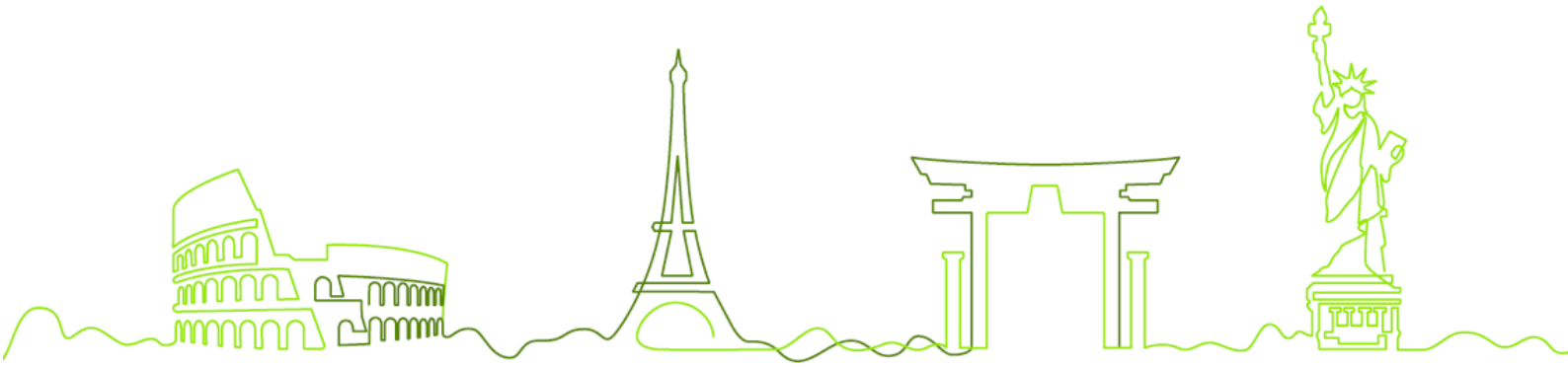

Política de Cibersegurança

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	31 mai 2025	Cibersegurança / Tec. Informação	Versão Original

Sumário

1. Objetivo

Estabelecer diretrizes, controles e responsabilidades para garantir a segurança cibernética no âmbito do "Intex Bank". O objetivo é assegurar a confidencialidade, integridade, disponibilidade e privacidade das informações.

2. Escopo

Esta política se aplica a todos os funcionários, prestadores de serviço, parceiros, fornecedores e quaisquer terceiros que tenham acesso às informações e aos sistemas de tecnologia do "Intex Bank". Aplica-se também a todas as instalações físicas, plataformas digitais, ativos de informação, redes e sistemas sob controle da instituição.

A Política de Cibersegurança do "Intex Bank" estabelece diretrizes para proteção da informação, gestão de riscos cibernéticos e conformidade regulatória. Está alinhada às normas do Banco Central do Brasil, incluindo as Resoluções BCB nº 85/2021 e 139/2021, CMN nº 4.893/2021 e 5.088/2023, além da Circular nº 3.909/2018, que tratam da estrutura de segurança, gestão de incidentes e continuidade de negócios.

A política adota como base técnica o NIST Cybersecurity Framework e os padrões internacionais ISO/IEC 27001, 27002 e 27701, além da norma PCI DSS para ambientes com dados de cartões. Também atende à LGPD (Lei nº 13.709/2018), com foco na proteção de dados pessoais, e à Lei nº 9.613/1998, com controles voltados à prevenção à lavagem de dinheiro e financiamento do terrorismo, conforme exigências do COAF.

3. Estrutura de Governança e Responsabilidades

A governança da cibersegurança no "Intex Bank" é composta por estruturas e papéis bem definidos. Uma área de Cibersegurança é formalmente instituído, atuando com papel deliberativo e consultivo responsável pela definição estratégica da segurança cibernética. Além disso, a instituição designa um Responsável pela Cibersegurança que atua com independência funcional, conforme a Resolução CMN 4.893/2021. Esse responsável garante o alinhamento entre os riscos cibernéticos e a governança corporativa, promovendo a integração das práticas de segurança ao modelo de gestão de riscos da organização.

4. Gestão de Riscos Cibernéticos

A gestão de riscos cibernéticos do "Intex Bank" segue metodologia formal baseada na Resolução BCB nº 85/2021, abrangendo as etapas de identificação, avaliação, tratamento e

monitoramento contínuo dos riscos. Os ativos da informação são classificados conforme seu grau de criticidade, e são considerados os impactos potenciais de incidentes de segurança sobre os serviços e operações. O processo de gestão de riscos cibernéticos segue as mesmas diretrizes previstas na Política de Gestão de Riscos do "Intex Bank", mantendo alinhamento entre os riscos operacionais, estratégicos e tecnológicos.

5. Controle de Acesso e Segurança dos Sistemas

Os controles de acesso aos sistemas e ativos digitais são implementados com base no princípio do privilégio mínimo e na segregação de funções. Para os sistemas críticos, são utilizados mecanismos de autenticação forte, como autenticação multifator (MFA), a fim de mitigar riscos de acessos indevidos. Todos os acessos são rigorosamente monitorados e registrados, permitindo rastreabilidade e auditoria contínua conforme as melhores práticas de segurança da informação.

As senhas no nível do sistema e no nível do usuário devem seguir a Política de Controle de Acesso. É proibido dar acesso a outro indivíduo, deliberadamente ou devido a falha na proteção de um aparelho.

