DIRETRIZES PARA CLASSIFICAÇÃO E PROTEÇÃO DAS INFORMAÇÕES – CONFIDENCIALIDADE

Banco Société Générale Brasil “BSGB”

Fonte: Política Regulatória de Segurança da Informação “BSGB”

Dezembro/2025

THE FUTURE IS YOU SOCIETE GENERALE

ÍNDICE

1. Introdução

A informação é um dos ativos mais importantes para o Grupo Société Générale "Grupo SG" e, portanto, para o Banco Société Générale Brasil S.A., doravante referenciado como "BSGB" ou compreendido em "entidades legais". Por esta razão, os Recursos de Tecnologia da Informação e Informações (sensíveis, confidenciais e/ou estratégicas) documentadas digital ou fisicamente devem ser protegidas e tratadas conforme as diretrizes da Política Regulatória de Segurança da Informação e das demais referências regulatóriasaplicáveis, as quais em conjunto têm o propósito de evitar a materialização de riscos relativos à segurança da informação em todas as atividades exercidas no BSGB.

O termo **"informação"** designa todos os dados que são digitalizados e estruturados de forma a permitir o processamento automatizado, o que, por sua vez, possibilita, otimiza ou facilita as atividades executadas pelo BSGB ou quaisquer outras entidades legais do Grupo SG. O processamento automatizado de informações e o acesso a essas informações são gerenciadas por "aplicações" executadas por meio de grupos de recursos (servidores, sistemas operacionais, software, arquivos, bancos de dados, redes, estações de trabalho etc.) que constituem coletivamente um **"sistema de informação".**

Este documento apresenta especificamente o conteúdo sobre "Classificação e Proteção das Informações" geridas pelo BSGB, referenciadas na Política Regulatória de Segurança da Informação do BSGB.

2. Objetivo e Escopo

2.1. Objetivo

O objetivo desta Política é apresentar a estrutura de gestão do risco de segurança da informação em vigor no BSGB, bem como as responsabilidades de seus colaboradores perante à esta estrutura, a qual foi concebida em conformidade com as leis e regulamentações locais, com as diretrizes e procedimentos locais "BSGB" que abarcam as diretrizes regionais de "SG AMER[1]" e Grupo SG (quando aplicáveis), os objetivos estratégicos do negócio e as melhores práticas, através de um Programa de Segurança da Informação abrangente, que requer um gerenciamento oportuno, eficiente e em conformidade com os seguintes princípios:

(i) **Confidencialidade**: proteger as informações contra a divulgação a partes não autorizadas ou vazamento de informação.

(ii) **Integridade**: assegurar que as informações estejam sempre completas, corretas e protegidas contra modificações por partes não autorizadas ou destruição acidental ou mal-intencionada.

(iii) **Disponibilidade:** assegurar que as pessoas autorizadas possam acessar as informações, quando necessário, mantendo assim a continuidade e recuperação em caso de incidente.

(iv) **Rastreabilidade:** assegurar que todos os requisitos de segurança relativos a cenários de risco tenham sido considerados, permitindo a identificação de todas as ações realizadas nos sistemas de informação através de trilhas de auditoria e/ou gravações telefônicas.

(v) **Compliance:** cumprir as exigências regulatórias e internas aplicáveis, no que tange a segurança da informação e cibersegurança.

2.2. Escopo

A Política Regulatória de Segurança da Informaçãose aplica a todos os departamentos e usuários das informações do BSGB, independentemente da função, cargo ou vínculo empregatício (funcionários efetivos, colaboradores terceirizados [consultores e contratados], estagiários, jovens aprendizes, expatriados e VIEs)[2] que em conjunto estão referenciados nesta política, apenas como "Colaboradores", no que tange como os dados são acessados e como a informação é processada, arquivada ou transferida durante seu ciclo de vida.

O não cumprimento desta Política pode resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho.

[1] SG AMER: Société Générale Américas, ou seja, representação regional à qual todas as entidades legais situadas na região de AMER está subordinada.

[2] VIE: *Volontariat International en Entreprise* [FR], jovem francês trabalhando temporariamente no BSGB.

3. Estrutura e Governança

Todas as decisões aprovadas pelo Comitê Regional de Cibersegurança são cascateadas para as entidades legais sob sua gestão, assegurando assim o alinhamento regional das atividades e a implantação de controles no âmbito de segurança da informação e de segurança cibernética, com o plano de negócios e riscos associados, além de decidir sobre a Governança, Gestão e Programa de Segurança da Informação.

