Política de Controles Internos

Banco Société Générale Brasil

(“BSGB”)

Novembro/25

Controle das Versões

nº	*Autor*	*Área*	*Alterações*	*Data da Revisão*
1	Glauber Motta	RISQ	Nova versão	30/11/2025

Aprovação

Nome	*Cargo*	*Versão*	*Data*
Gustavo Rezende	CRO	1	30/11/2025

ÍNDICE

1. Introdução

A Política de Controles Internos ("Política") do Banco Société Générale Brasil S.A. ("BSGB") atende os requisitos regulatórios constantes na Resolução CMN 4.968/2021, nos demais normativos internos e externos aplicáveis e apresenta os principais aspectos a serem observados sobre a estrutura de controles internos implementada no Banco, em linha com as melhores práticas de mercado e com os princípios estabelecidos pelo Grupo Société Générale ("Grupo SG") e pela área de Riscos não financeiros (RISQ/NFR) do Société Générale Américas ("SG AMER").

2. Objetivo e Escopo

Essa Política tem por objetivo descrever os principais processos, papéis e responsabilidades relacionados à governança, gestão e manutenção da estrutura de controles internos.

Essa Política se aplica ao BSGB, incluindo todos os seus colaboradores e em linha com a governança de SG AMER.

3. Referências Regulatórias e Normas Internas Relacionadas

- Resolução CMN 4.968/2021
- Resolução CMN 4.557/2017
- Resolução CVM 160
- Resolução CVM 161
- Código de Ofertas Públicas da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA.
- SG Code – Book B – Part 2 – Internal Control
- SG Group Target Operating Model of Permanent Framework
- SG Group Target Operating Model of the 2LOD
- AMER Permanent Control Framework Management Policy

4. Definição de Controles

O controle interno abrange todos os recursos implementados para ajudar a controlar os riscos do BSGB, incluindo:

- Controles permanentes, que contribuem para conter os riscos não financeiros ao nível aceito com base no apetite por riscos, baseando-se nos controles permanentes de Nível 1 e 2, cujos resultados são considerados na avaliação de risco do Grupo SG. Tais controles são implementados para prevenir e/ou conter perdas operacionais e incidentes, incluindo falhas de *compliance*[1];
- Controles periódicos (auditoria interna/inspeção geral), responsável pelas auditorias independentes das entidades operacionais para verificar a conformidade das operações, o nível de risco efetivamente incorrido, a correta aplicação dos procedimentos, a eficácia e relevância estrutura de controle permanente.

4.1 Controle de 1º Nível

O controle permanente de Nível 1 (L1C) inclui todos os mecanismos usados para conter riscos não financeiros e limitar a probabilidade de ocorrência de um risco, ou reduzir suas consequências. Os controles de Nível 1 podem assumir diferentes formas. No contexto de atender a um requerimento de controle[2] definido pelo Grupo SG, os controles de Nível 1 devem ser formalizados, registrados em uma ferramenta, fornecer uma trilha de auditoria adequada e estar incluído nos relatórios do Grupo.

Se essas regras não puderem ser respeitadas, os controles de Nível 1 ainda podem ser considerados como evidência do controle dos riscos subjacentes, desde que estejam sujeitos a um controle formalizado de execução adequada. Eles também podem estar sujeitos a controles de supervisão gerencial para verificar se são executados corretamente.

Os controles de Nível 1 incluem controles — automatizados ou não — que são integrados ao processamento de transações, controles locais incluídos em procedimentos operacionais, regras de segurança, dentre outros. Eles são realizados como parte das atividades diárias pelos colaboradores diretamente responsáveis pela atividade ou por seus gestores, com os seguintes objetivos:

- Garantir a correta aplicação dos procedimentos existentes e o controle de todos os riscos relacionados a processos, transações e/ou contas;

[1] SG CODE, Book B, par.B.101.
[2] Os requisitos de controle referem-se a um conjunto mínimo de princípios estabelecidos a nível do Grupo para prevenir ou mitigar o impacto e/ou a probabilidade de ocorrência de um risco. Eles definem metas a serem monitoradas para as diferentes atividades e processos associados. Abrangem os riscos operacionais (incluindo riscos de *compliance*) identificados nos processos e registrados na Biblioteca de Controles Normativos.

- Alertar os gestores em caso de anomalias ou falhas.

4.2 Controle de 2º Nível

Os controles permanentes de Nível 2 (L2C) garantem o funcionamento adequado dos controles permanentes de Nível 1 (o escopo inclui todos os controles permanentes de Nível 1, incluindo controles permanentes de supervisão e controles realizados por equipes dedicadas).

As funções de gerenciamento de riscos, conformidade e finanças supervisionam o controle permanente de Nível 2 (referidas como equipes CTL). O controle de Nível 2, na sua função de "controle dos controles", assegura o funcionamento adequado do controle permanente de Nível 1.

