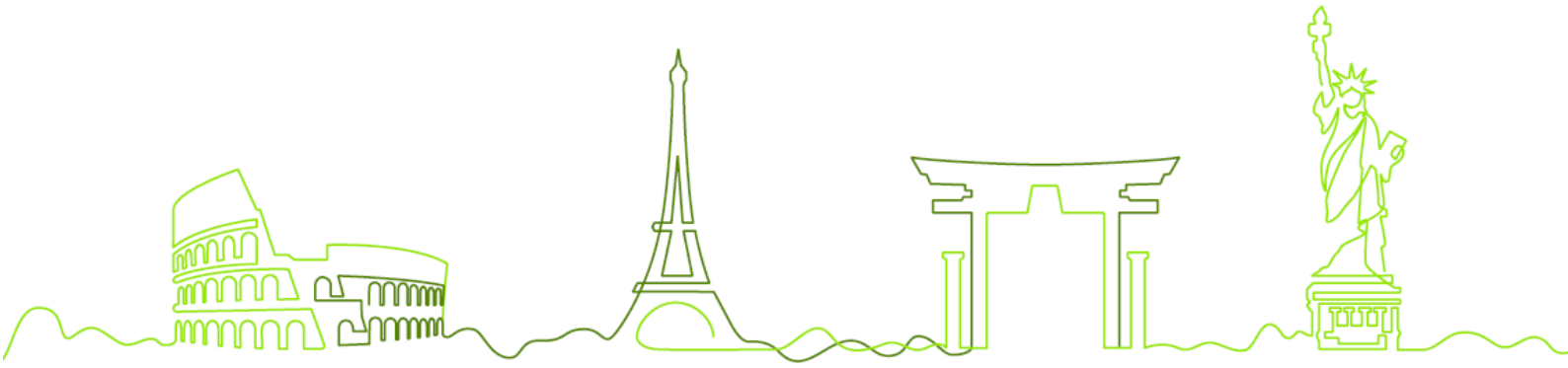

# Política de Gestão, Classificação e Proteção da Informação

**Intex Bank Banco de Câmbio S/A**

# Controle de Versões

| Versão | Data | Área Responsável | Motivo |
|---|---|---|---|
| 1.0 | 28/02/2025 | Cibersegurança | Versão Original |

***Interno:***
Este documento contém informações restritas e de propriedade do INTEX BANK BANCO DE CÂMBIO S/A, cujo conteúdo não poderá ser distribuído, publicado, divulgado ou copiado, mesmo que parcialmente, sem o prévio consentimento e aprovação do INTEX BANK BANCO DE CÂMBIO S/A.

## Sumário


1. Objetivo ..... 4
2. Escopo ..... 4
3. Política ..... 4
4. Diretrizes para Classificação de Informações ..... 5
4.1. Níveis de Classificação das Informações ..... 6
4.2. Rotulagem das Informações ..... 7
5. Tratamento de Dados ..... 7
5.1. Tratamento de Dados Confidenciais ..... 7
5.2. Tratamento de Dados Restritos ..... 8
5.3. Tratamento dos Dados Públicos ..... 9
5.4. Tratamento de Informações Pessoais ..... 9
5.5. Tratamento de Dados Secretos ..... 10
6. Retenção de Dados ..... 10
7. Descartes de Dados e Dispositivos ..... 11
8. Revisão Anual de Dados ..... 11
9. Requisitos Legais ..... 11
10. Conformidade com a Política ..... 12
11. Exceções ..... 12
12. Violações e Cumprimento da Política ..... 12
13. Vigência ..... 12
Apêndice ..... 14

## 1. Objetivo

Estabelecer diretrizes claras e detalhadas para assegurar que os dados e informações gerenciados pelo Intex Bank Banco de Câmbio S/A (doravante denominado "Intex Bank"), sejam corretamente classificados, protegidos, 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.

## 2. Escopo

Aplica-se a todos os dados, informações e sistemas de informação geridos pela "Intex Bank".

Esta Política está alinhada com as exigências da Resolução CMN nº 4.893/2021 e da Resolução BCB nº 85/2021, 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. Política

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.

