PCG_004 Segurança Cibernética e de Informação Vigente desde 11/01/2024

Objetivos

Esta política tem como objetivo estabelecer diretrizes e princípios gerais de segurança da informação e segurança cibernética para o Conglomerado Financeiro Votorantim (Conglomerado), em um esforço para garantir que os usuários atuem em observância às regras referentes ao tratamento e proteção das informações e ativos de informação, bem como assegurar a capacidade do Conglomerado em prevenir, detectar e reduzir sua vulnerabilidade a incidentes.

Diretrizes

1. Público-Alvo

1.1. Esta política de Segurança Cibernética e de Informação ("Política") é a declaração formal do Banco Votorantim S.A. ("Banco") e sociedades controladas, integrantes do Conglomerado Financeiro Votorantim, em conjunto denominadas nesta Política como "Conglomerado", referente ao compromisso com a proteção de suas informações e ativos de informação, bem como das informações e ativos de informação de seus clientes e fornecedores.

1.2. Esta política é aplicável a todos os colaboradores e usuários de informações e ativos de informação do Conglomerado no Brasil e no exterior.

1.3. Fornecedores e sociedades investidas do Conglomerado também estão sujeitos às diretrizes, procedimentos e controles estabelecidos nessa Política sempre que realizarem o tratamento de informações ou utilizarem os ativos informação do Conglomerado. Da mesma forma estão sujeitos, os clientes do segmento Banking as a Service "Clientes BaaS" que são co-controladores no que compete às decisões referentes ao tratamento dos dados pessoais de seus clientes no âmbito da prestação dos serviços pelo Banco, que atua como depositário dos recursos mantidos nas contas de pagamento individualizadas.

1.4. Para os fins desta política, "colaborador" significa empregados, contratados, subcontratados, estagiários, menores aprendizes e administradores do Conglomerado, e "fornecedor" significa todas as empresas fornecedoras, parceiras e prestadoras de serviços a

terceiros que celebraram um contrato de fornecimento, parceria e/ou prestação de serviços com o Banco e/ou suas controladas, bem como seus representantes, empregados e subcontratados.

1.5. Para os fins desta política, os termos "informações" e "ativos de informação" incluem o conceito de dado pessoal e/ou dado pessoal sensível, incluindo os locais de armazenamento e/ou processamento destes dados, tal como definido pela Lei Geral de Proteção de Dados, Lei Federal nº 13.709/18, conforme alterada.

1.6. Para os fins desta política, o termo "Clientes BaaS", significa empresas de diferentes segmentos que são contratantes do serviço Banking as a Service do
Banco e/ou que atuam no arranjo de pagamentos Pix na qualidade de "Participante Contratante", nos termos da regulamentação vigente, por meio de contrato específico com o Banco. O Banking as a Service é uma solução que possibilita que uma instituição de pagamento, conforme o caso, possa oferecer serviços financeiros aos seus clientes de forma personalizada e eficiente, por meio de integração sistêmica com uma instituição financeira.

1.7. Para os fins desta política, o termo "investida" ou "sociedade investida", significa qualquer sociedade na qual o Conglomerado possua investimento financeiro representado por participação societária, instrumentos conversíveis em participação ou outro arranjo que lhe permita ou facilite a criação de sinergias e relacionamento, visando geração de valor para o Conglomerado.

2. Princípios da Segurança da Informação

2.1. Por princípio, a segurança da informação abrange 4 (quatro) aspectos básicos destacados a seguir:

a. Confidencialidade: Garante que a informação e ativos de informação sejam acessíveis somente pelos usuários autorizados, pelo período necessário;

b. Integridade: Garante que a informação e ativos de informação estejam completos e íntegros e que não tenham sido modificados ou destruídos de maneira não autorizada ou acidental durante o seu ciclo de vida;

c. Disponibilidade: Garante que a informação e ativos de informação estejam disponíveis para os usuários autorizados sempre que necessários aos processos de negócio ou a clientes do Conglomerado;

d. Autenticidade: Garante a propriedade da informação e que esta seja proveniente da fonte anunciada e não foi alvo de alterações indevidas ao longo de um processo estabelecido.

2.2. Para os fins desta política, o termo usuário significa qualquer indivíduo, processo, dispositivo ou mecanismo que acesse, use, manipule ou trate informação ou ativo de informação.

