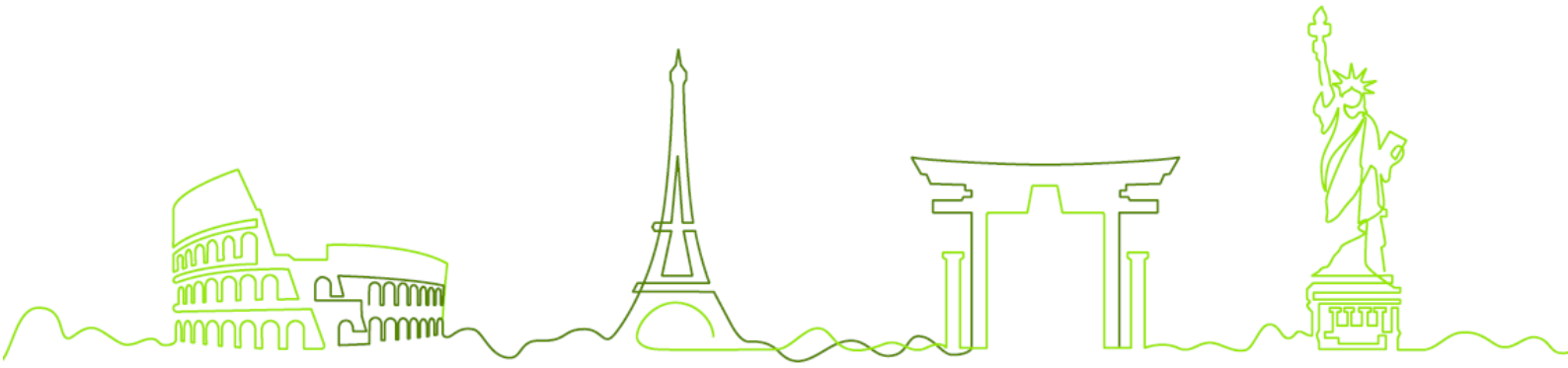

Política de Gestão, Classificação e Proteção de Dados

Intex Bank Banco de Câmbio S/A

PO07.09_08.2026

Controle de Versões

Versão	Data	Área Responsável	Motivo
1ª	02/2025	Cibersegurança	Versão Original
2ª	08/2026	Cibersegurança	Atualização

Mudanças ocorridas na atualização de 08/2026
Alterado o prazo de vigência para revisão da política para 12 (doze) meses, ao invés de 18 (dezoito) meses. Inseridas referências à Política de Privacidade. Alterado o nome da política de “Política de Gestão, Classificação e Proteção da Informação” para “Política de Gestão, Classificação e Proteção de Dados”. Adesão dos tópicos - 7 a 11 e 15.

Sumário

1. Objetivo

A presente Política estabelece as diretrizes, procedimentos e responsabilidades para assegurar que os dados e informações gerenciados pelo Intex Bank Banco de Câmbio S/A (doravante denominado “Intex Bank”) sejam corretamente classificados, protegidos, coletados, processados, analisados, armazenados e descartados, conforme seu valor estratégico e os requisitos de segurança aplicáveis.

Esta Política visa garantir que a proteção dos dados esteja alinhada com as melhores práticas de governança, conformidade regulatória e gestão de risco, atendendo aos seguintes objetivos:

- Estabelecer procedimentos padronizados para classificação, coleta, processamento e análise de informações e dados;
- Garantir qualidade, precisão e integridade dos dados coletados e processados;
- Implementar controles de segurança proporcionais ao nível de sensibilidade e criticidade dos dados;
- Garantir conformidade com a legislação e regulamentações aplicáveis ao setor financeiro e de câmbio;
- Estabelecer procedimentos de análise de dados para suportar a tomada de decisões;
- Definir responsabilidades das áreas envolvidas na classificação, coleta, análise e proteção de dados;
- Implementar procedimentos de auditoria e monitoramento contínuo;
- Documentar e manter registros de classificação, coleta e análise por período mínimo de cinco anos.

2. Escopo

Esta Política aplica-se a todos os dados, informações e sistemas de informação geridos pelo “Intex Bank”, bem como a toda coleta, processamento e análise de informações e dados realizados pela instituição, independentemente da fonte (clientes, colaboradores, fornecedores, terceiros, sistemas internos, fontes públicas).

O escopo inclui:

- Dados pessoais e dados pessoais sensíveis;
- Dados financeiros e transacionais;
- Dados operacionais;
- Dados de risco;
- Dados de conformidade;
- Dados de ativos virtuais;
- Dados de sistemas internos de desenvolvimento próprio;
- Dados coletados de fontes externas e públicas.

