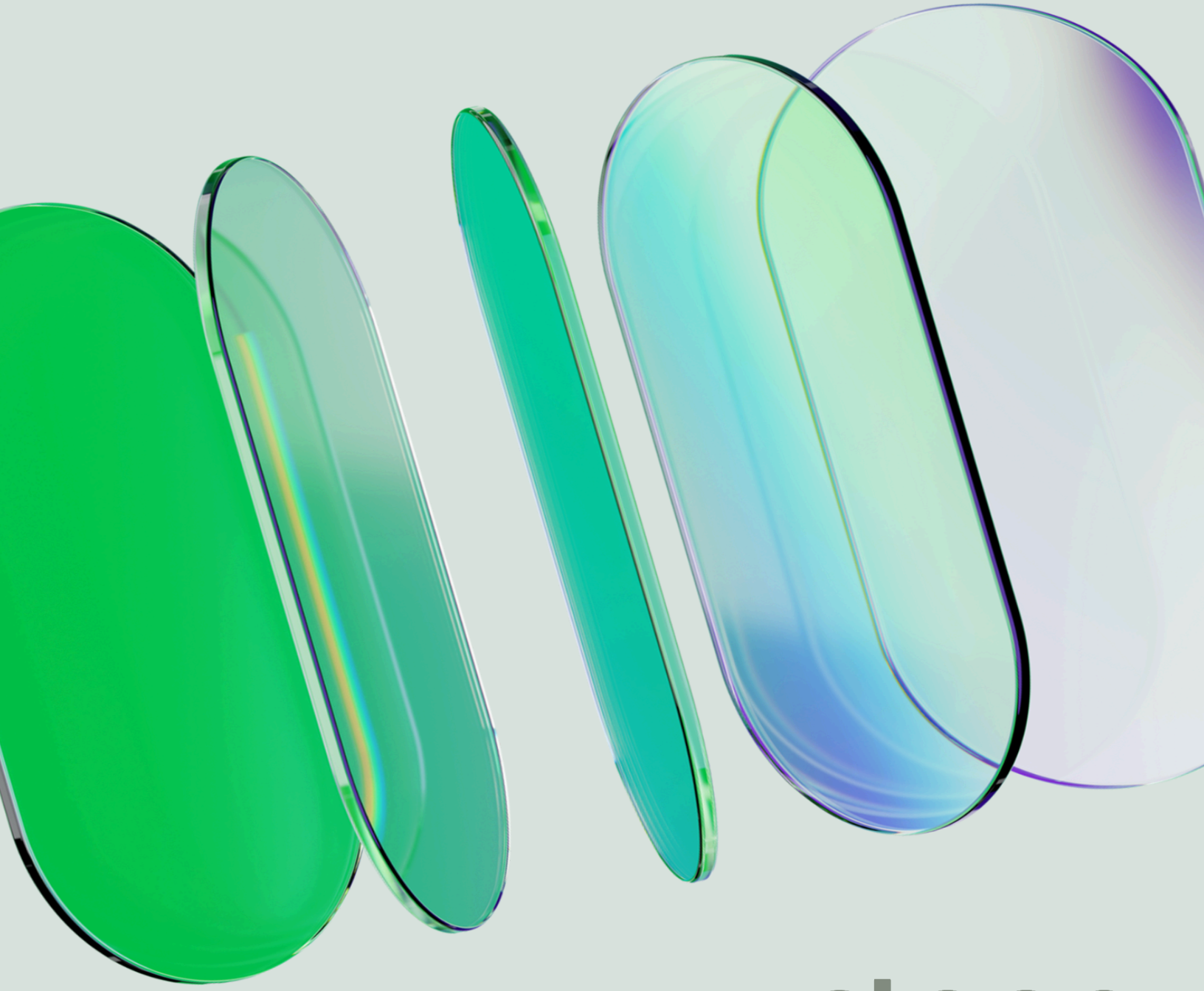

stone

Gerenciamento de Riscos – Pilar 3

4º Trimestre de 2023

ÍNDICE

1. OBJETIVO

O presente relatório apresenta as informações do Conglomerado Prudencial da Stone requeridas pelo Banco Central do Brasil (BACEN) conforme obrigações da Resolução BCB nº 54 que dispõe sobre a divulgação do Relatório de Pilar 3.

2. TABELA OVA: Visão geral do gerenciamento de riscos da instituição

2.1. A interação entre o modelo de negócios e o perfil de riscos da instituição

A Stone é uma provedora líder de tecnologia financeira e solução de software e seu propósito é servir o empreendedor brasileiro transformando seus sonhos em realidade.