## 4. Diretrizes para Classificação de Informações

As diretrizes estabelecidas para a classificação das informações visam assegurar que todos os ativos informacionais sejam adequadamente identificados e protegidos, de acordo com seu nível de sensibilidade e relevância estratégica para o "Intex Bank". Todos os ativos de informação **devem** ser claramente classificados e identificados, permitindo a definição precisa de mecanismos de acesso, controle e proteção. As diretrizes para a classificação das informações no "Intex Bank" 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.

a) 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.
b) 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.
c) 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.
d) 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.
e) 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.
f) Quando a 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.

## 4.1. Níveis de Classificação das 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 o compliance regulatório da corretora. 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 | 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. |

| | | |
|---|---|---|
| | rastreamento. | |
| **Secreto** | Informações de máxima sensibilidade, cujo acesso é extremamente restrito a membros da alta direção ou comitês executivos, conforme necessário. A divulgação inadequada destas informações pode comprometer a segurança institucional e a conformidade com regulamentos do Banco Central do Brasil. Somente diretores, membros executivos ou auditores podem classificar informações neste nível. | Prazo recomendado de 20 anos, conforme boas práticas de proteção institucional, e requisitos de compliance de longo prazo (Resolução CMN nº 4.893/2021). |

### 4.2. 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.

## 5. Tratamento de Dados

### 5.1. 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:

a) O acesso a dados confidenciais deve ser concedido apenas a colaboradores que comprovem necessidade clara de utilização, e sempre com autorização formal do proprietário dos dados. Cada acesso e atividade relacionada a esses dados devem ser registrados, e logs de acesso devem ser periodicamente auditados.
b) 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”.
c) 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.
d) 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.
e) 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.

f) 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.
g) Todas as cópias de backup contendo dados confidenciais devem ser criptografadas e armazenadas em locais seguros, sujeitos a controles de acesso rigorosos. A retenção de backups deve seguir os prazos de retenção estabelecidos nesta política, e a recuperação de dados deve ser monitorada para evitar acessos não autorizados.
h) 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.
i) 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.
j) 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.
k) A transferência de dados confidenciais para terceiros, incluindo prestadores de serviços, deve ser precedida de aprovação formal e respaldada por contratos de confidencialidade e proteção de dados, que assegurem o cumprimento das exigências legais e regulamentares.

## 5.2. 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.

a) 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.
b) A transferência de dados restritos para terceiros deve ser formalmente autorizada pela gerência e respaldada por contratos que garantam a proteção da informação. A responsabilidade pelo uso adequado e pela confidencialidade dos dados deve ser explicitamente definida.

c) 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.

## 5.3. 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.

## 5.4. Tratamento de Informações Pessoais

Os dados classificados como "Pessoais" são aqueles que identificam ou podem identificar um indivíduo, 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:

a) 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.
b) 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.
c) 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.
d) 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.
e) 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.
f) 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.
g) Dados pessoais devem ser revisados periodicamente para verificar a necessidade de retenção. Dados desnecessários ou sem finalidade justificável devem ser descartados de maneira segura.

### 5.5. Tratamento de Dados Secretos

Dados classificados como "Secretos" representam informações de máxima sensibilidade e são restritos a um número muito limitado de pessoas dentro da organização, geralmente membros da alta direção ou comitês executivos. O tratamento desses dados deve atender aos mais elevados padrões de segurança e confidencialidade, evitando qualquer possibilidade de exposição. As diretrizes de tratamento para dados secretos são:

a) O acesso a dados secretos é estritamente limitado a colaboradores autorizados de alto nível, e qualquer tentativa de acesso deve ser documentada e auditada. Esses dados não podem ser acessados por terceiros sem autorização formal.
b) Sistemas que processam ou armazenam dados secretos devem utilizar autenticação multifatorial com métodos adicionais de verificação, como biometria, para garantir que apenas os indivíduos autorizados tenham acesso. O monitoramento de acesso deve ser constante e revisado periodicamente.
c) Dados secretos devem ser armazenados e processados em ambientes altamente seguros e isolados, que possuam controle de acesso físico e lógico, e que estejam protegidos contra-ataques cibernéticos.
d) Dados secretos devem ser criptografados utilizando algoritmos de criptografia de alto nível e ferramentas de proteção que estejam em conformidade com as normas internacionais de segurança. A criptografia deve ser aplicada tanto em repouso quanto em trânsito.
e) A exclusão de dados secretos deve seguir protocolos rigorosos de eliminação definitiva, assegurando que nenhum dado possa ser recuperado após o descarte. Equipamentos de armazenamento devem ser destruídos fisicamente ou apagados de maneira irreversível.
f) Dados secretos não podem ser transferidos para terceiros sem aprovação formal e devem estar sempre respaldados por um contrato que assegure a confidencialidade e a integridade das informações. Qualquer transferência deve ser cuidadosamente monitorada.
g) Quaisquer incidentes envolvendo dados secretos devem ser imediatamente relatados à alta administração e ao comitê de segurança. A revisão de todos os processos e sistemas que tratam dados secretos deve ocorrer de forma contínua, garantindo que estejam sempre atualizados conforme as melhores práticas de segurança.