Esta Política está alinhada com as exigências da Resolução CMN nº 4.893/2021, que impõem a adoção de medidas eficazes de segurança da informação e proteção de dados, bem como com as boas práticas consagradas pelo NIST Cybersecurity Framework (CSF) e pela ISO/IEC 27001:2022, que orientam processos de classificação, proteção e tratamento seguro da informação. Além disso, assegura conformidade plena com a LGPD (Lei nº 13.709/2018), regulando o tratamento de dados pessoais e sensíveis em todas as suas fases, e reforça o compromisso com a Lei nº 9.613/1998, ao estabelecer controles para mitigar riscos relacionados à lavagem de dinheiro por meio da proteção e rastreabilidade dos dados armazenados e processados.

3. Abrangência

Esta Política se aplica aos colaboradores (funcionários e prestadores de serviços), diretores e membros dos órgãos de governança instalados ou que venham a ser instalados na estrutura do “Intex Bank”, bem como parceiros (correspondentes cambiais) e quaisquer outras partes colaborativas do “Intex Bank” (conjuntamente referidos como “Destinatários”).

4. Princípios Orientadores

O “Intex Bank” orienta a classificação, coleta, análise e proteção de dados pelos seguintes princípios:

- **Legalidade:** coleta, classificação e análise em conformidade com leis e regulamentações aplicáveis, incluindo a LGPD, as normas do Banco Central e a legislação anticorrupção.

- **Necessidade:** coleta apenas de dados estritamente necessários para a finalidade específica identificada.
- **Proporcionalidade:** o benefício da análise e os controles de proteção devem ser proporcionais ao risco e à sensibilidade dos dados.
- **Transparência:** informação clara ao titular sobre coleta, uso e análise de seus dados.
- **Segurança:** proteção de dados contra acesso não autorizado, perda, alteração ou destruição, utilizando controles técnicos e organizacionais adequados.
- **Qualidade:** garantia de precisão, completude, consistência e integridade dos dados coletados e processados.
- **Responsabilização:** documentação e auditoria de todas as atividades de coleta, classificação, processamento e análise de dados.
- **Não Discriminação:** a análise de dados não deve resultar em discriminação ilegal ou injusta contra titulares.

5. Diretrizes para Classificação de Informações

O “Intex Bank” adota uma abordagem estruturada para a classificação e proteção dos dados, fundamentada em requisitos legais, no nível de sensibilidade e na importância comercial das informações, de forma a garantir que todos os ativos informacionais estejam protegidos conforme o grau de criticidade e risco associado. Os proprietários de dados são designados como responsáveis pela determinação de requisitos específicos para suas respectivas informações e por identificar quaisquer exceções ao tratamento padrão que se façam necessárias.

Os sistemas e aplicações de informação devem ser classificados e protegidos de acordo com o mais alto nível de confidencialidade dos dados que processam ou armazenam, de modo a prevenir a exposição não autorizada e assegurar a integridade dos dados.

As diretrizes para a classificação das informações são as seguintes:

- Todos os ativos informacionais, incluindo documentos, dados e sistemas, devem ter seu nível de sigilo claramente identificado. Essa identificação deve

estar visível em todos os formatos, sejam físicos ou digitais, assegurando que o nível de proteção seja reconhecido e respeitado por todos os colaboradores.

- Os ativos que, ocasionalmente, não apresentem uma classificação explícita devem ser automaticamente classificados como INTERNOS. Essa classificação provisória visa assegurar um nível básico de proteção, evitando exposição indevida até que uma classificação formal seja atribuída pelo proprietário do ativo.
- No ato da classificação dos ativos, o proprietário deve estar atento à legislação vigente, normas institucionais e obrigações contratuais aplicáveis, assegurando que a classificação atribuída esteja em conformidade com os requisitos de confidencialidade, integridade e disponibilidade das informações, bem como com os regulamentos específicos do setor de câmbio.
- O nível de classificação das informações poderá ser alterado conforme o ciclo de vida do ativo. Um ativo inicialmente classificado como interno pode ter sua classificação alterada para público em resposta a mudanças de contexto ou necessidade de divulgação. Por exemplo, um balanço financeiro classificado inicialmente como confidencial pode ser reclassificado como público caso sua divulgação seja exigida por obrigações regulamentares.
- A análise de reclassificação das informações é um processo que deverá ser realizado periodicamente, sendo de responsabilidade direta do proprietário do ativo. Esse processo de revisão assegura que as informações permaneçam classificadas de forma condizente com sua sensibilidade e risco ao longo do tempo.
- Os direitos de acesso sobre os ativos informacionais, incluindo documentos e sistemas, serão concedidos somente após a devida aprovação dos respectivos proprietários. Esse controle de acesso visa garantir que o acesso seja restrito aos colaboradores ou áreas cuja função exija o conhecimento do ativo, promovendo uma gestão segura e controlada das informações.
- Quando da combinação de várias informações em um único ativo, o nível de proteção será estabelecido com base na informação classificada como a