No Brasil, a responsabilidade pela análise dos riscos, implantação dos controles e processos, acompanhamento de projetos e treinamentos aos usuários é da área de Gestão de Risco Operacional, subordinada ao COO (Diretor de Operações, que também é o Diretor Responsável pela Segurança Cibernética perante o Banco Central do Brasil) e ao CRO (Diretor de Riscos) do BSGB.

4. Proteção dos Dados

4.1. Classificação de Dados

A informação armazenada ou manuseada por todos os colaboradores, independente do formato ou mídia da informação, está sujeita aos requisitos de confidencialidade de dados do Grupo SG. Os dados deverão ser devidamente protegidos de acordo com o nível de risco do negócio, bem como classificados em uma das 4 categorias de sensibilidade da informação, podendo ser: **C0 - Público**, **C1 - Interno**, **C2 - Confidencial** e **C3 - Secreto**.

Adicionalmente, o programa de classificação dos dados deve identificar as informações "não-públicas" que podem ter um impacto material na imagem e reputação do BSGB se forem divulgadas de forma imprópria, adulteradas ou destruídas. Este tipo de informação inclui dados relacionados a negócios, pessoais identificáveis etc., e devem ser sempre classificados como **C2-Confidencial** ou **C3-Secreto**. O processo para classificação das informações é obrigatório e realizado através de ferramenta específica, que não permite a gravação e nem o compartilhamento de dados por e-mail se não estiverem devidamente classificados.

A proteção de dados também é imposta através da criptografia de comunicação sensível (e-mails internos são criptografados se classificados como **C2-Confidencial** ou **C3-Secreto**). É realizada uma classificação e avaliação dos dados hospedados e suportados e o nível de requisitos de segurança é proporcional à criticidade dos aplicativos e da infraestrutura de suporte (servidores e bancos de dados).

A classificação dos dados deve se orientar pelos princípios de confidencialidade, são eles:

- **PCPI-C – Princípio 1: Dever de Confidencialidade**

  Todos os usuários dos sistemas de informações têm o dever de confidencialidade em relação às informações que forem criadas, coletadas, mantidas e/ou manuseadas como parte integrante de suas atividades diárias.

  Este princípio se aplica a todas as informações, independentemente do formato, forma de armazenamento e contexto, e seucumprimento deve ser devidamente formalizado, sempre que aplicável, nos contratos firmados com terceiros (prestadores de serviços, parceiros e fornecedores), a fim de mitigar o risco de divulgação indevida das informações.

- **PCPI-C – Princípio 2: Restrição de Acesso ("*Need-to-Know*")**

  A informação, independente da sua natureza, deve ser distribuída apenas para os indivíduos que precisam ter conhecimento para realização das atividades diárias e em cumprimento ao princípio de **privilégio mínimo**, ou seja, os usuários devem receber apenas os privilégios estritamente necessários para o desempenho de suas funções e em coerência com as atividades profissionais diárias.

  Os beneficiários deste acesso devem ser:

  - Os destinatários formalmente designados para ter acesso à informação;
  - Os destinatários designados pelos Gestores ou pelos proprietários da informação;
  - Os gestores dos destinatários designados;
  - Qualquer pessoa que deve ter conhecimento da informação para realização das atividades diárias.

O "direito de acesso" da Auditoria (inspeção geral, auditoria interna), assim como das autoridades supervisoras e auditores externos, é definido de acordo com as necessidades e a forma de intervenção, em cumprimento a regulamentação e legislação local.

- **PCPI-C – Princípio 3: Propriedade da Informação e Responsabilidades em relação a Classificação**
  - **PCPI-C – Princípio 3.1:** qualquer colaborador do BSGB ou qualquer outro usuário interno ou externo com acesso aos sistemas de informações), é o proprietário da informação que gera ou recebe de remetentes externos.
  - **PCPI-C – Princípio 3.2:** o proprietário da informação é responsável pela sua classificação quanto ao nível de confidencialidade e, para tanto, deve:
    a. Definir e atualizar a classificação de confidencialidade da informação e comunicar às partes interessadas, a fim de implementar as medidas corretas de proteção e compartilhamento;
    b. Cumprir com as regras de utilização e classificação das informações;
    c. Cumprir com as medidas de proteção no manuseio das informações;

  Os **destinatários** são os usuários que recebem as informações, e possuem **as mesmas responsabilidades dos proprietários** em relação ao cumprimento das regras de utilização e proteção das informações, sujeitos ainda às disposições específicas para as informações restritas (classificadas como C3).

