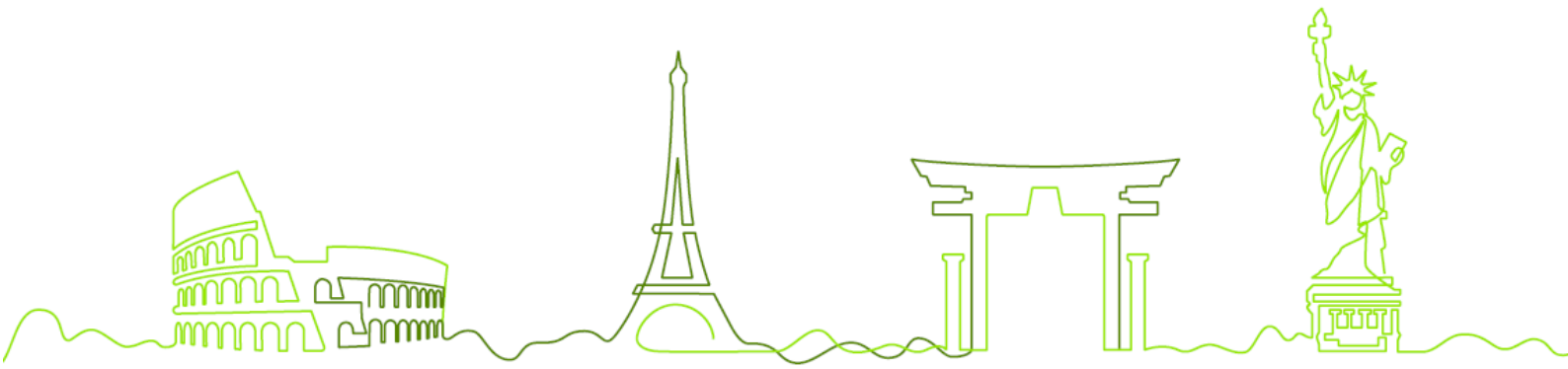

Política de Criptografia

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	30 nov 2024	Cibersegurança	Versão Original

Sumário

1. Objetivo

Esta política visa definir as diretrizes para o uso adequado e seguro de criptografia, estabelecendo medidas de proteção à confidencialidade, integridade e autenticidade das informações sensíveis processadas, armazenadas e transmitidas pelo Intex Bank Banco de Câmbio S/A (doravante denominado "Intex Bank"). Para tanto, este documento estabelece os requisitos mínimos para a aplicação de métodos criptográficos seguros e a gestão de chaves ao longo de todo o ciclo de vida da criptografia. O cumprimento dessas diretrizes objetiva reduzir riscos relacionados à exposição de dados e ao acesso não autorizado, assegurando que o "Intex Bank" atenda às normas regulatórias e melhores práticas de segurança da informação.

2. Escopo

Esta política aplica-se a todos os sistemas e processos do "Intex Bank" que envolvem dados confidenciais, incluindo armazenamento, processamento e transmissão de informações sensíveis, tanto em ambientes internos quanto externos. Ela abrange colaboradores, prestadores de serviço e parceiros, assegurando que todas as partes atendam aos requisitos de segurança criptográfica e proteção de dados definidos pela organização.

Esta Política está em conformidade com os requisitos estabelecidos pelas **Resoluções CMN nº 4.893/2021**, **nº 5.088/2023**, **Resoluções BCB nº 85/2021** e **nº 139/2021**, bem como pela **Circular nº 3.909/2018**, que tratam da segurança cibernética, gestão de riscos operacionais e proteção de dados em instituições reguladas pelo Banco Central do Brasil. Adicionalmente, observa as boas práticas do **NIST Cybersecurity Framework (CSF)**, os controles da norma **ISO/IEC 27001:2022** e suas extensões **27002** e **27701**, bem como os requisitos técnicos do **PCI DSS** para proteção de dados de titulares de cartão (CHD). Também atende à **Lei nº 13.709/2018 (LGPD)** e à **Lei nº 9.613/1998**, no que se refere à proteção contra fraudes e à prevenção à lavagem de dinheiro (PLD).