mais sensível, ou seja, aplicando o nível mais alto da classificação da informação ao ativo combinado. Essa abordagem garante que o ativo composto receba o nível de proteção adequado à informação mais crítica contida.

6. Níveis para Classificação de Informações

As informações do "Intex Bank" devem ser classificadas de acordo com os seguintes níveis, conforme sua sensibilidade e o potencial impacto em caso de divulgação não autorizada. As informações devem ser classificadas (isto é, agrupadas em "classes") para otimizar os controles que garantem seu acesso apenas por pessoas autorizadas. Essas classes alinham-se ao disposto na Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018 e nas leis que definem necessidade de classificação de informações, sigilos, como fiscal, bancário, comercial e aquele relativo a denúncias.

Classificação	Descritivo	Fundamento Legal / Restrição de Acesso
Público	Informações destinadas ao público geral, sem restrições de acesso. Incluem materiais de divulgação institucional e dados sobre produtos e serviços oferecidos ao mercado.	Não aplicável.
Interno	Informação de uso exclusivamente interno, e são autorizadas neste nível, trocas de informações, pelos meios de comunicação internos do "Intex Bank". São informações destinadas a todos os funcionários, colaboradores, prestadores de serviços e visitantes do "Intex Bank".	Lei nº 13.709/2018, Lei nº 12.527/2011.
Restrito	Informações com acesso restrito a áreas específicas e pessoas autorizadas, devido a requisitos legais, normativos ou contratuais. O acesso é concedido com base na necessidade de conhecimento para funções específicas.	Prazo mínimo de 5 anos conforme Circular BACEN nº 3.978/2020 (PLDFT), Lei nº 12.965/2014 (Marco Civil da Internet).

Confidencial	Informações críticas cujo acesso é limitado a um grupo específico de colaboradores com funções estratégicas ou gerenciais. A divulgação não autorizada poderia impactar negativamente as operações e a conformidade regulatório do banco. Apenas gestores ou superiores podem atribuir este nível de confidencialidade.	Prazo mínimo de 5 anos, conforme Lei nº 9.613/1998 (Lei de Lavagem de Dinheiro), Circular BACEN nº3.978/2020 (PLD), e LGPD (Lei nº 13.709/2018).
Pessoal	Informações que contêm dados pessoais identificáveis ou sensíveis, cujo acesso é restrito a colaboradores autorizados e controlado em conformidade com a Lei Geral de Proteção de Dados (LGPD). Esse nível de classificação destina-se a informações que, se divulgadas sem autorização, poderiam comprometer a privacidade dos indivíduos e a conformidade da corretora com regulamentações de proteção de dados. O acesso é concedido apenas para funções específicas e com controle rigoroso de acesso e rastreamento de acordo com a Política de Privacidade da instituição	Prazo mínimo de 5 anos após o término da relação contratual, conforme Circular BACEN nº 3.978/2020 (PLDFT) e LGPD. Em alguns casos, pode ser estendido a 10 ou 15 anos, dependendo de obrigações contratuais e requisitos legais adicionais.

6.1. Rotulagem das Informações

Todos os dados classificados como “Confidenciais” ou “Restritos” devem ser rotulados de maneira visível e clara, tanto em documentos físicos quanto em registros digitais. O rótulo apropriado deve constar em todas as páginas de documentos impressos, identificando a natureza sensível da informação e orientando o manuseio adequado pelos colaboradores. A rotulagem deve seguir as diretrizes definidas nesta Política e incluir, sempre que necessário, instruções adicionais de armazenamento, transporte e descarte seguro.

