Política para Classificação e Proteção das Informações – Confidencialidade (PPCPI-C)

Conglomerado do Société Générale Brasil

Novembro/2024

ÍNDICE

1. Introdução

Esta Política descreve os princípios e diretrizes para classificação e proteção das informações de propriedade do Conglomerado do Société Générale Brasil ("CSGB"), composto pelas Instituições: Banco Société Générale Brasil S.A. ("CSGB") e Société Générale Equipment Finance S.A. Arrendamento Mercantil ("SGEF").

Toda informação enviada ou recebida pelos colaboradores do CSGB durante o exercício de suas funções, independentemente do formato ou mídia, deve seguir os parâmetros de classificação descritos nesta política a fim de assegurar a integridade, disponibilidade e confidencialidade dos dados.

Adicionalmente ao disposto nesse documento, as informações que possuem dados pessoais e dados pessoais sensíveis para identificação de pessoas físicas, também seguem as diretrizes descritas nas Políticas internas do CSGB relacionadas ao cumprimento da Lei Geral de Proteção de Dados (Nº 13.709).

Todos os funcionários vinculados às Instituições Financeiras e seus congêneres, tem a obrigação de manter sigilo às informações de seus respectivos clientes e de terceiros, durante o exercício de suas funções, de acordo com a Lei Complementar 105/01, que dispõe sobre o **Sigilo Bancário.** A eventual quebra desse sigilo só pode ocorrer mediante autorização judicial, nos casos que houver suspeita de movimentação ilegal de recursos da conta dos clientes.

2. Objetivo

O objetivo desta Política é de assegurar a confidencialidade das informações manuseadas e gerenciadas pelos colaboradores do CSGB (funcionários, estagiários, terceiros e contratados), a fim de mitigar os riscos de fraude, vazamento de dados, perda e/ou roubo das informações, seguindo as regras e normas globais do Société Générale relacionadas aos critérios de classificação e proteção.

3. Princípios de Confidencialidade

Os seguintes princípios se aplicam ao critério de confidencialidade:

3.1. Dever de Confidencialidade

PCPI-C – Princípio 1
Todos os usuários do sistema de informações[1] do CSGB tem o dever de confidencialidade em relação às informações que forem criadas, coletadas, mantidas e/ou manuseadas como parte integrante de suas atividades diárias.

O dever de confidencialidade se aplica a todas as informações, independentemente do formato, forma de armazenamento e contexto.

Qualquer colaborador do CSGB tem o dever de confidencialidade com as informações por ele geridas ou manipuladas durante o exercício de suas atividades profissionais.

O cumprimento à esta regra 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.

O comprometimento com a confidencialidade das informações não é meramente uma condição que permite mitigar os riscos relacionados à segurança da informação, mas também uma forma de zelar pela imagem e reputação do CSGB.

[1] O Sistema de informações é composto por uma série de recursos (pessoas, software, procedimentos, dados, materiais, equipamentos de telecomunicações e de tecnologia da informação), que disponibilizam informações (em texto, imagem, som, vídeo, em formato físico ou digital), para coleta, armazenamento, modelagem, gerenciamento, manipulação, análise, transporte, troca e distribuição dentro de uma organização.

3.2. Restrição de acesso ("*Need-to-Know*" – Necessidade de Acesso)

PCPI-C - Princípio 2
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**[2].

A necessidade de acesso à informação deve estar diretamente ligada a realização das atividades profissionais diárias. Consequentemente, 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 controladores externos, é definido de acordo com as necessidades e a forma de intervenção, em cumprimento a regulamentação e legislação local.

3.3. Propriedade da Informação e Responsabilidades em relação a Classificação

PCPI-C - Princípio 3.1
Qualquer colaborador do CSGB (funcionário, estagiário, terceiro, contratado, temporário ou qualquer outro usuário interno ou externo com acesso ao sistema 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.**

Os proprietários das informações são responsáveis por:

– **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;
– **Cumprir com as regras** de utilização e classificação das informações;
– Cumprir com as **medidas de proteção** no manuseio das informações;

Os **destinatários** são os usuários que recebem as informações. Consequentemente, 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 - Secreto).

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

A classificação da informação deve estar visível para qualquer pessoa que for acessá-la, para cumprimento das regras de proteção correspondentes.

3.4. Manuseio Apropriado das Informações

PCPI-C - Princípio 4
Todos os usuários que possuem acesso ao sistema de informações do CSGB (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.

[2] Os usuários devem receber apenas os privilégios estritamente necessários para o desempenho de suas funções.

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 CSGB receber por engano informações ou documentos não direcionados a ele e/ou não relacionados à suas atividades, é responsabilidade deste colaborador comunicar imediatamente o time de Risco Operacional que avaliará quanto ao enquadramento da ocorrência em um incidente de vazamento de dados (*data leakage*), 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 tem o compromisso de zelar pela discrição no acesso às informações de negócios em lugares públicos.

3.5. Conscientização sobre a Classificação e Proteção das Informações

PCPI-C - Princípio 5
Todos os usuários que possuem acesso ao sistema de informações do CSGB (funcionário, estagiário, terceiro, contratado, temporário ou qualquer outro usuário interno ou externo), **devem participar de treinamentos e programas de conscientização** sobre a **classificação e proteção das informações** e aplicar sempre as melhores práticas no cumprimento de suas funções.