  A responsabilidade de classificar as informações de maneira visível e correta não deve ser transferida para o destinatário.

- **PCPI-C – Princípio 4: Manuseio Apropriado das Informações**

  Todos os usuários que possuem acesso ao sistema de informações do BSGB (funcionário, estagiário, terceiro, contratado, temporário ou qualquer outro usuário interno ou externo), devem cumprir com as regras relacionadas a proteção das informações de acordo com o nível de confidencialidade no manuseio, gerenciamento ou recebimento das informações durante todo o ciclo de vida.

  As regras de proteção das informações cobrem todo o ciclo de vida da informação: esboço, circulação (especialmente distribuição para terceiros), armazenamento e destruição. Consequentemente, os usuários deverão cumprir com as regras durante todos estes estágios.

  Se qualquer colaborador do BSGB receber por engano informações ou documentos não direcionados a ele e/ou não relacionados à suas atividades, o mesmo é responsável por comunicar imediatamente o time de Gestão Risco Operacional para avaliação quanto ao enquadramento da ocorrência em incidente de vazamento de dados, e orientará quanto ao destino da informação recebida (destruição da informação e a maneira adequada) bem como acionará o departamento de Compliance para bloqueio do acesso ao e-mail recebido via ferramenta de busca de correios eletrônicos, se aplicável.

  Todos os colaboradores deverão zelar pela discrição no acesso às informações de negócios em lugares públicos.

- **PCPI-C – Princípio 5: Conscientização sobre a Classificação e Proteção das Informações**

  A classificação das informações, de acordo com seu nível de sensibilidade e confidencialidade, é um **procedimento obrigatório** para assegurar a proteção e definir as restrições de acesso e compartilhamento. Nenhum documento poderá ser gravado na rede interna do BSGB ou compartilhado por email, sem a devida classificação, que deverá seguir os parâmetros listados abaixo (C0, C1, C2 e C3).

- **Níveis de classificação:**

  C0 PÚBLICO

  Qualquer informação ou documento que possa ser divulgado ao público sem ocasionar impactos às atividades de negócios do BSGB, aos seus clientes, parceiros, funcionários ou quaisquer *stakeholders*.

C1 INTERNO

Qualquer informação ou documento que não contém nenhuma informação confidencial, incluindo documentos pessoais e cujo vazamento teria um impacto baixo. Esta informação deve ser circulada apenas para aqueles que devem conhecê-la ("*need-to-know*").

C2 CONFIDENCIAL

Qualquer informação, dado ou documento que deve ser repassada exclusivamente para as pessoas envolvidas, devidamente identificadas, e cujo vazamento pode prejudicar um projeto, a atividade ou a imagem e reputação do BSGB.

Como regra geral, as informações e documentos "privilegiados", incluindo dados de funcionários, clientes e atividades de negócios (dados de operações, extratos de posição de clientes, contratos, termos de compromisso, confirmação de operações, dados de cargos e salários etc.), cujo conteúdo está sujeito às regulamentações e parâmetros jurídicos, devem ser classificadas como C2.

C3 SECRETO

Devem ser classificadas como **C3 – SECRETO** qualquer informação ou documento cujo vazamento possa ocasionar impactos relevantes e vitais à estratégia de negócios e danos à imagem e reputação do no nível do Grupo. Na prática, o número de itens classificados como C3 deve ser extremamente reduzido e seu uso é limitado a pessoas autorizadas.

Além dos parâmetros estabelecidos acima, existem 2 níveis de classificação adicionais para os documentos **C2** e **C3**, que devem ser utilizados para contribuir com a proteção das informações:

a) ***Cannot leave the Group*****:** qualquer documento classificado como C2 ou C3 que não possua nenhuma finalidade externa e que não pode ser compartilhado com destinatários externos (clientes, parceiros, fornecedores etc).

b) ***Can leave the Group*****:** qualquer documento classificado como C2 ou C3, que pode ser compartilhado com destinatários externos (clientes, parceiros, fornecedores etc).

Por padrão, todos os documentos C2 ou C3 são classificados como "*cannot leave the group*").