Dessa forma, o processo de gerenciamento de riscos é estratégico, dada a crescente complexidade dos produtos e serviços e o ambiente em que a Companhia está inserida. Para garantir uma abordagem eficaz da estrutura organizacional de gerenciamento de riscos, a Companhia baseia suas práticas em diretrizes sólidas, em conformidade com as regulamentações aplicáveis e melhores práticas.

A Companhia possui a Diretoria de Gestão de Riscos, unidade específica segregada das unidades de negócio e da unidade executora da atividade de auditoria interna, responsável pela atividade de gerenciamento de riscos e de capital..

Nesse contexto, a Companhia possui a Norma de Gestão de Riscos e Capital para a Diretoria, que estabelece a governança a ser observada no gerenciamento de riscos e de capital, definindo estruturas e órgãos e suas respectivas atribuições. A governança é estabelecida de modo a atender aos requisitos regulatórios aplicáveis à Companhia e a buscar eficiência na gestão de riscos e capital.

As atividades da Diretoria de Gestão de Riscos permitem a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos efeitos adversos resultantes das interações entre os riscos financeiros, operacionais, sociais, ambientais, climáticos, entre outros. São adotados processos para rastreamento e reporte tempestivo de

exceções às políticas de gerenciamento de riscos, aos limites e aos níveis de apetite por riscos fixados na RAS (Risk Appetite Statement).

Os tipos de risco e estruturas de gerenciamento podem ser assim resumidos:

2.1.1 Risco de Crédito

O Risco de Crédito é a possibilidade de ocorrência de perdas associadas ao: (i) não cumprimento pela contraparte de suas obrigações nos termos pactuados; (ii) desvalorização, redução de remunerações e ganhos esperados em instrumento financeiro decorrentes da deterioração da qualidade creditícia da contraparte, do interveniente ou do instrumento mitigador; (iii) reestruturação de instrumentos financeiros; ou (iv) custos de recuperação de exposições caracterizadas como ativos problemáticos.

No contexto operacional da Stone, o Risco de Crédito corresponde à possibilidade de inadimplência dos clientes tomadores de recursos, dos bancos emissores de cartões, subcredenciadores e estabelecimentos comerciais. A Companhia dispõe de mecanismos para o monitoramento e mitigação do Risco de Crédito para cada contraparte relacionada, realizando gestão ativa do portfólio nas visões de safra e carteira, bem como realizando monitoramento periódico da exposição junto aos emissores e subcredenciadores, além de estabelecer limites de crédito para cada estabelecimento comercial.

2.1.2 Risco de Liquidez

Risco de Liquidez é o risco de a Companhia não ser capaz de honrar suas obrigações esperadas e inesperadas, correntes e futuras sem afetar suas operações diárias e/ou sem incorrer em perdas significativas. Além disso, engloba ainda a possibilidade da instituição não conseguir negociar a preço de mercado uma posição devido ao seu tamanho elevado em

relação ao volume normalmente transacionado ou em razão de alguma descontinuidade de mercado. Constitui, ainda, o risco de não ser capaz de converter moeda eletrônica em moeda física ou escritural no momento da solicitação do usuário. A Companhia realiza o gerenciamento de Risco de Liquidez por meio de política interna, que inclui cenários de estresse.

2.1.3 Risco de Mercado

Risco de Mercado é a possibilidade de ocorrência de perdas financeiras resultantes da flutuação nos valores de mercado de instrumentos detidos pela Companhia, e inclui o risco de taxa de juros, que é relacionado com a possibilidade de perda financeira resultantes de oscilação das taxas de juros de mercado, e o risco cambial, que é relacionado com a possibilidade de perdas financeiras resultantes de flutuação da taxa de câmbio. A Companhia realiza o gerenciamento de Risco de Mercado por meio de política interna. A política abrange processos da Companhia que resultam em exposição ao Risco de Mercado e define métricas e procedimentos para gerenciamento do risco de taxa de juros e do risco cambial.

2.1.4 Risco Operacional

O Risco Operacional é definido como a possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas, incluindo o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, às sanções em razão de descumprimento de dispositivos legais e às indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição. Entre os eventos de Risco Operacional da Companhia, incluem-se: (i) fraudes internas; (ii) fraudes externas; (iii) demandas trabalhistas e segurança deficiente do local de trabalho; (iv) práticas inadequadas relativas a usuários finais, clientes, produtos e serviços; (v) danos a

ativos físicos próprios ou em uso pela instituição; (vi) situações que acarretem a interrupção das atividades da instituição ou a descontinuidade dos serviços prestados, incluindo o de pagamentos; (vii) falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI); (viii) falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da instituição, incluindo aquelas relacionadas aos arranjos de pagamento.