O objetivo do controle permanente de segundo nível é avaliar a eficácia dos controles de Nível 1 e emitir uma opinião sobre:

- A qualidade dos controles de Nível 1 (conceito, definição dos procedimentos operacionais, qualidade da implementação);
- Sua eficácia, e
- Sua adequação, em termos de cobertura dos riscos operacionais das atividades do Banco, contribuindo assim para a avaliação da eficácia operacional do sistema de gerenciamento de riscos da Unidade de Negócio/Unidade de Serviço (BU/SU), incluindo os controles de Nível 1 (inclusive a qualidade do reporte e acompanhamento das anomalias identificadas pelo controle permanente de Nível 1).

Para informações adicionais, consulte os SG AMER CTL Procedimentos de Testes (para CPLE e RISQ) e a Estrutura de Revisão DFIN/AME/CTL.

5. Princípios Chaves

O sistema de controles internos do BSGB é dimensionado e adaptado de forma proporcional à sua natureza, porte, complexidade operacional e perfil de riscos. Essa abordagem garante que os controles sejam adequados e eficazes para mitigar os riscos específicos enfrentados pela instituição, promovendo uma gestão equilibrada e alinhada às melhores práticas regulatórias e de governança.

Os controles permanentes de Nível 1 são definidos segundo a abordagem denominada de *Atividades-Processos-Riscos-Controles* (“APRC”). Para garantir a correta implementação das estruturas de controle interno em todo seu escopo de aplicação e a consistência da abordagem e dos relatórios relacionados em todo o Grupo para atividades comparáveis, as estruturas de controle interno e gerenciamento do risco operacional do Grupo SG se baseiam no referencial do Grupo, que lista todas as atividades (A), macroprocessos (MP) e processos (P), bem como em uma taxonomia única de riscos operacionais (R) e na Biblioteca de Controles Normativos (C, ou seja, a LNC/BCN “*Bibliothèque des Contrôles Normatifs*”). Todas as combinações relevantes dos elementos A, P, R e C, denominadas “matrizes APRC”, também constituem um referencial separado[3].

A decomposição de todos os processos que descrevem as linhas de negócio e funções de uma Instituição Financeira, para todas as atividades do Grupo SG, em todas as suas entidades, subsidiárias e locais, permite uma descrição abrangente do Grupo, e assim um mapeamento relevante que pode ser utilizado para identificar os riscos e as necessidades de controle associadas. Tal decomposição é refletida e materializada no “*blueprint*”.

Os controles permanentes de Nível 1 são implementados para atender aos requisitos de controle identificados no plano de controle de Nível 1. Cada controle permanente de Nível 1 deve estar vinculado a um ou mais requerimentos de controle, para um ou mais escopos (“Nós APRC”), e isso deve ser documentado em um ou mais “*blueprints*” estabelecidos conforme o formato definido pela área de RISQ/NFR do Grupo.

A melhoria contínua da estrutura de controles internos se baseia na análise dos resultados dos eventos de risco e dos componentes da estrutura de controle permanente. O ciclo de feedback de melhoria contínua consiste em usar os resultados dos diversos exercícios/processos-chaves de controle interno para fortalecer a cobertura dos riscos pelo controle permanente e reforçar a eficácia das nossas linhas de defesa[4].

6. Papéis e Responsabilidades

A estrutura de controles internos do BSGB é baseada no modelo das três linhas de defesa, em conformidade com o SG Code.

[3] Modelo Operacional Alvo (Target Operating Model - TOM) do Framework PC, seção 5.2, Princípios do referencial APRC.
[4] TOM do Framework PC, seção 1.8, Melhoria contínua do framework de controle permanente.

6.1 Departamento de Compliance

A área de CPLE realiza o mapeamento regulatório, em que monitora continuamente as normas, leis e regulamentações aplicáveis ao modelo de negócios do BSGB, garantindo a rastreabilidade dessas obrigações. Após a triagem inicial, CPLE encaminha as normas às áreas potencialmente impactadas por meio de sistema integrado que controla o fluxo, permitindo o registro e acompanhamento das manifestações das áreas sobre a aplicabilidade regulatória.

Com base nessas informações, as áreas analisam a aplicabilidade das normas em seus processos e identificam os pontos de controle necessários para assegurar o cumprimento regulatório e a mitigação dos riscos. Essas informações são integradas ao framework de controles internos do BSGB, garantindo atualização contínua e governança efetiva em toda a instituição.