Todos os Gestores diretos dos usuários devem conscientizar a sua equipe sobre a importância do cumprimento às regras relacionadas a classificação correta do nível de confidencialidade das informações.

3.6. Revisão da Classificação das Informações

- Princípio 6
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.

3.7. Cumprimento às regras

PCPI-C - Princípio 7
Todos os colaboradores internos ou prestadores de serviços do CSGB devem fornecer as evidências ao cumprimento desta Política, sempre que necessário.

4. Regras para classificação 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 CSGB ou compartilhado por e-mail, sem a devida classificação, que deverá seguir os parâmetros listados abaixo (C0, C1, C2 e C3).

Este procedimento deverá ser realizado através de aplicativo específico e disponibilizado nos equipamentos do CSGB, conforme diretrizes estabelecidas nesta Política.

Níveis de classificação:

- **C0 PÚBLICO**

  Qualquer informação ou documento que possa ser divulgado ao público sem ocasionar impactos às atividades de negócios do CSGB, 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 CSGB.

  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:

- ***Cannot leave the Group*** **(não pode ser divulgada fora Grupo Société Générale "SG"):** 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).
- ***Can leave the Group*** **(pode ser divulgada com público autorizado externo ao Grupo SG) :** 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*", ou seja, não podem sair do Grupo SG.

4.1. 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:

4.1.1. 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 CSGB com seus clientes, fornecedores, parceiros e prestadores de serviços;
- Dados relacionados a sistemas operacionais (logs de acesso, chaves de criptografia etc).

4.1.2. 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.

4.1.3. Elementos adicionais

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

4.2. Análise de Impacto

A fim de evitar o vazamento ou compartilhamento indevido de informações, os proprietários deverão seguir a matriz de impacto do CSGB para auxiliar na correta classificação quanto ao nível de confidencialidade, de acordo com o conteúdo.

4.3. Regras de Acesso às Informações e Armazenamento

Todas as informações deverão ser classificadas e gravadas nos diretórios de rede do CSGB, 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 "*owners*" correspondentes, através do aplicativo para gestão de acessos às áreas de rede e das campanhas globais de recertificação, lançadas anualmente, de acordo com a Política e Procedimento para Controle de Acessos do CSGB.

Nenhum documento deve ser gravado nos discos locais (*Drives* "C" e "D"), pois pode ser perdido em decorrência de falha nos equipamentos (*hardware*).

4.4. Atenção na troca de dados criptografados

A senha usada na criptografia das informações deve ser transmitida por outro meio que não aquele utilizado para o envio dos dados (por exemplo: enviar a informação por email e repassar a senha por telefone ou em um outro e-mail – lembrando sempre de checar a identidade do destinatário).

---

5. Regras para Proteção das Informações

Cada nível de confidencialidade deverá estar associado às regras de proteção do Grupo SG. A regra de proteção a ser aplicada deve ser diretamente proporcional ao nível de proteção necessária para mitigação dos impactos e riscos relacionados a um vazamento indevido.

Se outras regras de classificação forem requeridas quanto à integridade, disponibilidade ou rastreabilidade das informações, deverá sempre ser considerado o nível mais alto de proteção.

---

6. Referências Regulatórias

- **Leis de Aplicação no âmbito federal:**

  - Lei 13.709 de 14/08/2018, que dispõe sobre o tratamento de dados pessoais;
  - Lei complementar 105/01, que dispões sobre o sigilo bancário.

- **Normas Infralegais:**

  - Res. 4.557/17, que dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

- **Regulamentação Interna:**

  - Política Regulatória de Segurança da Informação do CSGB;
  - Política de Regulatória de Segurança Cibernética do CSGB;
  - *SG Code, Book C, Part 5 – Security, Safety, Business Continuity and Crisis Management, Title I – Security of People, Property and Information, Sub-Title – Security of Information*.

---

7. Prazos de Arquivamento

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

---

8. Treinamentos obrigatórios

Todos os colaboradores do CSGB devem realizar os treinamentos anuais mandatórios de Segurança da Informação publicados na plataforma eLearning.

Treinamentos práticos e obrigatórios sobre proteção e classificação das informações poderão ser organizados a qualquer tempo pelas áreas de Risco Operacional e Controles Internos e de Segurança da Informação, a fim de reforçar as regras e diretrizes internas sobre Segurança da Informação.

---

9. Plano de Ação e de Resposta a Incidentes

No caso de identificação de falhas e/ou violações aos tópicos tratados nesta Política, será necessário a abertura de um incidente operacional, informando a governança regional de Segurança da Informação, para investigação e definição de planos de ação para mitigação dos riscos.

---

10. Divulgação e Vigência

Esta Política é uma versão da "Política e Procedimento para Classificação e Proteção das Informações Confidencias (PPCPI-C).V6" para divulgação ao público geral. A qual será atualizada pelo menos anualmente ou quando ocorrer quaisquer alterações significativas nas diretrizes internas para gerenciamento dos riscos e/ou nos requerimentos regulatórios e aprovada pelo Diretor de Tecnologia da Informação (CIO), Diretor de Operações e Diretor Estatutário Responsável pela Segurança Cibernética e pelo Diretor de Riscos.