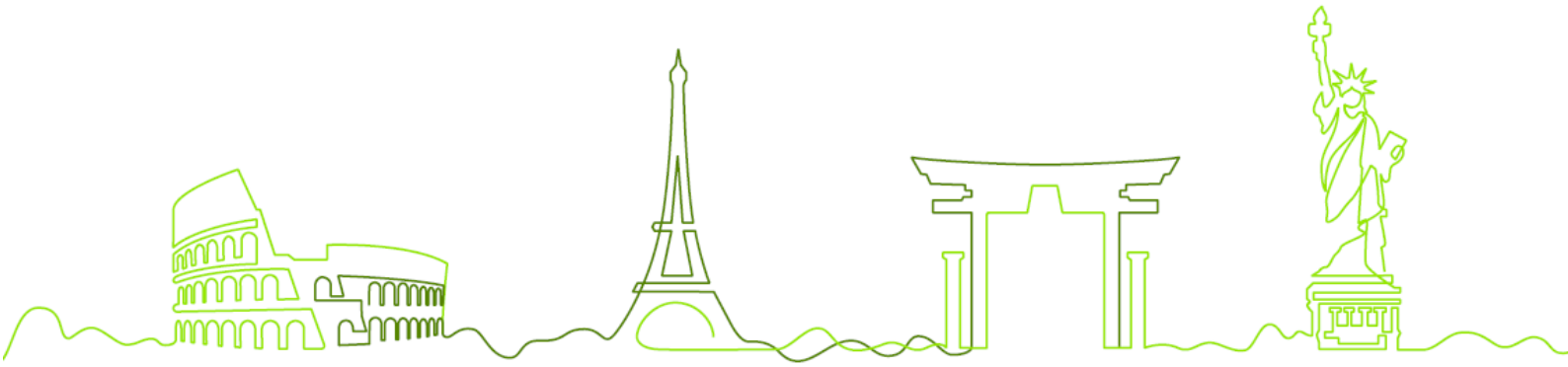
intex international exchange bank



Política de Segurança das Operações

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

Garantir a operação correta e segura dos sistemas e instalações de processamento de informações.

2. Escopo

Todos os sistemas de informação da Intex Bank Banco de Câmbio S/A, referenciada abaixo somente como “Intex Bank”, sejam essenciais aos negócios e/ou processem, armazenem ou transmitam dados da empresa. Esta política se aplica a todos os funcionários da “Intex Bank” e a outras entidades terceiras que tenham acesso às redes e aos recursos do sistema da “Intex Bank”.

Esta Política está alinhada às resoluções e circulares do Banco Central do Brasil (Resolução BCB nº 85/2021, Resolução BCB nº 139/2021, Resolução CMN nº 4.893/2021, Circular 3.909/2018 e Resolução CMN nº 5.088/2023), que tratam de segurança cibernética, incidentes, prevenção a vazamentos e continuidade de negócios; aos frameworks ISO/IEC 27001:2022 e NIST Cybersecurity Framework para gestão de riscos; e às legislações da LGPD (Lei nº 13.709/2018) e COAF (Lei nº 9.613/1998), reforçando a proteção de dados pessoais e a prevenção à lavagem de dinheiro.

3. Procedimentos Operacionais Documentados

Os procedimentos operacionais técnicos e administrativos devem ser documentados conforme necessário e disponibilizados a todos os usuários que precisem deles.

4. Gestão de Mudanças

Mudanças na organização, nos processos de negócios, nas instalações de processamento de informações, no software e na infraestrutura de produção e nos sistemas que afetam a segurança das informações no ambiente de produção e nos sistemas financeiros devem ser testadas, revisadas e aprovadas antes de serem implementadas na produção. Todas as mudanças relevantes nos sistemas e redes que fazem parte do escopo devem ser documentadas.

Documentação e Revisão de Mudanças:

a) Todas as grandes mudanças nos sistemas, redes e instalações de processamento devem ser documentadas.

b) A documentação deve abranger o objetivo da mudança, a especificação, o possível impacto considerando as dependências e o plano de implementação.

c) As mudanças devem ser testadas e revisadas em ambientes separados da produção e do desenvolvimento (por exemplo, ambientes de preparação).

Aprovação e Autorização:

a) As alterações com grande impacto sobre a segurança das informações e as funcionalidades operacionais devem receber autorização formal antes de serem implementadas.
b) As alterações emergenciais podem ser aceleradas, mas devem passar por revisão e autorização retrospectivas.

