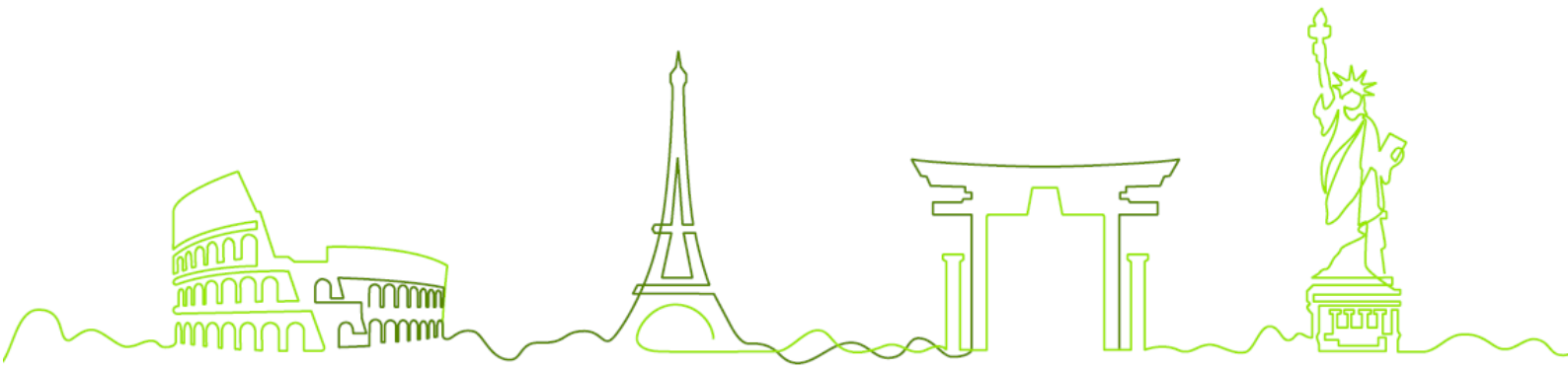

Resumo da Política de Segurança Cibernética

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	06/2026	Cibersegurança / Tecnologia da Informação	Versão Original

Público:
Este documento contém informações que podem ser compartilhadas internamente ou fora do INTEX BANK BANCO DE CÂMBIO S/A, com baixo risco ou até mesmo sem risco de imagem para a instituição, sob a condição de não haver alterações em seu conteúdo original.

Sumário

1. Introdução

O “Intex Bank” desenvolveu políticas e procedimentos de segurança cibernética para o controle, o processamento, o armazenamento, a transferência e a comunicação de informação de forma segura.

Este documento fornece as linhas gerais da Política de Segurança Cibernética do “Intex Bank” para cumprir a exigência regulatória da Resolução 4.893/2021, divulgada pelo Banco Central do Brasil.

2. Objetivo

As descrições e procedimentos descritos neste resumo aplicam-se ao “Intex Bank”. Para manter a confidencialidade, a integridade e a disponibilidade das informações da instituição, todos os colaboradores e terceiros contratados (doravante referidos como "usuários"), devem respeitar a Política de Segurança Cibernética e quaisquer processos e diretrizes relacionadas.

3. Política e Procedimentos

A Política de Segurança Cibernética descreve o programa de segurança cibernética do “Intex Bank” e os procedimentos de apoio relacionados. A segurança cibernética é tratada pelo “Intex Bank” como elemento essencial à gestão dos negócios, contribuindo para a proteção de clientes, parceiros e demais partes interessadas, e está fundamentada nos princípios de confidencialidade, integridade, disponibilidade e conformidade com a legislação e a regulamentação aplicáveis.

4. Resumo Geral da Diretrizes de Segurança Cibernética

A Política de Segurança Cibernética do “Intex Bank” está estruturada em pilares complementares que, em conjunto, asseguram a proteção do ambiente tecnológico e das informações sob custódia da instituição, em conformidade com a Resolução CMN nº 4.893/2021 e demais exigências regulatórias e legais aplicáveis.