6.2 Gerentes e Coordenadores de Controles Permanentes

O Gerente de Controle Permanente de AMER (“PC Manager”) em RISQ/AME/ERM coordena a estrutura de controles permanentes para fornecer uma visão consistente e abrangente de sua implementação e resultados em toda a organização de forma contínua. Além disso, a região designou o Coordenador de Controles Permanentes da 1ª Linha de Defesa de AMER (“PC *Coordinator*”), responsável pela coordenação dos Supervisores de Controle de Nível 1 (“L1C Relays”) e pela implementação da estrutura local de controles permanentes.

O PC Manager, com o suporte do PC *Coordinator*, representa a equipe de Coordenação Regional de Controle Permanente (“PCRC”), uma função de 2ª Linha de Defesa (2LOD), em linha com as diretrizes regionais específicas do Modelo Operacional Alvo da Estrutura de Controle Permanente (Seção 3.4).

6.3 Executores/Validadores de L1C

Os Executores/Validadores são os indivíduos dentro de cada Unidade Organizacional (“OU” - departamento) que possuem e executam os controles. Os Executores realizam os controles de Nível 1 atribuídos a eles, definem ratings, identificam anomalias e criam planos de ação, se necessário. Os Validadores, quando aplicável, supervisionam a execução e os resultados dos L1Cs sob sua responsabilidade.

O ponto de contato para os Executores e Validadores de L1C, em relação a qualquer dúvida ou questão sobre a estrutura de controle, por exemplo, design do controle, é o Supervisor de Controle de Nível 1 da sua Unidade Organizacional.

6.4 Supervisores de Controle de Nível 1 (L1C Relays)

Dentro de cada Unidade Organizacional (OU), o Supervisor de Controle de Nível 1 supervisiona a implementação, coordenação, desafio e dinamização da estrutura de controle para seu escopo. Eles auxiliam os gestores operacionais no design dos seus controles L1C, monitoram a implementação da estrutura L1C e fornecem suporte na definição da forma mais adequada de controles para conter os riscos dentro de níveis aceitáveis.

O Supervisor de Controle de Nível 1 supervisiona a produção de relatórios sobre os resultados dos controles e comunica-os à sua gestão, bem como ao departamento de Risco Operacional, quando relevante e aplicável. Além disso, ele também verifica a existência de medidas corretivas para anomalias, assegura que os planos de ação relacionados aos controles L1C e L2C dentro de seu escopo sejam implementados e reporta periodicamente o progresso desses planos para sua gestão.

Essa função monitora as extensões de prazos para anomalias classificadas como “Muito Alta” e “Alta” para garantir que estejam devidamente justificadas, reportando-as à equipe de Coordenação Regional de Controle Permanente, que compartilhará com as equipes de 2ª Linha de Defesa relevantes para revisão, conforme necessário, e para reporte aos Comitês relevantes. Qualquer extensão de prazo para planos de ação relacionados a anomalia “Muito Alta” e “Alta” deve ser devidamente justificada no comentário do plano de ação e reportada ao Supervisor de Controle de Nível 1.

Os L1C Relays devem possuir nível suficiente de senioridade para cumprir as responsabilidades requeridas, bem como conhecimento e expertise adequados para atuar como especialistas (SMEs) da estrutura de controle permanente sob sua responsabilidade e representar sua unidade como membro no Comitê Operacional de Controle Permanente Regional.

No Brasil, o desempenho dessa função é descentralizado e cada departamento possui o seu Supervisor de Controle de Nível 1. Com exceção das áreas de CPLE e GBTO, que possuem supervisores locais, todos os demais departamentos (OU) possuem supervisores regionais que cumprem igualmente as responsabilidades dessa função.

O departamento de Gestão de Risco Operacional desempenha essa função, cobrindo todas as áreas que compõem a estrutura de GBTO. Ademais, mensalmente, consolida o resultado da execução dos controles permanentes de forma transversal no BSGB e reporta os resultados no Dashboard de Risco Operacional aos membros do Comitê Executivo do BSGB e aos demais destinatários relevantes. Controles não performados ou execuções não qualificadas como

"Satisfatórias" ou "Aceitáveis", bem como as anomalias e planos de ação correspondentes, são escalados ao Comitê de Riscos do BSGB.

6.5 Grupos de Controle de Nível 2

Os controles de Nível 2 (L2C) são coordenados pelos grupos de controle de AMER CTL (CPLE, RISQ e DFIN) conforme as Políticas de CTL aplicáveis.

Os resultados e constatações dos controles L2C são apresentados ao Comitê de Controle Regional trimestralmente ("ControlCo"), para fornecer à Alta Administração as informações necessárias para monitorar riscos e direcionar ações corretivas para a região.

Para informações adicionais, consulte os SG AMER CTL Procedimentos de Testes (para CPLE e RISQ) e a Estrutura de Revisão DFIN/AME/CTL.