7. Tratamento de Dados

7.1. Tratamento de Dados Confidenciais

Os dados classificados como “Confidenciais” são considerados de alta sensibilidade e requerem tratamento rigoroso e controles avançados de

segurança. O acesso e uso desses dados devem seguir os seguintes requisitos:

- O acesso a dados confidenciais deve ser concedido apenas a colaboradores que comprovem necessidade clara de utilização, e sempre com autorização formal do proprietário. Cada acesso e atividade relacionada a esses dados devem ser registrados, e logs de acesso devem ser periodicamente auditados.
- Dados confidenciais devem ser acessíveis apenas a colaboradores, departamentos ou funções específicas, de acordo com a necessidade funcional e respeitando o princípio do "mínimo privilégio".
- Sistemas que processam ou armazenam dados confidenciais devem implementar autenticação multifatorial, impedindo acesso anônimo e garantindo a autenticação segura do usuário. Todos os acessos devem ser monitorados e as sessões devem ser registradas, possibilitando auditorias detalhadas.
- Dados confidenciais não devem ser utilizados em ambientes de teste ou desenvolvimento. Para esses fins, devem ser utilizados dados anonimizados ou simulados, assegurando que informações sensíveis permaneçam exclusivamente em ambientes de produção.
- Dados confidenciais devem ser criptografados tanto em repouso quanto em trânsito, utilizando algoritmos reconhecidos e auditados conforme as melhores práticas de segurança. Essa medida se aplica especialmente a dados transmitidos por redes públicas ou compartilhados em sistemas externos, garantindo a proteção contra interceptações.
- Dispositivos móveis que armazenam dados confidenciais, como laptops, devem ser criptografados e protegidos com autenticação biométrica ou senha forte. Além disso, esses dispositivos devem ser configurados para bloqueio automático após um período máximo de cinco minutos de inatividade, evitando acesso não autorizado.
- Todas as cópias de *backup* contendo dados confidenciais devem ser criptografadas e armazenadas em locais seguros, sujeitos a controles de acesso rigorosos.
- É expressamente proibido o armazenamento de dados confidenciais em

dispositivos pessoais, como smartphones ou mídias removíveis, exceto mediante autorização específica e quando existirem controles adequados de segurança.

- Documentos físicos que contenham informações confidenciais devem ser manuseados e armazenados em locais seguros, com acesso restrito, e devem ser rotulados conforme as diretrizes desta Política. A impressão deve ser evitada sempre que possível, e os documentos físicos devem ser descartados de maneira segura após o uso.
- Dispositivos e mídias que contenham dados confidenciais devem ser apagados utilizando técnicas de destruição segura, ou devem ser fisicamente destruídos de forma irreversível, conforme padrões aceitos de segurança da informação.
- A transferência de dados confidenciais para terceiros, incluindo prestadores de serviços, deve ser precedida de aprovação formal e respaldada por acordos de confidencialidade e proteção de dados, que assegurem o cumprimento das exigências legais e regulamentares.

7.2. Tratamento de Dados Restritos

Dados classificados como “Restritos” devem ser tratados com proteção adequada e limitações de acesso, conforme os seguintes requisitos:

- Somente os colaboradores cuja função exija acesso a dados restritos poderão visualizar ou manipular essas informações. A concessão de acesso deve seguir critérios de necessidade de conhecimento e ser revisada periodicamente.
- Sistemas que contêm dados restritos devem exigir autenticação robusta e permitir o rastreamento de todas as atividades, assegurando a identificação de acessos e fornecendo uma trilha de auditoria.
- A transferência de dados restritos para terceiros deve ser formalmente autorizada pela gerência e respaldada por acordos que garantam a proteção da informação. A responsabilidade pelo uso adequado e pela confidencialidade dos dados deve ser explicitamente definida.
- Antes do descarte de dispositivos ou mídias que contenham dados restritos,

os dados devem ser permanentemente apagados ou os dispositivos destruídos, evitando qualquer possibilidade de recuperação.

7.3. Tratamento dos Dados Públicos

Os dados classificados como "Públicos" são destinados ao consumo externo e podem ser compartilhados sem restrições. Não há necessidade de medidas adicionais de segurança para esses dados.

7.4. Tratamento de Informações Pessoais

O tratamento de dados pessoais classificados nesta categoria deve observar, além das diretrizes aqui estabelecidas, as disposições da ***Política de Privacidade,*** o ***Aviso de Privacidade*** e o ***Plano de Resposta a Incidentes*** envolvendo Dados Pessoais do "Intex Bank", incluindo dados sensíveis, conforme definido pela Lei Geral de Proteção de Dados (LGPD). O tratamento desses dados deve seguir rigorosamente os princípios da LGPD, garantindo a privacidade e a proteção dos direitos dos titulares. Abaixo estão os requisitos para o tratamento desses dados:

