Política de Gestão de Riscos e Contingência

I.Identificação:

Título	Política de Gestão de Riscos e Contingência
Objetivo	Este documento apresenta um conjunto de instruções e procedimentos para normalizar os riscos e as contingências, associados ao negócio e a segurança da informação
Estrutura	Segurança da Informação

II.Descrição da Política:

1. Objetivo

A presente Política de Gestão de Riscos e Contingência, tem como objetivo a estruturação dos procedimentos adotados pela Pagare, na gestão dos Riscos Operacionais relacionado à segurança da informação associada aos produtos e como contingencia-los.

A Política de Gestão de Riscos e Contingência, estabelece princípios, premissas, diretrizes, valores, responsabilidades, práticas, procedimentos, modelos e sistemas relacionados às atividades de Gerenciamento dos Riscos.

2. Aplicabilidade e Escopo da Política de Gestão de Riscos

Considerando a natureza das operações, a complexidade dos produtos, e a dimensão das exposições da Pagare, a Política de Gestão de Riscos visa estabelecer instrumentos e objetivos alinhados ao apetite de risco definidos pela instituição, sendo:

- Identificar, avaliar, monitorar e controlar a exposição relacionada ao Risco Operacional de Segurança da Informação, assegurando proteção contra as fontes de risco que resultem em exposição a perdas indesejáveis e que possam afetar a estratégia da PAGARE e até a sua viabilidade;
- Fornece ferramentas de Gerenciamento dos Riscos suficientes para propiciar à PAGARE capacidade de cumprir seus objetivos de negócio.
- Possuir um Plano de Contingência adequado que ofereça à PAGARE S a proteção apropriada contra a materialização dos eventos de risco, seja em termos de Risco Operacional, Risco de Crédito ou Risco de Mercado;
- Garantir que os processos e procedimentos relacionados ao Gerenciamento de Riscos da PAGARE atendam aos requerimentos regulatórios vigentes.

3. Responsabilidades

A estrutura de Gerenciamento de Riscos da Pagare é de responsabilidade pelo Gestor de Riscos no qual é o Gerente de Projeto.

O Comitê de Riscos é composto por:

- ✓ Gerente de Negócios

- ✓ Gerente de TI
- ✓ Gerente de Projeto

É de responsabilidade do Gestor de Riscos:

- Avaliar, monitorar e informar as posições de riscos, submetendo aos responsáveis quaisquer desvios ou extrapolação de limites estabelecidos;
- Gerenciar os riscos, por meio da análise dos pontos chaves de riscos e seus respectivos controles. O gerenciamento dos riscos e os resultados colhidos no acompanhamento merecerão avaliação de registros de ocorrência e da documentação inerente ao processo e à implementação de planos de ação.
- Acompanhar a implementação dos planos de ação e mitigadores, para os casos de extrapolação de limites;
- Atualização, com periodicidade máxima anual, das Políticas e Manuais de Procedimentos de Gestão de Riscos;
- Analisar as possíveis violações ou não conformidade com a documentação obrigatória dos procedimentos de controle de riscos e notificar casos de violação ou descumprimento ao Grupo do Comitê de Riscos, para adoção de medidas corretivas e outros;
- Assegurar a efetividade dos processos e procedimentos relacionados ao Gerenciamento de Riscos;
- Aplicar os cenários de estresse definidos para testes de estresse.
- Reportar ao Banco Central do Brasil (BACEN) e demais órgãos reguladores sempre que necessário, afim de mantê-los atualizados, além de definir sua estrutura de gerencimanto de risco operacional atendendo o Artigo 4º da Resolução CMN 3.380/06.

É responsabilidade do Comitê de Riscos:

- Estabelecer controles e procedimentos que suportem as atividades de gerenciamento relacionadas ao Risco Operacional e ao Risco de Mercado;
- Desenvolver os planos de ação e mitigadores, para os casos de extrapolação de limites;
- Avaliar o impacto de riscos para novos produtos;
- Realizar junto com as respectivas áreas a identificação e avaliação dos riscos e controles dos processos considerados relevantes;
- Disseminar a política de gerenciamento de risco aos colaboradores da instituição, em seus diversos níveis, estabelecendo papéis e responsabilidades, bem como as dos prestadores de serviços terceirizados.