A área de Risco Operacional, que inclui Controles Internos tem como objetivo assegurar a existência e eficácia do ambiente de controle nas áreas de negócios e tecnologia da informação, por meio de programas de monitoramento e testes de controles internos. Além disso, são realizados procedimentos específicos relacionados à segurança da informação e continuidade de negócios, com avaliações dos processos críticos da Companhia.

2.1.5 Segurança da Informação

Os principais riscos relacionados à segurança da informação estão associados à: (i) indisponibilidade da infraestrutura e (ii) o vazamento de dados sensíveis, incluindo credenciais de acesso de colaboradores e/ou clientes e informações relacionadas às transações de cartões de crédito.

A Stone emprega as melhores práticas de Segurança da Informação (abrangendo pessoas, processos e tecnologias) e percebe a segurança como um pilar estratégico para a continuidade de sua operação.

A Stone possui certificações de Segurança Internacionais que evidenciam o compromisso da companhia com o tema - ex.: PCI DSS (Payment Card Industry Data Security Standard)e ISO 27001.

2.1.6 Gestão da Continuidade de Negócios

A Companhia reconhece como risco relevante a indisponibilidade de processos críticos, que podem impactar a operação do nosso cliente e acarretar em impactos financeiros, reputacionais e regulatórios.

Por meio do Programa de Continuidade, a Stone analisa o impacto nos negócios ao identificar e classificar os processos críticos, além de avaliar os potenciais efeitos de suas interrupções. Em caso de indisponibilidade de recursos - tecnológicos, operacionais ou de fornecedores relevantes - essenciais para a execução das atividades-chave, a Companhia conta com políticas, planos, procedimentos, contingências sistêmicas e tecnológicas que têm por objetivo garantir a continuidade de negócios para responder e minimizar impactos que possam ocorrer tanto internamente na operação, quanto externamente em clientes e parceiros. Por fim, os planos de continuidade de negócios estabelecem procedimentos e prazos para reinício e recuperação das atividades, incluindo a comunicação necessária, e são regularmente testados e revisados.

2.1.7 Prevenção a Fraudes

A fraude é associada a práticas enganosas, ilegais ou desonestas com o intuito de obter vantagens financeiras indevidas. Os eventos na Stone associados ao tema são: (i) fraudes internas; (ii) fraudes externas.

O processo de prevenção a fraudes engloba medidas, estratégias e sistemas desenvolvidos e implementados com o objetivo de prevenir, detectar ou minimizar atividades fraudulentas.

Por meio de nossos processos e atividades de controles e monitoramentos contínuos, nossa missão principal é minimizar perdas financeiras provenientes de fraudes para a Companhia, assim como garantir que nossos clientes estejam cumprindo com as regras do mercado de pagamentos, de acordo com o estipulado pelas Bandeiras e pelo Banco Central do Brasil.

2.1.8 Riscos Social, Ambiental e Climático

A Stone considera os Riscos Social, Ambiental e Climático como parte integrante de sua gestão de riscos. Esses riscos estão relacionados a eventos que podem resultar em perdas relacionadas a condução dos negócios, atividades e processos da companhia:

- **Risco Social**: Relaciona-se à possibilidade de perdas decorrentes de violações de direitos fundamentais ou atos prejudiciais ao interesse comum.
- **Risco Ambiental**: Refere-se à possibilidade de perdas causadas por eventos relacionados à degradação do meio ambiente, incluindo o uso excessivo de recursos naturais.
- **Risco Climático**: Envolve a possibilidade de perdas devido a eventos associados ao processo de transição para uma economia de baixo carbono e à possibilidade de ocorrência de perdas ocasionadas por eventos associados a intempéries frequentes e severas ou alterações ambientais de longo prazo, que possam ser relacionadas a mudanças em padrões climáticos.

Para gerir esses riscos, a Stone adota sistemas, rotinas e procedimentos que têm como objetivo identificar, avaliar, mensurar, monitorar e mitigar seus efeitos. Periodicamente, avaliamos o impacto e a probabilidade dos riscos, bem como a mensuração das perdas e prejuízos decorrentes.

Ademais, buscamos tomar decisões conscientes e responsáveis em nossa cadeia de valor, equilibrando oportunidades de negócios com responsabilidade social, ambiental e climática, contribuindo para o desenvolvimento das regiões que atuamos.

Além dos riscos citados, a área de gestão de riscos é responsável pelas potenciais perdas decorrentes das interações entre eles, e pela gestão do capital regulatório.

