# Resumo da Política Regulatória de Segurança Cibernética, em atendimento a Resolução CMN Nº 4.893/21 e Resolução CVM Nº 35/21

A Política Regulatória de Segurança Cibernética do Banco Société Générale Brasil S.A. (BSGB) estabelece a governança e os princípios para a identificação, mensuração, mitigação, controle, tratamento de dados, monitoramento, testes, escalonamento, resposta a incidentes e reporte interno e regulatório relacionados à gestão do risco cibernético e operacional, alinhada integralmente às normas, programas e estruturas de gestão de riscos do Grupo Société Générale (Grupo SG) e do Société Générale Américas (SG AMER), além de cumprir a legislação e normativos brasileiros, especialmente a Resolução CMN Nº 4.893/21 publicada pelo Banco Central do Brasil e a Resolução CVM Nº 35/21.

Suportado pelo programa e pela estrutura de cibersegurança do Grupo SG e SG AMER, o BSGB assegura o gerenciamento dos riscos de segurança da informação e segurança cibernética, primando pela proteção de seus ativos digitais, dados, informações sensíveis relacionadas a seus *stakeholders* e sistemas críticos que suportam suas operações e serviços financeiros.

Na referida Política estão definidas as diretrizes e responsabilidades para implementar práticas robustas de gestão de riscos cibernéticos, com o objetivo principal de proteger a confidencialidade, integridade, disponibilidade e autenticidade das informações sob a gestão do BSGB.

## 1. Mecanismos de Defesa

Os mecanismos de defesa contra ameaças cibernéticas são construídos em torno dos três pilares essenciais de segurança: (i) **Prevenção**, (ii) **Identificação** e (iii) **Resposta**, e são formados por um conjunto de sistemas, ferramentas e serviços dedicados para monitoramento contínuo e efetivo de atividades maliciosas, que possam representar um risco para a rede interna do BSGB.

Para o BSGB é primordial monitorar de forma contínua e efetiva as atividades maliciosas que podem representar um risco para as informações sob sua custódia ou de sua propriedade, a fim de detectar tentativas e/ou ataques cibernéticos, seus impactos e limitar a duração e o impacto das tais ameaças. O BSGB atua nos estes três pilares em consonância com as diretrizes e práticas globais do Grupo SG, bem como com as exigências legais e regulatórias locais, visando sempre reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

## 2. Antecipação

O BSGB deve prever as ameaças, vulnerabilidades e os piores cenários para garantir que os pilares sejam adaptados de forma contínua e rápida, utilizando processos e tecnologias de defesa robustos e resilientes.

É essencial adaptar e melhorar as camadas de defesa tão rapidamente quanto a evolução das ameaças e técnicas de ataque. A capacidade de prevenção é centrada em torno de três elementos, Inteligência Cibernética, Testes Periódicos e Planos de Recuperação eficazes, conforme segue:

- **Inteligência Cibernética:** O BSGB deve reunir a inteligência de ameaças de fontes internas e externas, (incluindo agências governamentais, organizações privadas, fontes públicas, mídias sociais, fóruns de *hacking*, d*eep web*, e outras fontes) para prever as intenções, ferramentas e técnicas que representam ameaças aos negócios do BSGB.

- **Testes Periódicos:** O BSGB deve identificar os principais ativos, sistemas e informações (incluindo os alocados em terceiros) e analisar regularmente os riscos e o nível de proteção pertinentes, a fim de descobrir e corrigir os pontos fracos de forma proativa. É essencial realizar testes de segurança periodicamente, incluindo avaliações de risco, varredura de vulnerabilidades e testes de invasão.

- **Planos de Recuperação:** A segurança cibernética deve ser um fator a ser incluído no plano de recuperação para garantir que o BSGB esteja pronto para se recuperar dos piores cenários cibernéticos por meio de planos de continuidade, recuperação de desastres e crises. Um elemento principal deste recurso é exercitar os planos existentes regularmente (por exemplo, cenários de ataques cibernéticos simulados etc.).

## 3. Papéis e Responsabilidades

O gerenciamento do risco de segurança da informação e cibernética no BSGB é estruturado conforme a segregação de funções e responsabilidades dentro das três linhas de defesa.

A primeira linha de defesa (1LOD) é composta pelas unidades de negócios e de suporte locais e regionais, responsáveis pela avaliação, controle e monitoramento dos riscos cibernéticos em suas atividades, seguindo normativos aplicáveis. Dentro da 1LOD, duas unidades de suporte têm papel destacado na governança, definição e implementação do programa e estrutura de segurança da informação e cibernética, são elas: Unidades Organizacionais de Suporte de Segurança da Informação e Riscos, subordinada ao CISO (*Chief Information Security Officer*) do SG AMER, e a Unidade de Suporte de Gestão de Risco Operacional, que atua de forma independente no gerenciamento do risco operacional, incluindo risco de segurança da informação e segurança cibernética, subordinada ao Diretor de Riscos e ao Diretor Responsável pela Segurança Cibernética no BSGB.

A segunda linha de defesa atua de forma independente da 1LOD, supervisionando e analisando a exposição ao risco de segurança cibernética. Essa função é exercida pela área de Riscos Local, subordinada ao CRO, e pelas funções regionais correspondentes quando aplicável.

A terceira linha de defesa é representada pela Auditoria Interna, que supervisiona independentemente as atividades das duas primeiras linhas, garantindo a efetividade dos processos de gerenciamento e controle do risco de segurança cibernética.

## 4. Diretor de Segurança Cibernética

O Diretor de Segurança Cibernética deve supervisionar, assegurar e promover a aplicação desta Política Regulatória de Segurança Cibernética e seus princípios no BSGB, bem como a incorporação das diretrizes nas atividades diárias de forma efetiva e a execução do plano de ação e de resposta a incidentes.

## 5. Programa de Segurança Cibernética

O programa é formado por diversos processos, incluindo:

- Classificação mandatória das informações;
- Treinamentos e sessões de conscientização para todos os colaboradores (incluindo terceiros);
- Gestão de acessos e identidade (Autenticação);
- Criptografia de dados;
- Prevenção e detecção de intrusão;
- Vazamento de informações e infecção por *malwares*;
- Gestão de vulnerabilidades de segurança;
- Segurança de redes;
- Logs e Monitoramento;
- Simulação de cenários incorporados aos testes de continuidade dos negócios e recuperação de desastres; e
- Plano de ação e de resposta a incidentes de segurança cibernética.

A gestão do risco de segurança cibernética também inclui um processo de diligência sobre a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, notadamente sobre o atendimento aos requisitos regulatórios, a fim de garantir a confidencialidade, disponibilidade e integridade dos dados e a comunicação tempestiva sobre quaisquer incidentes de segurança por parte dos fornecedores.