3. Aspectos Gerais

3.1. As diretrizes desta política constituem os principais pilares do Sistema de Gestão de Segurança da Informação do Conglomerado, norteando a elaboração de instruções normativas e manuais de procedimento pelas áreas responsáveis.

3.2. A proteção das informações e ativos de informação do Conglomerado deve ser uma prioridade constante das áreas de negócio e de suporte do Conglomerado, de forma a reduzir riscos de falhas, bem como danos e/ou prejuízos que possam comprometer a imagem e os objetivos organizacionais do Conglomerado.

3.3. A proteção das informações e ativos de informação deve ser aplicada de forma compatível com seu impacto ao Conglomerado, abrangendo todos os processos, informatizados ou não.

3.4. Uma atitude engajada e proativa no que diz respeito à proteção das informações do Conglomerado deve ser prioridade constante de toda a organização, reduzindo-se os riscos de falhas, danos e/ou prejuízos que possam comprometer a imagem e os objetivos organizacionais.

3.5. As informações sob responsabilidade do Conglomerado devem ser manuseadas de acordo com as leis vigentes e instruções normativas internas e utilizadas apenas para a finalidade para a qual foram coletadas, evitando o comprometimento de sua confidencialidade, integridade, disponibilidade, autenticidade e privacidade.

3.6. Todos os processos do Conglomerado devem garantir a segregação das funções por meio da participação de mais de um colaborador ou equipe de colaboradores nas atividades, a fim de evitar o conflito de interesse e reduzir o risco de uso indevido acidental ou proposital dos ativos de informação e sistemas do Conglomerado.

3.7. Todos os colaboradores do Conglomerado ou de fornecedores, conforme aplicável, devem ter ciência de que o uso dos ativos de informação, dos sistemas e ambientes podem ser monitorados e que os registros podem ser utilizados para detecção de violações desta Política e instruções normativas de segurança da informação, servindo

de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais.

3.8. Os papéis e responsabilidades quanto à segurança da informação são amplamente divulgados aos colaboradores, que devem conhecer e cumprir essas diretrizes.

3.9. Os riscos de segurança da informação do Conglomerado, bem como dúvidas sobre a política e instruções normativas relacionadas devem ser reportados à Superintendência de Segurança da Informação.

3.10. Os sistemas, aplicações e infraestruturas tecnológicas, marcas, metodologias e quaisquer informações do Conglomerado não devem ser utilizados para fins pessoais. Sobre o uso da internet, para fins pessoais, deve
ser responsável, seguindo as legislações vigentes (sobre ações discriminatórias, privacidade, pirataria, pedofilia, terrorismo e etc.), não deve contrariar as instruções normativas internas, que possa trazer riscos de contaminação ao ambiente ou de vazamento de informações e não deve prejudicar os princípios de Segurança da Informação contidos nesta política ou o Código de Conduta.

3.11. Exceto com a expressa autorização do seu proprietário responsável, as tecnologias, marcas, metodologias e quaisquer informações do Conglomerado não devem ser repassadas ou compartilhadas com terceiros, ainda que tenham sido obtidas ou desenvolvidas pelo próprio colaborador do Conglomerado durante o exercício de suas funções.

4. Classificação das Informações

4.1. Toda informação criada ou recebida pelo Conglomerado deve ser classificada e protegida ao longo de todo seu ciclo de vida, nos termos das Instruções Normativas e Manuais de Procedimentos de Segurança da Informação do Conglomerado. O ciclo de vida das informações compreende sua criação ou coleta, manuseio, armazenamento, transporte e descarte.

4.2. Para assegurar a proteção adequada das informações, elas devem ser classificadas de acordo com o seu valor, requisitos legais, relevância, sensibilidade e criticidade para o Conglomerado. Os critérios de classificação devem considerar as necessidades de negócio, demandas regulatórias, compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

4.3. As diferentes classificações para as informações estão definidas em instrução normativa específica.

5. Tratamento das Informações

5.1. As informações devem ser tratadas de acordo com as leis vigentes, regulamentação aplicável, Instruções Normativas e sua classificação, e utilizadas apenas para a finalidade para a qual foram coletadas, ou para outras finalidades autorizadas, sempre observando os princípios previstos na Lei Geral de Proteção de Dados.