- O tratamento de dados pessoais deve ocorrer somente mediante consentimento explícito do titular ou com base em uma das hipóteses legais previstas pela LGPD, como execução de contrato, cumprimento de obrigação legal, ou legítimo interesse, entre outros.
- O acesso a dados pessoais deve ser limitado aos colaboradores cuja função exija essa informação, sempre em conformidade com a necessidade de conhecimento. O acesso deve ser monitorado e registrado.
- Sistemas que processam dados pessoais devem implementar autenticação multifatorial e monitoramento contínuo de acesso. Todos os acessos devem ser registrados, proporcionando uma trilha de auditoria para verificação de conformidade.
- Sempre que possível, dados pessoais devem ser anonimizados ou pseudonimizados, especialmente para uso em ambientes de teste ou desenvolvimento. Dados pessoais sensíveis devem ser criptografados em repouso e em trânsito para proteção adicional.
- A transferência de dados pessoais para terceiros deve ser feita somente quando houver base legal e mediante contrato que assegure a proteção e a privacidade dos dados, em conformidade com as disposições da LGPD.
- O titular dos dados pessoais tem o direito de solicitar a exclusão de seus dados a qualquer momento, quando não houver obrigação legal para

retenção. O “Intex Bank” deve respeitar e atender essas solicitações, conforme os prazos regulamentares.

- Dados pessoais devem ser revisados periodicamente para verificar a necessidade de retenção. Dados desnecessários ou sem finalidade justificável devem ser descartados de maneira segura.

8. Fontes e Procedimentos de Coleta de Dados

8.1. Fontes de Coleta

8.1.1 Coleta Direta

O “Intex Bank” coleta dados diretamente do titular através de formulários e aplicações, entrevistas, chamadas telefônicas, comunicações eletrônicas e sistemas de atendimento. Para coleta direta, o “Intex Bank” deve informar o titular sobre a finalidade, a base legal e os direitos do titular.

8.1.2 Coleta de Sistemas Internos

O “Intex Bank” coleta dados de seus sistemas internos, incluindo o sistema de contas correntes, sistema de câmbio, sistema de intermediação de ativos, sistema de risco e sistema de conformidade. Dados de sistemas internos são considerados confiáveis e não requerem validação adicional.

8.1.3 Coleta de Terceiros

O “Intex Bank” coleta dados de terceiros, incluindo serviços de *credit scoring*, serviços de análise de fraude, bancos de dados públicos e agências de classificação de risco. Para coleta de terceiros, o “Intex Bank” deve:

- Verificar conformidade do terceiro com a LGPD;
- Obter contrato especificando os termos de compartilhamento e uso;
- Validar a qualidade dos dados recebidos.

8.1.4 Coleta de Fontes Públicas

O “Intex Bank” coleta dados de fontes públicas, incluindo registros públicos, jornais e mídia, redes sociais e websites públicos. Para coleta de fontes públicas, o “Intex Bank” deve verificar conformidade com a LGPD e informar o

titular quando apropriado.

8.2. Procedimentos de Coleta

8.2.1 Identificação de Necessidade

Antes de coletar dados, o “Intex Bank” deve identificar e documentar:

- Finalidade específica da coleta;
- Dados estritamente necessários;
- Fonte de dados;
- Base legal aplicável;
- Direitos do titular;
- Tempo de retenção previsto.

Esta identificação deve ser documentada e aprovada pela área responsável.

8.2.2 Consentimento

O “Intex Bank” deve obter consentimento prévio do titular para coleta de dados pessoais, exceto quando outra base legal se aplica. O consentimento deve ser livre, informado, inequívoco e específico para cada finalidade.

8.2.3 Validação de Dados

O “Intex Bank” valida dados coletados para garantir qualidade, incluindo verificação de completude, verificação de formato, verificação de consistência, verificação de precisão e remoção de duplicatas.

8.2.4 Documentação da Coleta

O “Intex Bank” documenta para cada coleta: data e hora da coleta, fonte de dados, dados coletados, consentimento obtido (quando aplicável), validação realizada e responsável pela coleta.

9. Processamento de Dados

9.1. Limpeza de Dados

O “Intex Bank” limpa dados para remover valores faltantes, duplicatas, valores

inconsistentes e dados corrompidos. A limpeza é documentada e rastreável.

9.2. Transformação de Dados

O “Intex Bank” transforma dados para padronizar formato, converter unidades, normalizar valores e criar variáveis derivadas. A transformação é documentada e reversível.

9.3. Integração de Dados

O “Intex Bank” integra dados de múltiplas fontes, garantindo consistência, integridade, rastreabilidade e segurança. A integração é documentada com especificação de regras de mapeamento e reconciliação.