Procedimentos de Gerenciamento de Mudanças:

a) Devem ser avaliados os possíveis impactos das mudanças considerando as dependências do sistema.
b) Devem ser informadas as partes interessadas com antecedência, comunicando as mudanças planejadas, os cronogramas e o impacto esperado.
c) As alterações devem ser testadas minuciosamente e devem atender aos padrões de qualidade antes da implementação.
d) Deve ser seguido ao máximo o cronograma de implantação estabelecido.
e) Em casos de emergências, como a não realização das mudanças ou caso haja qualquer falha inesperada, a mudanças devem ser canceladas.
f) Os sistemas de emissão de tickets ou o repositório de códigos devem manter os registros das alterações, confirmações e implantações.

Continuidade e Coerência:

Os planos de continuidade, resposta, documentações operacionais e procedimentos documentados, devem ser atualizados para garantir que permaneçam apropriados e coerentes frente as alterações realizadas.

Segurança e Integridade:

As alterações não devem comprometer a confidencialidade, a integridade e a disponibilidade das informações nas instalações e nos sistemas de processamento.

5. Gerenciamento de Capacidade

O uso de recursos de processamento e armazenamento do sistema deve ser monitorado e ajustado para garantir que a disponibilidade e o desempenho do sistema atendam aos requisitos da “Intex Bank”.

As habilidades, a disponibilidade e a capacidade dos recursos humanos devem ser analisadas e consideradas como componentes do planejamento de capacidade e parte do processo anual de avaliação de riscos.

O dimensionamento de recursos para mais processamento ou capacidade de armazenamento, sem alterações no sistema, pode ser feito fora do processo padrão de gerenciamento de mudanças e implantação de código.

6. Prevenção de Vazamento de Dados

Em conformidade com a Política de Gestão, Classificação e Proteção de Informação, e para minimizar o risco de vazamento de informações confidenciais, a organização deve:

- Identificar e classificar as informações conforme estabelece a Política de Gestão, Classificação e Proteção da Informação.
- Oferecer treinamento para conscientização dos usuários, incluindo o uso e o tratamento adequados das informações confidenciais.

Considere a possibilidade de usar ferramentas de monitoramento técnico e de prevenção contra perda de dados (DLP) de acordo com os riscos para a organização e para os titulares dos dados.

Filtragem da Web

A organização deve garantir o uso seguro, protegido e apropriado da internet pelos funcionários da organização, podendo:

a) Implementar mecanismos, como DNS seguro e endereço IP ou bloqueio de domínio, para restringir o acesso a sites que representem um risco relevante devido ao seu conteúdo ou à distribuição conhecida de malware, vírus ou materiais de phishing.

b) Empregar navegadores e tecnologias anti-malware capazes de bloquear automaticamente sites ou a configuração deles.

c) Salvo se justificado por razões comerciais legítimas, considere a possibilidade de bloquear o acesso a sites:

- Com capacidade de envio de informações;
- Com conteúdo malicioso conhecido ou suspeito;
- Que atuem como servidores de comando e controle;
- Identificados como maliciosos por meio de inteligência sobre ameaças; e
- Que compartilhem conteúdo ilegal.

Regras e diretrizes de uso:

- O usuário deve estar em conformidade com todas as regras da empresa, conforme estabelecem o Código de Conduta e a Política de Uso Aceitável, disponível na Política de Segurança da Informação.

Separação dos Ambientes de Desenvolvimento, Preparação e Produção

Os ambientes de desenvolvimento e teste devem ser estritamente separados dos ambientes de produção de SaaS para reduzir os riscos de acesso não autorizado ou alterações no ambiente operacional. Os dados confidenciais do cliente para produção não devem ser usados em ambientes de desenvolvimento ou teste sem a aprovação expressa do aprovador do uso dos dados do cliente.

Consulte a Política de Gestão, Classificação e Proteção da Informação para ter uma descrição dos dados confidenciais. Se os dados de produção do cliente forem aprovados para uso durante o desenvolvimento ou teste, eles devem ser eliminados de qualquer informação confidencial sempre que possível.

Configuração, Fortalecimento e Revisão de Sistemas e Redes

Os sistemas e redes devem ser provisionados e mantidos de acordo com as normas de configuração e proteção descritas nas baselines de segurança, documentos internos, mantidos sobre supervisão da gestão da tecnologia da informação.

É necessário usar firewalls e/ou os devidos controles e configurações de acesso à rede para controlar o tráfego da rede e para o ambiente de produção, conforme estabelece esta política.

As regras de configuração de acesso à rede de produção devem ser revisadas pelo menos anualmente. Devem-se criar tickets para colher aprovações para as alterações necessárias.

