Resumo da Política de Segurança Cibernética, em atendimento a Res.4.658/18

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 a obrigações legais e regulatórias e devem ser protegidas de maneira efetiva para assegurar a integridade, disponibilidade e confidencialidade dos dados.

A Política de Segurança Cibernética do CSGB, visa estabelecer as diretrizes para implantação de processos e controles relacionados a 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 4.658, publicada pelo Banco Central do Brasil em 26 de Abril de 2018.

Principais objetivos da Segurança Cibernética no CSGB:

- 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.

1. Mecanismos de Defesa

Os mecanismos de defesa contra ameaças cibernéticas são construídos em torno dos três pilares essenciais de segurança: **Prevenção, Identificação e 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.

O objetivo principal é de detectar os ataques e prevenir seus impactos. É primordial, ainda, que estes três pilares sejam integrados e operados globalmente, visando sempre reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

2. Antecipação

O CSGB utiliza processos e tecnologias de defesa robustos e resilientes, para detectar ameaças, vulnerabilidades e considera os piores cenários para garantir que os mecanismos de defesa possam ser acionados de forma rápida e eficiente.
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, deep 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 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 das 3 linhas de defesa, conforme definido na Política de Gestão Integrada de Riscos do CSGB, em atendimento a Res.4.557/17.

4. Diretor de Segurança Cibernética

A gestão do risco de Segurança Cibernética foi incorporada à gestão integrada dos riscos, cumulativamente às funções do Diretor de Riscos do CSGB, que deve supervisionar, assegurar e promover a aplicação da 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. Definições e conceitos

As definições e conceitos a seguir devem ser observadas por todos os colaboradores do CSGB, dentro de seus perímetros de atuação. Os seguintes conceitos foram estabelecidos no âmbito da Política de Segurança Cibernética:

- **Ataque cibernético:** É a exploração e/ou tentativa, por parte de um agente malicioso, das vulnerabilidades no ambiente com a finalidade de obter algum ganho ou causar algum dano ou efeito negativo à instituição ou a algum de seus ativos. As principais fontes de ameaças cibernéticas são o crime organizado, hackers, grupos patrocinados por pessoas maliciosas, terroristas e detentores de informações privilegiadas. A exposição aos ataques cibernéticos não se limita aos sistemas do CSGB, os atacantes podem ter como alvo os clientes e/ou fornecedores, parceiros e

os próprios colaboradores, com o intuito de causar impactos significativos para a instituição.

- **Segurança Cibernética:** É a capacidade de resistir, conter e recuperar-se rapidamente de um ataque cibernético que venha a colocar em risco a segurança das informações, englobando a maturidade dos processos criados para proteger a confidencialidade, integridade e disponibilidade dos ativos tecnológicos e dos dados de propriedade do CSGB.
- **Riscos à Segurança Cibernética:** É composto de três elementos principais:
  - Acesso não autorizado ou mau uso de informações ou sistemas (por exemplo: furto de informações pessoais, fusões e aquisições, planos ou propriedade intelectual).
  - Furto e fraude financeira (por exemplo: redirecionamento de pagamentos, comprometimento de contas de clientes e roubo de identidade).
  - Interrupção da atividade comercial (por exemplo: sabotagem, extorsão e negação de serviço).

Estes riscos advêm tanto de dentro, quanto de fora da instituição. O impacto do risco à segurança cibernética engloba perda financeira, danos à reputação, multas regulatórias, perda de vantagem estratégica e interrupção das operações.

6. 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 da Res.4.658/18, a fim de garantir a confidencialidade, disponibilidade e integridade dos dados e a comunicação tempestiva sobre quaisquer incidentes de segurança por parte dos fornecedores.

7. Revisão e atualização das diretrizes

A Política de Segurança Cibernética do CSGB é revisada, no mínimo, anualmente, a fim de assegurar a adesão às normas legais, regulamentares, estatutárias e demais instruções relevantes de forma efetiva, para o correto desempenho das atividades.