CAIXA Cartões

POLÍTICA DE GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO DA CAIXA CARTÕES HOLDING S.A.

1. Objetivo

1.1 Estabelecer diretrizes e responsabilidades para a gestão de riscos no Conglomerado, visando o estabelecimento de sua cultura, a efetividade dos seus sistemas e a manutenção da exposição por riscos em níveis aceitáveis, propiciando considerável segurança à consecução dos objetivos corporativos.

1.2 Estabelecer diretrizes para proteção e disciplina do uso dos ativos de informação da Companhia, ou sob sua custódia, visando oferecer segurança quanto à disponibilidade, à integridade, à confidencialidade e à autenticidade de tais ativos.

2. Motivação

2.1 Alinhamento à Lei nº 13.303, de 30/06/2016, ao Decreto no 8.945, de 27/12/2016 e a Resolução CGPAR nº 48, de 06/09/2023, quanto às diretrizes para o estabelecimento de Políticas relacionadas à Gestão de Riscos.

2.2 Alinhamento à Lei nº 12.527, de 18/11/201 1, à Lei no 13.709, de 14/08/2018, à Instrução Normativa GSI/PR nº 1, de 13/06/2008 e à Norma Complementar GSI/PR nº 03, de 30/06/2009, quanto às diretrizes para o estabelecimento de Políticas relacionadas à Segurança da Informação.

3. Vigência

3.1A presente política deverá ser revista em, no máximo, 05 anos, ou quando a unidade gestora identificar necessidade de aprimoramento, considerando o ambiente regulatório, o contexto macroeconômico, a necessidade estratégica, ou quando identificada necessidade de adequação a novos quesitos legais ou regulamentares ou ainda por solicitação do colegiado o qual aprovou a matéria.

4. Diretrizes

4.1 GESTÃO DE RISCOS

4.1.1 A Companhia

4.1.1.1 Reconhece que o gerenciamento de riscos é parte integrante de suas atividades, e que a gestão integrada, rigorosa e abrangente dos riscos dá sustentabilidade aos seus resultados, contribuindo para a geração de valor e para sua consolidação.

4.1.1.2 Avalia, previamente a sua implementação, os riscos e controles dos produtos, serviços, projetos e das estratégias, e implementa e analisa sua adequação aos níveis de risco aceitos.

4.1.1.3 Estabelece a metodologia de gerenciamento de riscos, como conjunto de atividades estabelecidas de forma ordenada para a operacionalização do gerenciamento dos riscos que ameaçam os seus objetivos.

4.1.1.4 Prima por decisões colegiadas, obedecendo alçadas estabelecidas, valendo-se do devido subsídio técnico, e respeitando as definições de sua Declaração de Apetite por Riscos.

4.1.1.5 Exige competência compatível com a função exercida por seus administradores, conselheiros, gestores, empregados, colaboradores e indicados, bem como fomenta a capacitação do seu corpo funcional para adequado gerenciamento dos riscos.

4.1.1.6 Segrega as atividades de gestão de riscos das atividades negociais e da auditoria interna, mantendo unidades independentes de desenvolvimento e de validação e monitoramento de seus modelos, sendo distinguidas de acordo com seu propósito, atendendo a ditames legais e aos seus interesses.

4.1.1.7 A segregação de funções é estabelecida, de modo a evitar o conflito de interesses na gestão da Companhia.

4.1.1.8 Garante que a sua gestão de riscos se baseia nos padrões de boas práticas e de governança, nos princípios gerais previstos em leis específicas e nas demais normas regulamentares.

4.1.1.9 Define seus objetivos com clareza suficiente para permitir o gerenciamento dos riscos a eles associados.

4.1.1.10 Adota o modelo de linhas de defesa para o gerenciamento de riscos, sendo os papéis e as responsabilidades das três linhas de defesa assim definidos:

4.1.1.11 A primeira linha de defesa é composta por todas as unidades da Companhia, exceto as componentes da 2a linha de defesa no exercício de sua atividade de supervisão, sendo responsabilidade dessas, a operacionalização da gestão de riscos, descrita pela metodologia de gerenciamento de riscos da Companhia, nos processos sob sua gestão.

4.1.1.12 O exercício da primeira linha de defesa é responsabilidade de todo empregado na realização das suas atividades.

4.1.1.13 A segunda linha de defesa compreende as áreas de gestão de riscos e de controles internos da Companhia, responsáveis por monitorar e contribuir com a implementação de práticas eficazes de gestão de riscos e controles internos.

4.1.1.14 A terceira linha de defesa é exercida pela auditoria interna, responsável por fornecer aos órgãos de governança a avaliação objetiva e independente quanto à eficácia da gestão de riscos e dos controles internos.

4.1.2 A gestão de riscos:

4.1.2.1 É processo transversal na Companhia, sendo parte integrante de todas as suas atividades.

4.1.2.2 Observa riscos e oportunidades nos processos da Companhia, mantendo estrutura que abrange todos os níveis de seus negócios, adequada à natureza e à complexidade de suas operações, e à dimensão de sua exposição a riscos.

4.1.2.3 É dinâmica, está em constante transformação e evolução, antecipa, detecta e reconhece alterações que podem ocorrer em virtude da mudança dos contextos externo e interno, e responde a essas alterações de maneira apropriada e oportuna.