Proteção contra Malware

A fim de proteger a infraestrutura da empresa contra a introdução de software mal-intencionado, devem-se implementar controles de detecção, prevenção e recuperação para proteção contra malware, combinados com a devida conscientização dos usuários.

Devem-se utilizar proteções antimalware em todos os endpoints emitidos pela empresa, exceto aqueles que executam sistemas operacionais normalmente não propensos a sofrer ataques de software malicioso. Além disso, deve-se utilizar um software de detecção e resposta a ameaças no e-mail da empresa. As proteções antimalware utilizadas devem ser capazes de detectar formas comuns de ameaças maliciosas e executar a atividade de atenuação adequada (como remoção, bloqueio ou quarentena).

O “Intex Bank” deve fazer a varredura de todos os arquivos quando eles forem introduzidos nos sistemas e fazer a varredura contínua dos arquivos quando forem acessados, modificados ou baixados. A definição de antimalware e as atualizações do mecanismo devem ser configuradas para download e instalação automática sempre que houver novas atualizações disponíveis. Os incidentes conhecidos ou suspeitos com malware devem ser comunicados como incidente de segurança.

Desativar ou alterar a configuração das proteções antimalware sem autorização constitui uma violação da política da empresa.

Backup de Informações

Deve-se levar em consideração a necessidade de backups de sistemas, bancos de dados, informações e dados e deve-se projetar, planejar e implementar os processos de backup adequados. Os procedimentos de backup devem ser seguidos de acordo com a Política de Backup e Restore. As medidas de segurança para proteger os backups devem ser projetadas e aplicadas de acordo com a confidencialidade ou a sensibilidade dos dados. Os recursos de backup e restauração devem ser testados periodicamente, pelo menos uma vez por ano e devem ser armazenados separadamente do local dos dados de produção.

Os backups devem estar configurados para executarem diariamente em sistemas que fazem parte do escopo. Os cronogramas de backup são mantidos no software do aplicativo de backup.

O “Intex Bank” não faz backup regularmente dos dispositivos dos usuários, tais como notebooks. Espera-se que os usuários armazenem arquivos e informações importantes em repositórios de armazenamento de arquivos sancionados pela empresa.

7. Registro e Monitoramento

A infraestrutura de produção deve ser configurada para produzir registros detalhados adequados à função desempenhada pelo sistema ou dispositivo. Devem-se produzir registros de eventos que gravem as atividades dos usuários, exceções, falhas e eventos de segurança da informação, e eles devem ser mantidos e revisados por meio de processos manuais ou automatizados, conforme necessário. Devem-se configurar alertas apropriados para eventos que representem grande ameaça à confidencialidade, disponibilidade ou integridade dos sistemas de produção ou dos dados confidenciais.

O registro deve atender aos seguintes critérios para aplicativos de produção e infraestrutura de suporte:

a) Registrar o acesso e a saída do usuário.
b) Registrar operações de criação, leitura, atualização, exclusão em usuários e objetos do aplicativo e do sistema.
c) Registrar as alterações nas configurações de segurança (incluindo a desativação ou modificação do registro).
d) Registrar o acesso do proprietário ou administrador do aplicativo aos dados do cliente (ou seja, transparência de acesso).

e) Os registros devem conter a ID do usuário, endereço IP, carimbo de data/hora válido, tipo de ação executada e objeto dessa ação.
f) Os registros devem ser armazenados por pelo menos 30 dias e não devem conter dados confidenciais ou cargas úteis.

Proteção de Informações de Registro

As instalações de registro e as informações de registro devem ser protegidas contra adulteração e acesso não autorizado.

Registros de Administrador e Operador

As atividades do administrador e do operador do sistema devem ser registradas e revisadas e/ou alertadas de acordo com a classificação e a criticidade do sistema.

Registros de Restauração de Dados

Caso a empresa precise restaurar dados de produção a partir de backups, seja para fins de prestação de serviços ou para fins de teste, eles devem ser registrados ou rastreados em logs auditáveis.

Monitoramento da Integridade dos Arquivos e Detecção de Invasão

Os sistemas de produção do “Intex Bank” devem ser configurados para monitorar, registrar e se autorreparar e/ou alertar, sempre que possível, sobre alterações suspeitas em arquivos críticos do sistema.

As indicações devem ser configuradas para condições suspeitas e os engenheiros devem analisar os registros regularmente.

Penetrações não autorizadas e tentativas de acesso ou alterações nos sistemas do “Intex Bank” devem ser investigadas e corrigidas conforme estabelece o Plano de Resposta a Incidentes.

