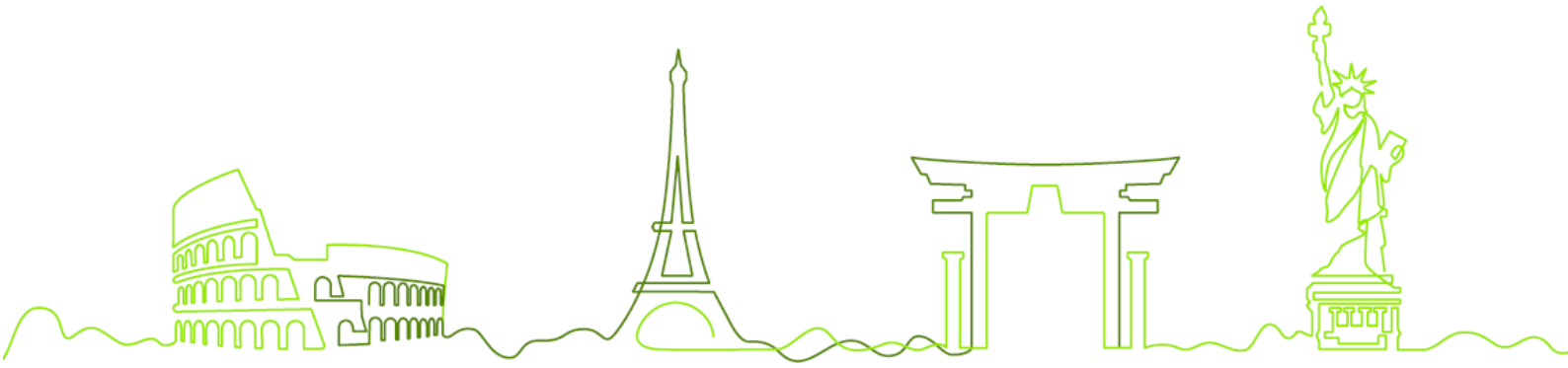

Política de Desenvolvimento Seguro

Intex Bank Banco de Câmbio S/A

Controle de Versões

Versão	Data	Área Responsável	Motivo
1.0	30 abr 2025	Cibersegurança / Tec. Informação	Versão Original

Sumário

1. Objetivo

Esta Política tem o objetivo de garantir a segurança das informações durante o desenvolvimento de aplicativos e sistemas. Ela estabelece regras para aquisição e desenvolvimento de software que devem ser seguidas no Intex Bank Banco de Câmbio S/A, referida a seguir como "Intex Bank".

2. Escopo

Aplica-se a todos os sistemas de informação desenvolvidos e/ou controlados pelo "Intex Bank" que armazenam e transmitem dados confidenciais.

Esta Política está alinhada às exigências regulatórias aplicáveis à segurança da informação no setor financeiro, incluindo a Resolução BCB nº 85/2021, que trata da segurança da informação e da gestão de incidentes; a Resolução BCB nº 139/2021, que exige a manutenção de registros e evidências para a elaboração do relatório anual de segurança cibernética; e a Resolução CMN nº 4.893/2021, que estabelece requisitos para a estrutura de segurança cibernética e gestão de incidentes nas instituições financeiras. Também observa os princípios da Circular nº 3.909/2018, no que diz respeito à proteção de dados e prevenção de vazamentos de informação. No âmbito das boas práticas, a política segue os fundamentos do *NIST Cybersecurity Framework* (CSF) e da norma ISO/IEC 27001:2022, com foco na gestão de riscos, controles técnicos e processos auditáveis. Adicionalmente, contempla os requisitos da LGPD (Lei nº 13.709/2018) quanto à proteção de dados pessoais, especialmente no tratamento e uso de dados em ambientes de desenvolvimento e teste.

3. Procedimentos de Controle e Alterações de Sistemas

As alterações realizadas nos sistemas durante o desenvolvimento devem ser controladas pelo uso de procedimentos formais de controle de alterações. Os procedimentos e requisitos de controle de alterações estão descritos na Política de Segurança das Operações do "Intex Bank".

Todas as alterações no código devem ser aprovadas pelo Diretor de Tecnologia da Informação antes de serem aplicadas em qualquer ambiente de produção. A formalização desse procedimento é obrigatória, devendo ser registrada em documento específico, que descreva as etapas de revisão, aprovação e aplicação das mudanças. A implementação de controles de verificação de código, atualmente em uso, deve ser formalizada e padronizada, garantindo que os procedimentos estejam documentados e

acessíveis para fins de auditoria.

Os procedimentos de controle de alterações devem garantir que o desenvolvimento, os testes e a implementação das alterações não sejam realizados por uma pessoa só, sem aprovação e supervisão.

3.1. Controle de Versão de Software

É mandatória a adoção de um sistema de versionamento distribuído, para todos os softwares desenvolvidos pelo "Intex Bank". Essa medida é essencial para assegurar a rastreabilidade e integridade das modificações de código, atendendo aos princípios de segregação de funções e controle de alterações. O processo de sincronização com o repositório central deve ser documentado e alinhado à esta Política, assegurando que o acesso ao repositório central ocorra de forma controlada, conforme as diretrizes de controle interno.

3.2. Revisão Técnica de Aplicativos após alterações na plataforma operacional

É obrigatório que todas as alterações nas plataformas operacionais sejam submetidas a uma revisão técnica abrangente, incluindo testes de regressão e de segurança, antes da liberação para produção. Esses testes devem ser registrados em conformidade com esta política, garantindo que todas as modificações sejam auditáveis e que os riscos de impactos adversos à segurança e à continuidade operacional sejam mitigados.

