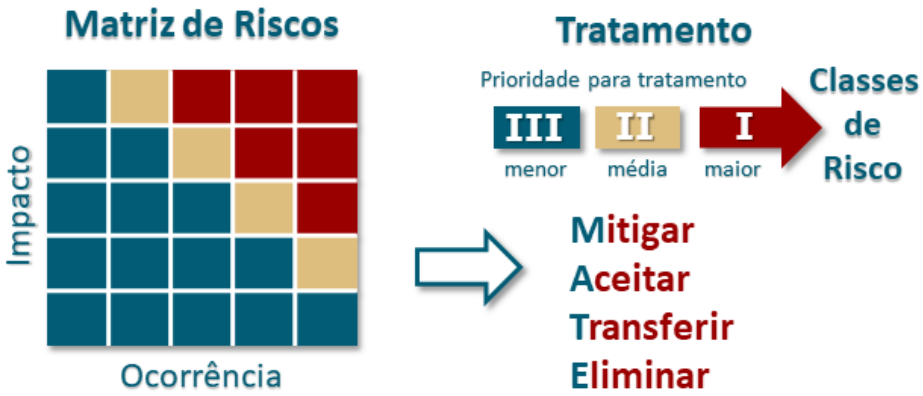

Figura I.2 – Matriz de riscos e definição do tratamento

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, entre 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 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 de Gestão de Riscos Corporativos toma conhecimento dos riscos de cada unidade.

Cada unidade, após a validação do diretor da área, deve registrar os Planos de Mitigação de Riscos (PMR), 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 BC.

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.

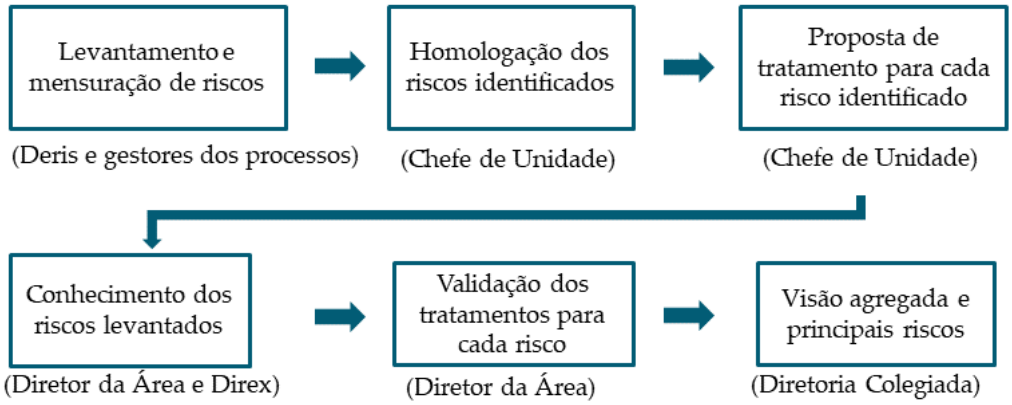

Figura I.3 – Informações de Riscos Operacionais

Anexo II – Resumo da Metodologia de Gestão de Conformidade

O gerenciamento de conformidade, cuja coordenação cabe ao Deris, visa a garantia de 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 BC.	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 abertura de sindicâncias ou inquéritos, provocar perdas financeiras (entre R$100 mil e R$1 milhão) e/ou danos à imagem do BC.	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 BC.	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 BC.	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

BC	Banco Central do Brasil
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 PGI do BC
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.
Mensageria	Sistema de envio e recepção automatizada de informações estruturadas (mensagens) entre seus participantes.
PCO-BC	Política de Conformidade (*Compliance*) do BC
PGI-BC	Política de Governança da Informação do BC
PMR	Planos de Mitigação de Riscos
POSTI	Procedimentos Operacionais de Segurança em TI
PSIBC	Política de Segurança da Informação do BC
RDR	Sistema de Registro de Demandas do Cidadão – https://www.bcb.gov.br/acessoinformacao/registrar_reclamacao
Registrato	Ferramenta que permite ao cidadão solicitar, via internet, relatórios com dados do Sistema de Informações de Crédito (SCR) e do Cadastro de Clientes do Sistema Financeiro Nacional (CCS)
RFB	Receita Federal do Brasil
RSFN	Rede do Sistema Financeiro Nacional – Estrutura de comunicação de dados que tem por finalidade amparar o tráfego de informações no âmbito do SFN para serviços autorizados pelo BC, conforme o disposto na Circular 3.970, de 28 de novembro de 2019. Seu objetivo principal é suportar o tráfego de dados diretamente relacionados a serviços críticos, podendo, desde que não haja interferência em seu objetivo principal, suportar o tráfego de dados de outra natureza
Sisbacen	Conjunto de sistemas e recursos de tecnologia da informação do BC para a condução de seus processos de trabalho
STA	Sistema que tem por objetivo permitir o intercâmbio de arquivos digitais entre o BC e outras instituições cadastradas no Sisbacen, de forma padronizada e segura, por meio de conexões na internet, utilizando o protocolo HTTPS
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