- Definir as estratégias de atuação da Gestão de Riscos;
- Assegurar o cumprimento da Política de Gestão de Riscos da PAGARE, bem como o adequado funcionamento da estrutura de gerenciamento de Riscos, compatível com a natureza e a complexidade dos produtos, serviços, canais, atividades, processos e sistemas;
- Aprovar os planos de ação e mitigadores, para os casos de extrapolação de limites;
- Aprovar com periodicidade mínima anual, a Política de Gestão de Riscos da PAGARE;
- Garantir a implantação de planos de continuidade dos negócios para atividades críticas priorizadas para o desenvolvimento;
- Analisar, revisar e reformular as estratégias de exposição a risco;
- Avaliar os resultados de testes de estresse;
- Alterar ou rever possíveis novos cenários de testes de estresse;
- Definir planos de ação para situações de estresse real;
- Garantir ao Gestor de Riscos suporte estratégico em relação às suas funções e responsabilidades quanto à aprovação de diretrizes operacionais e políticas institucionais, bem como o estabelecimento de limites de exposição a riscos para a gestão efetiva de cada risco, no âmbito das atividades realizadas pela PAGARE.

O Comitê de Riscos poderá, a seu exclusivo critério, convidar para as reuniões outros profissionais internos e externos que possam contribuir de forma relevante às decisões.

O Gestor de Riscos participará das reuniões do Comitê para apresentar os painéis de gestão de riscos e esclarecimentos necessários.

O Comitê de Riscos deverá reunir-se semestralmente e, extraordinariamente, sempre que convocado por um de seus membros.

Os membros do Comitê de Riscos devem ser periodicamente providos de informações que reflitam o grau de exposição da instituição frente aos diversos fatores de risco a que a mesma está sujeita;

Adicionalmente, outras áreas e responsáveis suportam as atividades relacionadas ao Gerenciamento de Riscos, sendo elas:

- Auditoria Interna: Revisar e avaliar a eficácia, qualidade, suficiência e aplicação dos procedimentos e controles do monitoramento e Gerenciamento dos Riscos
- Tecnologia: Fornecer uma infraestrutura eficaz – de tecnologia e operações – e bem controlada para executar as atividades de Gerenciamento dos Riscos.

4. Definição de Risco

Risco é definido como o nível de incerteza em uma dada situação ligada a um ou mais eventos (por exemplo, fraude, roubo, contratos obscuros, default, sistemas ineficazes etc.) que poderia levar a perdas ou danos.

Baseado na natureza de tais eventos, o risco é classificado em categorias diferentes, tais como a liquidez, mercado, operacional, riscos legais, entre outros. A Pagare visa identificar, compreender, medir, controlar e mitigar esses riscos para avaliação e Gestão de Riscos eficientes.

5. Composição da Planilha de Riscos

Para consolidação das informações de riscos geradas, as mesmas devem ser definidas e controladas na Planilha de Riscos na qual é de responsabilidade do Gestor de Riscos organizar e verificar se os mesmos estão sendo atendidos.

A Planilha de Riscos é composta das seguintes considerações:

Elaboração:	Responsável pelo preenchimento e controle da planilha de Risco
Aprovador	Responsável pela avaliação final e aprovação de todos os riscos, monitoramentos e plano de ação (com prazos e recursos definidos)
Versão	Revisão do documento atual
Data da Elaboração	Data no qual a planilha foi elaborada / revisada
Validade do Risco	Prazo máximo para reavaliação do risco (prazo máximo de 180 dias)