## 6. 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 na Matriz de Retenção de Dados, localizada no Apêndice B desta política. Esse documento será revisado anualmente para garantir que os prazos de retenção estejam em conformidade com as leis e regulamentos aplicáveis.

## 7. 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.

## 8. 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.

## 9. Requisitos Legais

Em circunstâncias específicas, o “Intex Bank” pode estar sujeita a procedimentos legais que exigem a retenção de dados relacionados a requisitos legais, ações judiciais ou outros assuntos, conforme determinado pelo Comitê Encarregado 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.

## 10. 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.

## 11. Exceções

Exceções a esta política devem ser formalmente submetidas 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@trevisocc.com.br.

## 12. Violações e Cumprimento da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente ao 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.

## 13. 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.

# Apêndice

## APÊNDICE 1 – EXEMPLO DE CLASSIFICAÇÃO DE INFORMAÇÕES

### ➢ 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.

a) Materiais de marketing e divulgação institucional;
b) Políticas de privacidade publicadas no site;
c) Relatórios anuais e demonstrações financeiras públicas;
d) Comunicados institucionais e notas de imprensa;
e) Informações sobre produtos e serviços oferecidos ao mercado;
f) Conteúdos em redes sociais e no blog institucional;
g) 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.

a) Políticas e procedimentos operacionais internos;
b) Manuais de processos e instruções de trabalho interno;
c) Relatórios de desempenho operacional (não publicados);
d) Calendário de treinamentos e agendas internas;
e) Guias e orientações de uso de sistemas internos;
f) Documentação de suporte técnico e manutenção de sistemas;
g) Inventário de ativos e controle de equipamentos;
h) Relatórios operacionais e dados financeiros em andamento;
i) Listas de clientes institucionais e dados de negociação;
j) Estruturas de preços e condições comerciais específicas;
k) Estratégias de mercado e planos de ação táticos;
l) Relatórios de gestão de riscos operacionais;
m) Documentação sobre segurança de infraestrutura física;
n) Planos de contingência operacionais (exceto informações críticas);
o) 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.

a) Dados pessoais de identificação (PII) de clientes e colaboradores (KYC);
b) Relatórios financeiros detalhados e projeções de desempenho;
c) Relatórios de compliance e auditoria interna;
d) Perfis de risco de clientes e avaliações estratégicas;
e) Documentos de due diligence para parceiros e clientes;
f) Registros de folha de pagamento, remuneração e benefícios de colaboradores;
g) Contratos confidenciais com cláusulas estratégicas;
h) Informações sobre políticas de segurança e controles internos;

### ➢ Nível 3 - Secreto

Informações de máxima sensibilidade, cujo acesso é extremamente restrito a membros da alta direção ou comitês executivos. A divulgação inadequada pode comprometer a segurança institucional e a conformidade com regulamentações. São informações cuja proteção é essencial para a continuidade e a integridade das operações da organização.

a) Estratégias corporativas de longo prazo e planos de expansão;
b) Planos de fusões, aquisições e reorganizações societárias;
c) Detalhes de operações de câmbio de alto valor e impacto financeiro;
d) Informações sobre segurança cibernética e incidentes críticos;
e) Dados sobre infraestrutura de segurança e tecnologia de alto risco;
f) Relacionamento estratégico com parceiros e fornecedores críticos;
g) Planos de resposta a incidentes e continuidade de negócios;
h) Investigações internas e análises de fraudes ou desvios;
i) Resultados de auditorias internas e investigações confidenciais.

As diretrizes de classificação 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.

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.