5.2. As informações podem ser tratadas em legítimo interesse do Conglomerado para proteger a segurança dos ativos de informação ou a segurança das operações comerciais do Conglomerado.

5.3. As informações são atribuídas a um proprietário formalmente designado como responsável pela autorização de acesso às informações sob sua responsabilidade.

5.4. Para fins desta política, o "proprietário" significa o indivíduo ou grupo com autoridade operacional sobre uma Informação específica e responsabilidade para estabelecer os controles por sua criação, coleta, processamento, disseminação e descarte.

5.5 As atividades de tratamento das informações devem ser rastreáveis e registradas em trilhas auditáveis.

6. Segurança Cibernética

6.1. O Conglomerado também aplica controles de segurança de informação de forma a manter constante evolução na sua segurança cibernética, com o objetivo de assegurar a disponibilidade, confidencialidade, integridade e autenticidade das informações e ativos de informação em seus ambientes tecnológicos.

6.2. De forma a auxiliar na implementação das diretrizes estabelecidas nesta política e dos controles, processos e procedimentos do Sistema de Gestão de Segurança de Informação e da Segurança Cibernética do Conglomerado, são adotados, por padrão, os seguintes mecanismos e as melhores práticas disponíveis no mercado:

a. Medidas de autenticação capazes de individualizar usuários que acessam ativos de informação, sistemas e ambientes do Conglomerado;
b. Emprego de criptografia, mascaramento e ofuscação, quando aplicável, para o armazenamento de informações relevantes e

sensíveis em ativos de informação, sistemas e ambientes do Conglomerado e de fornecedores;

c. Uso de tecnologia de criptografia e comunicação segura para a transmissão de informações entre colaboradores, usuários e fornecedores;
d. Soluções de prevenção e detecção de intrusão e acessos não-autorizados aos ativos de informação, sistemas e ambientes do Conglomerado;
e. Uso de procedimentos e controles para prevenir o vazamento de informações;
f. Testes e varreduras periódicas para a detecção de falhas e vulnerabilidades nos procedimentos, controles, sistemas e ambientes do Conglomerado;
g. Soluções de proteção contra softwares maliciosos (malwares, vírus) e etc.)

que podem afetar ativos de informação, sistemas e ambientes do Conglomerado;

h. Sistemas de rastreamento de atividade e registros (logs) para as atividades

realizadas em seus sistemas e ambientes, com o objetivo de garantir a segurança das informações;

i. Controle de acesso pelos usuários que façam uso dos sistemas e ambientes do Conglomerado;
j. Segregação e segmentação dos diferentes ambientes de rede disponibilizados pelo Conglomerado ou fornecedores por ele contratado aos seus colaboradores, fornecedores e clientes; e
k. Manutenção de cópias de segurança das informações.

6.3. Os controles mínimos listados no item 6.2 também devem ser aplicados no desenvolvimento de novos produtos, soluções, aplicativos, sistemas e ambientes, bem como na aquisição de novas tecnologias e serviços que integrarão as atividades operacionais do Conglomerado.

6.4. Da mesma forma, os controles mínimos listados no item 6.2 também devem ser adotados, conforme aplicável, por Fornecedores que processam ou armazenam dados pessoais e/ou informações sensíveis ou relevantes para a condução das atividades operacionais do Conglomerado, bem como, por Sociedades Investidas e por Clientes BaaS. Neste último caso, nas relações de tratamento de dados pessoais de maneira conjunta, conforme disposto no 1.2 desta política.

7. Gestão de Acessos

7.1. Os processos de concessão e revogação de acessos aos ativos de informação, sistemas de informação e/ou ambientes do Conglomerado são realizados pela área competente mediante aprovação formal do gestor do solicitante e do respectivo proprietário do perfil e/ou recurso.

7.2. São concedidos acessos para os colaboradores do Conglomerado e/ou de fornecedores somente às informações necessárias ao desempenho de suas funções e/ou determinação legal, seguindo as atribuições dos respectivos responsáveis.

7.3. São concedidos acessos privilegiados às informações, ativos de informações, sistemas e ambientes do Conglomerado aos seus colaboradores e/ou colaboradores de fornecedores mediante o cumprimento de regras específicas. Acessos privilegiados implicam em responsabilidades adicionais ao usuário.