- **Procedimento para classificação das informações:**

Os proprietários das informações são responsáveis pela análise da natureza e das características da informação para definir o nível de confidencialidade correspondente, a fim de mitigar os riscos inerentes ao vazamento ou compartilhamento indevido, de acordo com os parâmetros abaixo:

a) Natureza da informação:
- Protegida por Lei (dados pessoais, dados bancários etc);
- Dados de negócios, incluindo dados identificáveis de clientes, de produtos e serviços prestados para clientes e quaisquer informações sobre o relacionamento comercial do BSGB com seus clientes, fornecedores, parceiros e prestadores de serviços;
- Dados relacionados a sistemas operacionais (*logs* de acesso, chaves de criptografia etc).

b) Característica de informação:
- Dados individuais de informações bancárias (extratos de contas correntes, posições de investimentos etc);
- Dados que podem ser correlacionados, ou seja, lista de contas bancárias com os detalhes pessoais dos proprietários.

c) Elementos adicionais:
- Qualquer elemento que possa influenciar no nível de confidencialidade (por exemplo: informação externalizada na nuvem).

d) Análise de Impacto:
- A fim de evitar o vazamento ou compartilhamento indevido de informações, os proprietários deverão seguir a de impacto disponível na Política Regulatória de Segurança da Informação do BSGB para auxiliar na correta classificação quanto ao nível de confidencialidade, de acordo com o conteúdo.

- **PCPI-C – Princípio 6: Revisão da Classificação das Informações**
  A classificação das informações deve ser revisada pelos proprietários sempre que necessário, de acordo com o contexto ou algum evento significativo (mudança nos riscos ou medidas de segurança).

  Este processo deve ser aplicado pelos proprietários da informação sempre que ocorrer alguma alteração no contexto, a fim de adequar a sua classificação ao nível correto para mitigação dos riscos, incluindo aumento ou redução do nível de confidencialidade, sempre que aplicável.

- **PCPI-C – Princípio 7: Cumprimento às Regras**
  Todos os colaboradores internos ou prestadores de serviços do BSGB devem manter e fornecer as evidências ao cumprimento desta Política, sempre que requerido.

  Todas as informações deverão ser classificadas e gravadas nos diretórios de rede do BSGB, para que possam ser devidamente protegidas e recuperadas a qualquer tempo.

  Somente pessoas autorizadas podem acessar as informações. O controle de acesso dos usuários aos diretórios de rede deve ser realizado pelos "*proprietários*" correspondentes, através do aplicativo para gestão de acessos às áreas de rede e das campanhas globais de recertificação, lançadas anualmente, conforme descrito na Política e Procedimento para Controle de Acessos. Nenhum documento deve ser gravado nos discos locais (Drives "C" e "D"), pois pode ser perdido em decorrência de falha nos equipamentos (*hardware*).

  Para mais detalhes sobre as regras para classificação das informações, consulte o Princípio 5 acima.

4.2. Gestão de Registros

Os registros de segurança são capturados e armazenados de forma segura de acordo com as políticas de retenção de registros e regulamentações do Grupo SG. Os logs são mantidos em pontos de repositório central com o "propósito de controles". Restrições sobre os locais desses repositórios são aplicadas para respeitar os requisitos regulatórios locais.

4.3. Proteção Contra Vazamento de Dados

(i) Criptografia

Todas as comunicações sensíveis são criptografadas, por exemplo: autenticações seguras através de "https", e-mails sensíveis C2 e C3, comunicações com parceiros preferenciais por criptografia TLS etc.

Os *laptops/desktops* são totalmente criptografados seguindo o padrão (*BitLocker*). Quando possível, informações confidenciais não públicas são criptografadas, ainda que em repouso, bem como em trânsito em redes externas. Quando a criptografia for considerada inviável, controles de compensação são aplicados conforme apropriado com base nos riscos.

(ii) Controle de envio de e-mails

O BSGB segue um programa global extensivo para detectar e prevenir o risco de vazamento de dados. O programa inclui o monitoramento diário *"*Proteção Contra Vazemento de Dados*"* de todos os e-mails enviados com a endereços de e-mail externos e monitoramento de e-mails utilizando ferramentas de Prevenção de Vazemento de Dados.

Além disso, existem controles preventivos implementados, tais como: restrições aos direitos de acesso a e-mail (somente funcionários efetivos estão autorizados a enviar documentos para destinatários externos ao BSGB). Quaisquer exceções deverão ser submetidas a dois níveis de aprovação (Gestor Imediato e pelo time de Cibersegurança Regional) e validadas caso-a-caso.

Os e-mails enviados para destinatários externos com arquivos classificados como C2 - *Confidencial*, são bloqueados quando indicado no processo de classificação que o referido documento não pode ser circulado fora do grupo.