9.4. Armazenamento de Dados

O “Intex Bank” armazena dados em bancos de dados seguros, *data warehouses*, *data lakes* e sistemas de *backup*. O armazenamento implementa:

- Criptografia em repouso (AES-256 ou equivalente);
- Controle de acesso baseado no princípio do menor privilégio;
- Logs de auditoria para todas as operações;
- *Backup* regular com testes de recuperação periódicos.

10. Análise de Dados

O “Intex Bank” realiza diferentes tipos de análise de dados para suportar a tomada de decisões, conforme descrito a seguir:

10.1. Análise Descritiva

O “Intex Bank” realiza análise descritiva para resumir dados, identificar padrões, calcular estatísticas e criar visualizações. A análise descritiva suporta a compreensão básica dos dados e a identificação de tendências.

10.2. Análise Diagnóstica

O “Intex Bank” realiza análise diagnóstica para investigar causas, identificar correlações, entender relacionamentos e explicar variações. A análise diagnóstica suporta a identificação de problemas e suas causas raiz.

10.3. Análise Preditiva

O “Intex Bank” realiza análise preditiva para prever comportamentos futuros, estimar riscos, identificar oportunidades e otimizar decisões. A análise preditiva utiliza modelos estatísticos e machine learning, com validação periódica dos modelos.

10.4. Análise Prescritiva

O “Intex Bank” realiza análise prescritiva para recomendar ações, otimizar resultados, mitigar riscos e melhorar eficiência operacional. A análise prescritiva suporta diretamente a tomada de decisão estratégica e operacional.

11. Qualidade de Dados

11.1. Dimensões de Qualidade

O Intex Bank avalia a qualidade de dados nas seguintes dimensões:

- **Precisão:** os dados representam fielmente a realidade.
- **Completude:** os dados não têm valores faltantes críticos
- **Consistência:** os dados são uniformes entre diferentes fontes e sistemas.
- **Atualidade:** os dados são recentes e refletem a situação vigente.
- **Validade:** os dados estão em formato correto e atendem às regras de negócio.
- **Unicidade:** os dados não têm duplicatas não intencionais.

11.2. Monitoramento de Qualidade

O “Intex Bank” monitora continuamente a qualidade de dados através de testes automáticos, auditorias periódicas, relatórios de qualidade e alertas de anomalias.

11.3. Melhoria de Qualidade

O “Intex Bank” melhora a qualidade de dados através de identificação de problemas, implementação de correções, atualização de procedimentos e treinamento de equipes.

12. Segurança de Dados

12.1. Controle de Acesso

O “Intex Bank” implementa controle de acesso a dados através de:

- Autenticação: verificação de identidade do usuário, com autenticação multifatorial obrigatória para dados confidenciais e secretos.
- Autorização: verificação de permissões baseada em perfis e funções.
- Princípio do menor privilégio: acesso mínimo necessário para execução das funções.
- Segregação de funções: separação de responsabilidades para evitar conflitos de interesse e acesso indevido.

12.2. Criptografia

O “Intex Bank” criptografa dados conforme os seguintes padrões:

- Criptografia em trânsito: TLS 1.2 ou superior para todas as comunicações.
- Criptografia em repouso: AES-256 ou equivalente para dados sensíveis.
- Gerenciamento de chaves: armazenamento seguro de chaves criptográficas com rotação periódica.

12.3. Auditoria e Logs

O “Intex Bank” mantém logs de acesso a dados, modificações de dados, exclusão de dados e compartilhamento de dados. Os logs são armazenados de forma segura e revisados periodicamente, constituindo trilha de auditoria completa para fins regulatórios.

12.4. Backup e Recuperação

O “Intex Bank” realiza:

- *Backup* diário de dados críticos;
- *Backup* horário de dados em tempo real;
- Testes de recuperação mensais;
- Armazenamento de *backups* em local geograficamente distinto.

13. Retenção de Dados

O “Intex Bank” manterá dados pessoais e operacionais apenas pelo tempo necessário para atender às finalidades comerciais, regulamentares e contratuais. Todos os períodos de retenção serão definidos com base em requisitos legais e em práticas comerciais legítimas, visando proteger os direitos dos titulares e manter a conformidade com as regulamentações vigentes.

- Informações pessoais de identificação (PII) **devem** ser excluídas ou anonimizadas quando não forem mais necessárias para as finalidades originais, exceto se houver uma base legal para retenção adicional, como obrigações fiscais ou regulatórias.
- Todos os períodos de retenção para diferentes tipos de dados devem ser documentados em uma Matriz de Retenção de Dados. Esse documento será revisado anualmente para garantir que os prazos de retenção estejam em conformidade com as leis e regulamentos aplicáveis.

