Resumo da Política Regulatória de Segurança Cibernética, em atendimento a Res. CMN nº 4.893/21

Os sistemas de informação do Conglomerado Prudencial do Société Générale Brasil ("CSGB"), composto pelo Banco Société Générale Brasil S.A. ("BSGB") e pela Société Générale Equipment Finance S.A. – Arrendamento Mercantil ("SGEF"), armazenam informações financeiras, contratuais e de negócios, além de informações sensíveis relacionadas a clientes e colaboradores.

Todas essas informações representam um ativo estratégico para o CSGB e estão expostas a riscos de segurança da informação e cibernético, sujeitas à obrigações legais e regulatórias e devem ser protegidas de maneira efetiva para assegurar a integridade, disponibilidade e confidencialidade dos dados.

A Política estabelece as diretrizes para implantação de processos e controles relacionados à segurança da informação e cibernética, a fim de assegurar o gerenciamento dos riscos de forma efetiva, incluindo princípios, conceitos, valores e práticas que devem ser adotados pelos colaboradores, parceiros e prestadores de serviços contratados pelo CSGB no exercício de suas atividades, em cumprimento a Res. CMN nº 4.893/21, publicada pelo Banco Central do Brasil, e em consonância com as diretrizes locais, regionais e globais do Grupo Société Générale "SG, as quais têm como principais objetivos:

- Garantir a integridade da informação gerenciada, processada e armazenada pelos sistemas de informação do CSGB;
- Proteger as informações por meio da rastreabilidade, controle de acesso, criptografia, proteção de e-mail, entre outros;
- Identificar e avaliar os riscos internos e externos relacionados à segurança da informação e cibernética que podem vir a ser ameaças diretas ou indiretas aos sistemas de informação do CSGB;
- Detectar e responder a eventos de segurança da informação e cibernética a fim de mitigar todo e qualquer efeito negativo;
- Recuperar dos eventos de segurança da informação e cibernéticos e restaurar/normalizar as operações e serviços e;
- Possibilitar a tomada de decisão por meio de avaliação de riscos de segurança da informação e cibernética.

Para atender tais objetivos, o CSGB adota uma abordagem de defesa e antecipação contra ameaças, são elas:

1. Mecanismos de Defesa

Os mecanismos de defesa contra ameaças cibernéticas são construídos em torno dos <u>três pilares essenciais de segurança</u>: (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 CSGB.

Para o CSGB 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 CBSB atua nos estes três pilares em consonância com as diretrizes e práticas globais do Grupo SP, bem como com as exigências legais e regulatórias locais, visando sempre reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

2. Antecipação

O CSGB 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.

- **Inteligência Cibernética:** O CSGB 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 CSGB.

- **Testes Periódicos:** O CSGB 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 CSGB 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 e controle do risco de segurança cibernética é realizado através de funções e responsabilidades definidas para assegurar a devida segregação das atividades e controles, seguindo a estrutura regional (Américas) do Grupo Société Générale. Os papéis e responsabilidades definidos abaixo para as 3 linhas de defesa, são limitados ao gerenciamento do risco de segurança da informação e segurança cibernética.

O gerenciamento e controle do risco de segurança cibernética é realizado através de funções e responsabilidades definidas para assegurar a devida segregação das atividades e controles, seguindo a estrutura das 3 linhas de defesa, conforme definido na Política de Gestão Integrada de Riscos do CSGB, em atendimento a Res. CMN Nº 4.557 de 23/02/2017.

4. Diretor de Segurança Cibernética

O Diretor de Segurança Cibernética deve supervisionar, assegurar e promover a aplicação desta Política de Segurança Cibernética e seus princípios em todo o conglomerado, e a incorporação das diretrizes nas atividades diárias de forma efetiva, bem como 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;
- Criptografia de dados;
- Prevenção e detecção de intrusão;
- Vazamento de informações e infecção por *malwares*;
- Identificação de vulnerabilidades;
- Simulação de cenários incorporados aos testes de continuidade dos negócios e recuperação de desastres; e
- Implantação de mecanismos de segurança e monitoramento contínuo da rede interna do CSGB, incluindo um programa de resposta a incidentes.

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.