7.4. As revogações de acesso devido ao desligamento de colaboradores devem ocorrer tempestivamente mediante comunicado de desligamento enviado à Superintendência de Segurança da Informação pela Área Pessoas e Cultura, no caso de colaborador do Conglomerado. No caso de colaborador de fornecedor, a comunicação deve ser feita com igual tempestividade, ao gestor do respectivo contrato.

7.5. Toda credencial de acesso ao ambiente, seja ele físico ou lógico, é única, individualmente identificada e atribuída a um proprietário, qualificando-o como responsável pelas ações realizadas por esta credencial, não podendo ser transferida ou compartilhada entre usuários ou terceiros.

7.6. Contas de serviço, destinadas usualmente à execução de processamentos automatizados, devem seguir a governança estabelecida pela Área Segurança da Informação, garantindo a rastreabilidade dos acessos, bem como, os vínculos a área responsável e o processo de revisão periódico.

7.7. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria identifiquem individualmente o usuário, para que ele possa ser responsabilizado por suas ações.

8. Gestão de Riscos em Segurança da Informação

8.1. O Conglomerado possui um processo estruturado de monitoramento, análise e identificação de vulnerabilidades, ameaças e

impactos sobre os ativos de informação, para que sejam identificados os controles adequados e a eficácia periodicamente testada.

8.2. O Conglomerado desenvolve, documenta, homologa e testa periodicamente planos de contingência, e os aprova para ativação no caso de previsão, suspeita ou ocorrência de situações que comprometam a integridade, a disponibilidade e a continuidade das atividades do Conglomerado.

8.3riscos e controles de Segurança da Informação e Continuidade de Negócios em. O Conglomerado deve manter um processo estruturado de avaliação de
Fornecedores, Investidas e em Clientes BaaS, quando aplicável, para identificação do nível de risco que deve ser endereçado para o seu devido tratamento pelos gestores responsáveis pelas contratações.

9. Gestão de Incidentes de Segurança da Informação

9.1. O Conglomerado adota procedimentos, requisitos e controles específicos para a prevenção e resposta a incidentes ocorridos. Os procedimentos, controles e requisitos para fornecedores devem estar alinhados com os próprios níveis de complexidade, abrangência e precisão do Conglomerado.

9.2. Para os fins desta política, o termo "incidente" significa qualquer ocorrência no acesso, no uso das informações ou Ativos de Informação que afete ou possa afetar a confidencialidade, disponibilidade, integridade, autenticidade das informações ou dos ativos de informação ou a privacidade dos titulares dos dados.

9.3. A classificação de relevância de incidente deve seguir o critério de impacto nos processos de negócios do Conglomerado mensurados por meio de análises qualitativas e/ou quantitativas, que avaliam potenciais impactos decorrentes da violação das diretrizes desta política, conforme previstos nas respectivas instruções normativas.

9.4. O tratamento de incidentes relevantes que se caracterize como crise deve ser acompanhado pela Área Governança de SI, Gestão de Crise e Continuidade de Negócios (se aplica a Continuidade de Negócios), seguindo política e instrução normativa própria para garantia da execução das ações e

todos os envolvimentos necessários.

9.5. Compete à Área Centro de Operações de Cyber security realizar o registro, análise de causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do Conglomerado.

9.6. Cenários de incidentes de segurança de informação são incluídos nos testes de continuidade de negócio do Conglomerado.

9.7. Todo incidente de segurança da informação no Conglomerado ou em fornecedores, investidas e Clientes BaaS, aplicáveis, que envolvam informações e ativos de informação do Conglomerado, deve ser formalmente reportado à Superintendência de Segurança da Informação.

9.8. O Conglomerado informará, em atenção ao arcabouço regulatório aplicável, ao Banco Central do Brasil e aos demais reguladores, todos os incidentes relevantes e interrupções de serviços relevantes, bem como as medidas tomadas para o reinício das atividades. Quando o incidente acarretar risco ou dano relevante à privacidade e proteção de dados do titular dos dados, conforme definição da Lei Geral de Proteção de Dados, o Encarregado dos Dados deve avaliar e, após análise, poderá comunicar à Autoridade Nacional de Proteção de Dados.