(iii) Filtragem de Conteúdo da *Web*

O acesso a sites inapropriados, ilícitos e não-seguros (compras, jogos de qualquer natureza, armazenamento de arquivos etc.) são restringidos, em conformidade com as regras de segurança. As restrições de navegação na Web são aplicadas de forma global de acordo com as categorias definidas. As exceções são analisadas no caso-a-caso e aprovadas por 2 níveis de gestão e por um prazo determinado, de acordo com a necessidade.

(iv) Segurança "*end-point*"

O BSGB mantém um inventário contínuo de todos os dispositivos e sistemas físicos (servidores, banco de dados, equipamentos de rede e *laptops*/*desktops*), em um referencial global e dedicado. Cada equipe de Infraestrutura de Tecnologia é responsável pela atualização do referencial quando os dispositivos sob seu perímetro são colocados em produção ou removidos dele.

Além disso, o acesso remoto aos sistemas e arquivos de rede é feito através de conexões seguras (VPN) utilizando laptops fornecidos pelo BSGB, ambiente seguro com autenticação forte para qualquer acesso remoto usando um *desktop* pessoal e uso de ambiente seguro para acesso aos e-mails/Microsoft Teams corporativos utilizando *smartphones*. Qualquer comunicação de/para esses ambientes é criptografada. O acesso remoto é restrito, de acordo com as regras estabelecidas na Política de Teletrabalho (*home-office*).

Os *laptops/desktops* estão protegidos contra *malware* por meio de antivírus e contra vazamento de dados por meio de criptografia completa de seus discos rígidos. As portas USB são bloqueadas por padrão e as funções de gravação de DVD dos *laptops* são desativadas.

(v) Detecção de Transferência de Dados

Comunicações de saída por meio de *websites* com capacidades de armazenamento *online*, são monitoradas diariamente. Qualquer comunicação ou transferência de dados é bloqueada e um alerta é acionado para abertura de uma investigação formal e por escrito, a fim de confirmar se a comunicação e os dados enviados para os sites externos são relacionados aos negócios e justificados.

4.4. Gestão de Acessos e de Identidade

Os usuários do BSGB só precisam ter acesso aos recursos de TI de acordo com o princípio "necessidade de saber" e o princípio do "menor privilégio"[3], limitado ao exercício de suas atividades diárias.

BSGB mantém processos rigorosos para impedir qualquer escalação não autorizada de privilégios. Os perfis de acesso aos sistemas de negócios e acessos privilegiados são totalmente segregados para impedir o acesso não autorizado e a escalação inadequada de privilégios.

4.5. Gestão de Acessos

A gestão de acessos segue as diretrizes definidas na Política Regulatória de Segurança da Informação do BSGB, que objetivam assegurar um gerenciamento efetivo dos acessos de todos os colaboradores durante todos os eventos de movimentação dos usuários (admissão, desligamento, transferência e períodos de ausência prolongados) bem como estabelecer os processos para concessão, revogação e recertificação dos acessos a fim de identificar de quaisquer anomalias ou excesso de privilégios e/ou acessos indevidos que possam contribuir com a ocorrência de fraudes internas.

4.5.1. Gerenciamento de Senhas

Os sistemas do BSGB e os sistemas dos fornecedores estão sujeitos a uma política de senhas para prevenir o acesso não autorizado a dados e sistemas. Potenciais conluios também são prevenidos por meio de controles de acesso regulares, que realizam reconciliações entre os IDs de *laptops/desktop* usados para se conectar a determinadas aplicações. Anomalias são relatadas à gerência, solicitando explicações por escrito.

4.5.2. Gerenciamento de Sessão

Para evitar qualquer acesso não autorizado aos aplicativos e sistemas de negócios, o bloqueio da sessão (*lockout*) por inatividade é um recurso padrão nos sistemas do BSGB.

[3] Os conceitos de "necessidade de saber" ("*need to know basis*") e menor privilégio ("*least privilege*"), consistem em princípios de Segurança da Informação, onde o acesso à informação deve estar diretamente relacionado ao nível de responsabilidade de cada usuário.

As sessões na infraestrutura são geradas através de um *gateway* seguro que registra todas as atividades do pessoal de TI em servidores e bancos de dados. O *gateway* oferece recursos como a sessão "*4 eyes check*" (conferência para validação dos dados), para perímetros críticos.