3. Política

A política de criptografia do "Intex Bank" define diretrizes essenciais para garantir a proteção de dados sensíveis, alinhando-se às melhores práticas do setor e atendendo às exigências regulatórias e de conformidade. A organização adota uma abordagem robusta de segurança que abrange o armazenamento e a transmissão de dados, incluindo o uso de algoritmos avançados, como AES para dados em repouso e TLS para dados em trânsito, sempre com cifras recomendadas pelo setor. Essa proteção se estende também aos

serviços ofertados e às APIs, onde o uso de mTLS (Mutual TLS) e RSA assegura a integridade e a confidencialidade das informações trafegadas no barramento de dados e em integrações com sistemas externos

A gestão de chaves criptográficas é rigorosamente controlada, com procedimentos documentados para geração, rotação e descarte seguro de chaves, conforme diretrizes do **NIST SP 80057**. Esse controle minucioso reduz o risco de vulnerabilidades e acessos não autorizados, fortalecendo a segurança de toda a infraestrutura de dados do “Intex Bank”. A documentação detalhada de todos os processos e procedimentos relacionados à criptografia é mantida e revisada regularmente para garantir conformidade com atualizações do setor e para responder rapidamente a novas ameaças.

Adicionalmente, o “Intex Bank” realiza auditorias internas periódicas e revisões anuais das cifras, assegurando que as práticas de segurança acompanhem as evoluções tecnológicas e regulamentares. Esse compromisso é reforçado por treinamentos contínuos para conscientização dos colaboradores sobre a importância da criptografia e das práticas de segurança, consolidando uma cultura de proteção de dados e conformidade que permeia todas as áreas da organização. Dessa forma, esta política não apenas protege dados confidenciais
e serviços críticos, mas também fortalece a confiança de clientes e parceiros na segurança das operações da empresa.

4. Protocolos Criptográficos

Os conjuntos de cifras criptográficas e os protocolos em uso devem ser formalmente documentados e revisados pelo menos uma vez a cada 12 meses e devem incluir pelo menos:

a) Um inventário atualizado de todos os conjuntos de cifras criptográficas e protocolos em uso, incluindo a finalidade e onde usado.

b) Monitoramento ativo das tendências do setor em relação à viabilidade contínua de todos os conjuntos e protocolos de cifras criptográficas em uso. Como padrão de mercado, recomenda-se consultar regularmente o sítio eletrônico do NIST, filtrando por publicações especiais "SP" na série "800".

c) A política de gestão de vulnerabilidades deve contemplar respostas à mudanças identificadas em vulnerabilidades atreladas à criptografia.

5. Gerenciamento de Chaves Criptográficas

O gerenciamento de chaves criptográficas deve seguir rigorosos controles de acesso, em alinhamento com a ***Política de Controle de Acesso*** do "Intex Bank", para assegurar que somente indivíduos autorizados possam acessar chaves e segredos. As chaves devem ser gerenciadas durante todo o seu ciclo de vida, incluindo geração, distribuição, armazenamento, rotação e descarte seguro, para minimizar riscos de comprometimento.

A tabela a seguir especifica os usos mandatórios para chaves criptográficas em diferentes contextos:

Domínio	Tipo de Chave	Algorítimo	Comprimento da Chave	Vigência
Certificado Web	RSA ou ECC com assinatura SHA2+	RSA ou ECC com assinatura SHA2+	2048 bits ou superior RSA, 256 bits ou superior (ECC	Até 1 ano
Cifra da Web (TLS)	Criptografia Assimétrica	Cifras de grau B ou superior na classificação SSL Labs	Varia	N/A
Barramento / API interna	RSA + mTLS	RSA + mTLS	Determinado pelo padrão da API	N/A
Dados confidenciais armazenados / Cardholder Data (CHD)	Criptografia Simétrica	AES	256 bits	1 ano
Senhas	Hash unidirecional	Bcrypt, PBKDF2, scrypt, Argon2	256 bits+10K Stretch (com salt+pepper)	N/A
Armazenamento de endpoint (SSD/ HDD)	Criptografia Simétrica	AES	128 ou 256 bits	N/A
Banco de Dados	Conexão SSL/TLS	RSA com assinatura SHA256	RSA: 2048 bits (mínimo recomendado pelo OpenSSL)	1 ano (renovação recomendada para certificados SSL/TLS)

Tabela 1 - Aplicações e requisitos para uso de chaves criptográficas. Fonte: O autor.

As chaves de criptografia padrão de sistemas operacionais, software de segurança, aplicativos, terminais POS, SNMP, sistemas de proteção de dados e sistemas de autenticação devem ser alteradas ou excluídas após a instalação.