9.9 Sem prejuízo do dever de sigilo e da livre concorrência e por dever regulatório, o Conglomerado compartilhará as informações que possuir sobre incidentes relevantes de segurança de informação com demais instituições financeiras, incluindo informações sobre incidentes relevantes recebidas de empresas prestadoras de serviços a terceiros, por meio de canais estabelecidos para esse fim e sempre que tais informações forem para benefício e segurança do mercado financeiro.

10. Plano de Ação e Resposta a Incidentes

10.1. O Conglomerado possui um Plano de Ação e Resposta a Incidentes (PARI), que deve conter as ações a serem desenvolvidas para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta Política, e rotinas, procedimentos, controles e tecnologias que serão utilizadas na prevenção e na resposta de incidentes.

10.2. O Plano de Ação e Resposta a Incidentes deve ser revisto anualmente e aprovado pelo Conselho de Administração do Banco.

10.3. O Conglomerado elaborará anualmente um relatório contendo a efetividade das ações e um resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, previstas no Plano de Ação e Resposta a Incidentes, os incidentes

relevantes ocorridos no período, e os resultados dos testes de continuidade de negócios.

10.4. O relatório anual deve ser submetido ao Comitê de Controles e Riscos, ao Comitê de Riscos e de Capital e apresentado ao Conselho de Administração.

11. Conscientização em Segurança da Informação

11.1. A alta administração do Conglomerado, comprometida com a melhoria contínua do sistema de gestão de segurança de informação do Conglomerado, publica e assume seu compromisso em cumprir com as diretrizes elencadas nesta política.

11.2. Os papéis e responsabilidades quanto à segurança da informação são amplamente divulgados aos colaboradores e alta administração, que devem conhecer e cumprir essas diretrizes.

11.3. Como parte do seu compromisso, o Conglomerado adota ações e iniciativas para promover a capacitação, aculturamento e avaliação dos colaboradores sobre o tema segurança da informação, reforçando as diretrizes declaradas nesta política.

11.4. O Conglomerado também promove ações e iniciativas junto aos seus clientes com informações sobre precauções na utilização de seus produtos e serviços financeiros.

12. Divulgação desta Política

12.1. Um comunicado contendo uma versão resumida desta Política é divulgada aos colaboradores do Conglomerado e a sua versão completa fica disponível em local de fácil acesso para consulta.

12.2. Uma versão desta política é apresentada para os fornecedores do Conglomerado, contendo as diretrizes aplicáveis aqueles que prestarem serviços ou acessem informações, ativos de informação ou ambientes do Conglomerado, da mesma forma é apresentada às Investidas e aos Clientes BaaS com o nível de detalhamento compatível com o objeto do contrato, as funções desempenhadas ou sensibilidade das informações tratadas.

12.3. Um resumo com linhas gerais desta política é divulgado ao público geral, contendo linguagem clara e de fácil acesso.

13. Contratos

13.1. Os contratos entre o Conglomerado e empresas ou pessoas prestadoras de serviços, colaboradores, parceiros, contratados e estagiários, que tiverem acesso às informações, aos sistemas ou aos ambientes tecnológico corporativos devem conter cláusulas que garantam o devido tratamento de dados pessoais de acordo com as diretrizes da Lei Geral de Proteção de Dados e com as exigências do Termo de Tratamento de Dados Pessoais, bem como, a confidencialidade entre as partes, requisitos mínimos de segurança alinhados com os mesmos quesitos de segurança adotados pelo Conglomerado, e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a política e as instruções normativas de segurança da informação do Conglomerado.

13.2. Os contratos de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem estarão sujeitos a regime de contratação específico, obedecidos as disposições previstas pelas Áreas Segurança da Informação, Suprimentos e Jurídico Corporativo em observância ao arcabouço regulatório aplicável referente as diretrizes e requisitos de segurança e tecnologia da informação para terceiros.

14. Avaliação Independente

14.1. A efetividade desta política é verificada por meio de avaliações periódicas das áreas corporativas de controle, órgãos reguladores e auditorias interna e externa.

15. Medidas Disciplinares

15.1. As violações a esta política estão sujeitas a sanções disciplinares previstas nas instruções normativas internas do Conglomerado, na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas.

As diretrizes constantes nesta política são regulamentadas e operacionalizadas por meio de instruções normativas e procedimentos que definem regras e
processos para o correto cumprimento das políticas.