4.1. Governança e Gestão de Riscos

O “Intex Bank” mantém uma estrutura de governança de segurança cibernética com definição clara de responsabilidades e supervisão da alta administração. A

instituição realiza gestão contínua dos riscos cibernéticos, considerando fatores tecnológicos, operacionais, humanos, terceiros e relacionados a ativos virtuais.

4.2. Controle de Acesso e Identidade

O gerenciamento de identidade e acesso assegura que os acessos aos sistemas e informações sejam provisionados de forma controlada, revisados periodicamente e revogados quando necessário, observando os princípios de menor privilégio e segregação de funções.

4.3. Proteção de Dados e Criptografia

O “Intex Bank” adota mecanismos de proteção da informação para assegurar a confidencialidade, integridade e autenticidade dos dados, tanto em armazenamento quanto em transmissão.

4.4. Monitoramento e Resposta a Incidentes

A instituição realiza monitoramento contínuo do ambiente tecnológico e mantém processos formais para identificação, registro, análise e tratamento de incidentes de segurança cibernética.

4.5. Gestão de Vulnerabilidades

São conduzidas atividades regulares de identificação e tratamento de vulnerabilidades, com o objetivo de reduzir riscos e fortalecer a postura de segurança da instituição.

4.6. Continuidade de Negócios e Resiliência

O “Intex Bank” mantém planos e processos voltados à continuidade de suas operações e à recuperação em caso de incidentes ou indisponibilidades relevantes.

4.7. Gestão de Terceiros

O gerenciamento de terceiros e serviços em nuvem estende o compromisso com a segurança para além do perímetro institucional, verificando que prestadores de serviços e parceiros implementem controles compatíveis com os do “Intex Bank”, em observância aos requisitos regulatórios aplicáveis à contratação de serviços de

processamento, armazenamento de dados e computação em nuvem.

4.8. Segurança em Ativos Virtuais

O “Intex Bank” adota práticas de segurança voltadas às operações com ativos virtuais, incluindo avaliação de riscos, controles operacionais e proteção dos ativos e das transações.

4.9. Proteção contra Vazamento de Dados

São implementadas medidas para prevenir e mitigar o risco de vazamento ou uso indevido de informações sensíveis.

4.10. Capacitação e Conscientização

A instituição promove ações contínuas de conscientização e treinamento em segurança da informação, visando fortalecer a cultura de segurança entre colaboradores e terceiros.

5. Governança e Responsabilidades

- **Diretoria:** Responsável pela aprovação da Política de Segurança Cibernética e pela definição do apetite ao risco cibernético da instituição, além de ser responsável por assegurar os recursos necessários à implementação e supervisionar a execução do Programa de Segurança Cibernética.
- **Diretor de Tecnologia da Informação:** Responsável pelo Programa de Segurança Cibernética em toda a instituição e pela interlocução formal perante o Banco Central do Brasil, nos termos do art. 5º da Resolução CMN nº 4.893/2021, na condição de Diretor Responsável pela Segurança Cibernética (DRSC).
- **Encarregado pelo Tratamento de Dados Pessoais (DPO):** Responsável pela interlocução com a Autoridade Nacional de Proteção de Dados (ANPD) e titulares, nos termos da Lei nº 13.709/2018.
- **Áreas de Negócio:** Responsáveis pelo gerenciamento dos riscos associados ao uso de tecnologia e pelo cumprimento dos requisitos das políticas e procedimentos de Segurança Cibernética.

6. Aderência e Controles

O não cumprimento da Política de Segurança Cibernética poderá resultar em ações disciplinares, e as exceções podem ser analisadas e concedidas conforme políticas e procedimentos internos.

7. Observações Gerais

A Política de Segurança Cibernética é revisada, no mínimo, anualmente, ou sempre que houver evento relevante, considerando a evolução do ambiente tecnológico, das ameaças cibernéticas e das exigências regulatórias, se aplicando também a este "Resumo".

São Paulo, 01 de junho de 2026.

O presente documento foi aprovado pelo Comitê Diretivo conforme Ata de Reunião realizada em 01/06/2026.