Controle do Software Operacional

A instalação de software em sistemas de produção deve seguir os requisitos de gerenciamento de mudanças definidos nesta política.

Restrições à Instalação de Softwares

Devem-se estabelecer e implementar regras que regem a instalação de software pelos usuários de acordo com a Política de Segurança de Informação do “Intex Bank”.

Considerações sobre Auditoria de Sistemas de Informação

Os requisitos e atividades de auditoria que envolvam a verificação de sistemas operacionais devem ser planejados e acordados com máxima atenção para minimizar as interrupções nos processos dos negócios.

8. Inteligência sobre Ameaças

Deve-se coletar e analisar as informações relacionadas às ameaças à segurança da informação para produzir inteligência sobre ameaças.

a) **Coleta:** recorra a diversas fontes, como blogs, artigos de notícias, atualizações de fornecedores, bancos de dados públicos e comunidades do setor.

b) **Análise:** examine os dados para extrair informações práticas e viabilizar iniciativas de resposta proativas. Comunique à equipe de segurança as informações práticas ou ameaças específicas.

c) **Disseminação:** faça a comunicação eficaz da inteligência sobre ameaças às equipes pertinentes para viabilizar a ação eficaz. A equipe de segurança deve disseminar informações práticas por meio de canais de comunicação como o slack, e-mail e alertas de emergência.

d) **Comentários:** cultive a melhoria contínua utilizando os comentários para aperfeiçoar as políticas. Integre os comentários às alterações da política e revise a política regularmente.

9. Gestão de Vulnerabilidades Técnicas

As informações sobre as vulnerabilidades técnicas dos sistemas de informação que estão sendo usados devem ser colhidas em tempo hábil. A exposição da organização a essas vulnerabilidades deve ser avaliada e devem-se tomar as medidas apropriadas para tratar o risco associado. Deve-se usar uma variedade de métodos para conseguir informações sobre vulnerabilidades técnicas, entre eles a verificação de vulnerabilidades, os testes de penetração, a análise de alertas de fornecedores externos e o programa de recompensa por descoberta de erros.

Devem-se conduzir verificações de vulnerabilidade em sistemas voltados para o público no ambiente de produção pelo menos com periodicidade semestral.

Devem ser realizados testes de penetração das aplicações e da rede de produção pelo menos anualmente, além disso, devem ser realizadas verificações e testes após grandes mudanças nos sistemas e no software de produção.

Os departamentos de TI e Cibersegurança devem avaliar a gravidade das vulnerabilidades identificadas em qualquer fonte e, se for determinado que se trata de uma vulnerabilidade crítica ou de alto risco relevante, deve ser criado um chamado de suporte. O nível de gravidade avaliado do “Intex Bank” pode diferir do nível gerado automaticamente pelo software de verificação ou daquele determinado por pesquisadores externos com base no conhecimento interno e no conhecimento da arquitetura técnica e da possibilidade real de

exploração/impacto no “Intex Bank”. As vulnerabilidades são atribuídas aos proprietários do sistema, aplicação ou plataforma para maior investigação e/ou correção.

As vulnerabilidades avaliadas pelo “Intex Bank” devem ser corrigidas ou remediadas nos seguintes prazos:

Gravidade determinada	Tempo de remediação
Crítica	**30 dias**
Alta	**30 dias**
Média	**60 dias**
Baixa	**90 dias**
Informativa	**Conforme necessário**

Os tickets de serviço para qualquer vulnerabilidade que não possa ser remediada dentro do cronograma padrão devem apresentar um plano de tratamento de riscos e um cronograma de remediação planejado.

10. Requisitos e Avaliação de Segurança dos Sistemas

Devem-se considerar os riscos antes da aquisição ou de grandes alterações nos sistemas, tecnologias ou instalações. Quando os requisitos forem formalmente identificados, todos os requisitos de segurança relevantes devem ser incluídos. Deve-se fazer a aquisição de novos fornecedores e serviços de acordo com a Política de Gerenciamento de Terceiros.

A empresa deve realizar uma avaliação anual sobre a segurança da rede que inclua uma análise das principais alterações no ambiente, tais como novos componentes do sistema e topologia da rede.

11. Exceções

Exceções a esta Política devem ser formalmente submetidas ao Gestor de Tecnologia da Informação 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 suporte@intexbank.com.br.

12. Violações e Não Cumprimentos da Política

Qualquer violação das diretrizes estabelecidas nesta política deverá ser comunicada imediatamente ao Gestor de Tecnologia da Informação 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.

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.