14. Descartes de Dados e Dispositivos

O descarte seguro de dados e dispositivos é uma prática essencial no “Intex Bank”, garantindo que dados sensíveis não possam ser recuperados após o fim do ciclo de vida. Dados classificados como "Restritos" ou "Confidenciais" devem ser descartados de acordo com as melhores práticas de segurança, utilizando técnicas de destruição segura que atendam às regulamentações aplicáveis.

- Fornecedores que prestam serviços de descarte de dados e dispositivos devem atender aos requisitos de segurança estabelecidos pelo “Intex Bank”. Apenas fornecedores certificados e que garantam a conformidade com normas de segurança de dados serão autorizados a lidar com informações restritas ou confidenciais.
- Dados pessoais (PII) devem ser retidos apenas pelo tempo necessário para finalidades comerciais e regulamentares. Ao término do contrato ou da relação comercial, as PII devem ser excluídas ou desidentificadas, conforme exigido pela LGPD e demais regulamentações aplicáveis. As informações pessoais de identificação também devem ser eliminadas mediante solicitação do titular, exceto quando houver interesse legítimo ou obrigação legal para retê-las.

15. Revisão Anual de Dados

O “Intex Bank” realizará uma revisão anual dos requisitos de retenção e descarte de dados, assegurando que todos os procedimentos estejam atualizados e em conformidade com as regulamentações aplicáveis. Essa revisão visa ajustar os prazos de retenção conforme as melhores práticas e atender às diretrizes da LGPD e das regulamentações do Banco Central.

16. Governança e Responsabilidades

As responsabilidades relativas à gestão, classificação e proteção de dados estão distribuídas conforme a tabela a seguir:

Área	Responsabilidades
Diretoria de TI	Definição de necessidades de coleta e utilização de dados; aprovação de finalidades de coleta; classificação dos ativos de negócio.
Diretoria de Compliance	Conformidade legal e regulatória; monitoramento do cumprimento da LGPD; interface com Banco Central e ANPD; gestão da Matriz de Retenção de Dados.
Área de TI e Segurança	Infraestrutura e segurança dos sistemas de dados; implementação de controles técnicos de criptografia, acesso e *backup*; gestão do armazenamento seguro.
Área de Riscos	Qualidade e integridade dos dados; avaliação de riscos associados ao tratamento de dados; monitoramento de indicadores de qualidade.
Auditoria Interna	Auditoria e monitoramento contínuo; verificação de conformidade com esta Política; relato de resultados ao Conselho de Administração.
Encarregado de Proteção de Dados (DPO)	Supervisão do tratamento de dados pessoais; canal de comunicação com titulares e ANPD; avaliação de exceções a esta Política; gestão de solicitações de titulares.

17. Requisitos Legais

Em circunstâncias específicas, o “Intex Bank” pode estar sujeito a

procedimentos legais que exigem a retenção de dados relacionados a requisitos legais, ações judiciais ou outros assuntos, conforme determinado pelo Comitê de Proteção de Dados do “Intex Bank”. Esses registros e informações estão excluídos de quaisquer outros requisitos especificados nesta política que devem ser retidos de acordo com os requisitos identificados pelo Departamento Jurídico. Todas essas retenções e requisitos especiais de retenção estão sujeitas a revisão anual com o conselho jurídico do “Intex Bank” para avaliar os requisitos e o escopo contínuo.

18. Documentação e Guarda

O “Intex Bank” mantém documentação completa de:

- Procedimentos de coleta de dados;
- Validação de dados coletados;
- Processamento e transformação de dados;
- Análise de dados realizadas;
- Indicadores e relatórios de qualidade de dados;
- Controles de segurança implementados;
- Registros de incidentes de segurança;
- Relatórios de auditorias internas e externas;
- Registros de conformidade e classificação de ativos.

Toda documentação deve ser mantida por período mínimo de cinco anos e estar acessível para revisão pelo Banco Central do Brasil (BCB) e pela Autoridade Nacional de Proteção de Dados (ANPD).

19. Conformidade com a Política

O “Intex Bank” compromete-se a monitorar o cumprimento desta Política de maneira contínua, por meio de auditorias regulares, avaliações de conformidade e uso de ferramentas de monitoramento e controle. A conformidade será verificada por auditorias internas e externas, reforçando a integridade das práticas de gestão de dados e proteção de informações. Qualquer não conformidade identificada deverá ser prontamente corrigida, e as ações corretivas serão documentadas e monitoradas para evitar recorrências.