ID Risco	O ID do risco deve seguir a seguinte regra de formação: · RC_99, sendo: · RC, sigla para Risco; · 99, sequencial numérico; Exemplo: RC_01
Processo	Estrutura na qual o risco está inserido (ex.: Cartão Frete, Segurança da informação, etc)
Item Relacionado	Item no qual o risco se relaciona (ex.: norma, lei, etc)
Descritivo do Item	Informativo do item no qual informa questões importantes no qual podem ser gerados / avaliados riscos
Item Crítico / Risco / Vulnerabilidade	Texto que descreve o risco

Tríade CID	**Confidencialidade**	Avaliar nesse item o quanto o vazamento de informações possa impactar o negócio. Critérios: Baixo = 1 Médio = 2 Alto = 3
	Integridade	Avaliar a garantia que se pode depositar na informação de que ela realmente é o que ela deveria ser. Critérios: Baixo = 1 Médio = 2 Alto = 3
	Disponibilidade	Avaliar se as informações são disponíveis quanto a sua continuidade. Critérios: Baixo = 1 Médio = 2 Alto = 3
Consequência ao Negócio		Somatório automático da Triade CID – Quanto maior o valor maior o risco associado
Proprietário		Nome do proprietário / responsável (negócio) do risco
Possível Causa		Informar que falha pode ser causado para que o risco possa ocorrer de fato
Possibilidade de Ocorrência		Probabilidade do risco acontecer. Critérios: Muito Baixo = 1 Baixo = 2 Médio = 3 Alto = 4 Muito Alto = 5
Impacto		Avaliação do grau de magnitude em caso do risco ocorrer. Critérios: Insignificante = 1 Baixo = 2

	Médio = 3 Alto = 4 Extremo = 5	
Risco Puro	Combinação da Possibilidade de Ocorrência x Impacto. Critérios: Baixo 1 – 3 Médio 4 – 7 Alto 8 – 14 Crítico 15 – 19 Extremo 20 – 25 Quanto maior o valor maior a magnitude do problema.	
Controle e Monitoramento envolvido	Informação sobre como a PAGARE deve controlar e monitorar seus riscos de forma a que os mesmos não ocorram. Informar necessidade de plano de contingência para o item, caso haja.	
Não detectabilidade de Incidente	Informar nesse item o critério do quão o risco possa ser fácil de identificar Critérios: Muito Alto = 1 - Facilmente detectável Alto = 2 - Relativamente fácil de detectar Médio = 3 - Detectável com algum esforço Baixo = 4 - Dificilmente detectável Muito Baixo = 5 - Muito difícil de detector	
Risco Detectado	Combinação do risco puro x não detectabilidade de Incidente Quanto maior o valor, maior a necessidade de controle e possíveis contingências.	
	Ação	Ação a ser dada no caso de um risco não estar consolidadamente tratado / controlado.
	Responsável	Responsável pela ação

Plano de Ação	**Prazo**	Prazo no qual a ação será resolvida / tratada
	Recursos	Recursos humanos financeiros e/ou tecnológicos envolvidos para sanar o problema
	Situação Final analisada	Situação da ação: Em processo – ação está em andamento Satisfatório – processo fechado e adequado com controles testados e monitorados. Pendente – Ainda não iniciada
Comentários	Informações complementares sobre o risco e tratamento associado	

6. Plano de Contingência

A PAGARE possui Política de Contingência adequada que oferece a proteção apropriada contra a materialização dos eventos de risco.

Adicionalmente, na ocorrência de extrapolação de quaisquer limites de exposição aos riscos ou evidências de que os limites serão extrapolados, o Comitê de Riscos poderá, em conjunto com o responsável pela Gestão dos Riscos, reunir-se para reavaliar o tipo de crise, severidade e ações prudenciais a serem adotadas a fim de assegurar o reenquadramento dos limites.

III.Aprovadores da Política:

Aprovador	Data
Gerente de Negócios	22/09/2023
Gerente de Projeto	22/09/2023
Gerente Administrativo e Comercial	22/09/2023
Gerente de TI	22/09/2023