No BSGB, essa função é desempenhada por um recurso dedicado do departamento de RISQ, que atua em conjunto com as equipes regionais de CTL para cobertura de RISQ e CPLE, enquanto a cobertura de DFIN é realizada exclusivamente por esse profissional.

6.6 Equipes da Segunda Linha de Defesa (RISQ e CPLE)

A organização e atribuições das equipes de 2ª Linha de Defesa (2LOD) como parte da estrutura de controle permanente são definidas no SG *Code* (Livro A), no Modelo Operacional Alvo da Estrutura de Controle Permanente (Seção 6) e no Modelo Operacional Alvo do Grupo SG para a 2LOD, abrangendo o seguinte perímetro para AMER, incluindo o BSGB:

- Participar da definição e evolução da estrutura normativa APRC e auxiliar as Unidades de Negócio/Serviço (BU/SU) em sua compreensão para sua área de expertise;
- Contribuir para a definição das necessidades de controle que constituem a Biblioteca de Controles Normativos ("*Library of Normative Control - LNC*") em sua área de expertise;
- Em sua área de expertise, contribuir para a definição e implementação dos controles L1C, análise dos resultados dos L1C, incluindo anomalia "Alta" e "Muito Alta" e os planos de ação associados;
- Garantir que a estrutura de controle sob sua supervisão respeite os requisitos do Grupo SG (taxa de implantação dos L1C, taxa de execução dos L1C, etc.), solicitar e monitorar a efetiva implementação dos planos de ação, quando relevante;
- Realizar, em conjunto com a função de CTL que cobre a área de Finanças (DFIN/CTL), os controles permanentes de segundo nível, para verificar a adequação, desempenho e eficácia dos controles permanentes de primeiro nível;
- Contribuir para os órgãos de governança de controle interno do Grupo SG (Comitê de Coordenação de Controle Interno do Grupo SG, por exemplo GICCC, e Comitê de Coordenação de Controle Interno Pilar, por exemplo PICCC);
- Avaliar de forma independente a situação de risco das BU/SU em sua área de expertise e comunicar às comissões relevantes e às autoridades regulatórias;
- Oferecer assistência técnica sobre as anomalias de controle identificadas. Solicitar, se necessário, os correspondentes das Funções de Gerenciamento para aprofundar certos resultados reportados à SU, verificar que as causas das anomalias foram identificadas e que as ações tomadas são adequadas (incluindo vinculação com "*Issues*" conforme a Política de Gerenciamento de "*Issues*").

Por fim, como qualquer gestor de atividade no Grupo SG, cada membro da 2LOD (respectivamente RISQ e CPLE) é responsável pela implementação dos processos e controles de nível 1 em sua respectiva área.

6.7 Diretoria Executiva do BSGB

A Diretoria Executiva do BSGB possui responsabilidades no que diz respeito à estrutura de controles internos do Banco:

- Aprovar a Política de Controles Internos;
- Aprovar o relatório anual sobre os sistemas de controles internos do Banco
- Promover elevados padrões éticos e de integridade no que diz respeito aos sistemas de controles internos;
- Estabelecer cultura organizacional com ênfase na relevância dos sistemas de controles internos e no engajamento de cada funcionário no processo de controle interno;
- Manter estrutura organizacional adequada para garantir a qualidade e a efetividade dos sistemas e processos de controles internos;
- Garantir recursos adequados e suficientes para o exercício das atividades relacionadas aos sistemas de controles internos, de forma independente, objetiva e efetiva.

- Tomar as medidas necessárias para identificar, medir, monitorar e controlar os riscos de acordo com os níveis de riscos definidos;
- Garantir que as falhas identificadas sejam tempestivamente corrigidas;
- Monitorar a adequação e a eficácia dos sistemas de controles internos;
- Garantir que os sistemas de controles internos sejam implementados e mantidos de acordo com os requerimentos regulatórios.

7. Treinamento e Capacitação em Controles Internos e Gestão de Riscos

Os treinamentos específicos em gerenciamento de riscos, que podem ser mandatórios em virtude de requisitos regulatórios ou facultativos conforme a governança local ou regional, são fundamentais para assegurar uma compreensão aprofundada das ferramentas adotadas pelo BSGB na identificação e monitoramento de riscos, bem como dos mecanismos de controle implementados. A plataforma online disponibiliza uma grade abrangente de treinamentos, acessível em go/mylearning, que abrange distintos módulos, incluindo mapeamento de atividades, identificação de riscos e definição dos controles de primeira e segunda linha.

8. Padrões de Documentação de Controles Internos

Os Executores/Validadores de L1C são responsáveis pela documentação dos controles e anomalias na ferramenta de controle (por exemplo, MyControls). Os Supervisores dos controles L1C são responsáveis por verificar se esses padrões foram seguidos, no mínimo para controles classificados como “Muito Fraco” e “Fraco”, e para anomalias classificadas como “Muito Alta” e “Alta”.