2.2. Declaração de apetite por riscos - RAS

O apetite a riscos refere-se aos tipos e níveis de riscos que a Organização se dispõe a admitir na realização dos seus negócios e objetivos. A Companhia possui a Declaração de Apetite por Riscos (RAS), que abrange: (i) os níveis de riscos que a instituição está disposta a assumir, discriminados por tipo de risco e, quando aplicável, por diferentes horizontes de tempo; (ii) a capacidade de a instituição gerenciar riscos de forma efetiva e prudente; (iii) os objetivos estratégicos da instituição; e (iv) as condições de competitividade e o ambiente regulatório em que a instituição atua.

A RAS estabelece limites claros e definidos para os diferentes tipos de riscos que a Stone pode enfrentar. Esses limites são integrados à estrutura de gerenciamento de riscos.

Cabe à Diretoria aprovação e revisão com frequência mínima anual da RAS.

A Stone monitora o apetite de riscos e seus respectivos limites com frequência estabelecida para cada tipo de indicador conforme criticidade e ocorrência de eventos. O monitoramento resulta no nível de utilização do limite, o qual, por sua vez, determinará quais ações de governança serão executadas.

2.3. Governança do gerenciamento de riscos

A Companhia adota a estratégia de linhas integradas:

(i) O primeiro nível das linhas integradas é implementado pela função de negócios que executa as atividades operacionais. Estes são responsáveis por assegurar um ambiente de controle adequado, implementar políticas de gerenciamento de riscos em seus papéis e responsabilidades, estar cientes dos fatores de risco que devem ser considerados em cada decisão e ação, e devem ser capazes de executar controles internos eficazes, bem como o processo de monitoramento e a manutenção da transparência no controle interno em si;

(ii) A segunda linha é executada pela Diretoria de Gerenciamento de Riscos e pela área de Compliance. Estas são responsáveis pelo desenvolvimento do gerenciamento de riscos e pelo processo de monitoramento; Além disso, elas são incumbidas de garantir que todas as funções de negócios sejam implementadas de acordo com as políticas de gerenciamento de riscos e procedimentos operacionais padrão estabelecidos pela Companhia;

(iii) A terceira linha é ocupada por auditores internos e externos. As responsabilidades destes são: revisar e avaliar o desenho e a implementação do gerenciamento de riscos de forma abrangente, bem como assegurar a eficácia do primeiro e segundo nível de defesa.
Os papéis e responsabilidades conjuntas e individuais dos órgãos, instâncias, áreas e funções das estruturas de gerenciamento de riscos e de capital estão dispostas a seguir.

DIRETORIA

Compete à Diretoria, para fins do gerenciamento de riscos e do gerenciamento de capital:

A. Fixar os níveis de apetite por riscos da instituição na RAS e revisá-los, com o auxílio do comitê de riscos e do CRO;
B. Aprovar e revisar procedimentos, políticas e outros documentos relevantes para o gerenciamento de riscos e de capital na Stone;
C. Assegurar a aderência da instituição às políticas, às estratégias e aos limites de gerenciamento de riscos;
D. Assegurar a correção tempestiva das deficiências da estrutura de gerenciamento de riscos e da estrutura de gerenciamento de capital;
E. Aprovar alterações significativas nas políticas e nas estratégias da instituição, bem como em seus sistemas, rotinas e procedimentos;

F. Autorizar, quando necessário, exceções às políticas, aos procedimentos, aos limites e aos níveis de apetite por riscos fixados na RAS;
G. Promover a disseminação da cultura de gerenciamento de riscos na instituição;
H. Assegurar recursos adequados e suficientes para o exercício das atividades de gerenciamento de riscos e de gerenciamento de capital, de forma independente, objetiva e efetiva;
I. Estabelecer a organização e as atribuições do comitê de riscos, observado o disposto nesta Resolução;
J. Garantir que a estrutura remuneratória adotada pela instituição não incentive comportamentos incompatíveis com os níveis de apetite por riscos fixados na RAS;
K. Assegurar que a instituição mantenha níveis adequados e suficientes de capital e de liquidez.

COMITÊ INTERNO DE RISCOS

O Comitê Interno de Riscos é órgão de assessoramento da Diretoria para assuntos relacionados ao gerenciamento de riscos e de capital, fazendo recomendações para a Diretoria ou deliberando acerca de tais assuntos quando tal competência lhe for delegada pela Diretoria.