4.5.3. Autenticação Segura ("*Strong Authentication*")

A conexão remota aos sistemas de informação do Grupo SG exige autenticação de dois fatores (2FA) para todos os colaboradores (internos ou externos). O Grupo SG equipou seus *desktops* e *laptops* internos com várias tecnologias de autenticação robustas.
Além disso, tecnologias de impressão inteligente foram implementadas para reduzir o risco de vazamento de dados. Para isso, os colaboradores devem escanear seu crachá em uma impressora interna para obter as cópias impressas.

A autenticação forte oferece proteções em todo o sistema e dados do Grupo SG. Ela é utilizada para proteger informações não públicas, como dados sensíveis de clientes, informações pessoais identificáveis ou informações empresariais, contra acesso e uso não autorizados.

4.5.4. Segurança de Acesso Físico

O BSGB realiza avaliações de risco para identificar ameaças e vulnerabilidades físicas de segurança. As avaliações contínuas de segurança física são realizadas periodicamente para revisar o acesso físico às instalações internas e a áreas tecnológicas sensíveis (*Data Room*, Mesa de Negociações, Sala de Arquivo de Documentos Físicos e quaisquer outras áreas que vierem a ser classificadas como sensíveis pelo Comitê Executivo do BSGB. As avaliações incluem verificação de indivíduos que acessam áreas sensíveis, níveis de liberação para áreas sensíveis e monitoramento de *hardware* de portas.

O programa de segurança para os *Data Centers* inclui barreiras de segurança, controle de acesso e vigilância por vídeo 24 horas x 7 dias por semana.

5. Sessões de Conscientização e Treinamentos

Todos os colaboradores do BSGB recebem sessões de treinamento de conscientização de segurança da informação e cibernética ao longo do ano, tais como:

(i) Treinamento Inicial (Integração de Novos Colaboradores):
A área de Gestão de Risco Operacional ministra um treinamento inicial para todos os novos colaboradores do BSGB em seus primeiros dias de trabalho, no qual os colaboradores são apresentados às principais diretrizes e conceitos sobre Segurança da Informação.

(ii) Treinamentos mandatórios:
Todos os colaboradores do BSGB realizam periodicamente treinamentos mandatórios relativos à Segurança da Informação e Cibersegurança através da plataforma de treinamentos online oficial do Grupo SG, com o propósito de reforçar/atualizar o conhecimento de todos quanto ao uso apropriado dos sistemas de informação, às melhores práticas para manuseio, classificação e proteção das informações durante o cumprimento de suas funções.

(iii) Manutenção de registro de treinamento:
O BSGB mantém registros dos treinamentos realizados, tais como: agenda, material apresentado, lista de presença, , Relatório de Registro de Treinamento da plataforma de treinamentos *online*, e quaisquer outros materiais distribuídos como parte dos treinamentos.

Vários instrumentos são utilizados periodicamente para sensibilizar os colaboradores às regras de segurança da informação: treinamentos *online*, comunicados, notícias na intranet, além da ciência formal sobre as regras locais no ato da admissão de novos colaboradores. Além disso, as políticas e procedimentos aplicáveis ao BSGB, publicadas internarmente, complementam as diretrizes sobre Segurança da Informação.

6. Prazo de Arquivamento

O prazo de retenção para os documentos, informações e dados a que este documento se refere é de 10 (dez) anos.

Este documento deverá ser revisado, atualizado e publicado no *website* do BSGB no mínimo anualmente ou quando ocorrer quaisquer alterações significativas nas diretrizes internas do Grupo SG, SG AMER e/ou nos requisitos regulatórios sobre Segurança da Informação.

7. Indicador da Declaração de Apetite por Riscos

O(s) indicadore(s) de risco operacional relacionado(s) ao conteúdo deste documento definido(s) na Declaração de Apetite por Riscos do BSGB , são monitorados conforme periodicidade definida para cada métrica para assegurar aderência aos níveis de apetite de risco e em linha com a estratégia de negócios do BGSB.

Qualquer violação das métricas é reportada para o Diretor de Riscos (CRO) e ao Comitê de Riscos do BSGB, para análise e definição das ações corretivas, quando aplicável.

Quando houver excessos ou violações dos limites aprovados na Declaração de Apetite por Riscos, a área de Riscos deve ser acionada para assegurar o cumprimento das diretrizes e governança estabelecidas no documento de Declaração de Apetite por Riscos vigente.

O processo de coleta de dados, cálculo e divulgação estão definidos em procedimento interno específico quanto as métricas da Declaração por Apetite por Riscos de risco não financeiro para o escopo que cabe à área de Gestão de Risco Operacional.