Em caso de deficiências identificadas, os Supervisores dos controles L1C podem solicitar aos Executores/Validadores que revisem a documentação, e reportar quaisquer problemas à equipe PCRC (Coordenador Regional de Controle Permanente) para ações adicionais, incluindo escalonamento aos Comitês apropriados.

9. Metodologia e Ferramentas

A estrutura de controle permanente se baseia na metodologia APRC estabelecida pela área de RISQ/NFR do Grupo SG.

Uma das responsabilidades da estrutura organizacional descrita acima é manter os “*blueprints*” da Unidade de Negócio (departamentos) atualizados e manter o inventário de L1C alinhado e atualizado com a metodologia APRC. Essa estrutura também é responsável pela manutenção do mapeamento entre os controles L1C e as combinações *Blueprint*/Atividade/Processo na ferramenta MyAPRC.

Cada entidade do grupo definiu um conjunto de “*blueprints*” que descrevem as Atividades e Processos realizados pelos diversos departamentos (BU/SU). Esses “*blueprints*” estão disponíveis e são mantidos na ferramenta myAPRC.

Com base nesses “*blueprints*”, o modelo APRC e a ferramenta MyAPRC permitem que cada departamento inventarie os controles permanentes de Nível 1 (L1C) que realizam e os mapeiem em relação às Necessidades de Controle (“*Control Needs*”).

A lista completa das Necessidades de Controle disponíveis para as BU e SU do Grupo SG pode ser encontrada na *Bibliothèque de Contrôles Normatifs* (“BCN”), que é de propriedade e mantida pela área de RISQ/NFR do Grupo SG.

O “*blueprint*” é a fonte oficial para todas as atividades, processos e mapeamento de L1C para um determinado escopo.

10. Comitês de Governança

Como parte da governança do controle permanente, cada BU e SU do Grupo SG estabelece uma governança de Comitês para gerenciar a estrutura de controle permanente em seu perímetro e integrá-lo aos Comitês de Governança do Grupo SG. A governança do controle permanente de SG AMER é mantida por meio de dois Comitês: o Comitê Operacional de Controle Permanente (“OPCC”) e o Comitê de Controle Regional de AMER (“Control Co”).

No BSGB, o Comitê de Riscos é o órgão responsável pela governança de controles internos do Banco.

10.1 Comitê Operacional de Controle Permanente SG AMER

O Comitê Operacional de Controle Permanente Regional (“OPCC”) foi criado para proporcionar aos Supervisores de Controle de Nível 1 da região, ao Gerentes de Controle Permanente Regional e ao Coordenadores da 1ª Linha de Defesa Regional, um fórum para revisar o framework de controle permanente (cobertura, desempenho dos controles, planos de ação etc.) e discutir todos os aspectos relacionados ao desenvolvimento desse framework.

Esse comitê mensal alimenta o Comitê de Controle Regional de Amer (“Control Co”) trimestralmente e, reciprocamente, é informado das mensagens-chave do ControlCo.

10.2 Comitê de Controle Regional de SG AMER

O Comitê de Controle Regionald e AMER (“ControlCo”) é um subcomitê do Comitê Executivo das Américas (o “Exco”) criado para realizar uma reunião formal e dedicada trimestralmente sobre questões de controle interno e externo. O ControlCo é o equivalente para as Américas do Comitê Operacional Permanente de Controle de Nível 1 (que é distinto do OPCC).

10.3 Comitê de Coordenação de Controle Interno Pilar do Grupo SG

O SG AMER fornece um relatório anual sobre seu Framework de Controle Permanente aos Comitês de Coordenação de Controle Interno Pilar (PICCC), que oferecem uma visão consolidada da organização de controle interno do Grupo.

10.4 Comitê de Riscos do BSGB

O Comitê de Riscos do BSGB, que possui como membros os Diretores Executivos, monitora os resultados dos controles de supervisão permanente, incluindo as falhas apresentadas em sua performance, com o intuito de monitorar e garantir o adequado desempenho dos controles existentes. Ademais, o Comitê se encarrega da aprovação de qualquer mudança estrutural, sistêmica ou processual necessária para garantir que a instituição atenda os requisitos regulatórios de controles internos cumprindo a regulamentação vigente, incluindo o Relatório Anual de Controles Internos (requerido pela Resolução CMN 4.968/2021).

11. Gerenciamento da Estrutura de Controle Permanente

11.1 Atualizações ao Referencial de Atividades/Processos

A equipe de RISQ/NFR a nível de Grupo pode periodicamente realizar alterações no framework APRC (por exemplo, adição, fusão, modificação ou remoção de Atividades e/ou Processos).