6. Monitoramento Contínuo e Resposta a Incidentes

O "Intex Bank" conta com infraestrutura dedicada para o monitoramento contínuo de seus ativos e redes, por meio de soluções como SOC (Security Operations Center) e SIEM (Security Information and Event Management). A detecção precoce de incidentes e a resposta eficaz são componentes fundamentais da estratégia de cibersegurança. Todos os incidentes são registrados e, quando aplicável, comunicados às autoridades regulatórias em conformidade com a Circular Bacen nº 3.909/2018. Testes e simulações periódicas são conduzidos para avaliar a maturidade da capacidade de resposta e garantir a eficácia dos procedimentos estabelecidos.

7. Privacidade e Proteção de Dados

A proteção de dados pessoais é tratada com prioridade, conforme estabelecido na Lei Geral de Proteção de Dados (Lei nº 13.709/2018). O "Intex Bank" designa formalmente um Encarregado pelo Tratamento de Dados Pessoais (DPO), responsável por atuar como canal de comunicação com os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Medidas técnicas e administrativas são implementadas para garantir os direitos dos titulares, incluindo controles de acesso, anonimização, políticas de retenção e treinamento

contínuo dos colaboradores. As práticas adotadas seguem diretrizes da Política de Privacidade e da Política de Segurança da Informação.

8. Segurança no Tratamento de Dados de Cartão (PCI DSS)

A conformidade com os requisitos da norma PCI DSS é essencial para o tratamento de dados de cartão de pagamento. O "Intex Bank" adota controles específicos para garantir a segregação dos ambientes de dados de cartão, aplicando criptografia forte para proteger dados sensíveis tanto em trânsito quanto em repouso. Além disso, há exigências rigorosas para prestadores de serviços terceirizados, os quais devem cumprir com os requisitos aplicáveis da norma, sendo periodicamente avaliados. As diretrizes completas encontram-se na Política PCI-DSS.

9. Conformidade com PLD/FT

O "Intex Bank" mantém um programa robusto de prevenção à lavagem de dinheiro e ao financiamento do terrorismo (PLD/FT), em conformidade com a Lei nº 9.613/1998 e os normativos emitidos pelo COAF. O programa inclui procedimentos rigorosos de identificação e verificação de clientes (KYC), avaliações de risco, monitoramento de transações suspeitas e reporte tempestivo às autoridades competentes. A conscientização dos colaboradores sobre práticas de PLD/FT é promovida regularmente por meio de treinamentos específicos.

10. Capacitação, Conscientização e Cultura de Segurança

O "Intex Bank" mantém um programa contínuo de conscientização e capacitação em cibersegurança, visando fortalecer a cultura organizacional voltada à segurança da informação. As ações incluem campanhas educativas, treinamentos obrigatórios, simulações de ataques cibernéticos, como phishing e engenharia social, e avaliações periódicas de conhecimento.

Este programa é essencial para garantir que todos os colaboradores compreendam seus papéis e responsabilidades na proteção dos ativos da instituição.

11. Gestão de Terceiros e Fornecedores

A segurança da informação no relacionamento com terceiros é assegurada por meio de processos de due diligence e avaliação de riscos, alinhados à norma ISO/IEC 27036. Todos os contratos firmados incluem cláusulas específicas relacionadas à segurança da

informação e à proteção de dados.

Os fornecedores e prestadores de serviços são monitorados continuamente, podendo ser submetidos a auditorias para verificação da conformidade com os requisitos estabelecidos pelo “Intex Bank”. As diretrizes completas encontram-se na Política de Gestão de Terceiros.

12. Resiliência Operacional e Continuidade de Negócios

Para garantir a continuidade das operações e a recuperação rápida diante de incidentes cibernéticos ou desastres, o “Intex Bank” mantém planos atualizados de continuidade de negócios e recuperação de desastres. Esses planos são testados regularmente e incluem estratégias como redundância de sistemas, backups automatizados, comunicação de crise e definições claras de responsabilidades.

A resiliência cibernética é tratada como prioridade estratégica e os critérios, responsabilidades e métodos encontram-se descritos no Plano de Continuidade de Negócios e Recuperação de Desastres, bem como na Política e Procedimento de Backup e Restore.

13. Disposições Finais

A responsabilidade pela condução da revisão é da área de Cibersegurança, com apoio do Encarregado pelo Tratamento de Dados Pessoais (DPO) e do responsável pela área de Riscos. Toda revisão será aprovada e homologada pelo Comitê Diretivo.

14. Exceções

Exceções a esta política devem ser formalmente submetidas à área de Cibersegurança para avaliação e aprovação, garantindo que cada caso seja devidamente documentado e justificado.

Em casos de dúvidas, comentários ou necessidade de exceções, entre em contato pelo e-mail ciberseguranca@intexbank.com.br.

15. Violações e Não Cumprimento da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente à área de Cibersegurança e ao Diretor de Tecnologia para as providências cabíveis. Violações poderão resultar em sanções administrativas, incluindo a perda de privilégios de acesso a sistemas e redes, bem como medidas disciplinares conforme os procedimentos internos do “Intex Bank” que podem incluir rescisão de contratos ou

parcerias.

16. Vigência

Esta política entra em vigor na data de sua publicação, sendo revisada no prazo de 18 (dezoito) meses, ou a qualquer momento, conforme a necessidade.

São Paulo, 05 de junho de 2025

O presente documento foi aprovado pelo Comitê Diretivo conforme Ata de Reunião realizada em 05/06/2025.

Intex Bank Banco de Câmbio S/A