20. Exceções

Exceções a esta política devem ser formalmente submetidas à área de TI e ao Encarregado de Proteção de Dados (DPO) 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 dpo@intexbank.com.br.

21. Violações e Cumprimento da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente ao Gestor de TI ou 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.

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.

22. Vigência

Esta política entra em vigor na data de sua publicação, sendo revisada no prazo de 12 (doze) meses, ou a qualquer momento, conforme a necessidade.

São Paulo, 13 de agosto de 2026.

O presente documento foi aprovado pelo Comitê Diretivo conforme Ata de Reunião realizada em 13/08/2026.

Intex Bank Banco de Câmbio S/A

Apêndice

Apêndice 1 - Exemplo de Classificação de Informações

As diretrizes de classificação a seguir visam assegurar a proteção e o manuseio adequado das informações do Intex Bank, em conformidade com as melhores práticas de governança e as exigências regulatórias específicas do Banco Central do Brasil. A aplicação das classificações deve ser rigorosa e sistemática, garantindo que o acesso, armazenamento e compartilhamento das informações ocorram conforme seu nível de sensibilidade e criticidade.

➢ Nível 0 - Público

Informações destinadas ao público geral, com livre acesso e baixo impacto em caso de divulgação. Não apresentam restrições e são voltadas à comunicação e à transparência institucional.

- Materiais de marketing e divulgação institucional;
- Políticas de privacidade publicadas no site;
- Relatórios anuais e demonstrações financeiras públicas;
- Comunicados institucionais e notas de imprensa;
- Informações sobre produtos e serviços oferecidos ao mercado;
- Conteúdos em redes sociais e no blog institucional;
- Documentação de orientação pública sobre procedimentos gerais.

➢ Nível 1 - Restrito

Informações de uso exclusivo dos colaboradores e prestadores de serviço, necessárias para as operações internas da organização. São de acesso controlado e seu compartilhamento externo não é permitido.

- Políticas e procedimentos operacionais internos;
- Manuais de processos e instruções de trabalho interno;
- Relatórios de desempenho operacional (não publicados);
- Calendário de treinamentos e agendas internas;
- Guias e orientações de uso de sistemas internos;
- Documentação de suporte técnico e manutenção de sistemas;
- Inventário de ativos e controle de equipamentos;
- Relatórios operacionais e dados financeiros em andamento;
- Lista de clientes institucionais e dados de negociação;
- Estruturas de preços e condições comerciais específicas;
- Estratégias de mercado e planos de ação táticos;
- Relatórios de gestão de riscos operacionais;

- Documentação sobre segurança de infraestrutura física;
- Planos de contingência operacionais (exceto informações críticas);
- Informações sobre fornecedores e contratos de menor impacto;

➢ Nível 2 - Confidencial

Informações de alta criticidade, cujo acesso é restrito a um grupo específico de colaboradores com funções estratégicas ou gerenciais. A divulgação não autorizada pode impactar negativamente a empresa e comprometer o cumprimento de normas regulatórias.

- Dados pessoais de identificação (PII) de clientes e colaboradores (KYC);
- Relatórios financeiros detalhados e projeções de desempenho;
- Relatórios de compliance e auditoria interna;
- Perfis de risco de clientes e avaliações estratégicas;
- Documentos de due diligence para parceiros e clientes;
- Registros de folha de pagamento, remuneração e benefícios de colaboradores;
- Contratos confidenciais com cláusulas estratégicas;
- Informações sobre políticas de segurança e controles internos;
- Estratégias corporativas de longo prazo e planos de expansão;
- Planos de fusões, aquisições e reorganizações societárias;
- Detalhes de operações de câmbio de alto valor e impacto financeiro;
- Informações sobre segurança cibernética e incidentes críticos;
- Dados sobre infraestrutura de segurança e tecnologia de alto risco;
- Relacionamento estratégico com parceiros e fornecedores críticos;
- Planos de resposta a incidentes e continuidade de negócios;
- Investigações internas e análises de fraudes ou desvios;
- Resultados de auditorias internas e investigações confidenciais.

Cada categoria de classificação exige a implementação de controles apropriados de segurança, seguindo o princípio do "necessário ao conhecimento". A observância dessas diretrizes promove a conformidade regulatória, minimiza os riscos associados ao tratamento inadequado das informações e fortalece a cultura de responsabilidade institucional.