- Quando da sua ocorrência, esta equipe comunicará os detalhes das mudanças por meio de newsletters, sessões informativas, etc., incluindo no mínimo o Gerente de Controle Permanente de AMER, a comunidade de Supervisores de controle de nível 1 (L1C Relays) e representantes de L2C nesses canais de informação;
- A equipe PCRC (Coordenador Regional de Controle Permanente) disseminará essas mudanças para todos os stakeholders das Américas por meio do OPCC e/ou e-mail;
- Cada stakeholder avaliará os impactos dessas mudanças em seu escopo e realizará as alterações relevantes. O prazo para essas alterações pode ser definido pela equipe de RISQ/NFR a nível de Grupo e/ou pela equipe do PCRC. A equipe PCRC monitorará a implementação nas BU/SU para garantir consistência.

11.2 Atualizações da Biblioteca de Controles Normativos (LNC)

A equipe de RISQ/NFR a nível de Grupo pode publicar novas versões da LNC periodicamente (por exemplo, adição de novos Objetivos de Controle, remoção, fusão ou modificações de Objetivos de Controle existentes).

- Quando da sua ocorrência, esta equipe comunicará os detalhes das mudanças por meio de newsletters, sessões informativas, etc., incluindo no mínimo o Gerente de Controle Permanente de AMER, a comunidade de Supervisores de controle de nível 1 (L1C Relays) e representantes de L2C nesses canais;
- A equipe PCRC (Coordenador Regional de Controle Permanente) disseminará essas mudanças para todos os stakeholders das Américas por meio do OPCC e/ou e-mail;
- Cada stakeholder avaliará os impactos dessas mudanças em seu escopo e realizará as alterações relevantes. O prazo para essas alterações pode ser definido pela equipe de RISQ/AME/NFR e/ou pela equipe do PCRC.A equipe do PCRC monitorará a implementação nas BU/SU para garantir consistência.

11.3 Propostas AMER para Atualizações ao APRC

SG AMER pode solicitar alterações ao Referencial APRC, incluindo, mas não limitado a, a adição de novos Objetivos de Controle na LNC (por exemplo, cobertura de regulamentações específicas das Américas, como Regulamentações Bancárias).

- Qualquer membro de AMER pode solicitar tais mudanças. Portanto, todas as solicitações devem ser encaminhadas ao Supervisor de controle de nível 1 (L1C Relays) do departamento do solicitante para uma primeira revisão;
- O Supervisor de controle de nível 1 (L1C Relays), se considerar a solicitação justificada, encaminhará ao Gerente de Controle Permanente AMER para revisão. Em caso de solicitações de criação de Necessidades de Controle, o Supervisor de controle de nível 1 (L1C Relays) deverá documentar quais pesquisas na LNC foram

realizadas para comprovar que nenhuma Necessidade de Controle existente cobre a necessidade (por exemplo, redação ajustada, nível diferente de granularidade, etc.);

- A equipe PCRC coordenará as solicitações de atualização do referencial, incluindo as evidências fornecidas pelos Supervisor de controle de nível 1 (L1C Relays), com o Comitê Referencial NFR conforme o procedimento definido pela equipe de RISQ/NFR a nível de Grupo;
- A equipe PCRC facilitará a comunicação entre o solicitante, o Supervisor de controle de nível 1 (L1C Relays) e a equipe de RISQ/NFR a nível de Grupo e garantirá que todos os elementos necessários sejam fornecidos ao Comitê APRC. O solicitante e/ou o Supervisor de controle de nível 1 (L1C Relays) poderão ser convidados a apresentar sua solicitação ao Comitê e contribuir para a documentação do novo Objetivo de Controle, se relevante.

11.4 Atualizações nos "*Blueprints*" (Atividade/Processo)

Os Supervisor de controle de nível 1 (L1C Relays) são responsáveis pela manutenção dos blueprints em seu escopo e podem solicitar modificações nos "*blueprints*" de Atividades/Processos (por exemplo, adição ou remoção de Atividades e Processos).

- Os volumes de modificações nos "*blueprints*" de Atividade Nível 3 e/ou Processo são reportados no OPCC;
- RISQ/AME/NFR revisará a lista de exclusões de Atividades Nível 3 e/ou Processos e questionará a exclusão, se apropriado;
- RISQ/AME/NFR informará a equipe PCRC sobre quaisquer solicitações de modificação de "*blueprints*" feitas à 1LOD;
- Em caso de desacordo quanto a esse questionamento, a questão será escalada ao Gerente de Controle Permanente.

Separadamente dessa revisão da 2LOD, o "*blueprint*" de Atividades/Processos é certificado anualmente pelo Chefe de cada Unidade Organizacional da BU AMER.