3.3. Restrições sobre alterações em pacotes de software

As modificações realizadas nos pacotes de aplicativos de negócios de terceiros são desestimuladas, limitadas às alterações necessárias, além disso, todas as alterações devem ser estritamente controladas.

4. Princípios de Engenharia de Sistemas Seguros

É necessário estabelecer, documentar, manter e aplicar princípios para a engenharia de sistemas seguros em todas as ações de implementação de sistemas de informação.

Devem ser aplicados, no mínimo, os seguintes princípios de segurança e privacidade desde o design.

Princípios de segurança desde o design:

a) Minimizar a área de superfície de ataques.

b) Estabelecer padrões seguros.

c) Princípio do privilégio mínimo.

d) Princípio da defesa profunda.
e) Falhar com segurança.
f) Não confiar nos serviços.
g) Separação de tarefas.
h) Evitar a segurança por obscuridade.
i) Simplificar a segurança.
j) Corrigir os problemas de segurança corretamente.

Princípios de privacidade desde o design:

a) Proativo, não reativo. Preventivo, não corretivo.
b) Privacidade como configuração padrão.
c) Privacidade incorporada ao design.
d) Funcionalidade total: soma positiva, não soma zero.
e) Segurança de ponta a ponta: proteção de todo o ciclo de vida.
f) Visibilidade e transparência: manter a abertura.
g) Respeito à privacidade do usuário: manter o foco no usuário.

Espera-se que os desenvolvedores de software sigam os padrões de programação do "Intex Bank" durante todo o ciclo de desenvolvimento, inclusive os padrões de qualidade, comentários e segurança, sendo esses padrões definidos na documentação do procedimento de desenvolvimento.

5. Ambiente de Desenvolvimento Seguro

O "Intex Bank" deve estabelecer e proteger devidamente os ambientes para o desenvolvimento do sistema e as ações de integração que abrangem todo o ciclo de vida do desenvolvimento do sistema. Os ambientes a seguir devem ser segregados de forma lógica ou física:

a) Desenvolvimento.
b) Ambiente de teste/homologação.
c) Produção.

6. Desenvolvimento Terceirizado

O "Intex Bank" supervisionará e acompanhará a atividade de desenvolvimento terceirizado de sistemas. O desenvolvimento terceirizado deve seguir todas as normas e políticas do "Intex Bank".

7. Testes de Segurança do Sistema

Os testes da funcionalidade de segurança devem ser realizados em períodos definidos durante o ciclo de desenvolvimento. Nenhum código deve ser implementado nos sistemas de produção do "Intex Bank" sem que os testes tenham sido bem-sucedidos e seus resultados e a comprovação das atividades de correção da segurança estejam documentados.

7.1. Gerenciamento de Vulnerabilidade dos Aplicativos

O código do aplicativo deve ser verificado antes da implementação. As correções para solucionar as vulnerabilidades dos aplicativos que afetam a segurança de forma relevante devem ser implementadas em até 90 dias após a descoberta.

7.2. Testes de Aceitação do Sistema

É necessário estabelecer programas de testes de aceitação e critérios relacionados para novos sistemas de informação, atualizações e novas versões.

Antes de implementar o código, é obrigatório o preenchimento da lista de verificação para liberação, que contém uma lista de verificação de todos os planos de teste que mostram a conclusão de todos os testes associados e a correção dos problemas identificados.

7.3. Proteção dos Dados dos Testes

Os dados dos testes devem ser selecionados com atenção, protegidos e controlados. Os dados confidenciais dos clientes devem ser protegidos conforme estabelecem todos os contratos e compromissos. Os dados dos clientes não devem ser usados para fins de testes sem a permissão explícita do proprietário dos dados e do diretor de tecnologia da informação.

8. Aquisição de Sistemas e Softwares de Terceiros

A aquisição de sistemas e software de terceiros deve ser feita de acordo com os requisitos da Política de Gerenciamento de Terceiros do "Intex Bank".

9. Treinamento de Desenvolvedores

Os desenvolvedores de software devem receber treinamento adequado à sua função para desenvolvimento seguro pelo menos uma vez por ano. O conteúdo do treinamento deve ser determinado pela gerência, mas deve abordar a prevenção de ataques e vulnerabilidades comuns dos aplicativos da web. As ameaças e vulnerabilidades a

seguir devem ser tratadas conforme apropriado:

a) Prevenção de ataques de bypass de autorização.
b) Prevenção do uso de IDs de sessão inseguras.
c) Prevenção de ataques de injeção.
d) Prevenção de ataques de script entre sites (XSS).
e) Prevenção de ataques de falsificação de solicitação entre sites.
f) Prevenção do uso de bibliotecas vulneráveis.

10. Exceções

As solicitações de exceção a esta política devem ser enviadas para o diretor de tecnologia para aprovação.

11. Violações e Não Cumprimento da Política

Todas as violações conhecidas a esta política devem ser informadas à Cibersegurança ou diretamente ao diretor de tecnologia. As violações a esta política podem acarretar a retirada ou suspensão imediata dos privilégios do sistema e da rede e/ou em ações disciplinares de acordo com os procedimentos do "Intex Bank", inclusive a rescisão do contrato de trabalho.

12. 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.