DIRETORIA DE GESTÃO DE RISCOS

A atividade de gerenciamento de riscos é executada pela Diretoria de Gestão de Riscos, unidade específica na instituição, segregada das unidades de negócios e da unidade executora da atividade de auditoria interna, e possui quantidade suficiente de profissionais experientes e qualificados em gerenciamento de riscos, que por sua vez: (i) possuem conhecimento do mercado e dos produtos e serviços da instituição, (ii) têm acesso regular a

capacitação e treinamento; (ii) são capazes de questionar os riscos assumidos nas operações realizadas pelas unidades de negócios; e (iv) compreendem as limitações e as incertezas relacionadas às metodologias utilizadas na estrutura de gerenciamento de riscos.

A Diretoria de Gestão de Riscos desempenha um papel fundamental ao assegurar a conformidade dos gerenciamentos de riscos e de capital com a legislação aplicável. Sua responsabilidade abrange a garantia da continuidade das operações mesmo em cenários extremos, além de otimizar a alocação de capital de maneira transparente.

Dentre as diversas responsabilidades da Diretoria de Gestão de Riscos, destacam-se: (i) a definição de níveis aceitáveis de riscos; (ii) a identificação, mensuração e mitigação dos diversos tipos de riscos, levando em consideração interações e regulamentações específicas; (iii) desenvolvimento de políticas relacionadas à gestão de continuidade de negócios, gestão de crises e implementação de sistemas de controles internos; e (iv) manter processos e controles relativos à apuração do montante RWA, pelo cálculo dos requerimentos mínimos de PR, de Nível I e de Capital Principal e pelo cumprimento do Adicional de Capital Principal.

DIRETOR DE GESTÃO DE RISCOS / CRO (Chief Risk Officer)

As atribuições do CRO abrangem:

A. Supervisão do desenvolvimento, da implementação e do desempenho da estrutura de gerenciamento de riscos, incluindo seu aperfeiçoamento;
B. Responsabilidade pela adequação, à RAS e aos objetivos estratégicos da instituição, das políticas, dos processos, dos relatórios, dos sistemas e dos modelos utilizados no gerenciamento de riscos;
C. Responsabilidade pela adequada capacitação dos integrantes da Diretoria de Gestão de Riscos acerca das políticas, dos processos, dos relatórios, dos sistemas e dos

modelos da estrutura de gerenciamento de riscos, mesmo que desenvolvidos por terceiros;

D. Subsídio e participação no processo de tomada de decisões estratégicas relacionadas ao gerenciamento de riscos e, quando aplicável, ao gerenciamento de capital, auxiliando a diretoria.

AUDITORIA INTERNA

A Auditoria Interna possui o objetivo de avaliar periodicamente os processos relativos ao gerenciamento de riscos e de capital da Companhia.

2.4. Processos de mensuração, reporte e mitigação de riscos

A governança do processo de gerenciamento de riscos é definida por metodologia, parâmetros para classificação de riscos, alçadas para aprovação de planos de ação e assunção de riscos, e prazos para execução de planos de ação. A fim de obter consistência corporativa, a Companhia adota as mesmas classificações de riscos e governança de respostas para a Auditoria Interna, Compliance e Riscos.

De acordo com a metodologia estabelecida, as três etapas fundamentais para a gestão de riscos corporativos são:

1. Identificação de riscos: consiste em identificar os riscos inerentes às atividades da Companhia, considerando o modelo e estratégia dos negócios, produtos e serviços.
2. Classificação de riscos: consiste em quantificar e classificar os riscos identificados de acordo com frameworks internacionalmente reconhecidos. Isso é realizado considerando variáveis e critérios que estabelecem, para cada risco, intervalos de impacto e probabilidade:

- Impacto: pode abranger diversas esferas, incluindo aspectos financeiros, relacionamento com os clientes, reputação da Companhia e conformidade regulatória.
- Probabilidade: abarca tanto a probabilidade quanto a frequência de ocorrência.

3. Respostas aos riscos: após a identificação e classificação dos riscos, a fase de resposta aos riscos consiste em orientar a tomada de decisão para cada um dentre as opções viáveis, incluindo:
    - Assunção de riscos: decisão de incorrer no risco de acordo com o apetite;
    - Definição de planos de ação: não aceitação do risco e definição de ação para mitigar o risco conforme prazos estabelecidos pela metodologia da Companhia;
4. Respostas a incidentes: definição de planos de ação para riscos materializados.

GLOSSÁRIO

- BCB - Banco Central do Brasil
- CRO - Chief Risk Officer
- PR - Patrimônio de Referência
- RAS - Risk Appetite Statement
- RWA - Risk Weighted Assets (Ativos Ponderados pelo Risco)
- TI - Tecnologia da Informação
- VaR - Value at Risk (perda máxima dado horizonte de tempo e intervalo de confiança)