Introdução:

A Política de Segurança Cibernética e de Informação tem como principal objetivo garantir a: disponibilidade, integridade e confidencialidade das informações geradas e armazenadas pelo BKB. O BKB está comprometido com as diretrizes de segurança cibernética e com os elementos básicos da gestão de risco cibernético, dentre os quais se aplicam:

1. Classificação da Informação

O BKB classifica as informações de acordo com seu grau de confidencialidade e conforme regulamentação do Banco Central do Brasil (BACEN). Todas as informações são administradas de modo a preservar a integridade, confiabilidade, segurança e sigilo das transações realizadas, bem como a legitimidade das operações contratadas e dos serviços prestados.

2. Gestão de Acessos

O BKB controla os acessos lógicos e físicos através de inserção de login e senha, ou por identificação biométrica. Os acessos são liberados de acordo com o perfil e rotinas dos colaboradores.

3. Ambientes Lógicos

Os ambientes de acesso lógico que suportam as operações do BKB são confiáveis, íntegros e seguros. O BKB possui sistemas de proteção contra programas maliciosos e acessos indevidos.

4. Proteção de Dados Pessoais

O BKB possui controles para garantir a disponibilidade, integridade e confidencialidade, através de adoção de medidas de segurança que visam proteger dados pessoais contra acessos não autorizados, perda ou alteração indevida. Os dados são armazenamento de modo seguro, de forma a garantir a confidencialidade dos dados pessoais de seus colaboradores, clientes e parceiros de negócios.

5. Backup e Monitoramento

O BKB realiza cópia de segurança (back-up) de seus dados e os armazena em ambientes seguros, de forma a garantir a continuidade do negócio em caso de falhas ou incidentes do ambiente produtivo ou contingencial. O BKB possui monitoramento dos ambientes físicos e lógicos para garantir a eficácia dos controles implantados.

6. Auditoria

O BKB possui auditorias internas e externa sobre os processos e sistemas de TI, cuja finalidade é identificar possíveis vulnerabilidades e/ou oportunidades de melhoria de acordo com a legislação vigente.

7. Plano de Ação e Resposta a Incidentes

O BKB possui um Plano de Ação e Resposta a Incidentes, dividido em fases de acordo com sua categorização, que considerem seu nível de criticidade e possíveis impactos negativos para a instituição, visando assim assegurar que quaisquer incidentes e/ou potenciais incidentes sejam

tratados de forma efetiva, garantindo o adequado registro, análise e escalonamento em tempo hábil.

8. Contratos com Terceiros e Prestadores de Serviços

O BKB possui processo de análise prévia de risco cibernético na contratação de serviços de terceiros e todos os contratos devem prever cláusulas de obrigatoriedade de reporte de incidentes de Segurança Cibernética, que envolvam dados de propriedade ou estejam sob a responsabilidade do BKB.

A Política de Segurança Cibernética do BKB menciona diretrizes na contratação de terceiros que versam quanto à proteção de ambientes físicos, monitoramento de ambientes lógicos, gestão de riscos, vulnerabilidades em segurança cibernética e continuidade de negócio.

9. Desenvolvimento, Manutenção e Aquisição de Sistemas

O desenvolvimento de sistemas de uso interno ou externo, bem como sua aquisição, devem seguir os requisitos de segurança cibernética descritos na Política de Segurança Cibernética.

10. Treinamento

O departamento de TI em conjunto com o departamento de Riscos e *Compliance* promovem a disseminação da cultura de gestão de riscos cibernéticos junto aos Colaboradores e Prestadores de Serviço relevantes. Tais treinamentos versam sobre prevenção, identificação e reporte de incidentes. Além disso, os Colaboradores e Prestadores de Serviços são orientados sobre como proceder caso seja acionado um plano de contingência que possa afetar a continuidade dos serviços.

11. Canal de Comunicação

Denúncias, dúvidas, sugestões ou incidentes relacionados à Segurança Cibernética do BKB, constatadas por terceiros (público em geral), podem ser comunicadas aos Canais de Atendimento disponibilizados no *site* da instituição na internet.

12. Revisão Periódica

A Política de Segurança Cibernética é revisada anualmente pela diretoria e aprovada pelo Comitê de Risco e *Compliance* com periodicidade mínima anual ou sempre que houver mudança significativa nos procedimentos de gestão, no mercado de atuação ou no perfil de negócios da instituição.

Revisão realizada em **20/08/2025**