desenvolvido internamente, apurando o RSAC das operações as quais abrange em três níveis: Alto, Médio e Baixo. O gerenciamento de RSAC está estruturado e documentado em Norma de Procedimento interna, a qual determina a validade e periodicidade das avaliações, bem como apresenta as rotinas e procedimentos de gestão do risco.

f) Risco Cibernético

A Segurança da Informação e Comunicações (SIC) é um conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, sejam elas físicas ou digitais, contra diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar eventuais danos, maximizar o retorno dos investimentos e de novas oportunidades de negócio.

A Segurança Cibernética está contida dentro do âmbito da SIC e se configura como um conjunto de tecnologias, processos e práticas projetado para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado, permitindo o uso e o compartilhamento da informação digital de forma controlada. Sendo assim, a SIC é de maior abrangência, protegendo tecnologias, pessoas, informações físicas, entre outros, enquanto a Segurança Cibernética visa proteger somente ativos relacionados ao universo digital.

Nessa perspectiva, risco cibernético é o risco que se refere aos potenciais resultados negativos associados aos ataques cibernéticos. Por sua vez, os ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, a integridade e a disponibilidade de dados ou sistemas tecnológicos.

No Banco, a estrutura de Gerenciamento de Riscos cibernéticos atende ao previsto na Resolução CMN nº 4.893/2021 e se aplica a toda a Instituição, dispondo de:

- Política de segurança da informação e cibernética que tem por objetivo estabelecer o Sistema de Gestão da Segurança da Informação (SGSI) do Banco da Amazônia, considerando uma visão holística e coordenada dos riscos de SIC do Banco para definir e comunicar princípios, valores, conceitos, diretrizes, controles suficientes à preservação e proteção das informações do Banco da Amazônia e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade, em todo o seu ciclo de vida, contida em qualquer suporte ou formato.
- Normas de procedimentos de segurança da informação que apoiam a estratégia definida na Política.
- Planos de resposta a incidentes de cibersegurança.
- Comitê de Segurança Corporativa, da Informação e de Comunicações: de caráter consultivo e deliberativo, tem por finalidade participar do processo de gestão Segurança Corporativa, inclusive de Informação e de Comunicações do Banco.

A governança no Gerenciamento de Riscos cibernético adota também a abordagem das três linhas. Em que:

- A primeira linha, representada pelas áreas de tecnologia, pessoas e contratos, é responsável por identificar, avaliar, reportar e gerenciar os riscos cibernéticos em ativos de tecnologia, recursos humanos e cadeia de suprimento, respectivamente, e pela execução dos controles e mitigadores de riscos, e, ainda, pela definição e implementação de planos de ação para garantir a efetividade do ambiente de controle;
- Na segunda linha, a área responsável pelo Gerenciamento de Risco Cibernético define a estratégia e as políticas de segurança, bem como realiza o monitoramento dos riscos, a gestão de incidentes e é responsável pelo aculturamento da empresa acerca da segurança da informação. Ainda como parte da segunda linha, a área responsável pela gestão de continuidade de negócio, tema afeto à segurança da informação, é a área de controles internos responsável por definir as diretrizes e procedimentos inerentes a gestão de continuidade de negócios estabelecendo o processo para análise de impacto nos negócios, estratégias para assegurar a continuidade das atividades da instituição e limitar perdas decorrentes da interrupção dos processos críticos de negócio;
- A terceira linha é representada pela Auditoria Interna.

g) Risco Operacional

O Banco segue as diretrizes da Resolução CMN nº 4.557/2017, integrando a gestão do risco operacional à sua estrutura e a todos os níveis hierárquicos. Utiliza normas de procedimento com detalhamento de papéis e responsabilidades da Instituição conforme modelo das três linhas.

Realiza monitoramento contínuo dos eventos relacionados ao risco operacional, mantendo uma base histórica quantitativa e qualitativa de informações, reportando regularmente à Alta Administração. Ressalta-se, ainda, a promoção da cultura voltada à gestão de riscos e controles, com o objetivo de alcançar metas estratégicas e fortalecer a governança corporativa.

h) Risco Legal

Em conformidade com as determinações do Banco Central do Brasil e de demais órgãos reguladores, o Banco da Amazônia assegura a observância das legislações, normas e regulamentos aplicáveis às instituições financeiras.

A área de Controles Internos monitora, de forma sistemática, a publicação de normativos externos e acompanha o cumprimento das obrigações regulatórias pertinentes. Para isso, a Instituição utiliza um Sistema de Compliance que disponibiliza informações atualizadas sobre normas aplicáveis às atividades bancárias, assegurando o alinhamento das áreas envolvidas às diretrizes regulatórias e a aderência às exigências legais.

i) Risco de Integridade

O Banco mantém políticas, programas e instrumentos de integridade, com destaque para o Código de Conduta Ética, o Programa de Integridade e o Plano de Integridade, que orientam e monitoram a atuação institucional de forma preventiva e contínua.

Esses instrumentos estabelecem diretrizes de conduta, responsabilidades e padrões éticos, promovendo uniformidade de procedimentos e reduzindo a possibilidade de discricionariedade indevida. O Programa de Integridade, em especial, traduz essas diretrizes em práticas, contemplando ações de prevenção, detecção e resposta a desvios, além de fortalecer a cultura de ética e conformidade em todos os níveis da organização.

De forma integrada, esse conjunto reduz a exposição a fraudes, corrupção e desvios de conduta, fortalece os controles internos e reforça a confiança das partes interessadas na atuação ética, transparente e responsável da Instituição.

j) Gestão de Capital

O processo de gestão de capital adotado pelo Banco é estruturado de forma coerente com a complexidade operacional e os riscos assumidos pela Instituição, visando assegurar qualidade, consistência e transparência do capital, além de cumprir integralmente os requisitos regulatórios estabelecidos pela Resolução CMN nº 4.557/2017. Essa estrutura abrange áreas responsáveis pelo orçamento, planejamento estratégico, controle e monitoramento de riscos, além dos colegiados estratégicos de tomada de decisão.

A Instituição mantém um Plano de Capital que projeta o capital necessário para um horizonte de três anos, incluindo testes de estresse e um plano de contingência para garantir a gestão adequada do capital, alinhada ao apetite de risco definido na Declaração de Apetite por Riscos (RAS).

A adequação de capital é gerenciada considerando não apenas as exigências regulatórias, mas também uma meta interna declarada na RAS, superior aos limites mínimos estabelecidos para o Patrimônio de Referência (PR). O Plano de Capital é elaborado de maneira integrada ao Planejamento Estratégico, refletindo os objetivos institucionais e atendendo plenamente às determinações da Resolução CMN nº 4.557/2017.