Notas importantes:

- A adição de Atividades em um "*blueprint*" resultará na adição de um conjunto de nodes de Necessidade de Controle associados (nodes APC) a esse "*blueprint*". O Supervisor de controle de nível 1 (L1C Relays) deve qualificar esses nodes e, se aplicável, mapear novos L1C – este cenário. Além disso, o KPI "Taxa de implantação MyAPRC", acompanhado em cada OPCC, permitirá monitorar nodes APC adicionados mas ainda não qualificados;
- A remoção de Atividades em um "*blueprint*" resultará na remoção de um conjunto de nodes de Necessidade de Controle associados (nodes APC) do "*blueprint*". Isso é similar ao caso em que Supervisor de controle de nível 1 (L1C Relays) desmapeiam L1C de seus "*blueprints*";
- Qualquer não implantação de "*blueprints*" e/ou controles será escalada para RISQ/AME/DIR.

11.5 Criação de um novo L1C

Sempre que um novo controle (L1C) é criado – independente da ferramenta:

- O Supervisor de controle de nível 1 (L1C Relays) deve ser notificado sobre qualquer criação de L1C no departamento ou escopo relevante. A lista de controles criados é publicada mensalmente no material do OPCC;
- O Supervisor de controle de nível 1 (L1C Relays) auxiliará na criação do controle e garantirá que as melhores práticas sejam respeitadas;
- Uma vez criado o L1C, o Supervisor de controle de nível 1 (L1C Relays) atualizará os blueprints relevantes no myAPRC e mapeará o L1C para o(s) node(s) APC correspondente(s).

Reconciliações entre o MyAPRC e as ferramentas de L1C são realizadas regularmente para garantir que todos os controles recém-criados estejam devidamente inventariados no MyAPRC (controle "órfãos").

11.6 Descomissionamento / Desmapeamento de L1C no MyAPRC

Para qualquer controle considerado chave, a 1LOD deve propor uma justificativa e detalhes de suporte explicando por que o controle não é mais necessário, como o risco inerente é monitorado e/ou mitigado de forma contínua, e deve obter aprovação da 2LOD relevante antes de descomissionar o controle.

Para controles não-chave, a 1LOD pode descomissionar a seu critério. A lista de controles descomissionados é publicada no OPCC e compartilhada com a 2LOD relevante para supervisão e desafio conforme necessário.

Sempre que um L1C existente for excluído:

- O Supervisor de controle de nível 1 (L1C Relays) deve ser notificado sobre qualquer L1C descomissionado no escopo de sua responsabilidade. Após o descomissionamento, o Supervisor de controle de nível 1 (L1C Relays) atualizará os "*blueprints*" relevantes no MyAPRC e desmapeia o L1C do(s) node(s) APC correspondente(s);
- A taxa de implantação é monitorada regularmente: qualquer queda na taxa pode indicar que certos L1Cs não estão mais ativos ou que Necessidades de Controle foram adicionadas ao "*blueprint*", mas não qualificadas.

11.7 Modificação de um L1C existente

Os Supervisor de controle de nível 1 (L1C Relays) podem atualizar os detalhes de um L1C (por exemplo, vinculação a uma Necessidade de Controle, extensão do procedimento do controle para ampliar a cobertura e eficiência do risco ou para cobrir requisitos adicionais).

- O Supervisor de controle de nível 1 (L1C Relays) deve ser notificado sobre quaisquer atualizações de L1C no departamento ou escopo relevante;
- O Supervisor de controle de nível 1 (L1C Relays) garantirá que as mudanças estejam alinhadas com as melhores práticas de design de L1C;
- O Supervisor de controle de nível 1 (L1C Relays) também revisará, se as mudanças forem materiais, se o L1C precisa ser vinculado a outros nós APC (por exemplo, se o L1C agora atende a novas Necessidades de Controle da LNC, se o L1C cobre novas combinações de Atividades/Processos, etc.). Supervisor de controle de nível 1 (L1C Relays) atualizará os "*blueprints*" relevantes para refletir essas mudanças.

11.8 Qualificação de Necessidades de Controle como "No Mitigation"

A qualificação "Sem Mitigação" no MyAPRC é reservada para casos em que o Supervisor de controle de nível 1 (L1C Relays) e o gestor responsável pela atividade avaliam o risco associado ao L1C como menor ("baixo" ou "moderado"). Nesse caso, eles podem optar por não cobrir o risco ou não formalizar os meios implementados para cobri-lo.