4.1.2.4 É efetiva na busca do alcance dos propósitos e objetivos da Companhia, sendo realizada de maneira a alcançar os melhores resultados, com elevado padrão de qualidade e observação da relação custo-benefício.

4.1.2.5 Visa a melhoria contínua dos processos, é constantemente aprimorada por meio do aprendizado, de experiências e das melhores práticas de mercado.

4.1.2.6 Recebe e divulga, de forma adequada e oportuna, as informações pertinentes a sua atividade, proporcionando às partes interessadas o acompanhamento do desempenho e o gerenciamento dos riscos de forma a apoiar os negócios e subsidiar a tomada de decisão pela Administração.

4.1.2.7 A disseminação da cultura de riscos é prática adotada pela Administração, pelos conselheiros, gestores e empregados, favorecendo o adequado gerenciamento dos riscos dentro de seu escopo de atuação.

4.1.2.8 As decisões da Companhia são prudentes, baseiam-se em postura de comedimento, ponderando a suscetibilidade aos riscos dos seus negócios.

4.1.2.9 As informações de riscos são transparentes e se apresentam com clareza, permitindo seu correto entendimento e evitando dupla interpretação.

4.1.2.10 Administradores, conselheiros, empregados e indicados observam a presente política, visando assegurar solvência, liquidez e sustentabilidade à Companhia.

4.1.2.11 Unidade Responsável: SN Governança, Integridade e Riscos.

4.2 SEGURANÇA DA INFORMAÇÃO

4.2.1 A informação é:

4.2.1.1 Íntegra, completa, exata e preservada contra alterações, destruições, divulgações, cópias e impressões não autorizadas, acidentais ou intencionais.

4.2.1.2 Confidencial, podendo ser acessada ou conhecida somente por pessoas autorizadas e devidamente credenciadas.

4.2.1.3 Autêntica, proveniente de quem realmente diz ser e é fidedigna em relação à sua autoria, implicando no "não repúdio", ou seja, na incapacidade da negação da autoria da informação por seu autor.

4.2.2 A Companhia:

4.2.2.1 Preza pela disponibilidade da informação, sendo essa acessível, sempre que necessário, às pessoas autorizadas, e condizente com a necessidade do usuário para o desempenho de suas atribuições na Companhia.

4.2.2.2 Permite que os usuários tenham consciência quanto às suas responsabilidades na Segurança da Informação, inclusive em relação às práticas de "Mesa Limpa, Tela Limpa e Impressora Limpa".

4.2.2.3 Orienta que as informações e recursos disponibilizados são de uso exclusivo em atividades relacionadas aos seus objetivos.

4.2.2.4 Assegura a recuperação da informação, resguardando a continuidade dos seus negócios, por meio da realização periódica de backup das informações, permitindo sua pronta recuperação quando exigida.

4.2.2.5 Assegura que o acesso aos seus sistemas seja realizado com a utilização de senhas secretas, pessoais, intransferíveis e não compartilhadas, bem como, que o acesso seja concedido ao usuário por gestor responsável.

4.2.2.6 Classifica e segrega as informações de acordo com o seu grau de sigilo e confidencialidade, inclusive nos ambientes tecnológicos onde são tratadas, observados os critérios estabelecidos em norma específica.

4.2.2.7 Responsabiliza os usuários autorizados ao manuseio de informações próprias da Companhia ou advindas de contratos dessa com empresas externas.

4.2.2.8 Visa o estrito cumprimento da regulamentação e normatização correlata quanto ao correto endereçamento de mensagens, à cadeia de assinaturas, à classificação e à confidencialidade da comunicação.

4.2.2.9 Atende ao quesito de testes periódicos de segurança para os sistemas de informações e à finalidade, à adequação, à compatibilidade e ao tratamento dos dados, nos termos das normas vigentes.

4.2.2.10 Garante aos titulares o livre acesso aos dados, com consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

4.2.2.11 Garante aos titulares qualidade, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

4.2.2.12 Garante aos titulares a transparência dos dados, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial dispostos em legislação específica.

4.2.2.13 Preza pela segurança dos dados, com utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

4.2.2.14 Busca a proteção dos dados com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

4.2.2.15 Garante a não discriminação dos dados, impossibilitando a realização do tratamento para fins discriminatórios ilícitos ou abusivos.

4.2.2.16 Preza pela responsabilização e prestação de contas, pela adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

4.2.2.17 Trata dados pessoais sensíveis unicamente em conformidade às normas vigentes.

4.2.2.18 Utiliza para o tratamento de dados pessoais sistemas estruturados, de forma a atender aos requisitos de segurança, aos padrões de boas práticas de governança de dados e aos princípios gerais previstos em leis específicas e nas demais normas regulamentares.

4.2.3 A assinatura digital é prática incentivada em todos os processos da Companhia, como garantidor da autenticidade da informação.

4.2.4 Unidade Responsável: SN Governança, Integridade e Riscos.

5. Responsabilidades

5.1 É responsabilidade dos dirigentes, conselheiros e empregados de todas as Unidades da Companhia e do Conglomerado, quando couber, observar e aplicar as diretrizes desta política em seus processos e normas para a efetiva gestão das atividades no âmbito do Conglomerado.