As chaves de criptografia devem ser substituídas sempre que alguém com conhecimento ou acesso a elas deixar a empresa, mudar de cargo ou se houver comprometimento de sua integridade. Isso inclui chaves utilizadas em pontos de acesso, certificados, autenticação, proteção de dados confidenciais e outras chaves de criptografia estática, quando aplicável.

O acesso às chaves de criptografia deve ser restrito ao menor número possível de responsáveis.

Caso seja necessário utilizar criptografia de CHD (Cardholder Data) com chaves estáticas, as chaves secretas/privadas devem ser protegidas conforme os requisitos desta política. Essas chaves devem ser armazenadas e gerenciadas utilizando uma chave de criptografia com força criptográfica igual ou superior à da chave empregada para criptografar os dados, garantindo segurança e controle adequados.

As chaves criptográficas devem ser armazenadas em segurança e no menor número possível de locais, não podendo ser exportadas ou guardadas fora dos sistemas aprovados sem autorização explícita da gerência.

Se forem armazenados ou transmitidos CHD, devem ser empregadas exclusivamente chaves fortes, de acordo com esta política, para proteger os dados nesses processos. Durante a transmissão, as chaves devem ser protegidas com criptografia forte. Quando usadas na proteção de CHD (em trânsito ou em repouso), as chaves devem ser armazenadas com segurança, exclusivamente no cofre de senhas aprovado pela área de segurança da informação.

As chaves com fim de vida útil, utilizadas na proteção de CHD, devem ser substituídas ou retiradas de circulação. Chaves criptográficas desativadas ou substituídas só podem ser usadas para fins de descriptografia ou validação e não para operações de criptografia.

Se o PAN (Primary Account Number) for transmitido por redes públicas abertas (como a Internet), os certificados devem atender aos seguintes requisitos:

a) Somente chaves e certificados confiáveis devem ser aceitos;
b) Os certificados usados para proteger o PAN durante a transmissão em redes públicas abertas são confirmados como válidos e não estão vencidos nem foram revogados;
c) O protocolo em uso aceita apenas versões ou configurações seguras e não aceita o fallback nem o uso de versões, algoritmos, tamanhos de chave ou implementações inseguras;

d) A força da criptografia é apropriada à metodologia da criptografia em uso e segue as normas criptográficas;

e) Além disso, todas as chaves e certificados usados para proteger o PAN durante a transmissão em redes internas e externas devem ser inventariados e armazenados;

Valem os seguintes requisitos ao usar a gestão manual das chaves de texto não criptografado:

a) As chaves manuais de texto não criptografado exigem o controle duplo e o conhecimento dividido; nenhum indivíduo pode ter acesso às chaves secretas/privadas usadas para proteger o CHD, se armazenados, seja em repouso ou em trânsito;

b) Todas as alterações nas chaves devem seguir um processo formal e autorizado de rotação das chaves, e os indivíduos não podem alterar ou trocar uma chave secreta/privada sem autorização explícita da equipe de engenharia de TI;

c) Todos os custodiantes de cada chave criptográfica devem reconhecer formalmente (por escrito ou eletronicamente) que estão cientes e aceitam a responsabilidade de custodiante das chaves pelo menos anualmente; e

d) Ao compartilhar as chaves criptográficas com os clientes para transmissão ou armazenamento de dados da conta, as orientações sobre transmissão, armazenamento e atualização seguros dessas chaves devem ser documentadas e distribuídas aos clientes.

6. Exceções

Exceções a esta política devem ser formalmente submetidas ao Diretor de Tecnologia da Informação (CTO) e ao Encarregado de Proteção de Dados (DPO) para avaliação e aprovação, garantindo que cada caso seja devidamente documentado e justificado. Qualquer necessidade de mover, copiar ou armazenar dados confidenciais do cliente ou da empresa em dispositivos portáteis, mídias removíveis ou ambientes externos, incluindo integrações com serviços de terceiros, requer aprovação prévia. Todos os dispositivos e mídias que armazenam esses dados devem adotar criptografia em conformidade com os padrões de segurança estabelecidos pelo “Intex Bank”, mitigando riscos e assegurando a proteção das informações em todos os contextos de negócios.

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

7. Violações e Não Cumprimentos da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente ao Diretor de Tecnologia da Informação e Encarregado de Proteção de Dados 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. Esta política reflete o compromisso do "Intex Bank" com a segurança das informações e com o cumprimento de requisitos regulatórios, buscando a manutenção de um ambiente seguro e confiável para os negócios e relações com terceiros.

8. 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.