- A sub-BU/SU pode decidir que certos Objetivos de Controle, embora aplicáveis ao seu escopo, não precisam ser implementados como L1C devido ao risco baixo associado à Atividade/Processo coberto pelo Objetivo de Controle. No MyAPRC, esses serão qualificados como "Sem Mitigação";
- A qualificação "Sem Mitigação" é gerida pelas seguintes regras:
    - Uma explicação clara e abrangente da justificativa por trás da decisão deve ser fornecida na ferramenta MyAPRC;
    - Apenas Objetivos de Controle que tenham sido vinculados, no modelo APRC, a Riscos Intrínsecos qualificados como Baixos ou Moderados na mais recente RCSA podem ser qualificados como "Sem Mitigação";
    - A qualificação "Sem Mitigação" é permitida somente por um período limitado (máximo de 1 ano).
- Uma vez por ano, o Supervisor de controle de nível 1 (L1C Relays) deverá revisar todos os nós APC qualificados como "Sem Mitigação" e confirmar formalmente que a qualificação ainda é relevante;
- Uma vez por ano, o Gerente de Controle Permanente AMER verificará se as regras acima estão sendo corretamente seguidas. Caso contrário, será iniciada uma solicitação para que o Supervisor de controle de nível 1 (L1C Relays) faça a correção necessária.

11.9 Certificações Anuais

Certificação Anual dos "*Blueprints*":

- Os "*blueprints*" de Atividades/Processos são certificados anualmente pelo Chefe de cada sub-BU/SU, e as alterações nos "*blueprints*" são revisadas e desafiadas, se necessário, pela equipe de RISQ/AME/NFR;
- A validação do "*blueprint*" foca na seleção e qualificação das atividades e processos no "*blueprint*" sob responsabilidade da BU/SU (ou seja, a lista de A3Ps que será transmitida para o escopo da BU/SU pelo MyAPRC para as diversas ferramentas de Avaliação de Risco para uma avaliação no nível A3).

Certificação Anual do Plano de Controle:

- As Necessidades de Controle qualificadas como "Não Aplicável" ou "Aplicável – Sem Mitigação" são certificadas anualmente. A revisão também deve cobrir quaisquer nós ainda a serem qualificados para garantir que nenhum node de controle que atenda aos seguintes critérios esteja pendente de implantação:
    - Necessidades de Controle de Alta Prioridade do Grupo (HPC)
    - Nós que cobrem riscos intrínsecos "Altos" ou "Muito Altos"
    - Nós para os quais perdas e incidentes foram reportados
    - Nós de controle com recomendações das equipes CTL, auditoria interna ou reguladores, etc.

- Os Supervisor de controle de nível 1 (L1C Relays) realizam a revisão dessas qualificações para garantir que as justificativas (capturadas no comentário da Necessidade de Controle no myAPRC) estejam em conformidade com a metodologia do framework; a equipe PCRC valida os nós de controle qualificados como “Não Aplicável”.
- Decisões referentes a nós qualificados como “Aplicável – Sem Mitigação” são validadas pelo Chefe relevante de cada sub-BU/SU e/ou membro relevante do ExCo.

Validação Anual de Controles Multi-mapeados (Controles mapeados para múltiplas Necessidades de Controle):

- Os L1Cs multi-mapeados devem ser revisados e validados anualmente. Os Supervisor de controle de nível 1 (L1C Relays) realizam a revisão de todos os controles multi-mapeados sob sua BU/SU para garantir que os controles estejam mapeados adequadamente; qualquer controle multi-mapeado que não cubra pelo menos um elemento de uma necessidade de controle à qual está mapeado deve ser desmapeado no MyAPRC.
- O multi-mapeamento de um L1C com múltiplas necessidades de controle é aceitável se corresponder a um controle cuja execução cobre total ou parcialmente várias necessidades de controle às quais está multi-mapeado (ou seja, cobre alguns elementos de controle das necessidades de controle em questão).
- O multi-mapeamento de um L1C com múltiplas necessidades de controle não é aceitável:
    - Se o controle realizado não tiver relação com uma das necessidades de controle
    - Se o controle executado não estiver diretamente relacionado à necessidade de controle

12. Indicador da RAS

Não aplicável a essa Política.

13. Plano de Ação e de Resposta a Incidentes

No caso de identificação de falhas e/ou violações sobre os tópicos tratados nessa Política, o assunto será escalado para o CCO, para o CRO e será aberto um incidente operacional para investigação, análise dos impactos e definição de planos de ação mitigadores.

O incidente e o monitoramento dos planos de ação definidos para mitigação do risco deverão ser reportados à Diretoria Executiva do BSGB.

No caso de envolvimento de colaboradores do BSGB, será necessário analisar a aplicação de medidas disciplinares, de acordo com a recomendação do Comitê de Ética de cada entidade, caso seja aplicável.

14. Prazo de Arquivamento

O prazo de retenção para os documentos, informações e dados aos quais essa Política se refere é de 10 (dez) anos.

15. Revisão, Aprovação e Exceções

Esse documento deve ser revisado pelo Diretor de Riscos e aprovado anualmente pela Diretoria Executiva do BSGB.

16. Treinamento Obrigatório

Esse item não se aplica a esse documento.